Belgische Kamer van
volksvertegenwoordigers
en Senaat

Chambre des représentants et
Sénat
de Belgique

PARLEMENTAIR INTERNET FORUM

Colloquium

**Het gebruik van e-mail en de politieke,
juridische en sociologische implicaties**

FORUM PARLEMENTAIRE RELATIF A INTERNET

Colloque

**L'utilisation du courrier électronique et les implications
politiques, juridiques et sociologiques**

Met medewerking van :

ISPA BELGIUM

En collaboration avec :

**Congreszaal – Huis van de Parlementsleden
Salle des Congrès – Maison des Parlementaires**

**Maandag 14 januari 2002
Lundi 14 janvier 2002**

AGALEV-ECOLO	*:*	*Anders gaan leven / Ecologistes Confédérés pour l'organisation de luttes originales*
CD&V	*:*	*Christen-Democratisch en Vlaams*
FN	*:*	*Front National*
MR	*:*	*Mouvement Réformateur*
PS	*:*	*Parti socialiste*
cdH	*:*	*Centre démocrate Humaniste*
SP.A	*:*	*Socialistische Partij Anders*
VLAAMS BLOK	*:*	*Vlaams Blok*
VLD	*:*	*Vlaamse Liberalen en Democraten*
VU&ID	*:*	*Volksunie&ID21*

Afkortingen bij de nummering van de publicaties :

DOC 50 0000/000 :	*Parlementair document van de 50e zittingsperiode + basisnummer en volgnummer*
QRVA :	*Schriftelijke Vragen en Antwoorden*
CRIV :	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (op wit papier, bevat ook de bijlagen)*
CRIV :	*Voorlopige versie van het Integraal Verslag (op groen papier)*
CRABV :	*Beknopt Verslag (op blauw papier)*
PLEN :	*Plenum (witte kaft)*
COM :	*Commissievergadering (beige kaft)*

Abréviations dans la numérotation des publications :

DOC 50 0000/000 :	*Document parlementaire de la 50e législature, suivi du n° de base et du n° consécutif*
QRVA :	*Questions et Réponses écrites*
CRIV :	*Compte Rendu Intégral, avec à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (sur papier blanc, avec les annexes)*
CRIV :	*Version Provisoire du Compte Rendu intégral (sur papier vert)*
CRABV :	*Compte Rendu Analytique (sur papier bleu)*
PLEN :	*Séance plénière (couverture blanche)*
COM :	*Réunion de commission (couverture beige)*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers Publications officielles éditées par la Chambre des représentants

Bestellingen :
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.deKamer.be
e-mail : publicaties@deKamer.be

Commandes :
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.laChambre.be
e-mail : publications@laChambre.be

Op 14 januari 2002 hebben Kamer en Senaat, in samenwerking met ISPA Belgium (Internet Service Providers Association), de Belgische vereniging van internet providers, in de Congreszaal van het federaal Parlement een parlementair internet forum georganiseerd over «Het gebruik van e-mail en de politieke, juridische en sociologische implicaties».

Dit initiatief vormt de aanzet voor een heus discussieforum van parlementairen en deskundigen uit de ICT-wereld.

De Engelstalige referaten van de vier sprekers, die namens ISPA op de studiedag waren afgevaardigd, werden onder de deelnemers van het colloquium verspreid .

De uiteenzettingen waren gedurende enkele maanden in «real audio» te beluisteren op de webstek van Kamer en Senaat.

Dit verslag in de twee landstalen zal ook op de webstek van Kamer en Senaat te consulteren zijn. Het bevat de inleidende uiteenzetting van de heer Herman De Croo, Voorzitter van de Kamer, de bijdragen van de vier sprekers, die namens ISPA waren afgevaardigd, de heer Paul Thomas, voorzitter van de commissie voor de bescherming van de persoonlijke levenssfeer en professor Claude Javeau, het debat en het slotwoord van senator Guy Moens.

24 oktober 2002

Le 14 janvier 2002, la Chambre et le Sénat, en collaboration avec ISPA Belgium (Internet Service Providers Association), l'association de fournisseurs d'accès à l'internet, ont organisé, dans la Salle des Congrès du parlement fédéral, un forum parlementaire sur «L'utilisation de l'e-mail et les implications politiques, juridiques et sociologiques».

Cette initiative constitua l'ébauche d'un véritable forum de discussions parmi des parlementaires et experts du monde de l'ICT.

Les comptes rendus en anglais des quatres orateurs, qui représentaient ISPA lors de cette journée d'étude, ont été distribués aux participants du colloque.

Les exposés ont été disponibles pendant plusieurs mois, en «real audio» sur les sites de la Chambre et du Sénat.

Le présent rapport dans les deux langues nationales pourra également être consulté sur les sites de la Chambre et du Sénat. Il comprend l'exposé introductif de M. Herman De Croo, Président de la Chambre; les interventions des quatre orateurs, qui représentaient ISPA, de M. Paul Thomas, Président de la commission pour la protection de la vie privée et du professeur Claude Javeau, le débat et la conclusion par le sénateur Guy Moens.

24 octobre 2002

INHOUDSTAFEL

SOMMAIRE

Parlementair Internet Forum

«Het gebruik van e-mail en de implicaties
op politiek,
juridisch en sociologisch vlak»

UITEENZETTING DOOR DE HEER HERMAN DE CROO, VOORZITTER VAN DE KAMER VAN VOLKSVERTEGENWOORDIGERS

Geachte Collega's,
Mijnheer de Voorzitter van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer,
Mijnheer de Voorzitter van het Observatorium van de rechten op internet,
Waarde Professor Javeau,
Dames en heren,

Als Voorzitter van de Kamer van volksvertegenwoordigers is het mij een genoegen het parlementair internet forum te openen dat handelt over *«Het gebruik van e-mail en de implicaties op politiek, juridisch en sociologisch vlak».* Dit seminarie wordt door Kamer en Senaat georganiseerd, samen met de vzw ISPA Belgium, de Belgische vereniging van internet providers.

De ontwikkelingen op het vlak van Informatie- en communicatietechnologie of ICT plaatsen de beleidsverantwoordelijken voor talrijke uitdagingen. Internet en andere elektronische toepassingen vervullen een steeds grotere maatschappelijke functie. Opdat de wetgever de technologische evoluties niet te ver achterna zou hinken, is het noodzakelijk dat de parlementariërs de politieke, juridische en sociologische implicaties van het internet en e-mailgebruik tijdig analyseren en vertalen in beleidskeuzes. De ontwikkelingen inzake elektronische communicatie vereisen aanpassing van de regelgeving waarin de verouderde relatie tussen overheid, burgers en ondernemingen ligt verankerd.

Aandacht voor ICT dwingt ons ook de internationale en Europese ontwikkelingen terzake te volgen. Zo waren de toegang tot ICT en de ontwikkeling naar een concurrerende, dynamische op kennis gebaseerde samenleving centrale thema's van de Europese top die op 23 en 24 maart 2000 te Lissabon plaatsvond. Verder is er het Cybercrime-verdrag dat tot stand kwam in de Raad

Forum internet parlementaire

«L'utilisation du courrier électronique et
ses implications dans les domaines politique,
juridique et sociologique»

EXPOSÉ DE MONSIEUR HERMAN DE CROO, PRÉSIDENT DE LA CHAMBRE DES REPRÉSENTANTS

Chers Collègues,
Monsieur le Président de la Commission de la protection de la vie privée,
Monsieur le Président de l'Observatoire des droits sur internet,
Cher Professeur Javeau,
Mesdames et Messieurs,

J'ai l'honneur, en tant que Président de la Chambre des Représentants, d'ouvrir le forum parlementaire internet qui va traiter de «*l'utilisation du courrier électronique et ses implications dans les domaines politique, juridique et sociologique*». Ce séminaire est organisé conjointement par la Chambre et par le Sénat, avec l'asbl ISPA Belgium, l'association belge des fournisseurs d'accès à l'internet.

Les développements en matière de Technologies de l'information et de la communication ou TIC confrontent les responsables politiques à de nombreux défis. L'internet et autres applications électroniques remplissent une fonction sociale dont l'importance va croissant. Pour éviter que le législateur soit à la traîne des évolutions technologiques, les parlementaires doivent veiller à analyser en temps opportun les implications politiques, juridiques et sociologiques de l'internet et de l'utilisation du courrier électronique et les traduire sous la forme de choix politiques. Les évolutions qui se font jour en matière de communication électronique requièrent un aménagement de la réglementation dans laquelle est ancrée la relation obsolète entre l'autorité, les citoyens et les entreprises.

L'attention que requiert les TIC nous impose également de suivre l'évolution à l'échelle mondiale et européenne. L'accès aux TIC et l'évolution vers une société concurrentielle, dynamique et fondée sur la connaissance ont ainsi constitué les thèmes centraux du sommet européen qui s'est tenu les 23 et 24 mars 2000 à Lisbonne. Il faut citer aussi la convention Cyber-Crime

van Europa. De Raad van Europa, de Europese Unie, de OESO en de VN buigen zich ook over privaatrechtelijke onderwerpen en privacy-aspecten van het elektronisch communicatieverkeer.

In mijn uiteenzetting wens ik dieper in te gaan op de aspecten van het E-government en E-commerce, e-mail en de bescherming van de persoonlijke levenssfeer, de informaticacriminaliteit en de reglementering van het gebruik van de elektronische telecommunicatiemiddelen op de werkplaats.

Tot slot zal ik stilstaan bij de impact van voormelde materies op de parlementaire werkzaamheden.

1. E-governement

De burger moet in zijn relatie met de overheid kunnen kiezen tussen ofwel elektronisch, dan wel schriftelijk communiceren.

In het regeerakkoord van 7 juni 1999 werd aandacht besteed aan e-government dat het uitbouwen omvat van een informatica-infrastructuur en het nemen van initiatieven om administraties en burgers in staat te stellen de informatica- en communicatietechnologie te gebruiken voor bestuurshandelingen.

De commissie voor de Binnenlandse Zaken van de Senaat heeft in december 2000 aan dit onderwerp verschillende hoorzittingen gewijd met de bevoegde federale ministers[1].

De installatie van het e-government is op federaal vlak de verantwoordelijkheid van drie ministers, de minister van Ambtenarenzaken, die de back office[2] verzorgt, de minister van telecommunicatie die het public/private partnership uitwerkt en bevoegd is voor de informatie- en communicatietechnologie in het algemeen, en de minister van Economie, die binnen de wet op de elektronische handtekening verantwoordelijk is voor de vrijwillige certificatie van dienstverleners van elektronische handtekeningen.

De hoorzittingen in de Senaat resulteerden in enkele interessante aanbevelingen, zoals :

– een geïntegreerde aanpak van de publieke dienstverlening door alle Belgische overheidsdiensten samen te brengen in één structuur of toegangspoort ;

– de zorg voor een kwalitatieve zorgverlening aan de burgers via de mogelijkheden van ICT ;

qui a vu le jour au Conseil de l'Europe. Le Conseil de l'Europe, l'Union européenne, l'OCDE et les NU se penchent également sur des matières relatives au droit privé et sur les aspects liés à la vie privée de la communication électronique.

Je souhaiterais, dans le cadre de mon exposé, aborder les aspects de l'administration et du commerce électroniques, du courrier électronique et de la protection de la vie privée, de la criminalité informatique et de la réglementation relative à l'utilisation des moyens de communication électronique au travail.

En conclusion, j'évoquerai l'incidence des matières que je viens de citer sur les travaux parlementaires.

1. L'administration électronique

Dans ses rapports avec l'autorité, le citoyen doit pouvoir choisir entre la communication électronique ou écrite.

L'accord de gouvernement du 7 juin 1999 fait une place à l'administration électronique qui comprend la mise en place d'une infrastructure informatique et suppose des initiatives permettant aux administrations et aux citoyens d'utiliser la technologie de l'informatique et de la communication dans le cadre d'actes administratifs.

En décembre 2000, la commission de l'Intérieur du Sénat a consacré à ce sujet plusieurs auditions avec les ministres fédéraux compétents[1].

L'installation de l'administration électronique relève, au plan fédéral, de trois ministres, à savoir le ministre de la fonction publique, qui assure le traitement de l'information au plan interne (le *back office)*[2], le ministre des Télécommunications, qui définit le partenariat entre le secteur public et le secteur privé et est compétent pour la technologie de l'information et de la communication en général, et le ministre de l'Economie, qui est compétent, dans le cadre de la loi sur la signature électronique, pour l'agrément volontaire des prestataires de services pour les signatures électroniques.

Les auditions qui se sont tenues au Sénat ont débouché sur des recommandations intéressantes:

– mettre en œuvre une approche intégrée du service public en réunissant tous les services publics belges sous une même structure ou sous un même portail;

– veiller à la qualité du service au citoyen par le recours aux possibilités offertes par les TIC;

– het informeren van de burgers van de elektronische middelen die voor hen gereserveerd worden ;
– de spoedige inwerkingtreding via de nodige uitvoeringsbesluiten van de wet op de elektronische handtekening[3].

Het 5 sterrenplan ter bevordering van de informatiemaatschappij waar minister Daems in zijn recente beleidsnota naar verwees, probeert in ruime mate tegemoet te komen aan voormelde aanbevelingen[4].

De opbouw van een performant kader voor E-government en E-commerce is essentieel.
Enkele basisvoorwaarden voor de uitbouw van zo'n performant kader lijken mij :

– goedkope internettarieven en het wegwerken van allerlei hindernissen, zoals de hoge kostprijs van een internetverbinding voor burgers en ondernemers. De overheid moet niet alleen een regulator, maar ook een promotor zijn om de mensen aan te moedigen elektronische communcatietoepassingen te gebruiken[5] ;

– het klantgericht organiseren van de informatievoorziening door de overheid via een geïntegreerde informatievoorzieningsstrategie ;
– het vermijden van een digitale kloof, waarbij het niet kunnen omgaan met informatica als een soort analfabetisme geldt. Iedere burger heeft immers recht op toegang tot de informatiesnelweg ;
– Het recht moet vooral de groei van elektronische handel niet belemmeren en waar mogelijk ondersteunen. Hierbij moeten de regels voor de elektronische handel voorspelbaar zijn en het bedrijfsleven en de consument vertrouwen inboezemen.

2. De repercussies van het elektronisch communicatieverkeer op de rechten en vrijheden van de burger, op de veiligheid en op de organisatie van het gerecht :

Tot het bevoegdheidsdomein van justitie behoren de repercussies van het elektronisch communicatieverkeer op de rechten en vrijheden van de burger, op de veiligheidsaspecten van informatica (informaticacriminaliteit) en de e-justice.

Het ontstaan van de informatiesamenleving heeft voor de grondrechten en de vrijheden van de burgers inderdaad enkele veranderingen met zich meegebracht. In Nederland heeft de Commissie «Grondrechten in het digitale tijdperk» zinvolle voorstellen geformuleerd om de bestaande grondrechten in de Grondwet aan te pas-

– informer le citoyen sur les instruments électroniques qui leur sont réservés;
– faire entrer en vigueur à bref délai les arrêtés d'exécution de la loi sur la signature électronique[3].

Le plan 5 Etoiles pour la promotion de la société de l'information, auquel le ministre Daems a fait référence dans sa récente note de politique générale, tend à donner suite, dans une large mesure, à ces recommandations[4].
La création d'un cadre performant pour l'administration et le commerce électroniques revêt une importance capitale. Je citerai quelques éléments qui constituent à mes yeux les conditions de base de la mise en place d'un tel cadre:

– il faut réduire les tarifs pour l'accès à l'internet et éliminer des entraves diverses, comme le coût élevé d'une connexion internet pour les citoyens et les entrepreneurs. Les pouvoirs publics doivent jouer le rôle de régulateur mais aussi de promoteur en encourageant le public à faire usage des applications de la communication électronique[5];
– les pouvoirs publics doivent organiser des canaux d'information destinés à la clientèle, dans le cadre d'une stratégie intégrée de diffusion de l'information;
– il faut prévenir l'apparition d'une fracture digitale par laquelle l'incapacité à utiliser l'informatique serait assimilée à une sorte d'analphabétisme. Tout citoyen a en effet le droit d'accéder aux autoroutes de l'information;
– le droit ne doit pas constituer un frein au commerce électronique mais doit le soutenir lorsque la possibilité en est offerte. A cet égard, les règles du commerce électronique doivent être prévisibles et inspirer confiance aux entreprises et au consommateur.

2. Les répercussions de la communication électronique sur les droits et libertés du citoyen, sur la sécurité et sur l'organisation de la justice

Les répercussions de la communication électronique sur les droits et libertés du citoyen, sur les aspects de l'informatique liés à la sécurité (la criminalité informatique) et la justice électronique relèvent du domaine de compétence de la justice.

L'avènement d'une société de l'informatique a en effet induit, en ce qui concerne les droits fondamentaux et les libertés du citoyen, un certain nombre de changements. Aux Pays-Bas, la commission «Grondrechten in het digitale tijdperk» (les Droits fondamentaux à l'ère digitale) a formulé des propositions très pertinentes

sen[6]. Men zou ook in België kunnen onderzoeken in welke mate Titel II van de Grondwet dat handelt over de Belgen en hun rechten moet aangepast worden aan de onder invloed van ICT veranderende samenleving.

Enkele fundamentele beschouwingen dringen zich op:

– In welke mate kan «hacking» of «computervredebreuk» gekwalificeerd worden als een inbreuk op de onschendbaarheid van de woning, beschermd door art. 15 van de Grondwet ?

– Voorafgaande beperkingen of preventieve maatregelen zijn door de Belgische Grondwet verboden. In welke mate is het filteren van informatie op internet door de accessprovider een preventieve dan wel een repressieve maatregel tot beperking van art. 19 van de Grondwet dat handelt over de vrijheid van meningsuiting ?

– Is kennisname door de werkgever of de autoriteiten mogelijk van e-mails die bepaalde (tref)woorden of ongewenste boodschappen bevatten, of is dit een inbreuk op de privacy ?

– In welke mate vallen chat-vergaderingen en video-conferenties onder het recht op vreedzaam vergaderen van art. 26 van de Grondwet ?

– Zijn elektronische petities bij de assemblees mogelijk en impliceert art. 28 van de Grondwet een schriftelijkheidsvereiste in het petitierecht ?

– In welke mate moet de bescherming van het briefgeheim van art. 29 van de Grondwet niet vervangen worden door een algemeen recht op vertrouwelijke informatie waarbij alle communicatie die zich leent voor geheimhouding wordt beschermd ?

– Hoe vertaalt men het recht om elk bestuursdocument te raadplegen van art. 32 van de Grondwet naar de context van het elektronisch communicatieverkeer? In deze context kan verwezen worden naar het wetsvoorstel ingediend door de heer Yvan Mayeur en consoorten betreffende het gebruik van open communicatiestandaarden door de overheidsdiensten[7].

De wereld van het elektronisch communicatieverkeer kent ook computerfreaks en professionele criminelen die van het internet een rechteloze ruimte willen maken. Het «I Love You»-virus dat verleden jaar talrijke computers is binnengedrongen die op het internet waren aangesloten, heeft bewezen dat virus-aanvallen het economisch leven zware schade kunnen berokkenen. Een doeltreffend beleid en aangepaste middelen tegen computercriminaliteit moeten op deze plaag een duidelijk antwoord geven. Met de wet van 20 november 2000 inzake informaticacriminaliteit[8] heeft België een duidelijk wettelijk kader over deze aangelegenheid. In ons Strafwet-

tendant à adapter les droits fondamentaux consacrés par la Constitution[6]. En Belgique aussi, l'opportunité d'adapter le Titre II de la Constitution - qui traite des Belges et de leurs droits - sur la base des changements intervenus dans la société sous l'effet des TIC, pourrait être examinée.

Certaines considérations fondamentales s'imposent:

– Dans quelle mesure le «hacking» peut-il être considéré comme contrevenant à l'inviolabilité du domicile, consacrée par l'article 15 de la Constitution?

– La Constitution belge interdit les mesures limitatives ou préventives. Dans quelle mesure le filtrage d'informations sur l'internet par les fournisseurs d'accès constitue-t-il une mesure préventive ou répressive limitant l'exercice du droit de manifester ses opinions consacré par l'article 19 de la Constitution?

– L'employeur ou les autorités peuvent-ils prendre connaissance de courriers électroniques qui comportent certains termes (clés) ou des messages indésirables ou s'agit-il d'une violation de la vie privée?

– Dans quelle mesure les conférences chatting et vidéo relèvent-elles du droit de s'assembler paisiblement dont traite l'article 26 de la Constitution?

– Des pétitions électroniques peuvent-elles être adressées aux assemblées? L'article 28 de la Constitution impose-t-il pour l'exercice du droit d'adresser des pétitions une procédure écrite?

– Ne faut-il pas substituer à la protection du secret des lettres, consacré à l'article 29 de la Constitution, un droit général à la confidentialité de l'information protégeant toute communication susceptible de relever du secret?

– Comment transposer le droit de consulter chaque document administratif dans le contexte de la communication électronique? On peut citer à cet égard la proposition de loi déposée par Monsieur Yvan Mayeur et consorts[7] relative à l'utilisation de standards de communication ouverts dans l'administration.

L'univers de la communication électronique a aussi ses mordus de l'informatique et ses criminels professionnels qui entendent faire de l'internet un espace sans règles juridiques. Le virus «*I Love you*» qui a investi l'an dernier quantité d'ordinateurs reliés à l'internet, a montré que les attaques par virus peuvent causer d'importants dommages à l'activité économique. Il faut répondre résolument à cette plaie par une politique et des moyens appropriés pour contrer la criminalité informatique. Avec la loi du 20 novembre 2000 sur la criminalité informatique[8], la Belgique s'est dotée en cette matière d'un cadre législatif précis. Des notions nouvelles ont

boek en Wetboek van Strafvordering werden nieuwe begrippen ingevoegd zoals «valsheid in informatica»,»informaticabedrog» en een nieuw misdrijf *sui generis*, nl. de «ongeoorloofde toegang zowel door outsiders als insiders» (het zogenaamde «hacking»). Het antivirusalarmcentrum binnen het BIPT dient als referentie voor gans Europa als het gaat om de aangeboden oplossing voor de preventie van virusaanvallen.

«Spamming» of het overrompelen van de mailboxen met ongevraagde e-mail-advertenties is een negatief fenomeen dat door wetgeving efficiënter kan bestreden worden. Een spoedige omzetting van de richtlijn 2000/31/EG van 8 juni 2000 dringt zich op. Deze richtlijn voorziet dat de bestemmeling zijn weigering om ongevraagde elektronische post te ontvangen niet afzonderlijk aan elke afzender moet kenbaar maken, maar dit éénmalig kan door een inschrijving in een opt-out-register.

Wat de organisatie van het departement «Justitie» betreft, dient elk initiatief dat e-justice implementeert, te worden toegejuicht. De wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure (die steunt op een wetsvoorstel van collega's Bourgeois en Van Hoorebeke) was een lovenswaardige stap in het streven naar een elektronisch rechtsverkeer tussen de actoren van justitie[9]. Door deze wet worden proceshandelingen per elektronische post ook mogelijk na het sluitingsuur van de griffie. Advocaten kunnen gemakkelijker communiceren binnen een gerechtelijke procedure, onder meer door het neerleggen van besluiten per e-mail. Het Phenix-project, waarnaar de minister van Justitie in zijn beleidsnota voor 2002 verwijst, maakt het voor de rechtspleging mogelijk in de toekomst een elektronisch dossier op te bouwen en te beheren.

3. De repercussies van het elektronisch communicatieverkeer op de arbeidsverhoudingen (Is E-mailprivacy een grondrecht ?)

Om hen toe te laten op het web te navigeren en elektronische post te versturen, hebben vele werknemers een internetaansluiting op hun werkplek. Volgens een recente studie van de Gartner Group zou gemiddeld 40% van het gebruik van het web volstrekt onproductief zijn[10].

Het recent ingediende wetsvoorstel van Senator A. Destexhe betreffende het reglementeren van het gebruik van telecommunicatiemiddelen op de werkplaats[11] wil de werkgever een aantal middelen aanbieden om de controle uit te oefenen op het gebruik dat de werknété insérées dans notre Code pénal et dans notre Code de procédure pénale, tel «le faux en informatique», «la fraude informatique» , ainsi qu'un nouveau délit *sui generis,»* l'accès illicite, de l'extérieur comme de l'intérieur (le «hacking»)». Le système d'alerte anti-virus de l'IBPT a valeur de référence pour toute l'Europe en tant qu'outil de prévention contre les attaques par virus.

Le «*spamming*», qui consiste à inonder les boîtes aux lettres d'annonces électroniques non désirées constitue un phénomène négatif que la législation devrait permettre de mieux combattre. Il se recommande de transposer rapidement la directive 2000/31/EG du 8 juin 2000. Aux termes de cette directive, le destinataire ne doit pas notifier individuellement à chaque expéditeur son refus de recevoir du courrier non demandé mais peut le faire une seule fois par l'inscription dans un registre d'interdiction (*opt out).*

En ce qui concerne l'organisation du département de la Justice, il faut applaudir à toute initiative mettant en œuvre la justice électronique. La loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extra-judiciaire (qui résulte d'une proposition de loi de MM. Bourgeois et Van Hoorebeke) a constitué un pas méritoire vers la mise en place d'un commerce juridique électronique entre les acteurs de la justice[9] . Cette loi permet les actes de procédure par courrier électronique en dehors des heures d'ouverture des greffes. Les avocats peuvent communiquer plus aisément dans le cadre d'une procédure judiciaire, notamment en déposant des conclusions sous la forme de courrier électronique. En ce qui concerne la procédure, le projet Phenix, auquel le ministre de la Justice fait référence dans sa note de politique de 2002 permettra à l'avenir la constitution et la gestion d'un dossier électronique.

3. Les répercussions de la communication électronique sur les relations de travail (la confidentialité du courrier électronique est-elle un droit?)

De nombreux travailleurs disposent sur leur lieu de travail d'une connexion à l'internet pour naviguer et envoyer du courrier électronique. Il ressort d'une étude récente du Gartner group qu'en moyenne, 40% de l'utilisation du web seraient totalement improductifs[10].

La proposition de loi déposée récemment par le Sénateur Destexhe[11] visant à réglementer l'usage de l'internet et de l'e-mail sur le lieu du travail vise à fournir à l'employeur certains moyens de contrôler l'usage que le travailleur fait des moyens de télécommunica-

mer maakt van de telecommunicatiemiddelen die tot zijn beschikking staan, met inachtneming van de privacy [12] en de regels inzake proportionaliteit en transparantie.

Dit interessante wetsvoorstel kan een aanzet betekenen voor het parlementair debat omtrent elektronische telecommunicatie en privacy, waarbij nauwgezet de afweging moet gemaakt worden tussen het recht van de werkgever om te weten wat noodzakelijk is voor het uitoefenen van zijn leidinggevende functie en het recht van de werknemer op de bescherming van zijn persoonlijke levenssfeer.

De ontwikkelingen in de rechtspraak zullen hierbij niet over het hoofd mogen gezien worden. Zo heeft de sociale Kamer van het Franse Hof van Cassatie op 2 oktober 2001 beslist dat het recht van de werkgever op controle van de e-mailberichten van hun werknemers niet opweegt tegen het recht van de werknemer op bescherming van zijn privacy[13].

Ook het advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer verdient ruime aandacht. De commissie is van oordeel dat de kennisname van de inhoud van e-mails overmatig is, net zoals het afluisteren of opnemen van telefoongesprekken gevoerd door de werknemer. Er bestaan volgens de commissie andere oplossingen om misbruiken te bestrijden. Wat de controle betreft van de door de werknemer geraadpleegde internetsites is de commissie van oordeel dat deze controles moeten steunen op beperkte, objectieve gegevens en niet op een voorafgaande en systematische kennisname van de inhoud van alle gegevensverkeer van elke werknemer[14].

In de rechtsleer weerklinkt de kritiek dat dit advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer onvoldoende rekening houdt met de gerechtvaardigde nood van heel wat werkgevers om een doeltreffend controlebeleid binnen de onderneming te voeren. Het lijkt me redelijk dat een werkgever met inachtneming van het evenredigheidsbeginsel een zeker controlebeleid kan voeren. Een werkgever moet zijn netwerk kunnen beveiligen. Een werkgever is aansprakelijk voor fouten gemaakt door zijn werknemers, bijvoorbeeld in het kader van het verspreiden van virussen[15]. De werknemer is verplicht zijn werk zorgvuldig uit te voeren. Als e-mails waarin een concurrent wordt belachelijk gemaakt buiten het netwerk van het bedrijf raken, loopt een onderneming het risico een zware schadevergoeding te moeten betalen. Klachten van een werknemer tegen een collega die via e-mail ongewenste

tion mis à sa disposition, dans le respect de la vie privée[12] et des règles en matière de proportionnalité et de transparence.

Cette intéressante proposition de loi peut constituer l'amorce du débat parlementaire sur les moyens de communication électronique et la vie privée, dans le cadre duquel il faudra veiller à mettre en balance le droit de l'employeur d'être informé de ce qu'il doit savoir pour exercer sa fonction dirigeante et le droit du travailleur à la protection de sa vie privée.

Il ne faudra pas perdre de vue l'évolution de la jurisprudence. Ainsi, en France, la Chambre sociale de la Cour de cassation a estimé le 2 octobre 2001 que le droit du travailleur à la protection de sa vie privée l'emporte sur le droit de l'employeur de contrôler le courrier électronique de ses employés[13].

De même, l'avis de la Commission de la protection de la vie privée mérite de retenir l'attention. La commission estime, comme pour l'écoute ou l'enregistrement de communications téléphoniques, qu'il est excessif pour l'employeur de prendre connaissance du contenu de courriers électroniques. Elle considère que d'autres moyens permettent de réprimer les abus. La commission estime aussi que le contrôle des sites internet consultés par le travailleur doit reposer sur des données objectives restreintes et non pas sur une prise de connaissance préalable et systématique du contenu de toutes les données de trafic concernant chaque employé[14].

Dans la doctrine, cet avis de la Commission pour la protection de la vie privée est critiqué en ce sens qu'il ne tient pas suffisamment compte de la nécessité justifiée dans le chef de nombreux employeurs de mener une politique de contrôle efficace au sein de l'entreprise. Il me paraît raisonnable qu'un employeur puisse, dans le respect du principe de proportionnalité, mener une politique de contrôle. Un employeur doit être en mesure de sécuriser son réseau. Un employeur est responsable des erreurs commises par son personnel, par exemple dans le cadre de la diffusion de virus[15]. Le travailleur se trouve dans l'obligation de s'acquitter de sa tâche avec soin. Si des courriers électroniques dans lesquels un concurrent est ridiculisé sont diffusés en dehors du réseau de la société, une entreprise court le risque de devoir verser un important dédommagement. Des plaintes d'un travailleur contre un collègue qui se livre à des

intimiteiten verstuurt of het ontslag om dringende redenen van een werknemer die misbruik heeft gemaakt van email en internet zijn nieuwe fenomenen waar de arbeidsrechtbanken mee geconfronteerd worden.

Deze problematiek nodigt de wetgever uit een wettelijk kader hiervoor te scheppen. Tevens is het mogelijk door gedragscodes en via een toestemming van de werknemers tot een legitieme controlemogelijkheid van het e-mailgebruik te komen.

4. De repercussies van het elektronisch communicatieverkeer op de parlementaire werkzaamheden

In de Kamer van volksvertegenwoordigers werd onlangs het adviescomité voor wetenschappelijke en technologische vraagstukken opgericht. Dit comité kan op eigen initiatief dan wel op verzoek van de Kamer of één van haar commissies advies verstrekken over de wetenschappelijke en technologische vraagstukken die onder de bevoegdheid van de federale overheid ressorteren (art. 100*ter* Kamerreglement).

Gelet op het transversaal karakter van dit adviescomité zou het nuttig zijn dat dit adviescomité de knelpunten die ik hiervoor in mijn betoog heb uiteengezet - alsook andere aspecten van het elektronisch communicatieverkeer - nader analyseert en op grond van hoorzittingen een initiatiefrapport opstelt met aanbevelingen voor de andere vaste commissies.

Ook voor de interne werking van het Parlement opent het elektronisch communicatieverkeer nieuwe perspectieven. Ook in de Kamer dringen sommige fracties erop aan de ronddeling van gedrukte stukken aan de Kamerleden nader te onderzoeken, en er is een mentaliteitsverandering waar te nemen ten voordele van een elektronische ronddeling[16]. In de werkgroep Informatica van de Kamer, die ik voorzit, kan over deze aspecten verder van gedachten gewisseld worden.

Dames en Heren,

Ik dank u voor uw aandacht en wens dit parlementair internet forum alle succes toe.

Ik dank de leden van de federale, gemeenschaps- en gewestassemblees, alsook de medewerkers van de fracties en de diensten van de parlementen, voor hun interesse voor dit initiatief.

actes de harcèlement par courrier électronique interposé ou le licenciement pour motifs impérieux d'un travailleur qui aurait abusé de l'utilisation du courrier électronique et de l'Internet sont des phénomènes nouveaux auxquels les tribunaux du travail se trouvent confrontés.

Ce problème doit inciter le législateur à créer un cadre juridique dans ce domaine. Par ailleurs, l'élaboration de codes de conduite et une autorisation donnée par les travailleurs devraient permettre d'aboutir à la mise en place de possibilités de contrôle légitimes de l'utilisation du courrier électronique.

4. Les répercussions de la communication électronique sur les travaux parlementaires

La Chambre des représentants a procédé récemment à la création du Comité d'avis des questions scientifiques et technologiques. Le comité a pour mission de donner, de sa propre initiative ou à la demande de la Chambre ou d'une de ses commissions, des avis sur les questions scientifiques et technologiques qui relèvent de la compétence de l'autorité fédérale (art.100*ter* du Règlement de la Chambre).

Compte tenu du caractère transversal de ce comité d'avis, il serait utile qu'il analyse plus en profondeur et qu'il élabore – sur la base d'auditions – un rapport d'initiative contenant des recommandations à l'intention des autres commissions permanentes à propos des problèmes que je viens d'évoquer dans mon exposé et d'autres aspects liés à la communication électronique.

La communication électronique ouvre également de nouvelles perspectives pour le fonctionnement interne du Parlement. A la Chambre également, certains groupes insistent sur la nécessité de revoir le système de distribution de documents imprimés aux membres et on peut observer une évolution des mentalités en faveur d'une distribution électronique[16] . Un échange de vues à propos de tous ces aspects pourra avoir lieu au sein du groupe de travail Informatique de la Chambre, groupe de travail que je préside.

Mesdames, Messieurs,

Je vous remercie pour votre attention et je souhaite plein succès à ce forum internet parlementaire.

Je remercie les membres des assemblées fédérales, communautaires et régionales pour l'intérêt qu'ils ont manifesté en faveur de cette initiative ainsi que les collaborateurs des groupes et les services des parlements.

Een bijzonder woord van dank gaat naar de experts van ISPA, die hun expertise en bijstand leverden bij de organisatie van dit forum. ISPA, die ook al tijdens de hoorzittingen in de Senaat over het wetsontwerp inzake informaticacriminaliteit werd geraadpleegd, vertegenwoordigt meer dan 90 % van de markt van internetproviders in België en is als representatieve organisatie zeer goed geplaatst om aan de parlementairen advies te verlenen over de ontwikkelingen in de informatie- en communicatietechnologie. Ik spreek dan ook de hoop uit dat dit initiatief een vervolg kent, want de evoluties in de ICT-sector verlopen zo snel dat onze inzichten hierover permanent moeten geupdated worden.

Je voudrais également remercier tout particulièrement les experts de l'ISPA, qui ont apporté leur expertise et leur aide pour l'organisation de cet événement. L'ISPA, qui a également été consultée lors des auditions organisées au Sénat à propos du projet de loi sur la criminalité informatique, représente plus de 90% du marché belge des fournisseurs d'accès. En tant qu'organisation représentative, l'ISPA est donc l'organe approprié pour éclairer les parlementaires sur l'évolution dans le secteur des technologies de l'information et de la communication. J'espère dès lors que la présente initiative ne restera pas sans lendemain car l'évolution rapide dans le secteur ICT nécessite une mise à jour permanente de nos connaissances en la matière.»

---

1 Cfr. E-government op het vlak van de federale, provincie- en gemeentebesturen (verslag-Thijs en van Riet), Senaat, 2000-2001, 2-564/1.

2 Dat wil zeggen: het herdenken en organiseren van de relaties binnen de overheidsdiensten en tussen de overheidsdiensten onderling om aldus de elektronische dienstverlening te optimaliseren.

3 De minister van Economie heeft ondertussen twee richtlijnen omgezet, met name de richtlijn inzake «elektronische handel» en de richtlijn die een wettelijk kader schept voor de elektronische handtekening(cfr. wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen). Om de laatstgenoemde richtlijn toe te passen, moeten de procedures voor erkenning van de dienstverlening voor de echtverklaring worden opgezet (cfr. verslag-Tavernier over de rijksmiddelenbegroting voor het begrotingsjaar 2002 en ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2002, Kamer, 2001-2002, Parl. St. 1447/6, p. 473..

4 cfr. Beleidsnota van de minister van Telecommunicatie, Overheidsbedrijven en Participaties, belast met Middenstand, Parl. St., Kamer, 2001-2002, 1448/13, p. 4.

5 Het «Observatorium van de rechten op internet» (cfr. K.B. van 26 november 2001 – B.S. 15 december 2001), wiens hoofdopdracht erin zal bestaan om de regering te adviseren over de weerslag van de nieuwe technologieën op de Economie, over de bescherming van de rechten van de consumenten en over de ontwikkeling van de elektronische handel, is er ook mee belast brede acties te voeren om het publiek te sensibiliseren.

6 Cfr. S. NOUWT, e.a., «Grondrechten in het digitale tijdperk, een reactie op het rapport», NJB, afl. 27, 14 juli 2000, pp. 1321 –1327. Dit rapport is beschikbaar via: http://www.minbzk.nl/gdt

7 Wetsvoorstel (Mayeur, Genot, Vanhoutte, Chastel, Verlinde) betreffende het gebruik van open communicatiestandaarden door de overheidsdiensten, Parl. St., Kamer, 2000-2001, 1022/1.

8 wet van 20 november 2000 inzake informaticacriminaliteit (B.S.3 februari 2001).

9 Zie hierover: M.E. STORME, «Het verrichten van rechtshandelingen door middel van nieuwe telecommunicatiemiddelen – De nieuwe wetsbepalingen ingekaderd in de algemene leer van de kennisgeving», R.W., 2001-2002, nr. 11, 433-447.

10 Zie hierover: J. DUMORTIER, «Internet op het werk: controlerechten van de werkgever», Oriëntatie 2 – februari 2000, pp. 35-42.

11. Wetsvoorstel (A. Destexhe) betreffende het reglementeren van het gebruik van telecommunicatiemiddelen op de werkplaats, Parl. St., Senaat, 2000-2001, nr. 2-891/1.

---

1 Cf. L'administration électronique au niveau des pouvoirs fédéral, provincial et local (rapport de Mmes Thijs et Van Riet), Sénat, 2000-2001, 2/564/1.

2 Ce qui signifie: repenser et organiser les relations aux sein des services publics et entre les services publics, pour optimiser le service électronique.

3 Le ministre de l'Economie a entre-temps transposé deux directives, à savoir la directive sur le commerce électronique et la directive qui crée le cadre légal pour la signature électronique (cf. la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques). Pour l'application de cette dernière directive, il faudra mettre en place les procédures d'agrément des prestataires de services de certification (cf. le rapport de M. Tavernier sur le budget des Voies et Moyens pour l'année budgétaire 2002 et le projet de budget général des dépenses pour l'année budgétaire 2002, Chambre, 2001-2002, Doc. Parl. 1447/6, p. 473).

4 Cf. la note politique du ministre des Télécommunications, des Entreprises et participations publiques, chargé des Classes moyennes, Doc. Parl., Chambre, 2001-2002, 1448/13, p. 4.

5 L' «Observatoire des droits de l'internet» (cf. l'A.R. du 26 novembre 2001 – M.B. du 15 décembre 2001), dont la mission principale consiste à rendre des avis au gouvernement sur l'incidence des nouvelles technologies sur l'Economie, sur la protection des droits des consommateurs et sur le développement du commerce électronique, est également chargé de mener des actions de grande envergure pour sensibiliser le public.

6 Cf. S. NOUWT, «Grondrechten in het digitale tijdperk, een reactie op het rapport» (Les droits fondamentaux à l'ère digitale. Une réaction au rapport), NJB, n° 27, 14 juillet 2000, p. 1321 à 1327. Ce rapport peut être consulté sur le site http://www.minbzk.nl/gdt.

7 Proposition de loi (Mayeur, Genot, Vanhoutte, Chastel, Verlinde) relative à l'usage de standards de communication ouverts dans l'administration, Doc. Parl., Chambre, 2000-2001, 1022/1.

8 Loi du 20 novembre 2000 relative à la criminalité informatique (M.B. 3 février 2001)

9 Voir à ce sujet: ME. STORME, «Het verrichten van rechtshandelingen door middel van nieuwe telecommunicatiemiddelen – De nieuwe wetsbepalingen ingekaderd in de algemene leer van de kennisgeving», R.W., 2000-2001, n° 11, 433-447.

10 Voir à ce sujet: J. DUMORTIER, «Internet op het werk: controlerechten van de Wergever», Oriëntatie 2 - février 2000, p. 35 à 42.

11 Proposition de loi (de M. Destexhe) visant à réglementer l'usage des moyens de télécommunication sur le lieu de travail, Doc. Parl., Sénat, 2000-2001, n° 2-891/1.

[12] Het recht op privacy wordt gewaarborgd door art. 8 van het Europees Verdrag tot bescherming van de rechten van de mens.
[13] dit arrest kan men raadplegen op: http://www.courdecassation.fr/agenda/arrets/arrets/999-42942arr.htm
[14] Advies nr 10/2000 van 3 april 2000 (tekst te raadplegen op de website van de Commissie: www.privacy.fgov.be).
[15] Zie hierover: T. CLAEYS en D. DEJONGHE, «Gebruik van E-mail en Internet op de werkplaats en controle door de werkgever, JTT, 2001, pp.121-134.
[16] Cfr. verslag-Van Overtveldt, Parl. St., Kamer, 2001-2002, nr. 1531/1, p.15. (interventie van de heer J. Tavernier).

[12] Le droit à la vie privée est consacré par l'article 8 de la Convention européenne des droits de l'homme.
[13] Cet arrêt peut être consulté sur: http://www.courdecassation.fr/agenda/arrets/arrets/999-42942arr.htm
[14] Avis n° 10/2000 du 3 avril 2000 (texte à consulter sur le site internet de la Commission : www.privacy.fgov.be).
[15] Voir à ce sujet: T. CLAEYS et D. DEJONGHE, «Utilisation du courrier électronique et de l'Internet sur le lieu de travail et contrôle par l'employeur», JTT,2001, pp.121-134.
[16] Cf. rapport-Van Overtveldt, Doc. parl. Chambre, 2001-2002, n° 1531/1, p. 15 (intervention de M. J. Tavernier)

Voorzitter : de heer Peter VANHOUTTE, volksvertegenwoordiger (AGALEV-ECOLO)

A. **Hoe werkt E-mail? - Uiteenzetting door de heer Rudi ROTH, directeur ISPA**

Dames en heren,

Het is onze federatie ISPA en haar leden een waar genoegen en een grote eer aan dit forum te mogen deelnemen. Ik maak van de mij geboden gelegenheid gebruik om de Kamer, de Senaat en al diegenen die tot de organisatie van dit forum hebben bijgedragen, te bedanken. Om de belangstelling voor dergelijke debatten aan te zwengelen hebben wij als thema voor deze eerste forumdiscussie een instrument gekozen waarmee u allen vertrouwd bent en dat momenteel op de agenda staat van verscheidene parlementaire vergaderingen, namelijk : e-mail. Het toeval wil dat onze zusterorganisatie, ISPA UK, morgen voor het zesde opeenvolgende jaar een soortgelijk debat organiseert in Whitehall, maar dan over breedbandinternet. Wij zijn overigens volkomen bereid om volgend jaar opnieuw een dergelijke bijeenkomst te houden, met het oog op een diepgravende discussie over door u aangereikte thema's.

ISPA België vzw is de vereniging van internet service providers (ISP's) in België. Sinds twee jaar bekleed ik de functie van directeur van de vereniging, maar als medewerker van het eerste uur ben ik eigenlijk al van september 1996, d.i. van vóór de officiële oprichting ervan, bij de vereniging betrokken. Ons ledental is in de loop van de beginjaren gestegen. Het zou nu de komende maanden normaal gezien wat moeten dalen, gezien de fusies, maar onze leden worden dan wel grotere entiteiten. In de tekst worden de belangrijke gebeurtenissen vermeld die als mijlpaal beschouwd kunnen worden in het bestaan van de ISPA. Voorts bevat de tekst de lijst van internetaanbieders. Onze ledenlijst vindt u op de ISPA-website.

Sinds drie jaar verricht de ISPA studiewerk naar de ontwikkeling van het internet in België. Daarbij worden de exacte cijfers m.b.t. de abonnementen van de klanten van de ISPA-leden opgeteld. Het breedbandinternet (kabel en ADSL) zet zijn opmars onstuitbaar voort, in de eerste plaats dankzij een zekere *shift* (verschuiving) onder de abonnees, maar niettemin valt te vrezen dat de totale markt zal stagneren.

Een vergelijking met de markt van de mobiele telefonie in België is eveneens veelzeggend. We zien dat die markt blijft groeien dankzij een verder doorge-

Président. M. Peter VANHOUTTE, député (AGALEV-ECOLO)

A. ***Comment fonctionne le courrier électronique à l'heure actuelle? - Exposé de M. Rudi ROTH, diresteur ISPA***

Mesdames et Messieurs,

C'est un grand plaisir et un honneur pour notre fédération — ISPA — et ses membres de pouvoir participer à ce forum. Je profite de l'occasion qui m'est donnée ici pour remercier la Chambre, le Sénat et toutes les personnes qui ont contribué à la mise en place de ce forum. Afin de stimuler l'intérêt pour ce type de débat, nous avons choisi comme thème pour cette première un outil avec lequel vous êtes déjà familiarisé et qui est d'actualité dans plusieurs travaux parlementaires : l'e-mail. Le hasard du calendrier fait que notre association sœur, ISPA UK, organisera ce type de débat à Whitehall demain, pour la 6e année consécutive, mais sur le thème de l'Internet à large bande. Nous aussi, nous sommes tout disposés à renouveler cet exercice l'année prochaine sur des sujets plus approfondis que vous jugerez utiles.

ISPA Belgium ASBL est l'association des fournisseurs Internet en Belgique, ISP en abrégé. J'en assume le rôle de directeur depuis 2 ans, mais j'y étais impliqué depuis la veille de sa conception, en septembre 1996. Si le nombre de nos membres a grandi au cours des premières années, il devrait normalement diminuer au cours des mois à venir, mais englober des membres de taille plus importante à cause des fusions.Vous trouverez dans le texte les événements importants de la vie de l'ISPA, ainsi que la liste des fournisseurs d'accès. Pour la liste des membres adhérents, je vous renvoie au site de l'ISPA.

Depuis trois ans, ISPA fait une étude sur le développement de l'Internet en Belgique en additionnant les chiffres exacts des abonnements de la clientèle de ses membres. Si la croissance de la large bande (câble et ADSL) se poursuit, en raison surtout d'un certain shift (déplacement) parmi les abonnés, une stagnation du marché total est à craindre.

La comparaison avec le marché de la téléphonie mobile en Belgique est aussi très parlante. Ce marché continue de croître grâce à une libéralisation plus pous-

voerde liberalisering. Dat is niet het geval voor de internetmarkt.

Ondanks de toenemende penetratiegraad van breedbandaansluitingen - op dat gebied zijn wij nagenoeg koploper in Europa - moeten wij vaststellen dat België wat aansluitingen in het algemeen betreft, ver achterligt op het koppeloton. Ons inziens is dat fenomeen toe te schrijven aan de langzame liberalisering van de telecommunicatiemarkt, wat de introductie van nieuwe commerciële formules in de weg staat. Een van de gevaren daarvan is een mogelijke sociale breuk. Wij hopen dat we dat risico zullen kunnen ondervangen met het door minister Picqué opgerichte Observatorium van de Rechten op het Internet.

Tot zover deze kleine opheldering, en laten we ons nu concentreren op het Forum zelf.

1. *Hoe werkt e-mail ?*

Aangezien de telematica in het algemeen en het internet in het bijzonder vrij virtuele aangelegenheden zijn, zal voor deze toelichting bij de werking van e-mail teruggegrepen worden op vergelijkingen met andere communicatiesystemen waarmee u allen vertrouwd bent om de nodige functies te verduidelijken. Zoals alle vergelijkingen hebben ook de onze hun beperkingen, en het is dus zaak ze niet extreem te gaan extrapoleren. Sommige verschillen maken wel degelijk wat uit in de technische en wettelijke context.

E-mail, elektronische post, of nog «mèl» voor de Canadezen, bestaat al ruim dertig jaar op privécomputernetwerken en het universitaire internet. Met de komst van het door een Engelsman en de Belg Robert Cailliau bedachte www is die vorm van communicatie gemeengoed geworden. Vandaag is het de meest gebruikte toepassing op het internet. E-mail biedt gigantische mogelijkheden voor een betere en snellere wereldomspannende communicatie. E-mail is trouwens niet meer weg te denken in onze economie.

Na een toelichting over de onderscheiden soorten e-mail, zoals popmail en webmail, zullen we één en ander nader onder de loep nemen, en besluiten met een zeer eenvoudig gehouden technische uitleg over de werking van het geheel.

2. Popmail - Webmail - Private mail:

E-mail en gewone post hebben tal van functies gemeen. Ook bij e-mail is er sprake van een afzender en een geadresseerde. Elkeen heeft een brievenbus : in

sée, ce qui n'est pas le cas de l'Internet.

En dépit de la pénétration des connexions large bande, pour lesquelles nous dépassons pratiquement tous les autres pays européens, nous observons que la Belgique est loin du peloton de tête pour les connexions en général. Les raisons sont dues selon nous à cette lenteur de la libéralisation du marché des télécommunications, qui fait obstacle à l'introduction de nouvelles formules commerciales. Un danger qui en découle est une fracture sociale possible. Nous espérons pouvoir combattre ce risque dans le cadre de l'observatoire de l'Internet, qui a été mis en place par le ministre Picqué.

Après cette petite mise au point, concentrons-nous sur le sujet du Forum.

1. *Fonctionnement de l'e-mail*

Comme la télématique, en général, et l'Internet, en particulier, sont des matières assez virtuelles, cette explication du fonctionnement de l'e-mail fera appel à des comparaisons avec d'autres systèmes de communication qui vous sont familiers pour clarifier les fonctions nécessaires. Mais comme toutes comparaisons, les nôtres ont aussi leurs limites et il ne faudra surtout pas les extrapoler à l'extrême. Il y a aussi des différences qui ont leur importance dans le contexte technique et légal.

L'e-mail, c'est-à-dire les messages électroniques ou courriel ou encore mèl pour les Canadiens, existe depuis plus de 30 ans dans les réseaux informatiques privés et l'Internet universitaire. Avec l'arrivée du WWW, inventé par un Anglais et un Belge, Robert Cailliau, cette forme de communication s'est généralisée et est devenue le service le plus utilisé sur l'Internet. Elle apporte d'énormes possibilités pour améliorer et accélérer la communication au niveau planétaire. On ne pourrait d'ailleurs plus vivre sans e-mail dans notre économie.

Après une explication des types d'e-mail tels que le popmail et le webmail, nous allons décomposer ce courriel et terminer par une explication technique des plus simples sur le fonctionnement de l'ensemble.

2. Popmail - Webmail - Private mail:

Le courrier électronique a plusieurs fonctions similaires au courrier postal. Il comporte notamment un expéditeur et un destinataire. Chacun dispose d'une

het ene geval betreft het een échte, een reële brievenbus, in het andere geval een elektronische brievenbus, op de computer. De structuur van de postdiensten wordt bij e-mail vervangen door het internet. Momenteel zijn er twee grote typen van diensten : popmail en webmail.

Popmail bestaat al langer, en vermoedelijk maakt u met uw internetaanbieder gebruik van deze e-mailoplossing. De berichten worden beheerd door een e-mailclientsoftwareprogramma, zoals Outlook, Outlook Express, Netscape Messenger, Eudora, enz. Kopieën van de berichten worden bewaard op de harde schijf van uw computer.

Om e-mailberichten te versturen brengt het e-mailclientprogramma (Outlook, etc.) een aansluiting tot stand met het netwerk, en onder meer ook met een SMTP-serverprogramma (Simple Mail Transfer Protocol), waar de berichten die je verzendt afgeleverd worden. Die SMTP-server wordt beheerd door de internetaanbieder (bv. Planet Internet, Skynet, of andere leden van onze federatie). Hij doet dienst als postkantoor en verzamelt alle door de eigen gebruikers verzonden berichten.

De internetaanbieders gaan na of de afzender wel het recht heeft om gebruik te maken van deze dienst. Dat gebeurt via de identificatie bij de aansluiting. Die operatie kan je vergelijken met de controle van de herkomst van de postzegel die op een brief plakt. Zo mag een Planet Internet-abonnee geen gebruik maken van de SMTP-server van Skynet om zijn e-mailberichten te versturen, want hij beschikt niet over de juiste, bij zijn aansluiting behorende, virtuele postzegel.

Op grond van het adres van de geadresseerde gaat de SMTP-server op het internet op zoek naar de plek waar het e-mailbericht moet worden afgeleverd. De zoektocht leidt meer bepaald naar een andere computer, namelijk : de POP3-server. De POP3-server is, mutatis mutandis, niets anders dan het postkantoor van de stad of gemeente waar de geadresseerde woont. De POP3 ontvangt het bericht en slaat het op op een aan de geadresseerde voorbehouden plaats. De geadresseerde kan zijn bericht nu openen door gebruik te maken van dezelfde e-mail-clientsoftware, Outlook bijvoorbeeld, die dus als het ware als postbode fungeert. Er is uiteraard een controle om zeker te zijn dat de berichten door de juiste geadresseerde geopend worden : daarom moet je een ID en wachtwoord intikken om de aansluiting tot stand te brengen. Op dat moment bevinden de e-mails zich op je PC, en kan je ze openen, en lezen.

Webmail is een ander type van elektronische post. Voorbeelden van webmail zijn : Hotmail, Yahoo, Caramail, enz. Deze vorm van e-mail werkt volgens een ander principe, en is veeleer te vergelijken met een “poste restante”-berichtendienst op een plaats zon-

boîte aux lettres ; dans un cas, elle est physique, dans l’autre, elle est électronique, se trouvant dans l’ordinateur. La structure des services postaux est ici remplacée par le réseau Internet. Aujourd’hui, on compte deux types importants de service : le popmail et le webmail.

Le popmail existe depuis plus longtemps et c’est ce type que vous utilisez sans doute avec votre fournisseur d’accès à l’Internet. Les messages sont gérés par un logiciel informatique appelé «client e-mail» tel qu’Outlook, Outlook Express, Netscape Messenger, Eudora, etc. Des copies des messages sont gardées sur le disque dur de votre ordinateur.

Afin d’envoyer le courriel, le programme client e-mail (Outlook, etc.) établit une connexion avec le réseau et, entre autres, avec un programme informatique serveur SMTP (Simple Mail Transfer Protocol) auquel il délivre les messages sortant de votre ordinateur. Ce serveur SMTP est géré par votre fournisseur Internet (comme Planet Internet, Skynet ou d’autres membres de notre Fédération). Il agit comme un bureau de poste et récolte tous les messages envoyés par ses propres utilisateurs.

Les fournisseurs d’accès à l’Internet vérifient que l’expéditeur a bien le droit d’utiliser ce service par le moyen de son identification pendant la connexion. On peut comparer cette opération à la vérification de la provenance du timbre collé sur une lettre. Ainsi, un abonné de Planet Internet n’a pas le droit d’utiliser le serveur SMTP de Skynet pour expédier ses e-mails, puisqu’il ne dispose pas du timbre virtuel correct, lié à sa connexion.

Sur la base de l’adresse du destinataire, ce serveur SMTP cherche dans l’Internet l’endroit où distribuer ce courriel. Il s’agit de trouver un autre ordinateur : le serveur POP3. Ce POP3 est, par analogie, le bureau de poste de la ville ou de la commune où réside le destinataire. Il reçoit le message et le stocke à un endroit réservé au destinataire. Ce dernier peut alors y accéder en utilisant le même programme client e-mail, Outlook, par exemple, qui joue donc un peu le rôle du facteur. Il y a bien sûr un contrôle afin de s’assurer que c’est bien la bonne personne qui accède aux messages qui lui sont destinés et cela se fait par une connexion avec identification et mot de passe. C’est à ce moment que les e-mails se trouvent sur votre PC et que vous pouvez les ouvrir et les lire.

Un autre type de messagerie électronique est le Webmail, comme Hotmail, Yahoo, Caramail, etc. Le principe est différent et se compare plutôt à une poste restante dans un endroit où il n’y aurait ni facteurs ni boîtes postales dans la rue. Les messages sont et restent

der postbodes of brievenbussen op straat. De berichten blijven opgeslagen op een computer die speciaal voor die dienstverlening geconfigureerd werd, en die om het even waar op het internet kan staan. Het programma dat gebruikt wordt, is de browser, zoals Netscape of Internet Explorer, aan de hand waarvan je, althans zolang je ingelogd bent, berichten rechtstreeks op het web kan lezen en schrijven - alsof je je brieven zou lezen en schrijven in het postkantoor en daar ook zou achterlaten, in je eigen postvakje. Om toegang te krijgen, zowel om berichten te lezen als om berichten op te stellen, moet je weliswaar een wachtwoord ingeven, maar het personeel van dat virtuele postkantoor zou ook toegang kunnen hebben tot je postvakje. Het voordeel is dan weer dat er met een virtueel postkantoor wordt gewerkt, dat dus vanop elke PC bereikbaar is, op voorwaarde dat je je wachtwoord onthoudt. Op je eigen computer worden normaal gezien geen kopieën bewaard van je e-mailberichten.

Een bedrijf of organisatie kan deze berichtendienst ook aanbieden. Voorwaarde is dat men over computers, de nodige software en een internetaansluiting beschikt. In Kamer en Senaat bijvoorbeeld wordt die dienstverlening aangeboden, waarbij Kamer en Senaat fungeren als lokaal postkantoor. De brieven worden niet langer één voor één, maar met postzakken tegelijk verstuurd via de permanente internetverbinding. Geregeld worden er nieuwe oplossingen ontwikkeld op grond van het popmail- of het webmailprincipe, of een combinatie van beide.

3. <u>De componenten van een e-mailbericht:</u>

Een e-mailbericht bestaat uit twee grote delen : een header of briefhoofd, en de body of tekst zelf van het bericht. De informatie in de header is te vergelijken met wat er op een enveloppe staat: naam en adres van geadresseerde en afzender, voor zover deze laatste niet anoniem wenst te blijven.

Anders dan bij brieven op papier bevat een e-mailheader bovendien een vakje voor het onderwerp, dat mee weergegeven wordt bij ontvangst, net als de identiteit van de afzender en de geadresseerden.

a) Header of briefhoofd
From :/Van : afzender
Die informatie is normaal gezien beschikbaar op je computer of kan via het e-mailprogramma, zoals Outlook, worden bekomen. In de meeste gevallen kan je die informatie zelf ingeven of wijzigen, maar in het merendeel van de bedrijven en instellingen die zich hebben toegerust om als lokaal postkantoor te fungeren, zal het programma door de dienst Informatica zodanig

dans un ordinateur spécialement configuré pour fournir ce service. Il peut être n'importe où dans l'Internet. Le programme utilisé est alors le butineur ou le browser, comme Netscape ou Internet explorer et il vous permet de lire et écrire les messages directement sur le Web pendant votre connexion. C'est un peu comme si vous écriviez et lisiez votre courrier dans le bureau de La Poste et le laissiez sur place dans un casier à vous. Pour y accéder, tant pour lire que pour écrire, il faut utiliser un mot de passe, mais le personnel de cette poste virtuelle pourrait aussi avoir accès à votre casier. Un avantage est que ce bureau de poste est virtuel et donc accessible de n'importe où, à condition de ne pas oublier son mot de passe. Et sur votre ordinateur il n'y a donc normalement pas de copies de vos e-mails.

Une société ou une organisation peut aussi fournir ce service, à condition de disposer d'ordinateurs, de programmes informatiques et d'une connexion à l'Internet. Vous disposez de ce service à la Chambre et au Sénat, qui fonctionne alors comme un bureau de poste local. Au lieu d'expédier les lettres une à une, le courrier est acheminé par sacs entiers au moyen de la connexion permanente à l'Internet.Et régulièrement de nouvelles solutions voient le jour en se basant sur le principe du Popmail ou du Webmail ou d'une combinaison des deux.

3. <u>Les parties principales d'un e-mail:</u>

Un courrier électronique se compose de deux parties principales : un en-tête et le corps du message. L'entête se compare à ce qui se trouve sur une enveloppe : les noms et adresses du destinataire et de l'expéditeur, dans la mesure où celui-ci ne souhaite pas rester anonyme.

À la différence du courrier papier, vous disposez d'une case qui permet d'indiquer le sujet et qui s'affiche quand il est reçu, exactement comme les identités de l'expéditeur et des destinataires.

a) Header ou en-tête
From:/De: à expéditeur
Cette information est normalement disponible dans votre ordinateur ou votre programme e-mail comme Outlook. Dans la plupart des cas, vous pouvez l'introduire ou le changer vous-même. Dans la majorité des sociétés ou organisations qui se sont équipées comme bureau de poste local, le programme sera configuré pour vous par le service informatique de telle façon

geconfigureerd zijn dat je je identiteit niet kan veranderen of verbergen.

To :/T.a.v.: geadresseerde
Bevat het e-mailadres of de e-mailadressen van de geadresseerde(n) (dat kunnen personen zijn of organisaties). Bij ontvangst van het bericht kan je onmiddellijk zien wie de eventuele andere geadresseerden van het mailtje zijn. Het is niet nodig het bericht daarvoor te openen of te lezen. Dat is nog een verschil met papieren brievenpost.

Cc : (carbon copy/carbonkopie)
Bevat de adressen van de personen die een kopie van het bericht ontvangen. Die informatie is voor iedereen toegankelijk.

Bcc :/Cci : (blind carbon copy/vertrouwelijke kopie)
Dit zijn verborgen of geheime kopieën. Deze adressen of geadresseerden kunnen de andere geadresseerden niet zien. De afzender zelf weet natuurlijk aan wie een kopie gestuurd werd, en voorts weet elke geadresseerde enkel van zichzelf dat hij een kopie van het bericht ontvangen heeft.
Sommige ISP's beperken het aantal geadresseerden, en vooral het aantal vertrouwelijke kopieën, om te voorkomen dat er grote aantallen e-mails ongevraagd rondgestuurd worden.

Subject :/Betreft :
Dit vakje maakt deel uit van de header, en kan desgewenst worden ingevuld.

Ter opfrissing van het geheugen volgt nu een korte ontleding van een e-mailadres.
Voorbeeld : info@ispa.be

Aan de hand van het tweede gedeelte, «ispa.be», kan je de POP3-server van de geadresseerde identificeren.

- «.be»

Het suffix «.be» is welbekend en geeft over het algemeen de plaats aan waar de elektronische berichtendienst gelokaliseerd is, in casu België. De suffixen «.fr» en «.nl» verwijzen respectievelijk naar Frankrijk en Nederland. Bij andere suffixen, zoals «.com» of «.org», is er geen specifieke geografische link.

- «ispa»

De domeinnaam ISPA duidt op de organisatie die de e-mailservice aanbiedt. Vaak staat hier de naam van de internetaanbieder, zoals Planet, Skynet, enz.

que vous ne pourrez ni cacher ni changer votre identité.

To :/À : à destinataire
Contient la ou les adresses e-mail des personnes ou organisations destinataires. Chacun voit, à la réception du courrier, qui sont les autres destinataires, sans devoir ouvrir ou lire le courrier. Une différence avec le courrier papier.

Cc : (carbon copy/copie carbone)
Les adresses de personnes copies, aux vu et su de tout le monde.

Bcc :/Cci : (blind carbon copy/copie confidentielle)
Ce sont les copies cachées ou secrètes. Ces adresses ou personnes ne sont pas visibles pour les autres destinataires. Il n'y a que l'expéditeur et la personne même qui savent qu'ils ont reçu ce courrier.

Certains ISP limitent le nombre de destinataires et surtout le nombre de copies cachées afin d'éviter des distributions de grande quantité d'e-mails non sollicités.

Subject :/Objet :
Fait partie de l'en-tête et peut être complété ou non.

Pour rappel, décomposons très brièvement une adresse e-mail :
Exemple : « info@ispa.be»

La deuxième partie ispa.be permet de localiser le serveur POP3 du destinataire.

- «.be»:

Cette partie, le suffixe .be, est bien connue et indique, en général, l'endroit où la messagerie est localisée. Dans ce cas, il s'agit de la Belgique. Les codes .fr et .nl sont ceux de la France et des Pays-bas. Mais il existe également d'autres suffixes tels que .com ou .org qui n'ont pas de lien géographique particulier.

- «ispa»:

Le nom de domaine ISPA est celui de l'organisation qui fournit le service e-mail. Dans de nombreux cas, il s'agit du nom du fournisseur d'accès tel que Planet, Skynet ou autres.

• «@»

Het apenstaartje of at-sign, ook slingeraap genoemd (arobas in het Frans), scheidt de domeinnaam van de gebruikersnaam.

• «info»

Dit is de naam van de gebruiker. Bij het in ons voorbeeld gebruikte «info» gaat het meestal om een acroniem ter aanduiding van een geadresseerde binnen een organisatie, zonder dat het bericht tot één welbepaalde geadresseerde gericht is. Normaal gezien staat hier de naam van een persoon of dienst; en het is ook de sleutel om toegang te krijgen tot de brievenbus op de POP3-server.

b) Body

Hiermee bedoelen we de tekst zelf met de boodschap die je wil meedelen.

Het bericht kan ook een *attached file* bevatten, wat je kan vergelijken met een pakje dat je met een begeleidende brief verstuurt. Het kan daarbij gaan om een Excelbestand, een Word-document, een afbeelding of zelfs een geluidsfragment, of andere computerdocumenten. Van belang is dat de geadresseerde het bestand kan lezen en te dien einde over het overeenkomstige programma beschikt. Ook computervirussen worden wel eens verspreid onder de dekmantel van een *attached file*. De grootste waakzaamheid is dan ook geboden bij het openen of inkijken van een *attachment.*

4. <u>De weg die een e-mail aflegt</u>

Voor ik u toon welke weg een e-mail aflegt van afzender tot geadresseerde, moet ik u nog wat uitleg geven over drie andere componenten van het proces :

het IP-adres, de router en enkele principes van het TCP/IP-protocol.

a) e-mailadressen – IP-adressen

Het internet is een netwerk van computerknooppunten, een soort spinnenweb zo u wil, vandaar ook de benaming World Wide Web.

Op elk knooppunt zitten er één of meer computers (of PC's). Elk daarvan heeft een uniek nummer op het internet. Dat is het IP-adres (Internet Protocole), dat tot identificatie dient.

Dat adres is nodig om elke knoop in het netwerk te kunnen bereiken. Wanneer een gebruiker een internetverbinding tot stand brengt, krijgt hij een voorlopig IP-

• @:

Le «a» commercial, appelé arobas, «at-sign» ou apestaart en néerlandais joue le rôle de séparateur entre le nom de domaine et le nom de l'utilisateur.

• «info»:

C'est le nom de l'utilisateur. Dans le cas de «info», il s'agit, en général, d'un acronyme pour un destinataire au sein d'une organisation, sans s'adresser à une personne en particulier. Normalement, on y trouve le nom de la personne ou du service et il s'agit aussi de la clé pour accéder à la boîte aux lettres sur le serveur POP3.

b) Body

Ceci est le corps du message avec le texte que l'on veut communiquer.

On peut y retrouver aussi un fichier attaché, comme un colis que l'on envoie avec la lettre. Il peut s'agir d'un fichier Excel, d'un document Word, d'une image ou même d'un fragment sonore ou d'autres documents informatiques. L'important est que le destinataire puisse lire le fichier et dispose du programme correspondant.Des virus informatiques sont aussi envoyés en tant que fichiers attachés, et la prudence extrême est recommandée avant d'ouvrir ou de visualiser des fichiers attachés.

4. <u>Le cheminement d'un e-mail</u>

Avant de vous montrer le cheminement complet d'un e-mail, nous avons besoin de donner une explication sur trois éléments supplémentaires.

Il s'agit de l'adresse IP, du router, et de quelques principes du protocole TCP/IP.

a) Email adresses – IP adresses

L'Internet est un réseau de nœuds d'ordinateurs, appelé aussi le World Wide Web ou Toile, comme une toile d'araignée.

À chaque nœud se trouvent un ou plusieurs ordinateurs (ou PC). Chacun dispose d'un numéro unique dans l'Internet : l'adresse IP (pour Internet protocole) qui l'identifie.

Cette adresse est nécessaire afin de pouvoir atteindre chaque nœud du réseau. Quand un utilisateur se connecte à l'Internet, il reçoit une adresse IP tempo-

adres, aan de hand waarvan hij door de overige knooppunten in het netwerk herkend kan worden. De gebruiker wordt geïdentificeerd door middel van de combinatie van het IP-adres en het uur waarop van het adres gebruik werd gemaakt.

Voor de gebruiker zijn die adressen echter niet zo gebruiksvriendelijk. Daarom heeft men de domeinnamen bedacht. Dankzij die domeinnamen kan er gewerkt worden met gemakkelijker te onthouden adressen voor e-mail of websites. Het systeem waarmee dat alles beheerd wordt, is het DNS, het Internet Domain Name System of domeinnaamsysteem. Het is te vergelijken met een adresboek of de lijst van telefoonnummers in je GSM. Het e-mailadres en de domeinnaam in het e-mailadres worden door dat adresboeksysteem vertaald in een IP-adres.

b) Routers

Routers zijn als het ware de wisselwachters van het web; ze bepalen de weg die een e-mailbericht volgt van de ene computer naar de andere. Het zijn computers die constant op de hoogte zijn van de situatie op het netwerk, de drukte van het verkeer op het web en de beschikbaarheid van de routes. Zij bevinden zich op de communicatieknooppunten van het web.

c) TCP/IP

Dat alles functioneert dankzij afspraken die gemaakt werden met betrekking tot de routers en het web zelf : de TCP's (Transmission Control Protocol) en IP's (Internet Protocol). E-mails worden verzonden met gebruikmaking van die principes. We zullen maar enkele aspecten van die overeenkomsten bespreken.

Het TCP-gedeelte betreft de manier waarop de berichten worden getransporteerd. Om tal van technische redenen worden ze niet als één geheel verstuurd, maar worden ze opgedeeld in kleinere pakjes ter grootte van (het equivalent van) 1500 lettertekens. In elk pakje zit het IP-adres van de afzender en van de geadresseerde, opdat elk pakje op eigen kracht de weg zou kunnen vinden. Dankzij die overeenkomst kan de software bij de geadresseerde de pakjes ook weer samenvoegen tot het oorspronkelijke geheel.

De IP-overeenkomst - vandaar : IP-adres - betreft de routing bij de routers, en heeft tot doel de meest efficiënte weg uit te stippelen.

De SMTP-server zoekt het IP-adres van de geadres-

raire, ce qui lui permet d'être reconnu par les autres nœuds du réseau. La combinaison de l'adresse IP et de l'heure de son utilisation permet d'identifier l'utilisateur.

D'un autre coté, pour les utilisateurs, ces adresses ne sont pas très conviviales. À cette fin, on a inventé le système des noms de domaines, Domain names.Cela permet d'avoir une adresse plus facile à retenir pour les e-mails ou pour les sites Web à visiter. Le système qui gère cela s'appelle Domain Name System et fonctionne comme un carnet d'adresses ou comme le répertoire dans votre GSM. L'adresse e-mail et sa partie domaine sont traduites en adresse IP par ce système de carnet d'adresses.

b) Routers

Les routers jouent dans la toile le rôle d'aiguillages, qui permettent de décider de la route à prendre par ces e-mails. Ce sont des ordinateurs qui se tiennent au courant de l'état du réseau, du trafic et des disponibilités des routes. Ce sont eux qui se trouvent aux nœuds de communication dans le Web.

c) TCP/ IP

Le tout fonctionne grâce à une convention utilisée dans les routers et le Web: les protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol). Les e-mails sont envoyés sur la base de ces principes. Nous ne verrons que quelques aspects de ces conventions.

La partie TCP s'occupe de la méthode de transport au niveau des messages. Pour de multiples raisons techniques, ils ne sont pas envoyés comme des colis entiers, mais bien décomposés en petits paquets équivalant à 1500 caractères de texte. Dans chaque paquet se trouve l'adresse IP de l'expéditeur et du destinataire, afin que chacun d'eux puisse retrouver son chemin indépendamment. La même convention permet au programme informatique, qui se trouve chez le destinataire, d'assembler les paquets pour reconstituer le message original.

La convention IP, qui a donné le nom à l'adresse IP, s'occupe du routage dans les routers afin de trouver la meilleure route.

SMTP cherche l'IP du destinataire, TCP découpe en

seerde; het TCP deelt het bericht op in pakjes, telkens met het adres van de afzender en van de geadresseerde; en dit is een gedetailleerde weergave van de weg die het bericht vervolgens aflegt …

Bij aankomst worden de pakjes weer samengevoegd.

Wij hopen dat u door deze uiteenzetting een beter inzicht gekregen heeft in wat er zich allemaal afspeelt achter de coulissen van het internet. Ik wijs er nogmaals op dat het om een weliswaar juiste doch vereenvoudigde uitleg gaat, die zinvol is voor een beter begrip van de specifieke aspecten van hetgeen vandaag verder nog op het programma staat. Bij gebrek aan tijd zal ik niet nader ingaan op de proxy's of cachegeheugens, computers die onontbeerlijk zijn voor de goede werking van het web en die tijdelijke kopieën maken van de gegevens. Ik dank u voor uw aandacht.

B. **Misbruik en Gebruik van e-mail - Uiteenzetting door de heer Carlos van Nunen, Legal Manager, Planet Internet**

Geachte Voorzitter, dames en heren,

Ik ben zelf de juridisch directeur van 1 van de grootste internet providers van ons land, en word in die hoedanigheid regelmatig geconfronteerd met misbruik van e-mail naar onze klanten toe.

4 dagen geleden werd mijn eerste kindje geboren, Alexander. We hebben dan ook meteen een gepersonaliseerd e-mailadres voor hem geregistreerd, namelijk alexander@vannunen.be . Om de kersverse opa en oma te verrassen, zijn we naar Yahoo gesurft om hen vandaar een electronische wenskaart te versturen. U kent dat wel: net zoals een traditionele wenskaart, maar dan via e-mail. Om zo'n kaart te kunnen verzenden, moet je dus eertst een gegevenslijst invullen, waaronder ook – logisch – het e-mail adres van de verzender. Ik vulde dus Alexanders emailadres in: alexander@vannunen.be . Toen ik gisteren deze speech doornam, merkte ik dat mijn zoontje van amper 4 dagen oud reeds 3 e-mailberichten had. Een kleine die zo snel al aan netwerking doet, is een grote politieke toekomst beschoren, dacht ik nog, tot ik merkte dat 1 mail van opa kwam en de andere twee mails spam waren. Ik was inderdaad zo dom geweest om z'n emailadres op de gegevenslijst van Yahoo te zetten, en zo moeten de spammers er reeds op uitgekomen zijn. Dit voorbeeld illustreert perfect waar ik het in deze bijdrage met u

paquets avec les adresses de l'expéditeur et du destinataire et voici le cheminement en détail….

À l'arrivée : assemblage des paquets.

Nous espérons que ceci vous a permis d'avoir une meilleure vue de ce qui se passe dans les coulisses de l'Internet. Je vous rappelle qu'il s'agit d'une explication correcte mais simplifiée, qui a son importance pour mieux saisir les aspects spécifiques de la suite. Par manque de temps, nous n'allons pas nous étendre sur le système des mémoires proxy ou cache, c'est-à-dire des ordinateurs indispensables au fonctionnement correct du Web qui font des copies temporaires des informations. Je vous remercie.

B. **Usage normal et abusif d'e-mails - exposé de M. Carlos van Nunen, Legal Manager, Planet Internet**

M. le Président, Mesdames et Messieurs,

Je suis le directeur juridique d'un des providers les plus importants du pays. En cette qualité, je suis régulièrement confronté aux abus d'e-mails envoyés à nos clients.

Voici quatre jours, mon premier enfant, Alexander, est né. Nous avons donc enregistré pour lui une adresse e-mail personnalisée, à savoir alexander@vannunen.be. Afin de faire une surprise à la grand-mère et au grand-père, nous avons surfé sur Yahoo afin de leur envoyer une carte de vœux électronique à partir de ce site. Vous savez ce dont il s'agit: elle ressemble à une carte de vœux traditionnelle mais elle est envoyée comme un e-mail. Pour pouvoir envoyer une telle carte, vous devez d'abord remplir un formulaire dans lequel vous devez logiquement mentionner l'adresse de l'expéditeur. J'ai donc introduit l'adresse d'Alexander: alexander@vannunen.be. Lorsque, hier, j'ai relu ce speech, j'ai constaté que mon fils, âgé d'à peine quatre jours, avait déjà reçu trois e-mails. Je me suis dit qu'un bébé qui noue des contacts aussi rapidement a un grand avenir politique devant lui. J'ai alors remarqué que l'un des e-mails venait du grand-père mais que les deux autres étaient des spams. J'avais en effet été assez bête pour mentionner son adresse e-mail sur le formulaire de Yahoo. Les spammers étaient déjà passés par là. Cet

over wil hebben: ik wil u een overzicht geven van de belangrijkste vormen van misbruik van of met e-mail. Let op: alle vormen van misbruik die we gaan zien, bestonden reeds lang voor e-mail werd uitgevonden. De nieuwe technologie is slechts een nieuwe vorm waarmee deze inbreuken gepleegd worden.

Ik zal u achtereenvolgens volgende misbruiken tonen:
– SPAM of junk-mail
– Andere vormen van misbruik, zoals e-mail-bombardementen, kettingmails en stalking

– Anonieme mails
– En de taak van de Abuse-afdeling van de ISP's

Om ten slotte te eindigen met een belangrijk positief gebruik, namelijk Direct Marketing via e-mail.

1. *Spam*

a) Wat is spam? (ongewenste e-mail, courriel non-sollicité, unsollicited e-mail)

Iedereen van u heeft ongetwijfeld reeds zo'n mails ontvangen.

Spam kan gedefinieerd worden als het versturen van ongevraagde en ongewenste berichten naar vele e-mail-adressen in één keer.

De inhoud kan variëren van gewoon commercieel, over sex tot racisme of andere illegale acties en het aanbieden van illegale producten

Bij spam ligt de grootste kost bij de internetproviders en de ontvangers. De spammer hoeft slechts één bericht te versturen naar een lijst ontvangers; dat kost hem gewoon 1 druk op de knop. De internetprovider moet elk bericht naar een bepaald adres individueel behandelen, wat tot een grote belasting van het systeem leidt. De ontvanger van zijn kant moet e-mail binnenhalen die hij niet gevraagd heeft en betaalt daar de verbindingskosten voor.

b) Hoe gaat een spammer te werk?

1° Om massa's e-mail te kunnen versturen heeft de spammer eerst een adressenlijst nodig. Hij gaat dus op zoek naar e-mailadressen van het publiek dat hij wil

exemple illustre parfaitement ce dont je veux vous parler lors de cette intervention: je souhaite vous donner une vue d'ensemble des principales formes d'usage abusif d'e-mails ou d'abus commis à l'aide de ceux-ci. Attention: toutes ces formes d'abus existaient déjà avant l'invention du courrier électronique. La nouvelle technologie n'est qu'un nouveau vecteur par le biais duquel ces infractions sont commises.

Voici une liste de ces abus:

– Spam ou junk-mail
– D'autres formes d'abus, telles que le bombardement d'e-mails, des chaînes d'e-mails et le harcèlement ou stalking
– Les messages anonymes
– La mission du département *Abuse* des ISP

Et, pour terminer, une utilisation positive importante, à savoir le *direct marketing* par le biais des e-mails.

1. *Spam*

a) Qu'est-ce qu'un spam? (ongewenste e-mail, courriel non sollicité, unsollicited e-mail)

Chacun d'entre vous a sans doute déjà reçu de tels messages.

Le spamming peut-être défini comme l'envoi de messages non souhaités et non sollicités à de nombreuses adresses électroniques, et ce en une seule fois.

Le contenu peut être de nature simplement commerciale, mais aussi sexuelle ou raciste, ou encore porter sur des actions illégales ou des offres de produits prohibés.

La plus grande partie du coût du spamming est supportée par les providers ou fournisseurs d'accès et les destinataires des messages. Le spammer doit simplement envoyer un seul message à une liste de destinataires; il ne doit cliquer qu'une seule fois. Par contre, le fournisseur d'accès doit acheminer chaque message à plusieurs adresses individuelles différentes, ce qui génère une charge importante pour le système. De son côté, le destinataire doit télécharger un e-mail qu'il n'a pas demandé et paie donc les coûts de connexion y afférents.

b) Comment agit un spammer?

1° Pour pouvoir envoyer un e-mail à une multitude de personnes, le spammer a d'abord besoin d'une liste d'adresses. Il va donc rechercher les adresses élec-

bereiken. Deze kan hij aankopen of zelf maken. Er bestaan verschillende programma's zoals bijvoorbeeld Atomic Harvester, die in staat zijn om een adressenlijst te maken. Deze speciale software werkt als een zoekrobot die adressen zoekt in nieuwsgroepen, webmaillijsten en op het internet. Men kan zelfs ingeven volgens welk thema de zoekrobot adressen moet vinden.

= Dit noemen we de Harvest, of Oogst

In Alexanders geval heeft de spammer dus - ongetwijfeld op een zeer geautomatiseerde wijze – z'n e-mailadres gevonden in de gegevensregistratie van Yahoo. Ik had beter moeten weten en dat adres niet doorgeven.

2° Het verzenden van die ene e-mail naar die massa adressen gebeurt ook door middel van een speciaal programma zoals bijvoorbeeld Desktop Server 2000. Op die manier moet de spammer niet zelf naar elk e-mailadres zijn bericht versturen, maar wordt het onmiddellijk naar de hele lijst verstuurd.

= Dit noemen we Push

3° Aangezien weinig mensen blij zijn spam in hun mailbox te vinden, gebeurt het vaak dat de spammer zijn werkelijke identiteit verbergt. Verder zorgt het er ook voor dat hij moeilijk op te sporen valt.

= Dit noemen we Spamouflage en we zullen verder in dit hoofdstuk zien hoe misbruikers hun e-mailadres anoniem maken !

Straks krijgt u meer uitleg over het juridische luik van dit alles, maar ik wil nu al even wijzen op een juridische uitdaging waar wij allen samen nu voor staan. Het gaat met name over het probleem van de extraterritorialiteit: e-mail is niet gebonden aan grenzen. Met 1 druk op de knop verstuur ik even gemakkelijk een e-mail naar iemand in Oezbekistan als naar mijn buur in Gent. Ook spammers kennen geen grenzen. Daarom kan het voor een spammer interessant zijn om een buitenlands e-mailadres te nemen, met name in de Verenigde Staten van Amerika, om zo buiten het toepassingsveld van de Europese regels en verboden omtrent spam te ontsnappen.

Neem deze drie stappen samen en je hebt de typische actie van een Spammer.

c) Mogelijke oplossingen voor spam

Niemand krijgt graag spam in z'n electronische postbus. Als ik 's ochtends mijn computer opstart en ik zie

troniques du public qu'il veut atteindre. Il peut acheter cette liste ou la créer lui-même. Différents programmes, tels que *Atomic Harvester*, peuvent générer une liste d'adresses. Ce logiciel spécial fonctionne comme un moteur de recherche qui repère des adresses dans des newsgroups ou groupes de discussion, des listes d'adresses et sur internet. Il est même possible de choisir un thème en fonction duquel le moteur doit trouver des adresses.

= c'est ce que nous appelons la Harvest ou Moisson

Le spammer a donc trouvé – probablement de manière automatisée – l'adresse électronique d'Alexander dans la base de données de Yahoo. J'aurais mieux fait de le savoir et ne pas communiquer cette adresse.

2° L'envoi de cet e-mail à cette multitude d'adresses est également effectué au moyen d'un programme spécial tel que, par exemple, *Desktop Server 2000*. De cette manière, le spammer ne doit pas envoyer son message à chaque adresse; l'e-mail est immédiatement envoyé à toute la liste.

= c'est ce que nous appelons le Push

3° Étant donné que peu de personnes sont ravies de trouver des spams dans leur boîte aux lettres, le spammer cache souvent sa véritable identité. En outre, il veille à ce qu'il soit difficile de retrouver sa piste.

= c'est ce que nous appelons le spamouflage. Nous verrons plus loin comment les personnes qui commettent des abus peuvent rendre leur adresse électronique anonyme!

Je fournirai tout à l'heure davantage d'informations sur l'aspect juridique de ce phénomène, mais je voudrais dès à présent souligner le défi juridique devant lequel nous nous trouvons. Il s'agit notamment du problème de l'extraterritorialité: les e-mails ne s'arrêtent pas aux frontières. En un clic de souris, j'envoie tout aussi facilement un e-mail en Ouzbékistan que dans mon quartier à Gand. Les spammers ignorent tout autant les frontières. C'est pourquoi il peut être intéressant pour eux de prendre une adresse à l'étranger, en l'occurrence aux USA, afin d'échapper aux règles et interdictions européennes relatives au spamming.

Additionnez ces trois étapes et vous obtenez l'action typique d'un spammer.

c) Solutions possibles au spamming

Personne ne reçoit avec plaisir des spams dans sa boîte aux lettres électronique. Je n'aime pas, lorsque

dat ik 70 nieuwe berichten heb, waarvan 30 spamberichten zijn die mij niet interesseren, dan vind ik dat niet leuk. Het kost mij tijd en verbindingskosten om ze te ontvangen, en dan moet ik ze nog gaan uitwissen ook. Gelukkig zijn er een aantal manieren om spam de toegang tot uw computer te ontzeggen.

– Soms kan u zich laten verwijderen uit de adressenlijst van de spammer.

Wanneer het bericht van de spammer een mailadres bevat om zich te laten uitschrijven, en u daarop antwoordt, dan wordt u automatisch door zijn computer van de lijst verwijderd.

Het gebeurt echter niet altijd dat men deze mogelijkheid heeft, aangezien anders bijna alle bestemmelingen zich dan zouden laten uitschrijven. Meestal zijn het alleen de serieuze bedrijven die deze regel volgen. Een tweede probleem is dat de spammers niet altijd hun werkelijke identiteit gebruiken, waardoor de mail die je zendt hen ook niet zal bereiken.

– Spam tegenhouden via e-mailprogramma:

De meeste e-mailprogramma's en de e-mail servers (SMTP) van bedrijven bevatten een spam filter of blocker. Deze laten toe het adres van de ontvangen spam in de filter te plaatsen waardoor je geen spam van die afzender meer kan ontvangen. Dit betekent dus wel dat je eerst een spam bericht moet ontvangen en dat je ook nog de moeite neemt om dat adres in je filter te plaatsen. Spammers veranderen echter vaak van adres, precies om dit te vermijden.

– Uw ISP kan bepaalde spam blokkeren:

ISP's kunnen via hun router opdracht geven om e-mail van bepaalde adressen te blokkeren zodat deze niet in het netwerk komen. Deze tussenkomst kan echter beschouwd worden als een inbreuk op de privacy van de gebruiker.

– Spammers op een Blacklist plaatsen:

Een blacklist is een lijst waarop spammers gezet worden en kan gebruikt worden door de ISP's of de individuele gebruiker om filters op de mail te plaatsen. Op deze lijst worden de IP-adressen van de spammers die je wil blokkeren vermeld. Dit heeft dus effect, maar we hebben daarstraks reeds gezien dat een echte professionele spammer vaak verandert van IP-adres of zijn mail zelfs omleidt via andere gebruikers hun adres, zodat men het gevaar loopt de verkeerde persoon op de lijst te plaatsen.

– Wetten die spam reguleren of verbieden:

De huidige wetgeving, meer bepaald de Wet handelspraktijken van 14 juli 1991, verbiedt SPAM maar laat

j'allume mon ordinateur le matin, constater que 30 des 70 nouveaux messages que j'ai reçus sont des spams qui ne m'intéressent pas. Cela me coûte du temps et de l'argent de recevoir ces messages. Et je dois encore les effacer. Heureusement, il existe plusieurs manières d'interdire l'accès de votre ordinateur aux spams.

– Parfois, vous pouvez vous effacer de la liste d'adresses du spammer.

Lorsque le message du spammer contient une adresse électronique permettant de vous désinscrire et que vous y envoyez une réponse, son ordinateur vous supprime automatiquement de la liste.

Cette possibilité n'existe toutefois pas toujours car, dans ce cas, presque tous les destinataires se désinscriraient. La plupart du temps, seules les sociétés sérieuses suivent cette règle. Un deuxième problème est que les spammers n'utilisent pas toujours leur véritable identité et, de ce fait, le message que vous envoyez n'arrive jamais chez eux.

– Faire barrage aux spams grâce aux logiciels de courrier électronique:

La plupart des logiciels de courrier électronique et les serveurs d'e-mails (SMTP) d'entreprises possèdent un filtre ou un bloqueur de spams. Il suffit de placer l'adresse du spam reçu dans le filtre pour ne plus recevoir de spams de cet expéditeur. Cela signifie donc que vous devez d'abord recevoir un spam et ensuite prendre encore la peine de placer l'adresse dans votre filtre. Les spammers changent cependant souvent d'adresse, justement afin d'éviter les filtres.

– Votre ISP peut bloquer certains spams:

Par le biais de leur routeur, les ISP peuvent bloquer les e-mails provenant de certaines adresses de manière à ce qu'ils ne pénètrent plus sur le réseau. Cette intervention peut toutefois être considérée comme une violation de la vie privée de l'utilisateur.

– Placer les spammers sur une liste noire:

Une liste noire est une liste sur laquelle sont placés les spammers. Elle peut être utilisée par les ISP ou les utilisateurs individuels afin de mettre en place des filtres d'e-mails. Les adresses IP des spammers que vous voulez bloquer figurent sur cette liste. Cette méthode est donc assez efficace mais nous avons déjà vu qu'un spammer professionnel change souvent son adresse IP ou dévie ses messages par l'adresse d'autres utilisateurs, de telle sorte qu'on court le risque de placer la mauvaise personne sur la liste.

– Des lois qui régulent ou interdisent le spamming:

La législation actuelle, et plus précisément la loi sur les pratiques du commerce du 14 juillet 1991, interdit

terecht wel ongevraagde reclame toe via art. 23, 5°, op voorwaarde dat deze door de afnemer duidelijk en ondubbelzinnig als zodanig herkenbaar is. Bovendien moeten de naam en de adresgegevens van de verkoper duidelijk in de mail vermeld worden op basis van art.23, 3° (het verbod op reclame die misleidt omtrent de identiteit van de verkoper).

Hieruit volgt m.i. de verplichting dat de header een duidelijke identificatie moet bevatten.

– U kan zelf preventieve maatregelen nemen:

Let op waar je het e-mail adres plaatst en aan wie je het geeft. Wanneer je naar nieuwsgroepen mailt, kan je ervoor zorgen dat je e-mailadres niet wordt meegezonden door het afzender-gedeelte van je e-mail adres te bewerken. Verder kan je de webmaillijsten verwittigen dat je niet langer in hun lijst wil staan, op die manier kunnen zoekrobots je er niet meer in terugvinden. Zoals ik daarstraks reeds zij bij m'n voorbeeld: ik had beter moeten weten en Alexanders adres niet mogen doorgeven, wou ik spam vermijden.

2 *Andere misbruiken van e-mail*

Natuurlijk kan e-mail ook nog voor andere vormen van misbruik aangewend worden. Ik haal nu kort enkele daarvan aan:

– Flooding of mail bombing:

Een e-mail bombardement is het massa's post verzenden naar 1 bepaald persoon, of 1 website om welke beweegreden dan ook (bvb. Wraak, pesterijen,…). Dit is dus precies het tegenovergestelde van spam: hier stuur je een massa berichten naar 1 bestemmeling. Deze vloed aan mail veroorzaakt een overload en kan uiteindelijk de crach van de mailserver veroorzaken.

– Kettingbrieven:

Kettingbrieven bestonden ook reeds lang voor er van e-mail sprake was. Het zijn soms grappige, soms lasterlijke e-mails die rondgestuurd worden en waarin gevraagd wordt deze naar zoveel mogelijk mensen door te zenden. Een bekend voorbeeld is:

–> Haat-propaganda, racisme, en dergelijke bedreigende boodschappen

Deze worden ook veel per e-mail verzonden en dan soms nog als kettingbrieven.

le spamming mais autorise, dans son article 23, 5°, la publicité non sollicitée à la condition que celle-ci soit identifiable comme telle d'une manière claire et non équivoque. En outre, le nom et les coordonnées du vendeur doivent figurer clairement dans le message, conformément à l'article 23, 3° (interdiction de la publicité qui trompe sur l'identité du vendeur).

En découle, selon moi, l'obligation de mentionner, dans l'en-tête, une identification claire.

– Vous pouvez prendre vous-même des mesures préventives:

Soyez attentifs à votre adresse électronique; faites attention aux endroits où vous la placez et à qui vous la communiquez. Lorsque vous envoyez des messages à un groupe de discussion ou newsgroup, vous pouvez veiller à ce que votre adresse ne soit pas transmise en modifiant, dans votre adresse électronique, le champ relatif à l'expéditeur. En outre, vous pouvez signaler que vous ne voulez plus figurer sur la liste en question. De cette manière, les robots de recherche ne peuvent plus vous y retrouver. Comme je l'ai déjà dit, j'aurais mieux fait de le savoir et ne pas communiquer l'adresse d'Alexander. J'aurais ainsi évité les spams.

2 *Autres abus commis au moyen d'e-mails*

Bien entendu, les e-mails peuvent être utilisés pour d'autres formes d'abus. Je vous en détaille brièvement quelques-unes:

– Flooding ou mail bombing:

Un bombardement d'e-mails consiste en l'envoi massif de messages à une personne ou à un site internet, pour quelque motif que ce soit (vengeance, harcèlement,…) Il s'agit donc du contraire du spamming, à savoir l'envoi d'une grande quantité de messages à un seul destinataire. Ce flot provoque une surcharge et peut engendrer le plantage du serveur d'e-mails.

– Les chaînes de lettres:

Les chaînes de lettres existaient bien avant qu'il ne soit question d'e-mails. Il s'agit de messages parfois amusants, parfois injurieux, qui sont envoyés à plusieurs personnes en leur demandant de les transmettre à autant de personnes que possible. Voici un exemple connu:

–> Incitation à la haine, racisme et autres messages de menaces

Nombre d'entre eux sont envoyés par e-mail, et parfois également sous la forme de chaînes de lettres.

–> Stalking (harcelement, harassment)
is het iemand achtervolgen op een obsessieve wijze, en lastig vallen. De manier waarop stalking gebeurt kan verschillende vormen aannemen, zoals via de telefoon, achtervolgen, brieven, maar ook e-mails vormen een mogelijkheid. Dit soort gedrag is strafbaar in België.

– Verspreiding van Illegale inhoud
Illegale content of inhoud, zoals mp3's, links naar illegale sites, illegaal fotomateriaal,... kan ook via e-mails meegezonden worden. Ze staan meestal in attachment en kunnen zo de wereld rond gestuurd worden.

Zoals gezegd: al deze vormen van misbruik bestaan ook in de niet-digitale wereld; informatica en internet zijn slechts een bijkomend instrument waarmee dezelfde misbruikers dezelfde oude misbruiken begaan. ISP's staan in de eerste lijn om hier mee aan te verhelpen; ik zal verder in mijn betoog uitleggen wat de Abuse-afdeling van een ISP doet om misbruiken te bestrijden.

3. *Anonieme e-mail*

Een laatste element van misbruik dat ik vandaag wil aanhalen is de anonieme e-mail. Net zoals een dief geen sporen wil nalaten, is het voor de afzender van een misbruik-mail belangrijk om zijn identiteit geheim te houden. Daartoe heeft hij enkele mogelijkheden:

– De misbruiker kan geen of een fout e-mailadres als afzender ingeven. Dit kan zoals de vorige spreker reeds uitlegde zeer eenvoudig in elk e-mail programma. Deze methode is echter zeer makkelijk doorprikbaar, omdat de misbruiker in zo'n geval nog steeds geïdentificeerd kan worden aan de hand van het IP-adres dat met de header verzonden wordt. Onze abuse-afdeling krijgt regelmatig het verzoek van de overheden om de gebruiker achter een bepaald IP- adres te identificeren. Dit is dus een oplossing voor amateurs; de «echten» gaan veel verder:

– Via programma's zoals Anonymizer is het echt mogelijk om anoniem toegang te krijgen tot het web, dit kan volledig legitiem gebruikt worden om privacyredenen (bv als je wil dat spammers je adres niet te weten komen), maar wordt ook gebruikt om misbruik te maken en bijvoorbeeld spam te verzenden.

–> Stalking (harcèlement, harassment)
Il s'agit de poursuivre une personne de manière obsessionnelle, et de lui rendre la vie impossible. Le harassement peut prendre diverses formes: coups de téléphone, être suivi, des lettres mais aussi des e-mails. En Belgique, ce genre de comportement est punissable.

– Diffusion de contenus illégaux
Des contenu illégaux, tels que des MP3, des liens vers des sites illégaux, des photos illégales,... peuvent aussi être transmis par e-mail. La plupart du temps, ils sont attachés à un message et peuvent ainsi être envoyés à travers le monde.

Comme je l'ai déjà dit, toutes ces formes d'abus existent aussi dans le "monde non digital"; l'informatique et internet ne sont que des instruments complémentaires grâce auxquels les mêmes personnes peuvent commettre les mêmes vieux abus. Les ISP sont en première ligne pour trouver une solution; j'expliquerai plus tard ce que fait le département *Abuse* d'un ISP pour combattre les abus.

3. *Courrier électronique anonyme*

Le courrier électronique anonyme constitue une dernière forme d'abus que je tiens à évoquer aujourd'hui. Pour l'expéditeur d'un courrier électronique abusif, il importe de garder secrète son identité, à l'instar d'un voleur qui ne veut pas laisser de traces. Il dispose, pour ce faire, de plusieurs possibilités:

L'utilisateur abusif peut ne mentionner aucune adresse électronique ou en renseigner une fausse. Comme l'a déjà expliqué l'intervenant précédent, cela peut se faire aisément dans n'importe quel programme de courrier électronique. Cette méthode est cependant très facile à percer à jour, l'utilisateur abusif pouvant encore, dans un tel cas, être identifié au moyen de l'adresse IP qui est transmise avec l'en-tête. Notre département *Abuse* reçoit régulièrement de la part des autorités des demandes d'identification d'un utilisateur dissimulé sous une adresse IP déterminée.. Cette méthode est donc une solution pour les amateurs. Les "professionnels" vont beaucoup plus loin:

– Des programmes comme Anonymiser permettent vraiment d'accéder au réseau en gardant l'anonymat. Cela peut être fait en toute légitimité, pour des raisons de respect de la vie privée (par exemple pour éviter que les spammers ne puissent connaître votre adresse) mais également dans le but de commettre des abus et, par exemple, d'expédier des spams.

– Men kan zijn e-mail verzenden via een bepaalde server en omleiden via andere e-mailservers waardoor het moeilijk wordt het oorspronkelijke adres van de afzender te achterhalen. Hoe meer e-mailservers er tussendoor aan te pas komen hoe moeilijker het wordt.

4. *The ISP's ABUSE-departments*

Hiermee hebben we min of meer de toer gemaakt van misbruik van e-mail. Ik heb u ook verteld dat de ISP's zelf in de frontlinie staan om tegen dergelijk misbruik te strijden. Elke ernstige ISP heeft daartoe een Abuse-departement; u kan dit vergelijken met een anti-computer-crime-unit. Deze staat ten dienste van onze eigen klanten en van de overheid

a) ISP'S WERKEN SAMEN MET DE OVERHEDEN OM MISBRUIK TE BESTRIJDEN

Door co-regulatie tussen ISPA en de federale overheid via het samenwerkingsprotocol, leveren de ISP's alle mogelijke hulp aan de politiediensten (Federal Computer Crime Unit, federale politie, …) die ons opdracht geven met mandaat van procureur of onderzoeksrechter voor ondermeer opsporing en identificatie (ondermeer d.m.v. IP adressen) van misbruikers. Uiteraard zijn wij verplicht om de wettelijke regels omtrent opsporing strikt te volgen, maar dankzij het samenwerkingsprotokol kunnen wij vooral sneller en soepeler samenwerken met de overheden.

Als ik even vanuit mijn ervaring bij Planet Internet mag spreken, worden vragen van de overheid met de grootste geheimhouding behandeld. Zij bereiken ons op een speciaal daartoe bestemd telefoon- en faxnummer, dat beveiligd is en waartoe enkel de medewerkers van de abuse-afdeling toegang hebben. Andere personeelsleden van Planet Internet hebben geen toegang tot die vragen, zodat het geheim van het onderzoek optimaal verzekerd wordt.

b) ISP'S NEMEN AUTONOOM MAATREGELEN OM MISBRUIK AAN BANDEN TE LEGGEN

Dit is het autoregulatiemodel: Zoals gezegd zijn de ISP's de belangrijkste benadeelden bij misbruik van e-mail: onze systemen worden misbruikt, we krijgen overloads en crashes, enz. Bovendien kunnen onze klanten misbruik-mails ook niet echt waarderen , wat voor ons een reden te meer is om deze te bestrijden. Daarom leggen ISP's zichzelf ook regels op en auto-

– On peut envoyer son courrier électronique via un serveur déterminé en le faisant passer par d'autres serveurs de courrier électronique, ce qui complique la recherche de l'adresse initiale de l'expéditeur. Plus le nombre de serveurs de courrier électronique impliqués est élevé, plus la recherche est difficile.

4. *Les départements Abuse des ISP*

Nous avons ainsi à peu près fait le tour des formes d'abus du courrier électronique. Je vous ai également dit que les ISP eux-mêmes sont les premiers à vouloir lutter contre de tels abus. A cet effet, chaque ISP sérieux dispose d'un département *Abuse*, que l'on peut comparer à une unité de lutte contre le crime informatique, au service de ses propres clients et des autorités.

a) LES ISP COLLABORENT AVEC LES AUTORITES POUR LUTTER CONTRE LES ABUS

Grâce à la co-régulation entre l'ISPA et l'État fédéral, via le protocole de collaboration, les ISP apportent toute l'aide possible aux services de police (Federal Computer Crime Unit, police fédérale,...) qui nous chargent, en vertu d'un mandat du procureur ou du juge d'instruction, entre autres de la recherche et de l'identification d'utilisateurs abusifs(notamment au moyen des adresses IP). Bien entendu, nous sommes obligés de respecter strictement les règles légales concernant les recherches, mais grâce au protocole de collaboration, nous pouvons avant tout travailler de manière plus rapide et plus souple avec les autorités.

Si vous me permettez de me référer à mon expérience chez Planet Internet, je puis vous assurer que les demandes provenant des autorités sont traitées avec la plus grande discrétion. Elles nous arrivent via un numéro de téléphone et de fax spécialement réservé à cet usage, qui est protégé et auquel seuls les collaborateurs du département *Abuse* ont accès. Les autres membres du personnel de Planet Internet n'ont pas accès à ces demandes, ce qui permet de garantir le secret des recherches de manière optimale.

b) LES ISP PRENNENT DES MESURES DE MANIERE AUTONOME POUR COMBATTRE LES ABUS

Voici en quoi consiste le modèle d'autorégulation. Comme cela a été dit, ce sont les ISP qui subissent les principaux préjudices résultant de l'utilisation abusive du courrier électronique: on abuse de nos systèmes, ce qui provoque des surcharges, des plantages, etc. De plus, nos clients n'apprécient pas vraiment les courriers abusifs, ce qui constitue pour nous une rai-

reguleren het gebruik van hun systemen en netwerken. Elke ernstige ISP vraagt haar klanten een Acceptable Use Policy te aanvaarden en na te leven. De Acceptable Use Policy is een soort netiquette en omvat de basis regels voor beleefd en correct e-mail gebruik; zij zijn deel van de overeenkomst tussen de klant en de ISP en vormen op die manier contractueel afdwingbare voorwaarden.

Indien correct opgesteld kunnen ze de ISP helpen om ernstige misbruikers van het netwerk te weren en indien nodig hun abonnement af te sluiten, al is dit laatste een maatregel die pas in uiterste noodzaak en na voorafgaandelijke waarschuwingen genomen wordt.

Gebeurt het vaak dat wij mensen en hun abonnement moeten afsluiten? Nee
Kunnen we het doen op een correcte wijze? Ja
Zijn we er op voorbereid om zoiets snel te doen ? Ja

Zo, hiermee hebben we het hele luik over misbruik gezien. Uiteraard krijgt u door deze opsomming een verkeerd idee: het is niet allemaal kommer en kwel. De mogelijkheden voor misbruik bestaan inderdaad, zoals in elke andere omgeving, maar gelukkig gebeurt het niet vaak.

5. *Direct Marketing E-mail*

E-mail biedt vooral ook zeer interessante en positieve mogelijkheden. Er is er één waar ik het bij wijze van afsluiting van dit hoofdstuk even over wil hebben, en dat is een onderwerp dat tegenwoordig heel wat wetgevende aandacht krijgt, zowel op Europees als op nationaal niveau. Ik heb het over Direct Marketing.

Via e-mail is het mogelijk een organisatie, product of dienst bij verschillende mensen te promoten op een snelle, efficiënte en kost-vriendelijke wijze. Zowel overheden en politieke organisaties, als bedrijven maken hiervan gebruik.

Je kan de beste producten aanbieden, maar als niemand je kent, beteken je ook niets op de markt. Elektronisch adverteren is dan ook de meest betaalbare manier om mensen te bereiken. De kost is vrij laag en men verkrijgt een vrij hoge en snelle respons.

son de plus de les combattre. C'est la raison pour laquelle les ISP s'imposent également des règles, tout en veillant à une autorégulation de l'utilisation de leurs systèmes et réseaux. Chaque ISP sérieux demande à ses clients d'accepter et d'observer des règles d'utilisation acceptables, appelées *Acceptable Use Policy*. L'*Acceptable Use Policy* est une sorte de netiquette et comporte les règles de base pour une utilisation courtoise et correcte du courrier électronique. Ces règles font partie du contrat passé entre le client et l'ISP et constituent, de cette manière, des conditions contractuelles contraignantes.

Lorsqu'elles sont correctement rédigées, ces règles permettent aux ISP de se défendre contre des utilisateurs coupables de graves abus du réseau et, si nécessaire, de clôturer l'abonnement, bien que cette dernière mesure ne soit prise qu'en cas d'absolue nécessité et après avoir adressé des avertissements préalables.

Est-il fréquent de devoir mettre fin à l'abonnement d'utilisateurs? Non.
Pouvons-nous le faire de manière correcte? Oui.
Sommes-nous préparés à le faire rapidement? Oui.

Nous avons ainsi terminé l'examen du volet consacré aux abus. Cela ne doit pas vous donner l'impression qu'il ne s'agit que d'une suite de malheurs. Des abus sont effectivement possibles, comme dans d'autres domaines, mais heureusement, ils sont rares.

5. *Courrier électronique de marketing direct*

Le courrier électronique offre aussi des possibilités très intéressantes et positives. Il en est une dont je voudrais parler brièvement, en guise de conclusion de ce chapitre. Il s'agit du marketing direct qui, actuellement, retient l'attention des législateurs, tant au niveau européen que national.

Via le courrier électronique, il est possible de promouvoir rapidement, efficacement et à un prix favorable, auprès de différentes personnes, une organisation, un produit ou un service. Tant les autorités et les organisations politiques que les entreprises font usage de cette possibilité.

Il ne suffit pas d'offrir les meilleurs produits. Si personne ne vous connaît, vous ne représentez rien sur le marché. Aussi, la publicité électronique est-elle la manière la plus abordable financièrement d'atteindre les gens. Son coût est assez faible et elle suscite assez rapidement un taux de réponse relativement élevé.

Wanneer echter de wetgeving in de verschillende landen niet geüniformiseerd of minstens gelijklopend is, zou dit voor bepaalde landen zeer nadelig kunnen uitvallen, met name voor die landen met de strengste regeling. Wanneer bijvoorbeeld in België direct marketing enkel mogelijk zou zijn nadat de ontvanger expliciet daarom vraagt, en wanneer in andere landen niet op dezelfde manier wordt gewerkt, zou een Belgische organisatie benadeeld zijn tegenover organisaties in andere landen met een meer soepele wetgeving, waar het verzenden bijvoorbeeld wel wettelijk mogelijk is. We hebben eerder reeds het extraterritorialiteitsprobleem aangehaald, en het feit dat internet geen grenzen kent. Men dient dus op te letten dat de Belgische rechtsonderhorige niet gesanctioneerd wordt t.o.v. andere landen.

Grosso modo zijn er twee manieren om er voor te zorgen dat direct marketing geen spam wordt. Deze zijn enerzijds Opt Out en anderzijds Opt In.

– Opt out

Opt out berichten worden naar een door de verzender te kiezen doelgroep verstuurd maar voorzien een specifiek vak waarmee de ontvanger duidelijk kan laten weten dat hij geen reclamemails meer wenst te ontvangen.

Het voordeel van dit soort mails is dat de verzender in staat is om nieuwe contacten te leggen en zijn zaak uit te breiden.

Voor de ontvanger heeft dit het voordeel dat hij of zij zich op simpele wijze kan laten uitschrijven om de reclamemails van de verzender in kwestie niet langer te ontvangen.

Deze praktijk leunt het dichtst aan bij de Belgische wetgeving zoals we die gezien hebben in art. 23 van de Wet Handelspraktijken. Eigenlijk gaat dit systeem nog iets verder dan de wet vereist, door mensen de mogelijkheid te geven zich met 1muisklik uit te schrijven.

– Opt in-maillijsten

Opt in-mailinglijsten werken met een omgekeerd systeem. Zij vereisen dat een bestemmeling zich eerst inschrijft alvorens hij reclamemails kan ontvangen. De gebruiker moet dus nadrukkelijk te kennen geven dat hij mail wenst te ontvangen door zich in te schrijven.

Het nadeel is dat men moeilijk nieuwe contacten kan leggen en uitbreiding van de organisatie moeilijk is: op deze manier kan je immers geen nieuw publiek aanboren en blijf je binnen de beperkte kring van personen die jou reeds kennen.

Ik hoop dat ik u hiermee wat mee duidelijkheid ge-

Cependant, en l'absence d'uniformisation ou, du moins, d'harmonisation des législations des différents pays, la situation pourrait se révéler très désavantageuse pour certains pays, notamment ceux dont la réglementation est la plus stricte. Si en Belgique par exemple, à la différence d'autres pays, le marketing direct ne devait être possible qu'à la demande explicite du destinataire, une organisation belge serait désavantagée par rapport à celles des autres pays dont la législation, plus souple, autoriserait l'expédition de tels messages. Nous avons déjà évoqué le problème de l'extraterritorialité et le fait qu'internet ignore les frontières. Il convient donc de veiller à ce que le justiciable belge ne soit pas pénalisé par rapport à d'autres pays.

Sans entrer dans le détail, il existe deux manières de veiller à ce que le marketing direct ne se transforme pas en spamming. Il s'agit, d'une part, de l'Opt out et, d'autre part, de l'Opt in.

Opt out

Les messages Opt out sont envoyés à un groupe cible choisi par l'expéditeur, mais comportent une case spécifique, permettant au destinataire de faire savoir clairement qu'il ne souhaite plus recevoir de courriers publicitaires.

L'avantage de ce type de messages est que l'expéditeur est en mesure d'établir de nouveaux contacts et d'étendre ses affaires.

Pour le destinataire, l'avantage est de pouvoir se faire rayer aisément de la liste afin de ne plus recevoir les courriers publicitaires de l'expéditeur en question.

Cette pratique se rapproche le plus de la législation belge telle qu'elle figure dans l'article 23 de la loi sur les pratiques commerciales. À vrai dire, ce système va encore plus loin que ne l'exige la loi, en offrant aux personnes la possibilité de se faire rayer au moyen d'un simple clic de souris.

Listes de courrier Opt in.

Ces listes fonctionnent selon un système inverse. Elles exigent que le destinataire s'inscrive d'abord avant de recevoir des courriers publicitaires. L'utilisateur doit donc faire savoir expressément, en s'inscrivant, qu'il souhaite recevoir du courrier.

L'inconvénient est qu'il est difficile d'établir de nouveaux contacts et de développer l'organisation. En effet, cette manière de procéder ne vous permet pas de vous adresser à un public nouveau et vous confine à l'intérieur du cercle restreint des personnes qui vous connaissent déjà.

J'espère que cet exposé aura permis de mettre clai-

geven heb over enkele voor- en nadelen van e-mail, en hoe daar oplossingen voor te vinden. Indien er nog vragen zijn, zal ik nu graag proberen om daarop te antwoorden.

Ik dank u voor uw aandacht.

De heer Peter Vanhoutte, voorzitter: Dank u wel, mijnheer van Nunen. Ik wil u graag nog welgemeend gelukwensen met de geboorte van uw kind. Aangezien hij al gebruik maakt van het Internet, is hij een nieuwe wereldburger.

Ik apprecieer het dat u toch nog de tijd hebt gevonden om die boeiende toespraak voor te bereiden. Ik wil meteen het woord geven aan de zaal. Heeft iemand uit de zaal nog vragen?

Mevrouw Erika Thijs, senatrice (CD&V): Mijnheer van Nunen, de laatste tijd wordt er veel gesproken over universele dienstverlening door de overheidsbedrijven zoals De Post en de NMBS. Zonet zei u dat iedereen zomaar een e-mailadres kan aanmaken. Wij zijn echter op weg naar e-governement. Is het mogelijk om mensen te verhinderen op het Internet te komen?

D**e heer Carlos van Nunen**: Mevrouw Thijs, uw opmerking is terecht. In de huidige fase wordt naar regulering gezocht. Tot nu toe wordt, bijvoorbeeld voor onze Internet Service Provider, alleen op contractuele basis gewerkt. Bij grove en flagrante misbruiken kan de Internet Service Provider tussenbeide komen, maar alleen als die misbruiken herhaaldelijk gebeuren. Ik heb van nog maar minder dan tien gevallen gehoord die op die manier van het Internet zijn geweerd. De mogelijkheid bestaat dus wel, want misbruiken vormen vooral een zware last voor andere gebruikers.

Het feit dat één Internet Service Provider iemand zou uitsluiten, betekent uiteraard niet dat die persoon niet de mogelijkheid heeft om bij andere Internet Service Providers aan te sluiten.

De heer Vincent Van Quickenborne, senator (VU&ID): Mijnheer van Nunen, ook politici maken vaak gebruik van e-mail. Bij verkiezingen gaan politici veel vaker de weg van het elektronische verkeer op, zodat zij niet meer de straat op moeten of pensenkermissen moeten organiseren. Door e-mail komen zij meteen in de huiskamers. Daarover heb ik de volgende vragen.

Ten eerste, kan tijdens de verkiezingsperiode de reclame voor campagne of een programma als spam worden gedefinieerd? Wat heeft dat voor gevolg?

rement en évidence quelques avantages et inconvénients du courrier électronique et de contribuer à la recherche de solutions. Je répondrai volontiers aux questions que vous souhaiteriez me poser.

Je vous remercie de votre attention.

M. Peter Vanhoutte, président.- Nous vous remercions, monsieur van Nunen. Je voudrais vous féliciter de tout cœur pour la naissance de votre enfant. Étant donné qu'il fait déjà usage d'internet, il sera un citoyen du monde.

J'apprécie que vous ayez toutefois trouvé le temps de préparer cette intervention captivante. Je donne à présent la parole à l'assemblée. Y a-t-il encore des questions ?

Mme Erika Thijs, sénatrice (CD&V).- Monsieur van Nunen, ces derniers temps, on parle beaucoup du service universel des services publics comme La Poste et la SNCB. Vous venez de dire à l'instant que tout le monde peut créer une adresse e-mail. Nous sommes en train de mettre au point l'administration électronique. Est-il possible d'empêcher que des personnes aient accès à internet ?

M. Carlos van Nunen.- Madame Thijs, votre remarque est pertinente. Dans la phase actuelle, on cherche une régulation. Jusqu'à présent, comme par exemple pour notre Internet Service Provider, on travaille uniquement sur une base contractuelle. En cas d'abus grossiers et flagrants, l'Internet Service Provider peut intervenir, mais uniquement si ces abus se produisent fréquemment. À ma connaissance, il y aurait eu moins de dix cas. La possibilité existe donc, car les abus embarrassent considérablement et principalement les autres utilisateurs.

Le fait qu'un Internet Service Provider exclue quelqu'un ne signifie pas, bien entendu, que cette personne n'a pas la possibilité de se raccorder à un autre Internet Service Provider.

M. Vincent Van Quickenborne, sénateur (VU&ID).- Monsieur van Nunen, les hommes et les femmes politiques utilisent aussi souvent les e-mails. Lors des élections, les politiciens empruntent beaucoup plus souvent la voie électronique, de telle sorte qu'ils ne doivent plus circuler en rue ni organiser des kermesses aux boudins. Grâce aux e-mails, ils arrivent instantanément dans les foyers. Sur ce point, j'aimerais vous poser les questions suivantes.

Premièrement, pendant les périodes électorales, la publicité pour une campagne ou un programme peut-elle être définie comme un spam ? Quelle en est la conséquence ?

Ten tweede, politici kunnen ook een database bijhouden van e-mailadressen van mensen die hen hebben aangeschreven of gecontacteerd. Zij zouden die adressen kunnen gebruiken voor de verkiezingen of voor andere gelegenheden. Valt dat gebruik onder de genoemde wet van 1991? Moeten de politici daarvan een aparte lijst maken? Moeten de mensen ervan worden ingelicht dat zij met hun e-mailadres in de database van die politici zijn opgenomen?

Deuxièmement, les hommes politiques peuvent aussi tenir une base de données reprenant les adresses électroniques de personnes qui leur ont écrit ou les ont contactés. Ils pourraient utiliser ces adresses pour les élections ou pour d'autres occasions. Cet usage tombe-t-il sous l'application de la loi précitée de 1991 ? Les hommes politiques doivent-ils faire une liste séparée de ces adresses ? Les gens doivent-ils être informés du fait que leur adresse électronique est reprise dans les bases de données de ces hommes politiques ?

De heer Carlos van Nunen: Mijnheer Van Quickenborne, uw tweede vraag is een juridische vraag over het feit of de wet op de privacy van toepassing is. Die hete aardappel zou ik graag naar één van mijn twee collega's doorschuiven.

In het algemeen en in antwoord op uw eerste vraag kan ik het volgende zeggen. Over dat onderwerp wordt momenteel gedebatteerd. De huidige definitie van spam is ook voor mij op dit moment een open vraag. Enkele elementen van spam zijn wel duidelijk: het gaat om een repetitief, ongevraagd en bovendien ongewenst aspect. Voldoet dat om uw reclame of promotie als spam te catalogeren? De toekomst en vooral uw wetgevend werk zal dat moeten uitwijzen.

M. Carlos van Nunen.- Monsieur Van Quickenborne, votre deuxième question est une question juridique portant sur le fait de savoir si la loi relative à la protection de la vie privée est d'application. J'aimerais qu'un de mes deux collègues réponde à cette question brûlante.

De manière générale et pour répondre à votre première question, je puis vous dire ceci. Ce sujet fait actuellement l'objet d'un débat. En ce moment, la définition actuelle du spam est pour moi aussi une question ouverte. Quelques éléments sont clairs : il y a un aspect répétitif, non sollicité et, en outre, non désiré. Cela suffit-il pour cataloguer de spam votre publicité ou votre promotion ? L'avenir et, surtout, votre travail législatif devront le démontrer.

De heer P. Thomas, Voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer:

Als antwoord op een vraag die zonet gesteld werd door senator Van Quickenborne onderstreep ik dat de wet tot bescherming van de persoonlijke levenssfeer zonder enige twijfel toepasselijk is op bestanden met en op de verwerking van persoonsnamen uit e-mails die een parlementslid op kantoor ontvangt of verstuurt. De wetgever heeft voor zichzelf geen uitzondering willen maken. Dat betekent dat de geregistreerde personen moeten weten dat ze geregistreerd worden en waarom. Ze moeten zich er ook tegen kunnen verzetten dat ze in een bestand worden opgenomen, als ze daar gegronde redenen toe hebben. Als het de bedoeling is de gegevens te gebruiken voor politieke of electorale propaganda, hoeft wie bezwaar maakt zelfs geen reden op te geven tot staving van zijn bezwaar.

M. P. Thomas, président de la Commission pour la Protection de la Vie Privée :

En réponse à une question posée il y a quelques instants par M. le Sénateur Van Quickenborne, je tiens à dire que, sans aucun doute, la loi sur la protection de la vie privée est d'application aux fichiers et traitements de noms de personnes à partir des E-mails entrant ou sortant d'un bureau du parlementaire. Le législateur n'a pas voulu faire d'exception à son propre égard. Cela signifie que les personnes ainsi fichées doivent le savoir et savoir dans quel but. Elles doivent également pouvoir s'opposer à figurer dans ce fichier si elles ont une raison sérieuse pour ce faire. Si le but est de faire de la propagande politique ou électorale, l'opposant ne doit même invoquer aucune raison.

De heer Wim Verreycken, senator (VB): Mijnheer van Nunen, ik heb een technische vraag. U verwijst naar de letter van de etiquette die het mogelijk maakt

M. Wim Verreycken, sénateur (VB).- Monsieur van Nunen, j'aimerais vous poser une question technique. Vous faites référence à la « netiquette » grâce à la-

zich uit te schrijven van de toezending van spam, direct mail of verkiezingspropaganda. Mijn ervaring daarmee is echter de volgende. Veel van die remove-berichten komen gewoon in de mailbox terug. Daardoor heeft de ontvanger dubbel werk. Enerzijds ontstaat op die manier een lus, waarnaar u al verwezen hebt. Anderzijds raakt de mailbox op die manier ook vol, en daarover gaat mijn vraag.

Ik krijg vaak het signaal van een volle mailbox. Ik neem aan dat er een bepaalde systematiek voor is, maar volgens mij is de provider daarvoor verantwoordelijk. Bestaat er een mogelijkheid om een mailbox te vergroten, uiteraard op kosten van de aanbieder van de spam, zelfs als de gebruiker gewild een erg kleine mailbox houdt om weinig remove-berichten te ontvangen? Kan de provider de vergroting van de mailbox aan zijn klant aanrekenen omdat hij teveel remove-berichten krijgt?

De heer Carlos van Nunen: Mijnheer Verreycken, uw opmerking is terecht en correct. Over spam wil ik ten eerste het volgende zeggen. Het is de bedoeling van de spammer dat hij u spam kan blijven toesturen. Een spammer heeft er lak aan of u zich daarvan al dan niet wilt uitschrijven. In het beste geval en voor de goede vorm staat er misschien ergens: «Klik hier om u uit te schrijven.» Bij echte spam werkt dat echter niet. Er wordt gewoon geen gevolg aan gegeven of de spammer werkt met een volle mailbox.

Ten tweede, een Internet Service Provider kan uw mailbox wel degelijk vergroten als hij dat wenst. Daarvoor moet ik opnieuw verwijzen naar de contractuele relatie tussen de klant en de Internet Service Provider. In bepaalde gevallen bestaat de mogelijkheid om een mailbox die overloopt, te vergroten. Eigenlijk kan dat niet zomaar eenzijdig als dat aan de klant zou worden aangerekend. Ik ben het met u eens dat de Internet Service Provider daarvoor een bepaalde verantwoordelijkheid draagt. Daarvoor dienen onze abuse-afdelingen.

Sta me toe een concreet voorbeeld te geven. De Internet Service Provider die tussenbeide kan komen, is die waar de spammer een account heeft, dus niet om het even welke Internet Service Provider kan daarvoor worden aangesproken. Veronderstel dat bij ons een spammer zit, waarover wij van gebruikers en van collega-Internet Service Providers veel reacties krijgen. Wij zouden die persoon kunnen contacteren en duidelijk maken dat er een probleem zit. Wij kunnen laten weten dat de spammer de contractuele grenzen

quelle il est possible de se désabonner de l'envoi de spams, de mails directs ou de propagande électorale. Toutefois, mon expérience est la suivante. Beaucoup de ces messages reviennent tout simplement dans la boîte aux lettres électronique. De ce fait, celui qui les reçoit a un double travail. Il y a d'une part la boucle à laquelle vous avez fait référence. D'autre part, la boîte de réception est pleine, et ma question porte sur ce point.

Je reçois souvent le signal indiquant que ma boîte de réception est pleine. J'imagine qu'il y a une systématique particulière pour ce problème mais, selon moi, le provider en est responsable. Est-il possible d'agrandir une boîte de réception, bien entendu aux frais du présentateur du spam, même si l'utilisateur conserve délibérément une très petite boîte de réception afin de limiter les spams ? Le provider peut-il facturer au client l'agrandissement de sa boîte de réception parce qu'il reçoit trop de spams ?

M. Carlos van Nunen.- Monsieur Verreycken, votre remarque est justifiée et correcte. Je dirai tout d'abord ceci en ce qui concerne le spam. Le but du spammer est de pouvoir continuer à vous envoyer un spam. Cela ne l'intéresse pas de savoir si vous voulez ou non le recevoir. Dans le meilleur des cas et pour la bonne forme, il peut être inscrit : « Cliquez ici pour ne plus recevoir de message. » Mais pour le vrai spam, cela ne marche pas. On n'en tient tout simplement pas compte ou le spammer envoie le spam à une boîte de réception pleine.

Deuxièmement, un Internet Service Provider peut agrandir sérieusement votre boîte de réception s'il le souhaite. À cet égard, je dois à nouveau renvoyer à la relation contractuelle entre le client et l'Internet Service Provider. Dans certains cas, il est possible d'agrandir une boîte de réception qui est pleine. À vrai dire, cela ne peut se faire unilatéralement si cette opération est facturée au client. Je suis d'accord avec vous quand vous dites que l'Internet Service Provider a une certaine responsabilité à ce sujet. C'est à cela que servent nos départements traitant les abus.

Permettez-moi de donner un exemple concret. L'Internet Service Provider qui peut intervenir est celui où le spammer a un compte ; on ne peut donc s'adresser à n'importe quel Internet Service Provider à ce sujet. Imaginons que nous ayons un spammer chez nous, à propos duquel nous recevons de nombreuses réactions de la part d'utilisateurs et de collègues Internet Service Providers. Nous pourrions contacter cette personne et lui faire comprendre qu'il y a un problème. Nous pouvons faire savoir que le spammer dépasse les limites

overschrijdt. De spammer moet dan stoppen, zoniet moet de Internet Service Provider verdere acties ondernemen.

De heer Peter VANHOUTTE, voorzitter: Daarmee zou ik de vragenronde graag afronden. Omwille van de beperkte tijd, zou ik graag overgaan naar de volgende spreker, de heer Bart Vansevenant

C. **De veiligheidsaspecten in verband met e-mail: -Uiteenzetting voor de heer Bart Vansevenant, Senior Manager Field Marketing, Ubizen**

Veiligheid en privacy op het Internet en bij e-mail in het bijzonder heeft verscheidene aspecten. Is de afzender van een e-mail wel degelijk de persoon die hij beweert te zijn? Wie kan wat zien? Welke sporen laat men na? Hoe zit het nu met virussen?

We behandelen kort deze verschillende vragen en schetsen ook enkele van de antwoorden.

1. *Wie is wie?*

Het is niet makkelijk om op het Internet na te gaan met wie je communiceert. In de realiteit zien we dat gelijk welke Internet gebruiker een e-mail adres kan aanmaken en daarbij de identiteit kiezen die hij wil.

Een concreet voorbeeld: ik kan naar de Internet site hotmail.com surfen, en daar een e-mail adres Herman_Decroo@hotmail.com aanmaken, en vanaf dan e-mails beginnen versturen in naam van Herman De Croo. De ontvanger van mijn e-mails kan niet controleren wie ik werkelijk ben. We zullen later zien hoe dit identiteitsprobleem opgelost kan worden.

2. *Wie kan wat lezen?*

Laat ons concreet even bekijken wat er met een e-mail gebeurd die over het Internet verstuurd wordt, en daarbij aangeven wie op welk moment wat kan lezen. Nadien volgt bij wijze van voorbeeld een korte uitleg over twee Amerikaanse projecten Echelon en Carnivore.

We starten zoals gezegd met een typische e-mail set-up. Ik typ op mijn PC een e-mail, en ik connecteer mijn computer met mijn Internet leverancier via m'n telefoonlijn. The mail server van mijn Internet leverancier zal mijn bericht verwerken, en over het Internet versturen naar de mailbox van de ontvanger.

contractuelles. Le spammer doit alors cesser, sinon l'Internet Service Provider doit entreprendre d'autres actions.

Monsieur le président, Peter VANHOUTTE.- Je voudrais terminer par cette question. En raison du temps limité, je voudrais en venir à l'intervention suivante, celle de M. Bart Vansevenant.

C. **L'utilisation abusive du courrier électronique : - Exposé de M. Bart Vansevenant, Senior Manager Field Marketing, Ubizen**

La sécurité et la protection de la vie privée sur internet et dans les e-mails en particulier a différents aspects. L'expéditeur d'un e-mail est-il vraiment la personne qu'il prétend être ? Qui peut voir quelque chose ? Quelles traces laisse-t-on ? Où en est-on en matière de virus ?

Nous allons brièvement traiter ces différentes questions et ébaucher quelques-unes des réponses.

1.*Qui est qui ?*

Il n'est pas facile de voir avec qui on communique sur internet. Dans la réalité, nous voyons que n'importe quel utilisateur d'internet peut créer une adresse e-mail et choisir l'identité qu'il veut.

Un exemple concret : je peux surfer sur le site internet hotmail.com, créer une adresse Herman_Decroo@hotmail.com et commencer à envoyer des e-mails au nom d'Herman De Croo. Celui qui reçoit mes e-mails ne peut contrôler qui je suis réellement. Nous verrons plus tard comment ce problème d'identité peut être résolu.

2. *Qui peut lire quoi ?*

Voyons de manière concrète ce qui se passe quand un e-mail est envoyé par internet et qui peut lire quoi et à quel moment. Nous aurons ensuite en guise d'exemple une brève explication de deux projets américains, Echelon et Carnivore.

Comme nous l'avons dit, nous commençons avec le set-up typique d'un e-mail. Je tape un e-mail sur mon PC et je connecte mon ordinateur à mon fournisseur internet par l'intermédiaire de ma ligne téléphonique. Le serveur de mon fournisseur internet va traiter mon message et l'envoyer sur internet vers la boîte de réception du destinataire.

a) Telefoonlijn

E-mails worden verdeeld in pakketjes vooraleer ze via een modem over de telefoonlijn verstuurd worden. Maar gezien deze nog allemaal netjes bij elkaar zitten in de juiste volgorde kunnen ze dus onderschept worden en gereconstrueerd naar het persoonlijke bericht. Dit natuurlijk ingeval men over het nodige materiaal en programmatuur beschikt.

b) Mail server

Popmail veronderstelt dat de e-mails langs een server passeren, zowel om te ontvangen als te verzenden. Het e-mail bericht wordt gedownload naar je lokale computer op het moment dat je je verbindt met de mail server. Meestal kan je daarbij aangeven of je een kopij van de berichten op de mail server wil bewaren. Een hacker kan trachten toegang tot de mail server te krijgen en zodoende e-mails lezen, schrijven of verwijderen.

Bij webmail blijft de mail op de server staan tot je deze zelf verwijdert, zolang je dit dus niet doet kunnen deze op de server door anderen gelezen worden.

c) TCP/IP

E-mails gaan lezen tijdens hun transport is zeer moeilijk aangezien deze door het TCP/IP protocol opgedeeld worden in kleinere pakketten en deze niet allemaal dezelfde route volgen.

d) Echelon en Carnivore

Echelon:

De eerste eigenschap die dit systeem werd toegeschreven, is de mogelijkheid van een nagenoeg totale observering. Hoewel dit vaak in de pers wordt beweerd, is het niet juist dat dit netwerk al het Europese telefoon-, fax-, telex- en internetverkeer (inclusief e-mail) kan afluisteren. Echelon zou vooral de berichten kunnen onderscheppen die via de Intelsat-satellieten worden verstuurd.

Slechts 1 procent van de communicatie verloopt echter via satelliet, de rest gaat vooral via optische fibrekabels.

Als tweede kenmerk van echelon werd erop gewezen dat het systeem door de samenwerking tussen meerdere landen (het Verenigd Koninkrijk, de Verenigde Staten, Canada, Australië en Nieuw-Zeeland) wereldwijd functioneert, waardoor het, vergeleken met nationale systemen, aan belang wint.

a) Ligne téléphonique.

Les e-mails sont divisés en groupes avant d'être envoyés par l'intermédiaire d'un modem sur la ligne téléphonique. Mais étant donné qu'ils sont encore regroupés, précisément dans l'ordre d'arrivée, ils peuvent être interceptés et restitués en message personnel, si on dispose bien entendu du matériel et du software nécessaires.

b) Mail server

Le popmail suppose que les e-mails passent par un serveur, aussi bien pour les recevoir que pour les envoyer. Le message e-mail est téléchargé sur votre ordinateur local au moment où vous vous connectez au serveur. Généralement, vous pouvez préciser si vous souhaitez conserver une copie des messages sur le serveur. Un pirate peut essayer d'avoir accès au serveur et ainsi lire, écrire ou supprimer des e-mails.

Pour les webmails, le mail reste sur le serveur jusqu'à ce que vous le supprimiez vous-même ; tant que vous ne le faites pas, ils peuvent être lus par d'autres personnes sur le serveur.

c) TCP/IP

Lire les e-mails pendant leur transfert est très difficile, étant donné qu'ils sont divisés en plus petits paquets par le protocole TCT/IP et qu'ils ne suivent pas tous le même chemin.

d) Echelon et Carnivore

Echelon:

La première propriété attribuée à ce système est la possibilité d'effectuer une observation à peu près totale. Bien que la presse l'ait souvent affirmé, il est inexact de dire que ce réseau peut écouter tout le trafic téléphonique, de fax, de télex et d'internet (y compris le courrier électronique). Echelon pourrait surtout intercepter les messages envoyés via les satellites Intelsat.

Un pour cent seulement des communications s'effectue par satellite ; le reste passe surtout par des câbles de fibres optiques.

La deuxième caractéristique d'Echelon réside dans le fait que le système fonctionne dans le monde entier grâce à la collaboration de plusieurs pays (le Royaume-Uni, les Etats-Unis, le Canada, l'Australie et la Nouvelle-Zélande), ce qui augmente son importance par comparaison avec les systèmes nationaux.

Carnivore Diagnostic Tool

Carnivore is een internet surveillantie middel van de FBI. Het systeem tapt de internetcommunicatie af ter hoogte van de ISP en maakt een exacte kopie van de data, zonder dat het de werking van de ISP hindert. Het systeem is in staat om niet alleen e-mail surveillantie te doen, maar ook pakketjes te filteren die informatie bevatten over de websites die een gebruiker bezocht heeft en ongeveer welke communicatie er gebeurd is. Uitbreidingen naar andere mogelijkheden voor het systeem zijn in de toekomst steeds mogelijk, zoals telefonie via internet.

De toepassing van de interceptie van communicatie moet steeds gebeuren onder de toelating en beperkingen van het Departement van Justitie. De interceptie is steeds beperkt tot maximum 30 dagen en in het bevel staat ook steeds exact omschreven welke types van communicatie mogen onderschept worden, bv e-mails van of naar een persoon, online shopping, bezoek van websites, …

Wanneer de ISP op zichzelf over de middelen beschikt om te voldoen aan het rechtsbevel, wordt Carnivore niet gebruikt. In de gevallen waar Carnivore wel gebruikt wordt is dit steeds met bijstand van de ISP. Carnivore mag enkel gebruikt worden om dat specifieke segment van het internet verkeer te bekijken dat in het rechtsbevel staat.

3. *Achtergelaten sporen*

Om informatie juist te verzenden van je computer naar een server wordt het TCP/IP protocol gebruikt. Elke computer krijgt een IP-adres toegewezen gedurende een internetsessie, dit IP-adres wordt steeds meegezonden met je e-mail, waardoor je ook steeds identifieerbaar bent. (dit wil zeggen, je computer is identificeerbaar).

Bij je internetprovider worden ook zogenaamde access logs bijgehouden, dit is dus je IP-adres en wanneer je op het net bent gegaan en wanneer je uitgelogd hebt.

Op de SMTP en POP-server worden ook je gegevens bewaard omwille van technische redenen in zogenaamde logs, dit echter slechts voor korte tijd. Maar in principe laat je dus ook daar achterhaalbare sporen achter.

Op http laat je veel meer sporen achter, maar hier bespreken we enkel degene die belangrijk zijn bij web-

Carnivore Diagnostic Tool

Carnivore est un instrument de surveillance internet du FBI. Le système met les communications Internet sur table d'écoute au niveau du FAI et réalise une copie exacte des données, sans interférer dans le fonctionnement de ce dernier. Le système est capable non seulement de surveiller du courrier électronique, mais aussi de filtrer des paquets de données contenant des informations sur les sites internet visités par un utilisateur et d'indiquer quelles communications ont eu lieu. Des extensions de cette surveillance à d'autres moyens de communication sont toujours possibles à l'avenir, comme la téléphonie via internet.

L'interception de communications doit toujours s'effectuer avec l'autorisation du département de la Justice et dans les limites fixées par celui-ci. L'interception est toujours limitée à 30 jours maximum et l'autorisation contient toujours la description exacte du type de communications pouvant être interceptées, par exemple du courrier électronique provenant ou à destination d'une personne, des achats en ligne, des visites de sites internet…

Lorsque le FAI dispose lui-même des moyens d'accomplir le mandat, Carnivore n'est pas utilisé. Dans les cas où il est effectivement utilisé, c'est toujours avec l'assistance du FAI. Carnivore ne peut être utilisé que pour la surveillance de la partie du trafic internet spécifiée dans le mandat.

3. *Traces laissées*

Pour simplement envoyer des informations d'un ordinateur vers un serveur, on utilise le protocole TCP/IP. Chaque ordinateur reçoit une adresse numérique IP attribuée lors d'une session internet. Cette adresse IP est toujours envoyée avec le courrier électronique, de telle façon que l'utilisateur est toujours identifiable. (C'est-à-dire que l'ordinateur est identifiable).

Des historiques des liaisons sont également conservés chez le fournisseur d'accès, contenant l'adresse IP de l'utilisateur, le moment où il s'est connecté à internet et celui où il s'est déconnecté.

Les données de l'utilisateur sont également conservées dans des historiques sur les serveurs SMTP et POP pour des raisons techniques, mais seulement pour une courte période. En principe, il laisse là aussi des traces identifiables.

Sur http, on laisse beaucoup de traces, mais nous ne parlerons ici que de celles qui sont importantes pour

mail. Wanneer je een webpagina opent wordt de log daarvan bewaard bij je eigen internetprovider. Hij kan dus zien welke site je bezocht, niet wat de inhoud ervan was. Ook je login bij je webmail wordt door de webserver bewaard.

4. *Virussen*

Hier zullen wij dan bekijken wat zijn virussen? Welke soorten bestaan er vandaag want er worden dagelijks nieuwe virussen ontdekt)? Wat kan het zoal op uw computer veroorzaken? Welke gevaren gaan ermee gepaard?

a) Wat is een virus?

Een computervirus is een programma dat zichzelf verbergt in een programma of bestand, zoals in een attachment van een e-mail. Het vermenigvuldigt zichzelf, waarbij het andere programma's of het operating systeem kan infecteren en gaan aantasten. Het virus wordt pas geactiveerd wanneer het geïnfecteerde programma of bestand wordt uitgevoerd.

Virussen vind je in vele varianten. Een categorie van virussen zijn de zogenaamde computerwormen. Een computerworm is een zelfstandig programma (of geheel van programma's) dat in staat is om functionele kopieën van zichzelf of van zijn segmenten te verspreiden op het eigen systeem maar ook naar andere computersystemen (gewoonlijk via netwerkverbindingen). Een voorbeeld dat de voorbije zomer de pers haalde was het zogenaamde Code Red wormvirus dat zichzelf automatisch verspreidde over het Internet.

Een «paard van Troje» is een andere virusvariant. Een «paard van Troje» is een programma dat wordt verborgen in een ander programma of bestand dat de gebruiker interessant of nuttig vindt, maar die iets heel anders zal gaan doen dan wat de gebruiker verwacht. Iemand die een «Trojaans paard» uitstuurt naar een andere gebruiker heeft meestal de bedoeling om via het trojaans paard via het Internet binnen te komen op de computer van de andere gebruiker en er de controle van over te nemen. Een «Trojaans paard» wordt pas geactiveerd wanneer het programma of bestand geopend wordt, en is niet in staat om zichzelf te kopiëren of te verspreiden.

Een «Logic bomb» is dan weer een kwaadaardig programma dat door een bepaalde set van omstandigheden afgaat, iets dat gebeurt of juist niet gebeurt. Net zoals Trojaanse paarden is ook de «Logic bomb» een

le courrier électronique. Lorsqu'un utilisateur ouvre une page internet, la trace est conservée auprès de son fournisseur d'accès. Ce dernier peut donc voir quel site a été visité, mais pas le contenu de celui-ci. Le mot de passe du courrier électronique est également conservé par le fournisseur d'accès.

4. *Virus*

Nous allons examiner ce que sont les virus, les différentes variétés existant aujourd'hui (car chaque jour on découvre de nouveaux virus), l'influence qu'ils peuvent avoir sur votre ordinateur et les dangers qui y sont associés.

a) Qu'est-ce qu'un virus ?

Un virus d'ordinateur est un programme qui se dissimule lui-même dans un programme ou un fichier, comme dans la pièce jointe à un courrier électronique. Il se multiplie lui-même, de sorte qu'il peut infecter et atteindre d'autres programmes ou le système interne de l'ordinateur. Le virus n'est activé que quand le programme ou le fichier infecté est en fonctionnement.

Il y a beaucoup de variantes de virus. Une catégorie de virus est constituée par ce que l'on appelle les « vers » d'ordinateur. Un « ver » est un programme indépendant (ou un ensemble de programmes) capable de propager des copies fonctionnelles de lui-même dans l'ordinateur où il se trouve ou vers d'autres ordinateurs (généralement via des connexions internet). Un exemple repris dans la presse l'été dernier est le virus appelé Code Red qui s'est automatiquement propagé sur internet.

Le « cheval de Troie » est une autre variante de virus. Il s'agit d'un programme caché dans un autre programme ou fichier que l'utilisateur trouve intéressant ou utile, mais qui va faire tout autre chose que ce qu'attend l'utilisateur. Quelqu'un qui envoie un cheval de Troie à un autre utilisateur a souvent l'intention d'entrer via internet dans l'ordinateur de ce dernier et d'en prendre le contrôle.

Un cheval de Troie n'est activé que lorsque le programme ou le fichier qui le contient est ouvert et n'est pas capable de se copier ou de se propager lui-même.

La « bombe logique » est un programme pernicieux, déclenché par un certain concours de circonstances, quelque chose qui se passe ou ne se passe pas. Comme le cheval de Troie, la bombe logique est également un

programma dat als virus beschouwd wordt, het repliceert zichzelf niet, maar kan wel geprogrammeerd zijn in een virus of trojaans paard. Een logic bomb is iets wat vaak gebruikt wordt uit wraak door ontevreden (ex-)werknemers en viseert meestal enkel het systeem van het bedrijf.

Een hoax (vals alarm) tot slot is een waarschuwing voor een onbestaand, uiterst vernietigend stukje»malware». Hoax-waarschuwingen worden normaal verspreid als kettingbrieven die u vragen om die waarschuwing te versturen naar iedereen die u kent. Wettige waarschuwingen worden niet als kettingbrief verspreid en bevatten altijd links naar de website van de auteur, waar aanvullende informatie te vinden is. Een zeer gekende is de waarschuwing om het bestand Sulfnbk in windows/command directory te verwijderen. Dit is echter een essentieel bestand om uw computer correct te laten werken en de verwijdering richt ernstige schade aan.

b) Hoe wordt je computer geïnfecteerd ?
Virussen krijg je via geinfecteerde computers.

De meest voorkomende manier om een virus te krijgen is via bestanden die men bij een e-mail voegt, de zogenaamde attachments. De e-mail tekst zelf kan nooit een virus bevatten of verspreiden.

Naast attachments vormt ook het uitwisselen van diskettes een bron van virusverspreiding.

c) Welk gevaar vormen ze?
Virussen infecteren afhankelijk van hun programmatie bepaalde onderdelen van je systeem, gaande van gewoon infecteren tot het volledig uitwissen van sommige zaken. Virussen kunnen diverse symptomen vertonen die de goede werking van je systeem verstoren (frequente systeemcrash, onverklaarbare vergroting van bestandsgrootte, vertraging van het hele systeem, vreemde en ongewone berichten die te pas en onpas op het scherm verschijnen, moeilijkheden bij toegang tot data, vreemd gedrag van programma's). Ze verschillen dus niet echt zoveel van het gewone slecht functioneren van een systeem.

Virussen kunnen nooit de hardware van een computer beschadigen aangezien hardware niet kan beschadigd worden door software en een virus is software.

programme qui est considéré comme un virus. Il ne se diffuse pas lui-même, mais peut être programmé dans un virus ou un cheval de Troie. La bombe logique est souvent utilisée comme vengeance par des personnes insatisfaites (par exemple d'anciens employés) et ne vise le plus souvent que le système de l'entreprise.

Enfin, une hoax (fausse alerte) est un avertissement concernant un élément soi-disant très destructeur, mais en réalité inexistant. Les avertissements hoax sont normalement propagés comme les lettres en chaîne qui demandent à l'utilisateur d'envoyer ces avertissements à tous ceux qu'il connaît. Les véritables avertissements ne sont pas diffusés comme des lettres en chaîne et contiennent toujours des liens vers le site internet de l'auteur, où l'on peut trouver des informations complémentaires. Un avertissement très connu est celui qui vise à éliminer le fichier Sulfnbk dans windows/command directory. C'est un fichier essentiel qui permet à l'ordinateur de fonctionner correctement et dont l'élimination provoque de sérieux dégâts.

b) Comment l'ordinateur est-il infecté ?
L'utilisateur reçoit un virus par le biais d'ordinateurs infectés.
Le plus souvent, ce virus est transmis par l'intermédiaire de fichiers joints à un courrier électronique, ce que l'on appelle des pièces jointes. Le texte du courrier électronique lui-même ne peut jamais contenir ou propager un virus.
En plus des pièces jointes, l'échange de disquettes constitue également une source de propagation de virus.

c) Quels dangers présentent-ils ?
En fonction de leur programmation, les virus infectent certaines parties du système, allant de la simple infection jusqu'à l'effacement de certains éléments. Les virus peuvent présenter divers symptômes qui perturbent le bon fonctionnement du système (fréquents accidents du système, accroissement inexplicable de la taille du fichier, ralentissement de l'ensemble du système, messages étranges et inhabituels apparaissant à tort et à travers sur l'écran, difficulté d'accès aux données, comportement étrange des programmes). Ils diffèrent donc peu du simple fonctionnement défectueux d'un système.

Les virus ne peuvent jamais endommager le matériel d'un ordinateur. En effet, ce matériel ne peut pas être endommagé par un logiciel et le virus est précisément un logiciel.

5. *Oplossingen om tot veiligheid en vertrouwen te komen:*

In dit laatste deel rond beveiliging gaan we een aantal oplossingen bekijken die een antwoord vormen op de vragen die we tot nogtoe gesteld hebben.

a) het oplossen van het probleem van identificatie en het beschermen tegen het lezen van e-mail door anderen: encryptie

Doel van versleuteling

Elke telecommunicatie houdt het gevaar in dat de boodschap in de handen van onbevoegden valt. Om te voorkomen dat buitenstaanders de inhoud van een bericht achterhalen, moet het door versleuteling voor hen onbegrijpelijk worden gemaakt. Op militair en diplomatiek gebied wordt daarom reeds van oudsher van versleutelingstechnieken gebruikgemaakt.

Men gebruikt encryptie voor een aantal doeleinden.

1/ Authenticatie

Bij authenticatie gaat het erom zeker te zijn dat de andere partij wel degelijk de partij is die ze beweert te zijn. In de context van e-mail gaat het er dus om er zeker van te kunnen zijn dat de verzender die bovenaan de e-mail staat wel degelijk die persoon is.

2/ Integriteit

Bij integriteit gaat het erom ervoor te zorgen dat gegevens niet gewijzigd worden terwijl ze verstuurd worden.

Opnieuw vertaald naar de context van e-mail betekent dit dat de tekst in de body van je e-mail niet gewijzigd wordt terwijl die over het Internet verstuurd wordt.

3/ Confidentialiteit

Bij confidentialiteit gaat het erom zeker te zijn dat niemand anders dan de ontvanger de gegevens te lezen krijgt.

In het geval van e-mail communicatie gaat het er dus om dat niemand anders de boodschap te lezen mag krijgen.

Encryptie: hoe gaat men tewerk

Wanneer de gegevens door het encryptie-programma gaan worden ze door middel van een sleutel herleid tot een reeks onleesbare tekens. Een ‘sleutel’ is in praktijk vaak een complex wiskundig algoritme. De ontvanger moet de correcte sleutel hebben om de boodschap te

5. *Solutions pour assurer la sécurité et la confiance:*

Dans cette dernière partie relative à la sécurité, nous allons envisager une série de solutions qui constituent une réponse aux questions posées jusqu’à présent.

a)Solution du problème de l’identification et de la protection contre la lecture par d’autres du courrier électronique : le cryptage.

But du cryptage.

Chaque télécommunication présente le danger que le message tombe dans les mains de personnes non autorisées à le recevoir. Pour éviter que des intrus n’interceptent le contenu d’un message, celui-ci doit être rendu incompréhensible grâce au cryptage. Dans le domaine militaire et diplomatique, on utilise depuis toujours des techniques de cryptage.

On utilise le cryptage à diverses fins.

1/ Authentification.

L’authentification est utilisée pour certifier que l’interlocuteur est réellement celui qu’il prétend être. Dans le cas du courrier électronique, elle permet de s’assurer que l’expéditeur indiqué en tête du message est bien le bon.

2/ Intégrité.

Il s’agit de faire en sorte que les données ne soient pas modifiées pendant leur expédition.

Dans le cas du courrier électronique, cela signifie que le corps du texte du message n’est pas modifié durant sa transmission par internet.

3/ Confidentialité.

La confidentialité consiste à être certain que personne d’autre que le destinataire des données ne pourra prendre connaissance de celles-ci.

Dans le cas du courrier électronique, cela signifie que personne d’autre ne pourra lire le message.

Cryptage: fonctionnement

Les programmes de cryptage transforment, à l’aide d’une clé, les données en une série de signes illisibles. En pratique, une « clé » est souvent un algorithme mathématique complexe. Le destinataire doit disposer de la bonne clé pour pouvoir déchiffrer le message. Les

kunnen ontcijferen. De andere lezers van de boodschap krijgen echter een volledig onleesbare tekst te voorschijn.

Er bestaan twee vormen van encryptie, symmetrische en asymmetrische encryptie. De eerste werkt op basis van één geheime sleutel die door beide partijen gekend is ; de tweede encryptie methode maakt gebruik van een private en een publieke sleutel.

Bij symmetrische encryptie zal de verstuurder dus de boodschap versleutelen met dezelfde sleutel als diegene waarmee de ontvanger deze ontsleutelt.

Het belangrijkste nadeel van deze encryptie methode is de veilige uitwisseling van de geheime sleutel. Dat maakt het in de praktijk zeer moeilijk deze methode te gebruiken voor grotere groepen.

In het geval van asymmetrische encryptiemethodes zal gebruik gemaakt worden van 2 sleutels, een 'private' en 'publieke' sleutel, die onlosmakelijk met elkaar verbonden zijn. De private sleutel blijft steeds in het bezit van één enkel persoon. De publieke sleutel daarentegen wordt centraal opgeslagen en is beschikbaar voor een grote groep mensen.

Laat ons twee voorbeelden nemen om uit te leggen hoe deze asymmetrische encryptie kan gebruikt worden om e-mail communicatie te gaan beveiligen.

1/ We willen een confidentieel bericht naar iemand versturen. In dit geval zoek je de publieke sleutel op van de persoon naar wie je het bericht wil versturen en versleutelt hiermee je boodschap. De ontvanger is dankzij zijn private sleutel de enige die het bericht terug kan ontsleutelen. Je kan er dus zeker van zijn dat niemand anders het bericht kan lezen. Als de ontvanger op zijn beurt een confidentieel antwoord wil terugsturen, zal hij jouw publieke sleutel gebruiken om het bericht te versleutelen, en zal alleen jij met je private sleutel het bericht terug kunnen ontcijferen.

2/ We willen een bericht versturen waarvan de ontvanger 100% zeker is dat het bericht van mij afkomstig is. In dit geval gebruik je je eigen private sleutel om je bericht te versleutelen. De ontvanger krijgt je bericht ; en indien hij met jouw publieke sleutel in staat is het bericht te ontcijferen, kan hij er zeker van zijn dat jij inderdaad de afzender bent geweest. Deze methode is een van de technieken die gebruikt wordt voor de zogenaamde digitale handtekening ; waarbij het vanzelfsprekend belangrijk is dat de partijen zeker zijn van de correcte identiteit van mekaar.

autres lecteurs ne voient du message qu'un texte parfaitement illisible.

Il existe deux types de cryptage : le symétrique et l'asymétrique. Le premier utilise une seule clé secrète connue des deux parties ; le deuxième utilise une clé privée et une clé publique.

Dans le cas du cryptage symétrique, l'expéditeur utilise pour sécuriser son message la même clé que celle qu'emploie le destinataire pour déchiffrer le message.

Le principal point faible de cette méthode se situe au niveau de la sécurité d'échange de la clé secrète. Il est par conséquent très difficile d'utiliser cette méthode pour les grands groupes.

Le cryptage asymétrique recourt à une clé « privée » et une clé « publique » indissociablement liées entre elles. La clé privée reste en possession d'une seule personne. En revanche, la clé publique est stockée de manière centrale et est accessible à une groupe important de personnes.

Voici deux exemples permettant de comprendre comment le cryptage asymétrique permet de sécuriser la communication par e-mail.

1/ Nous voulons envoyer un message confidentiel à quelqu'un. Dans ce cas, nous recherchons la clé publique du destinataire et nous l'utilisons pour crypter le message. Grâce à sa clé privée, le destinataire est le seul qui puisse décrypter le message. Nous pouvons donc être sûrs que personne d'autre ne pourra le lire. Si, à son tour, le destinataire souhaite envoyer une réponse confidentielle, il emploiera notre clé publique pour coder le message. Nous serons les seuls à pouvoir déchiffrer ce message grâce à notre clé privée.

2/ Nous voulons envoyer un message dont le destinataire soit sûr à 100% qu'il provient de nous. Dans ce cas, nous utiliserons notre propre clé privée pour crypter notre message. Le destinataire reçoit notre message. S'il parvient à le déchiffrer au moyen de notre clé publique, il peut être certain que nous en sommes bien l'expéditeur. Cette méthode est l'une des techniques utilisées pour la signature électronique, où il importe évidemment que les parties soient sûres de leur identité respective.

In de praktijk bestaan er verschillende combinaties van encryptie technologiën die ervoor zorgen dat zowel authentificatie, integriteit en confidentialiteit van e-mail communicatie kunnen gegarandeerd worden.

We beschikken over de middelen om e-mails te encrypteren waardoor ze onderweg niet onderschept, gelezen of gewijzigd kunnen worden. Dankzij de digitale handtekening kunnen we ook zeker zijn van de identiteit van de verschillende partijen. Je zou dus verwachten dat beveiligde e-mail een wijd verspreid gebruik zou kennen. En toch is dat niet zo. Waarom?

De voornaamste reden vinden we terug op het vlak van vertrouwen. Werken met sleutels verondersteld dat er een onafhankelijke partij is die door alle andere partijen wordt vertrouwd, en die instaat voor het uitgeven maar ook het terug intrekken van digitale certificaten. Op het Internet bestaan reeds geruime tijd wat men noemt certificatie autoriteiten zoals GlobalSign en VeriSign. Maar in de praktijk zien we dat vooral bedrijven niet voldoende vertrouwen hebben in deze partijen om er het beveiligen van hun bedrijfscommunicatie aan toe te vertouwen.

b) Tegen het achterlaten van sporen

Hiertegen valt weinig te doen. Het wordt wettelijk vereist dat logs worden bijgehouden bij de ISP. Dit is volgens de wetgeving nu minimum 12 maand wat het in- en uitloggen met het Internet betreft. Maar ook op je eigen computer wordt er automatisch zeer veel informatie bewaard. Zo worden door het operating systeem (Windows), maar ook door vele andere programma's tijdelijke bestanden aangemaakt die niet automatisch vernietigd worden. Dit kan in sommige gevallen nuttig zijn ; bijvoorbeeld wanneer de politie een huiszoeking doorvoert.

c) Tegen virussen en aanvallen van buitenaf

Hoe kan men zich beschermen tegen virussen?

Met een anti-virusprogramma komt men al heel ver, maar aangezien dagelijks nieuwe virussen uitkomen is regelmatig een update noodzakelijk.

Verder moet je heel goed uitkijken met attachments die meegezonden worden met e-mail, ook als je de persoon kent van wie de mail komt. De persoon kennen garandeert niet dat hij geen virus kan hebben op zijn computer.

En pratique, il existe plusieurs combinaisons de technologies de cryptage garantissant l'authentification, l'intégrité et la confidentialité du courrier électronique.

Nous disposons donc des moyens permettant de crypter les e-mails afin qu'ils ne soient pas interceptés, lus ni modifiés. Et grâce à la signature électronique, nous pouvons en outre être certains de l'identité des différentes parties. On pourrait donc s'attendre à ce que l'e-mail sécurisé soit d'un usage répandu. Ce n'est cependant pas le cas. Pourquoi ?

La première raison est une question de confiance. L'usage de clés suppose qu'une partie neutre jouisse de la confiance de toutes les autres parties et puisse délivrer mais aussi retirer les certificats numériques. Sur internet, il existe déjà depuis un certain temps des « autorités de certification » telles GlobalSign et VeriSign. En pratique, on observe toutefois que ce sont surtout les entreprises qui n'ont pas suffisamment confiance en ces autorités pour leur confier la sécurisation de leur communication.

b) Contre les traces

On ne peut pas faire grand-chose contre les traces. La loi exige que l'ISP conserve les logs, au minimum 12 mois en ce qui concerne les connexions à internet et les déconnexions. Les ordinateurs personnels conservent eux aussi automatiquement de nombreuses informations. Ainsi, le système d'exploitation (Windows), ainsi que de nombreux autres programmes constituent des fichiers temporaires qui ne sont pas détruits automatiquement. Dans certains cas, cela peut être utile, par exemple lorsque la police effectue une perquisition.

c) Contre les virus et les attaques extérieures

Comment se protéger contre les virus ?

Les programmes anti-virus sont très efficaces, mais comme de nouveaux virus apparaissent tous les jours, une mise à jour régulière s'impose.

Par ailleurs, il convient d'être très prudent avec les pièces jointes attachées aux e-mails, même si l'on connaît bien l'auteur du mail. Ce n'est pas parce qu'on connaît cette personne que celle-ci ne peut pas avoir de virus dans son ordinateur.

Geregeld een back-up maken van je bestanden kan handig zijn voor het geval er toch iets mis gaat.

Het voornaamste is echter op de hoogte te blijven van nieuwe virussen, zodat je ook preventief kan handelen door bijvoorbeeld verdachte bestanden niet te openen.

Wel opmerkelijk is het feit dat de laatste twee gevaarlijkste virussen: het «I Love You» en «Goner» respectievelijk het werk waren van een Filipijnse student en Israëlische 15-jarigen, beide niet als virus werden opgemaakt maar programma's waren welke volledig uit de hand liepen.

www.bipt.be
In het BIPT (Belgisch Instituut voor Post en Telecommunicatie) is een security platform dat de bedoeling heeft het grote publiek zo snel mogelijk te waarschuwen wanneer er een virus opduikt. De meeste ISP's krijgen deze informatie het eerst door internationale waarschuwingen, door hun klanten of door het gedrag van het Internet.

Wanneer bij het BIPT een waarschuwing binnenloopt over een mogelijk virus wordt dat eerst onderzocht door externe experten om de gevaarlijkheid te onderzoeken. Wanneer dat gebeurd is wordt op het Bureau van het Ministerie van Telecommunicatie een beslissing genomen en een waarschuwing naar het publiek toe gezonden (via hun mailinglijst, banners, webpagina, radio, televisie en pers).

In ISPA is ook een groep opgericht welke ondeling op snelle wijze virus-informatie of andere gevaren van het Internet in België kan uitwisselen.

De heer Peter VANHOUTTE, voorzitter: Mijnheer Vansevenant, bedankt voor uw uiteenzetting. Ik denk dat uw toespraak ook heel wat vragen heeft losgeweekt. Omwille van de beperkte tijd zullen wij tijdens de koffiepauze met de experts overleggen over de vragen of onze computer aan en flinke wasbeurt toe is en of de beveiliging nog wel up to date is. Ik stel voor dat wij bij het debat, op het einde van dit colloquium, eventueel nader ingaan op specifieke aspecten die met de gestelde problematiek te maken hebben.

*
* *

Effectuer régulièrement des back-ups de ses fichiers peut être pratique au cas où un problème surviendrait.

La principale mesure à prendre est toutefois de se tenir informé de l'apparition de nouveaux virus. Il sera ainsi possible d'agir préventivement, par exemple en n'ouvrant pas les fichiers suspects.

Remarquons que les deux derniers virus les plus dangereux, "I Love You" et "Goner", étaient respectivement le fait d'un étudiant philippin et de jeunes Israéliens de 15 ans, et n'étaient pas conçus au départ comme des virus mais ce sont des programmes qui ont échappé à tout contrôle.

www.ibpt.be
L' IBPT (Institut belge pour la poste et les télécommunications) est une plateforme de sécurité destinée à prévenir le grand public aussi rapidement que possible de l'apparition des nouveaux virus. La plupart des ISP reçoivent cette information d'abord par le biais des avertissements internationaux, de leurs clients ou via internet.

Lorsque l'IBPT est prévenu de l'existence possible d'un virus, des experts externes en examinent la dangerosité. Le Bureau du ministère des Télécommunications prend ensuite la décision d'envoyer un avertissement au public (au moyen de mailing-lists, de bannières, de pages web, par la radio, la télévision et la presse).

L'ISPA comprend en outre un groupe capable d'échanger rapidement en Belgique des informations relatives aux virus ou à d'autres dangers liés à internet.

M. Peter VANHOUTTE, président: Monsieur Vansevenant, je vous remercie de votre exposé. Je pense que votre intervention a suscité de nombreuses questions. Puisque notre temps est limité, je propose que nous profitions de la pause-café pour discuter avec les experts de la question de savoir s'il est temps de nettoyer nos ordinateurs et si notre système de sécurité est encore à jour. Je propose que nous revenions plus en détail sur certains aspects spécifiques du problème à la fin de ce colloque.

*
* *

Voorzitter: de heer Jean-François Istasse, Gemeenschapssenator (PS) : Geachte collega's, dames en heren, mijn naam is Jean-François Istasse. Ik ben gemeenschapssenator en neem op de voorzittersstoel de fakkel over van volksvertegenwoordiger Peter Vanhoutte, aan wie ik bij deze mijn dank betuig. Ik zal het tweede, meer juridische gedeelte van het forum voorzitten, dat tegen het einde van de middag met een debat zal worden afgerond.

Tijdens het eerste deel van deze forumbijeenkomst hebben we een uitstekende inleiding gekregen over ons thema van vandaag, e-mail. Ter inleiding van het tweede gedeelte van de middag wil ik u vertellen dat de jeugd, vóór *Star Academy* er was, naar westerns keek op televisie. In zo'n western reed er altijd wel een diligence rond met postzakken op het dak. Steevast werd de diligence op geregelde tijdstippen overvallen door uiterst gevaarlijke indianen. Die indianen zitten naar ik verneem tegenwoordig op Trojaanse paarden en hun pijlen zijn geïnfecteerd of vergiftigd door virussen. Kortom, erg gevaarlijke toestanden allemaal, en zelfs de cowboys zijn niet langer te vertrouwen.

Wat wij nodig hebben is een sheriff, en wetten om wat regel en orde te brengen in die Far West. Het is mij een groot genoegen mevrouw Saskia Mermans, verantwoordelijke voor de juridische dienst bij Belgacom Skynet, het woord te mogen geven. Zij zal het hebben over de wetgeving betreffende elektronische post.

Mevrouw, kan u ons vertellen of de wetgeving toereikend is ? Het hoeft geen betoog dat de parlementsleden bijzonder aandachtig naar u zullen luisteren.

D. **De wetgeving in verband met e-mail : Uiteenzetting van mevrouw Saskia Mermans, Belgacom Skynet**

Dames en Heren,

Sinds ettelijke jaren is het Internet een actueel thema. Ik verwijs enkel maar naar hetgeen we dagelijks in onze kranten konden lezen; de «big hype» rond de internet start-ups; de berichtgeving rond Napster, de MP3 files, om er maar enkelen te noemen.

Gelet op het korte tijdsbestek dat mij werd toegewezen, zal ik in mijn tussenkomst de volgende punten toelichten:

– allereerst, wens ik het standpunt van ISPA, de Belgische Internet Service Providers Association, te vertolken ten aanzien van de regelgeving en het internet;

– verder zal ik de belangrijkste bestaande en toekomstige wetgeving inzake e-mail toelichten.

Président: M. Jean-François Istasse, Sénateur de Communauté (PS) : Chers collègues, mesdames, messieurs, je m'appelle Jean-François Istasse. Je suis sénateur de Communauté. Je succède à la tribune à M. le député Peter Vanhoutte que je remercie. Je vais assurer la deuxième partie, plus juridique, qui va nous mener à un débat en fin d'après-midi.

La première partie a très bien introduit notre sujet, les *e-mail*. Pour introduire cette seconde partie, je vous dirai qu'avant de regarder *Star Academy*, les jeunes regardaient les westerns à la télévision. Dans ces films; il y avait toujours une diligence postale qui transportait les sacs postaux sur son toit. Cette diligence était régulièrement attaquée dans tous les films par des indiens très dangereux, indiens qui sont maintenant montés sur des chevaux de Troie, ai-je entendu, qui envoient des flèches infectées ou empoisonnées par des virus. Bref, tout cela est extrêmement dangereux et même les cow-boys ont des mines patibulaires et sont devenus inquiétants.

Nous avons besoin d'un shérif, nous avons besoin de lois pour mettre un peu d'ordre dans ce Far West. Je suis très heureux d'accueillir à notre tribune Mme Saskia Mermans, responsable du service juridique chez Belgacom Skynet, qui va nous parler de la législation relative au courrier électronique.

Chère madame, pouvez-vous nous dire si la législation est suffisante? Inutile de vous dire que les parlementaires seront particulièrement attentifs.

D. **Législation relative au courrier électronique: Exposé de Mme Saskia Mermans, Belgacom Skynet**

Mesdames et Messieurs,

Depuis plusieurs années, internet est au cœur de l'actualité. Il suffit de penser à ce que nous lisons quotidiennement dans nos journaux : la folie suscitée par les start-ups; l'affaire Napster, les fichiers MP3, pour n'en citer que quelques-uns.

Étant donné le peu de temps qui m'est imparti, je me limiterai aux points suivants.

Je voudrais tout d'abord exposer la position de l'ISPA, l'association belge des fournisseurs de service internet, quant à la législation et à internet.

J'expliquerai ensuite les principales lois existantes et à venir relatives au courrier électronique.

1. ISPA en de regelgeving

Sinds de oprichting van ISPA hebben de leden ISPs, met verschillende instanties van allerlei aard samengewerkt teneinde een regelgeving na te streven, waarbij elke belanghebbende partij zijn of haar rol kan spelen in de ontwikkeling van het Internet in België.

Internet was een nieuw medium en heeft een grensoverschrijvend karakter. Men noemt niet voor niets één onderdeel van dit nieuwe medium het «world wide web». Juist gelet op het feit dat het Internet geen territoriale grenzen kent, werden in Europa verschillende oplossingen nagestreefd in het kader van de ontwikkeling van de regelgeving. In verschillende landen werd de optie van zelf-regulering gevolgd: verschillende gedragscodes zagen dan ook het levenslicht. Als grote voorbeeld kan naar de Verenigde Staten worden verwezen. ISPA België is echter van in de beginne de weg van co-regulering ingeslagen en dit onmiddellijk voor wat betreft de strijd tegen illegale en ongeoorloofde inhoud op het internet.

Waarom deze optie ? Wij gaan ervan uit dat de huidige wetgeving het mogelijk maakt het nieuwe medium dat Internet is, te omvatten en dat derhalve geen internet specifieke wetgeving ontwikkeld dient te worden inzake illegale inhoud op het Internet. In concreto werden dan ook de volgende stappen ondernomen:

– enerzijds heeft ISPA in samenwerking met de betrokken Ministeries een Gedragscode ontwikkeld teneinde het vertrouwen van de consument in het Internet, vooral naar de electronische handel toe, te bevorderen;

– teneinde dit zelfregulerend initiatief te vervolledigen, heeft ISPA op 28 mei 1999 een Protocol ondertekend met de Ministers van Telecommunicatie en Justitie in het kader van de strijd tegen de illegale en ongeoorloofde inhoud op het internet. Eén contactpunt werd aangeduid aan de kant van de gerechtelijke autoriteiten aan dewelke gevallen van illegale inhoud, zoals kinderpornografie, gemeld dienen te worden. Teneinde een mogelijk strafonderzoek niet in gevaar te brengen, dient de ISP op dat moment te wachten op de instructies van de gerechtelijke autoriteiten ten aanzien van de maatregelen die genomen dienen te worden. Hier is echter één uitzondering voor wat kinderpornografie betreft, hetgeen volledig begrijpelijk en aangewezen is: dergelijke inhoud dient onmiddellijk verwijderd te worden. Dit samenwerkingsprotocol bewerkstelligt vanzelfsprekend regelmatige contacten tussen ISPA en zijn leden en de gerechtelijke autoriteiten, hetgeen de samenwerking enkel ten goede kan komen. Wij zijn ervan overtuigd

1. L'ISPA et la réglementation

Depuis la création de l'ISPA, les ISP membres ont collaboré avec plusieurs instances de nature différente afin d'aboutir à une réglementation permettant à chaque partie ayant des intérêts en jeu de contribuer au développement d'internet en Belgique.

Internet est un nouveau moyen de communication qui ne connaît pas les frontières. Ce n'est pas pour rien qu'une partie de ce nouveau média est appelée "world wide web". C'est justement parce qu'internet ne connaît pas de frontières territoriales que les États membres de l'Europe ont suivi des voies différentes dans la recherche d'une réglementation. Plusieurs pays ont choisi l'option de l'autorégulation: plusieurs codes de conduite ont ainsi vu le jour, principalement aux États-Unis. L'ISPA Belgique a, quant à elle, suivi dès le départ la voie de la corégulation et ce, immédiatement en ce qui concerne la lutte contre les contenus illégaux et interdits sur internet.

Pourquoi cette option ? Nous partons du principe que la législation permet d'inclure ce nouveau média qu'est internet, et qu'il n'est dès lors pas nécessaire de développer de législation spécifique à internet en matière de contenu illégal. Concrètement, nous avons entamé les démarches suivantes:

– l'ISPA a développé un Code de conduite en collaboration avec les ministères concernés afin de renforcer la confiance du consommateur dans internet, surtout en ce qui concerne le commerce électronique;

– afin de compléter cette initiative d'autorégulation, l'ISPA a signé le 28 mai 1999 un Protocole avec les ministres des Télécommunications et de la Justice dans le cadre de la lutte contre les contenus illégaux et interdits sur internet. Les autorités judiciaires ont désigné un point de contact auquel il convient de signaler les cas de contenu illégal, comme la pornographie enfantine. Afin de ne pas compromettre une éventuelle enquête pénale, l'ISP doit attendre les instructions des autorités judiciaires quant aux mesures à prendre. Il y a toutefois une exception en ce qui concerne la pornographie enfantine, ce qui est tout à fait compréhensible et souhaitable: ce contenu doit être retiré immédiatement. Ce protocole de coopération donne évidemment lieu à des contacts réguliers entre l'ISPA et ses membres et les autorités judiciaires, ce qui ne peut qu'être bénéfique à la collaboration. Nous sommes convaincus que c'est surtout en matière de contenu illégal que l'autorégulation n'est pas suffisante. Plusieurs autres associa-

dat vooral inzake illegale inhoud een zelf-regulering niet voldoende is. Verschillende andere Internet Service Providers Associations in Europa zijn nu ook de weg van co-regulering ingeslagen.

2. *Algemene beschouwing ten aanzien van het wettelijk kader voor het Internet in Europa en België*

Alvorens naar de kern van mijn exposé te gaan, wens ik allereerst een belangrijke algemene beschouwing te maken ten aanzien van het wettelijk kader voor het Internet in Europe en België in het algemeen.

Bij het ontstaan van het Internet werd ervan uitgegaan dat voor dit nieuwe medium een specifieke wetgeving nodig was. Het Internet diende volledig afzonderlijk geregeld te worden.

Men is er steeds vanuit gegaan dat het Internet een spectaculaire groei zou kennen. Maar de feiten tonen het tegenovergestelde aan. De «big hype» rond e-commerce, de electronische handel heeft echter in de realiteit nooit het levenslicht gezien, ook al leken de financiële markten begin 2001 de voorbode van een belangrijke groei te zijn.

Tijdens een Telco conferentie in Genève gaf John Roth, Voorzitter en CEO van Nortel Networks, de volgende cijfers van hoeveel jaren bepaalde communicatiemiddelen nodig hadden om 50 miljoen mensen te bereiken:

– de telefoon : 75 jaar;
– de radio : 35 jaar;
– de televisie : 13 jaar;
– de GSM : 12 jaar;
– het Internet : enkel 4 jaar.

Ook al nam het maar 4 jaar in beslag, de cijfers die Rudi Roth bij de aanvang van deze conferentie heeft toegelicht, toonden nog een belangrijk groeipotentieel in de meerderheid van de West Europese landen.

Deze marktgegevens hebben aanleiding gegeven tot de beschouwing dat het Internet niets anders is dan een nieuw technisch communicatiemiddel, een nieuwe technologie. Derhalve werd de weg ingeslagen van het aanpassen van de «oude» wetgeving aan deze nieuwe technologie. De richtlijn inzake auteursrecht, waarover we het later zullen hebben, is daarvan een goed voorbeeld.

Het uitgangspunt is dan ook dat wat wij noemen de «off-line» wereld gelijk is aan de «on-line» wereld.

Tot besluit kunnen we besluiten dat het «recht» geleid wordt door marktdynamieken en globalisatie, dit

tions européennes de fournisseurs de services internet ont également suivi la voie de la corégulation.

2. *Considération générale concernant le cadre légal de l'internet en Europe et en Belgique*

Avant d'en venir au fond de mon exposé, je voudrais faire une remarque importante à propos du cadre légal de l'internet en Europe et en Belgique en général.

Au début, on était parti du principe que ce nouveau mode de communication appelait une législation spécifique et qu'il fallait donc le soumettre à une réglementation distincte

Alors qu'on avait toujours prédit un développement spectaculaire de l'internet, les faits on montré qu'il n'en était rien. En fait, le commerce électronique n'a pas suscité l'engouement alors que, début 2001, les marchés financiers montraient les signes avant-coureurs d'une croissance importante.

Lors d'une conférence Telco organisée à Genève, John Roth, président-directeur général de Nortel Networks, a indiqué le nombre d'années que chaque mode de communication avait mis pour atteindre 50 millions de personnes :

- le téléphone : 75 ans ;
- la radio : 35 ans ;
- la télévision : 13 ans ;
- le GSM : 12 ans ;
- internet : 4 ans seulement.

Malgré ce laps de temps très court, les chiffres cités par Rudi Roth au début de cette conférence ont montré qu'il y avait encore un potentiel de croissance important dans la plupart des pays d'Europe occidentale.

De ces données, on a déduit qu'internet n'était qu'un nouveau mode de communication, une nouvelle technologie, sans plus. On y a donc adapté l'« ancienne » législation. Citons à ce propos la directive en matière de droits d'auteur, dont nous parlerons ultérieurement.

L'idée de départ était que les mondes « off-line » et « on-line » étaient identiques.

Pour conclure, nous pouvons dire que le « droit » est régi par les dynamiques de marché et, pour l'ins-

wil zeggen «op dit moment» want «Nothing is permanent, but change».

3. *De Wetgeving inzake de electronische briefwisseling*

Zoals reeds vermoed kon worden op basis van de voorgaande beschouwing, is er geen specifieke wetgeving inzake e-mail. Ik heb dan ook gepoogd mijn presentatie rond drie pijlers van het recht te centraliseren.

Wie electronische briefwisseling zegt, zal onmiddellijk aan privacy denken. Privacy is gelinkt met cybercrime, aangezien in verschillende situaties de privacy dient te wijken voor een hoger belang.

Er is ook een link tussen e-mail en e-commerce, de electronische handel. De laatste tijd heeft het topic «spam» in dat kader ook onze berichtgeving bereikt. Waarschijnlijk heeft ieder van ons reeds een e-mail ontvangen met een duidelijke commerciële boodschap die men niet gevraagd heeft te ontvangen.

Een laatste luik dat behandeld zal worden is copyright, het auteursrecht.

a) Privacy & cyber-crime, informaticacriminaliteit

Zoals met een gewone brief, wenst men dat een e-mail niet alleen de bestemmeling bereikt, maar ook dat er een zekerheid is dat de inhoud ervan niet door een derde gelezen kan worden. Uit de technische presentatie is de complexiteit van het versturen van een e-mail gebleken.

Meer dan een jaar geleden werd in de Verenigde Staten de theorie verdedigd dat de electronische brief niet beschermd kon worden door het briefgeheim aangezien de e-mail niet vergeleken kon worden met een de brief onder omslag. Een e-mail is niet beveiligd. In de Verenigde Staten werd de e-mail als een brief onder open omslag beschouwd. Zij baseerden zich daarbij op de technische aspecten inzake het verzenden van een e-mail.

Deze theorie werd niet volledig gevolgd in Europa. Privacy wetgeving dient dan ook in achtgenomen te worden inzake e-mail. Andere aspecten van e-mail zoals spamming worden eveneens behandeld in de privacy wetgeving: het opstellen van mailinglists valt onder de privacy wetgeving vooral wanneer het privé-personen betreft.

Een ander element dat sinds enige tijd aan de orde is, is het gebruik van e-mail in de professionele wetant en tout cas, par la globalisation car « Nothing is permanent but change ».

3. *La législation en matière de courrier électronique*

De ce qui précède, on aura compris que le courrier électronique ne fait pas l'objet d'une législation spécifique. Aussi ai-je tenté de centrer mon exposé autour de trois piliers du droit.

Qui dit courrier électronique songe d'emblée à la protection de la vie privée. Il y a un lien entre la vie privée et le cybercrime puisque dans un certain nombre de situations, la vie privée doit céder devant un intérêt supérieur.

Il y a aussi un lien entre le courrier électronique et le commerce électronique. Ces derniers temps, on a souvent évoqué la question du « spam » à ce propos. Sans doute chacun d'entre nous a-t-il déjà reçu sans l'avoir demandé un courrier électronique comportant un message à caractère commercial évident.

Le dernier volet dont nous traiterons concerne le copyright, le droit d'auteur.

a) Vie privée et cybercrime, criminalité informatique

Comme pour une lettre ordinaire, on souhaite non seulement qu'un courrier électronique atteigne son destinataire, mais en outre être sûr que son contenu ne pourra être lu par un tiers. L'exposé technique a montré la complexité de l'envoi d'un courrier électronique.

Il y a plus d'an an, on a défendu aux États-Unis la théorie selon laquelle le courrier électronique ne pouvait être protégé par le secret des lettres puisqu'il n'était pas comparable à une lettre sous enveloppe. L'e-mail n'est pas sécurisé. Aux États-Unis, il était considéré comme une lettre envoyée sous enveloppe ouverte et ce en fonction des modalités techniques liées à l'envoi d'un courrier électronique.

Cette théorie n'a pas été entièrement suivie en Europe. La législation relative à la protection de la vie privée doit aussi s'appliquer au courrier électronique. Elle englobe également d'autres aspects du courrier électronique, comme les courriers non sollicités. L'établissement de listes de mailing, surtout si elles concernent des individus, relève également de la législation sur la protection de la vie privée.

Un autre élément à l'ordre du jour depuis quelque temps est l'utilisation du courrier électronique dans la

reld, meer bepaald op de «werkplaats». De hamvraag daar is te weten of de werkgever het recht heeft het gebruik van het e-mailsysteem door de werknemer te controleren. Is het zo dat de werknemer het recht heeft om in beperkte mate het e-mail systeem van de werkgever te gebruiken voor privé-doeleinden? In dat kader heeft Senator Alain Destexhe een wetsvoorstel ingediend. In een recente uitspraak van het Hof van Cassatie in Frankrijk, werd besloten dat een werknemer niet ontslagen kon worden voor het verzenden van privé e-mails vanop het werk.

Verschillende teksten op Europees en Belgische niveau regelen de bescherming van het privé-leven.

Op Europees niveau dient verwezen te worden naar de volgende teksten:
– De «data protection directive» 95/46 inzake privacy in de telecommunicatiesector;
– Deze werd vervangen door de «data protection directive» 97/66 die ik hierna de «privacy richtlijn» zal noemen.

Op dit moment is er eveneens een belangrijke ontwerp -richtlijn van het Europees Parlement en de Europese Commissie inzake het verwerken van persoonsgegevens en de bescherming van de privacy in de electronische handel. Dit ontwerp dient de privacy richtlijn te vervangen. In dat kader verwijs ik naar de verschilende debatten die hebben plaatsgevonden inzake de opt-in/opt-out issue in het kader van spam.

Opt-out betekent dat je persoonlijke gegevens door een bedrijf gebruikt kunnen worden, zoals je e-mail adres, en dit voor marketing doeleinden, maar waarbij je aan het bedrijf kan melden dat je je hiertegen verzet. Dit betekent dat je e-mail adres automatisch kan gebruikt worden, tenzij je je verzet.

Opt-in is de omgekeerde situatie. Een bedrijf kan je e-mail adres maar gebruiken als je er expliciet mee akkoord gaat. Het is u onmiddellijk duidelijk geworden dat opt-in de bedrijven het moeilijker zal maken in haar prospectie activiteiten.

Inzake België verwijs ik naar:

– in de allereerste plaats de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. In uitvoering van deze wet is er het Koninklijk Besluit van 13 februari 2001.

sphère professionnelle et plus particulièrement sur le lieu de travail. La question cruciale est de savoir si l'employeur a le droit de contrôler l'usage que fait le travailleur du système de courrier électronique. Celui-ci a-t-il effectivement le droit d'utiliser, de manière limitée et à des fins privées, le système de courrier électronique de son employeur ? Le sénateur Alain Destexhe a déposé une proposition de loi en la matière. En France, la Cour de Cassation vient de rendre un jugement important à cet égard en décidant qu'un travailleur ne pouvait être licencié pour avoir envoyé des courriers électroniques privés depuis son lieu de travail.

Différents textes de loi européens et belges réglementent la protection de la vie privée.

Au niveau européen, il s'agit de :
- la « data protection directive » 95/46 relative à la protection de la vie privée dans le secteur des télécommunications ;
- elle a été remplacée par la « data protection directive » 97/66 que j'appellerai par la suite la « directive relative à la protection de la vie privée ».

Le Parlement européen et la Commission examinent actuellement un projet important de directive européenne en matière de traitement des données à caractère personnel et de protection de la vie privée dans le commerce électronique. Ce projet de directive doit remplacer celle relative à la protection de la vie privée. Je renvoie à ce propos aux différents débats autour de la question de l'*opt-in/opt-out* dans le cadre du *spam*.

L'*Opt-out* signifie que des données à caractère personnel, par exemple notre adresse électronique, peuvent être utilisées par une entreprise à des fins de marketing sauf si nous signalons notre opposition. Par conséquent, sauf refus de notre part, notre adresse électronique peut être utilisée d'office.

L'*Opt-in* est l'inverse. Une entreprise ne peut utiliser notre adresse électronique que moyennant notre accord explicite. On aura immédiatement compris que l'*opt-in* gênera l'entreprise dans ses activités de prospection.

Pour ce qui concerne la Belgique et la vie privée, je dois renvoyer :

– en premier lieu, à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et, en exécution de cette loi, l'arrêté royal du 13 février 2001.

– verder is er de Wet van 11 december 1998 tot omzetting van de richtlijn 95/46 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van deze gegevens, die ik de «privacy richtlijn» heb genoemd.

Zoals reeds eerder gesteld, is er een duidelijke link tussen «spam» en privacy. Evenwel situeert spam zich in de commerciële wereld. Derhalve komt in beperkte mate ook de Wet van 14 juli 1991 op de handelspraktijken aan bod. Deze wet omvat een bepaling in het hoofdstuk publiciteit inzake het verzenden van een commerciële e-mail. Deze bepaling komt erop neer dat in de «subject header» van de e-mail duidelijk vermeld dient te worden dat het om een commerciële, publicitaire e-mail gaat.

In datzelfde kader is er het wetsontwerp van 30 november van dit jaar van de Minister Picqué inzake de electronische handel. In dit wetsontwerp komt de opt-in/opt-out issue aan bod, waarbij om dit moment geopteerd wordt voor een volledig opt-in systeem voor commerciële e-mails.

Meermaals is het woord spam reeds gevallen en het debat rond opt-in en opt-out inzake commerciële e-mails. Op dit moment geldt in België een opt-out regeling. De laatste status is dat op Europees niveau voor een «zachte» opt-in regeling wordt geopteerd. Het Belgisch wetsontwerp omvat een stricte opt-in regeling. Wat dit betreft dienen wij erop te wijzen dat indien éénzelfde weg niet op Europees niveau wordt ingeslagen, dit een ernstige beperking voor de Belgische bedrijven betekent zeker in het kader van de ontwikkeling van e-commerce. Internet/e-commerce kent geen landsgrenzen. Via één website, één e-mail kan je verschillende personen in verschillende landen bereiken. Het kan niet zijn dat een Engels bedrijf in dat kader meer rechten heeft dan een Belgisch bedrijf.

Bij de aanvang van mijn exposé inzake privacy heb ik reeds aangehaald dat er een fijne lijn is tussen privacy en de uitzonderingen erop die een hoger belang dienen. Bescherming van het privé leven is geen absoluut recht. Zo belanden we in de cyber-crime, de informaticacriminaliteit, waarbij de gerechtelijke autoriteiten het recht hebben de bescherming van het privé leven van een individu te doorbreken.

– ensuite, à la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, que j'ai appelée « directive relative à la protection de la vie privée ».

Comme indiqué plus haut, il y a un lien évident entre le *spam* et la vie privée. Le *spam* se situe cependant dans la sphère commerciale. Par conséquent, la loi du 14 juillet 1991 sur les pratiques du commerce s'y applique également de manière limitée. Dans son chapitre consacré à la publicité, cette loi comporte une disposition relative à l'envoi de courrier électronique à caractère commercial. Il en ressort que le *subject header* du courriel doit indiquer clairement qu'il s'agit d'un courrier électronique commercial à caractère publicitaire.

Dans le même cadre, il y a le projet de loi du 30 novembre 2001 du ministre Picqué en matière de commerce électronique. Il traite de la question de l'*opt-in/opt-out*, l'option actuelle étant celle du système *opt-in* pour les courriers électroniques commerciaux.

À plusieurs reprises, le terme *spam* est revenu dans la discussion sur l'*opt-in* et l'*opt-out* à propos des courriers électroniques à caractère commercial. Actuellement, c'est le système *opt-out* qui est en vigueur en Belgique. Récemment, l'Europe a pris position en faveur d'un *opt-in* souple alors que le projet de loi belge opte pour un *opt-in* strict. Si l'Europe n'édicte pas un règlement unique en la matière, les entreprises belges seront évidemment sérieusement limitées dans le développement de leur commerce électronique. Internet et le commerce électronique ignorent en effet les frontières. Un seul site web, un seul e-mail permettent de joindre plusieurs personnes dans différents pays. Il est impensable qu'une entreprise anglaise puisse ainsi bénéficier de plus de droits qu'une entreprise belge.

Au début de mon exposé sur la vie privée, j'ai évoqué le fil ténu qui sépare la vie privée et les exceptions en la matière qui servent un intérêt supérieur. La protection de la vie privée n'est pas un droit absolu. Nous en arrivons ainsi au cybercrime et à la criminalité informatique ainsi qu'au droit qu'ont les autorités judiciaires de porter atteinte à la protection de la vie privée d'un individu.

Bepaalde misbruiken waar er sprake is van cybercrime:

– racistische en gelijkaardige e-mails, haat propaganda waarop de strafwet van toepassing is. In dat kader is het interessant te wijzen op de Yahoo zaak in Frankrijk. In Frankrijk is verkoop van nazistische items verboden; in de Verenigde Staten niet: quid met een dergelijk conflict? Dit in een notendop. Verschillende documenten inzake deze zaak zijn terug te vinden op het internet.

– Andere misbruiken zijn virussen die verspreid worden via e-mail («Trojanen»). Op dergelijke misbruiken is de wet op de informaticacriminaliteit van 28 november 2000 van toepassing. Het is eveneens belangrijk te onderlijnen dat de Europese Unie op een strikte wijze wenst op te treden tegen cyber-crime, in het bijzonder voor wat kinderpornografie, racisme en de drugshandel betreft.

Een aantal beschouwingen ten aanzien van de Belgische Wet inzake informaticacriminaliteit.

Vóór de inwerkingtreding van de wet informaticacriminaliteit was er geen echte wettelijke basis voor dergelijke misdrijven. Bepaalde artikels uit de Telecommunicatiewet konden toegepast worden, alsook de strafwet of de privacy wetgeving, maar er was geen sluitende oplossing. Ik verwijs hierbij naar de Red Attack zaak, waar op basis van de telecommunicatiewet een hacker werd veroordeeld.

Een belangrijk kenmerk van de wet informaticacriminaliteit is het feit dat deze werd opgesteld op een technologisch neutrale wijze. De bepalingen kunnen met andere woorden op verschillende «informatie» systemen toegepast worden, zoals daar zijn mainframe computers, PCs, het internet, het mobiele internet, internet via de GSM (dat meer en meer zijn opgang kent), electronische agenda's etc).

Verschillende nieuwe misdrijven en straffen worden in het Belgische Strafwetboek opgenomen, waarbij de straffen die opgelegd kunnen worden niet onaanzienlijk zijn.

Er is nog één punt dat onopgelost blijft, zijnde cross-border computer crime. Dit is één van de punten waarop de Cybercrime convention op Europees niveau waarschijnlijk antwoord zal bieden, alsook de maatregelen die genomen zullen worden na 11 september.

Certains usages abusifs où il est question de cybercrime.

courriers électroniques à caractère raciste et similaire, incitation à la haine tombant sous le coup de la loi pénale. Dans ce domaine, il est intéressant de se référer au dossier Yahoo en France, où la vente d'articles nazis est interdite mais pas aux États-Unis. Que faire lorsqu'il y a un tel conflit? Tout cela résumé en un mot. Divers documents relatifs à ce dossier se retrouvent sur internet.

Autre abus, la propagation de virus par courrier électronique (« cheval de Troie »). La loi du 28 novembre 2000 relative à la criminalité informatique s'applique à ce type d'usages abusifs. Il importe également de souligner que l'Union européenne souhaite intervenir rigoureusement contre le cybercrime, en particulier pour ce qui concerne la pornographie infantile, le racisme et le commerce de drogues.

Quelques mots à propos de la loi belge relative à la criminalité informatique.

Avant l'entrée en vigueur de cette loi, il n'existait pas de véritable base légale pour de tels délits. Certains articles de la loi relative aux télécommunications pouvaient être utilisés, de même que la loi pénale ou la législation relative à la protection de la vie privée, mais ce n'était pas une solution concluante. Je renvoie à ce sujet à l'affaire « *Red Attack* » où un *hacker* a été condamné sur la base de la loi relative aux télécommunications.

Une caractéristique importante de la loi relative à la criminalité informatique est d'être neutre du point de vue technologique. Autrement dit, les dispositions de cette loi peuvent être appliquées à différents systèmes d'information, comme les *mainframe computers*, les PC, internet, l'internet mobile, internet via GSM qui connaît de plus en plus de succès, les agendas électroniques, etc.

Différents nouveaux délits et sanctions sont repris dans le Code pénal belge et les sanctions qui peuvent être infligées ne sont pas négligeables.

Un problème reste à résoudre, celui du *cross-border computer crime*. C'est un des problèmes auxquels la convention Cybercrime et les mesures qui seront prises après le 11 septembre apporteront vraisemblablement une réponse au niveau européen.

Afluisteren van een e-mail, eigenlijk het onderscheppen van de inhoud van een e-mail:

Zoals reeds uiteengezet, kunnen bepaalde data of een e-mail onderschept worden. Maar een duidelijke wettelijke basis is daarvoor nodig, waardoor de gerechtelijke autoriteiten onder welbepaalde voorwaarden bepaalde gegevens kunnen opvragen.

De belangrijkste Belgische wetteksten in dit verband zijn:

– De wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en telecommunicatie.
– In uitvoering van deze wet ligt er momenteel een Koninklijk Besluit ter tafel dat vooral de technische aspecten en financiële aspecten van de samenwerking tussen gerechtelijke autoriteiten en de operatoren, ISPs zal regelen.

De laatste versie van dit ontwerp van Koninklijk Besluit omvat geen bepalingen inzake tapping/afluisteren op het internet. Internet werd uit het Koninklijk Besluit gehaald en dit om volgende reden: er is nog geen werkelijke technische oplossing die afluisteren op het Internet mogelijk maakt. Daarenboven is afluisteren op het Internet een dure aangelegenheid gelet op de specifiteit van dit medium. Het zou de kosten voor de ISPs doen toenemen, wat nadelig zou zijn in de huidige marktcondities binnen de Internet markt. Evenwel zal ISPA, naar bepaalde oplossingen zoeken in samenwerking met de gerechtelijke autoriteiten teneinde tegemoet te komen aan hun vragen.

Naast de opheffing van de privacy ten behoeve van het algemeen belang zijn er nog een aantal technische redenen waarom ISPs onder bepaalde voorwaarden toegang zullen hebben tot e-mails. Ik denk hierbij aan de facturatie van bepaalde diensten alsook de technische tussenkomsten die een ISPs dient te verrichten op zijn netwerk, servers om de goede werking van de dienst te waarborgen.

De wettelijke basis daartoe kan gevonden worden in de Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, in het bijzonder artikel 109 ter D en E.

Eén van de belangrijkste key issues in de Wet informaticacriminaliteit is het feit dat voor de eerste maal de ISPs verplicht werden data te bewaren gedurende minimum 12 maanden. Dit is echter het principe aangezien in uitvoering van deze wet een Koninklijk

Mise sur écoute d'un e-mail, **en fait, l'interception du contenu d'un e-mail:**

Comme il a déjà été expliqué, certaines données ou un e-mail peuvent être interceptés. MAIS il faut pour cela une base légale précise qui permette aux autorités judiciaires de réclamer certaines données à des conditions bien précises.

Les principaux textes de loi belges à cet égard sont les suivants :

La loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance de communications et de télécommunications privées.

En exécution de cette loi, un arrêté royal actuellement en préparation réglera principalement les aspects techniques et financiers de la collaboration entre les autorités judiciaires et les opérateurs, les ISP.

La dernière version de ce projet d'arrêté royal ne contient aucune disposition en matière de *tapping,* mise sur écoute, et d'internet. Internet a été exclu de l'arrêté royal pour les raisons suivantes : techniquement, il n'est pas encore vraiment possible de le mettre sur écoute et en outre, cette écoute est onéreuse vu la spécificité de ce média. Les frais des ISP augmenteraient, ce qui serait préjudiciable aux conditions actuelles du marché de l'internet. En collaboration avec les autorités judiciaires, l'ISPA recherchera cependant des solutions spécifiques afin de répondre à leurs attentes.

Outre la suppression de l'intimité au profit de l'intérêt général, il y a un certain nombre de motifs techniques qui justifient l'accès des ISP aux e-mails sous certaines conditions. Je pense ici à la facturation de certains services ainsi qu'aux interventions techniques qu'un ISP doit effectuer sur son réseau, sur ses serveurs, afin de garantir le bon fonctionnement du service.

La base légale nécessaire peut être trouvée dans la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, en particulier à l'article 109ter D et E.

Une des principales *key issues* concernant la loi relative à la criminalité informatique est que pour la première fois, les ISP se sont vu imposer l'obligation de conserver leurs données pendant une période minimum de 12 mois. Tel est du moins le principe puisqu'en exécution

Besluit duidelijk dient te bepalen welke data voor hoe lang bewaard moeten worden.

Om een rechtszekerheid te hebben als ISP is het belangrijk dat in detail bepaald wordt welke data juist bewaard moeten worden. Vanzelfsprekend dient eveneens gewezen te worden op het financiële aspect inzake de bewaring van gegevens alsook het feit dat een harmonisatie doorheen Europa op dit niveau noodzakelijk is.

Een ander punt dat ik reeds heb aangehaald is het feit dat er geen wettelijke regeling is inzake het afluisteren op het Internet. Daar ook dienen de financiële en technische aspecten niet uit het oog te worden verloren.

b) **Copyright**

Het is perfect mogelijk om illegale inhoud, in de zin van de auteurswet, over te maken. Ik denk daarbij aan muziek in MP3 formaat. Daarbij moet onderlijnd worden dat de techniek van MP3 alsdusdanig niet illegaal is, maar wel illegaal gekopieerde muziek. De verdeling ervan valt duidelijk onder de auteurswetten. Ik verwijs daarbij naar de Napster case in de Verenigde Staten.

Europa :

In Europa is de basistekst de Copyright richtlijn 2001/29EG.

Deze richtlijn is het resultaat van een lang en moeilijke strijd om te komen tot een evenwichtige balans tussen de rechthouders (artiesten, schrijvers, producenten, etc.) en andere personen die vrij toegang dienen te hebben tot deze beschermde werken zoals daar zijn de wetenschappelijke en de educatieve wereld, maar ook de ISPs.

Belangrijk is dat deze richtlijn het auteursrecht in de digitale tijd binnenbrengt. Het feit dat dergelijke beschermde werken op het internet terug te vinden zijn, betekent niet hierop het auteursrecht niet toepasselijk is.

Eén van de moeilijkste punten in de totstandkoming van deze richtlijn was het probleem van het «techical copying», het technisch kopiëren van dergelijke beschermde werken door de ISP. Ik verwijs hierbij naar het caching dat essentieel is voor de goede werking van het internet. Het betreft enkel maar het tijdelijk opslaan van deze werken in het kader van een technische process of een netwerk transmissie. Dit probleem was zo con-

de cette loi, un arrêté royal doit préciser clairement quelles données doivent être conservées et pour combien de temps.

Pour qu'un ISP bénéficie d'une sécurité juridique, il importe de préciser exactement quelles données doivent être conservées. Il faut évidemment aussi signaler l'aspect financier de la conservation de données ainsi que la nécessité d'une harmonisation au niveau européen en la matière.

Un autre problème auquel j'ai déjà fait allusion est l'absence de réglementation légale en matière d'écoute sur internet. Là aussi il ne faut pas perdre de vue les aspects financiers et techniques.

b) **Copyright**

Il est parfaitement possible de transmettre un contenu illégal au sens de la loi sur le droit d'auteur. Je pense à la musique en format MP3. Il faut souligner que ce qui est illégal, ce n'est pas la technique du MP3 en tant que telle mais la musique copiée illégalement, dont la diffusion tombe clairement dans le champ d'application des lois sur le droit d'auteur. Je me réfère à cet égard au cas Napster aux États-Unis.

Europe :

En Europe, le texte de base est la directive 2001/29EC relative au copyright.

Cette directive résulte d'un long et difficile combat pour atteindre un équilibre entre les détenteurs du droit (artistes, écrivains, producteurs, etc.) et d'autres personnes qui doivent pouvoir accéder librement à ces travaux protégés, comme le monde scientifique et éducatif et les ISP.

Ce qui importe est que cette directive introduise le droit d'auteur dans le monde numérique. Le fait que des travaux protégés se retrouvent sur internet ne signifie pas que le droit d'auteur n'est pas d'application.

Un des points les plus difficiles dans l'élaboration de cette directive fut le « *technical copying* », la copie technique de travaux protégés par les ISP. Je me réfère ici au stockage des pages téléchargées (*caching),* essentiel au bon fonctionnement d'internet. Cela concerne uniquement le stockage temporaire de ces travaux dans le cadre d'un processus technique ou d'une transmission par réseau. Ce problème était tellement controversé

troversieel dat artiesten naar het Europees Parlement zijn gegaan om hun eigen zaak te bepleiten.

Maar de richtlijn heeft rechtszekerheid geboden voor de ISPs: technical copying dient gedoogd te worden.

België :

De basistekst in België is de Wet van 30 juni 1994 betreffende het auteursrecht en de naburige rechten in de context van de ontwikkeling van de informatiemaatschappij.

In het kader van de omzetting van de copyright directive in Belgisch recht ligt op dit moment een Wetsvoorstel van Senator Monfils ter tafel.

c) **E-commerce : direct marketing via e-mail**

Sinds ettelijke jaren wordt benadrukt dat e-commerce gestimuleerd moet worden. Het is dan ook noodzakelijk de beste oplossing te vinden voor de Europese en Belgische bedrijven.

Zoals reeds eerder aangehaald, dient het opt-in / opt-out debat inzake commerciële e-mails ook hier gesitueerd te worden.

Ik herhaal dat op dit moment in België een regeling ter tafel ligt die afwijkt van de Europese regeling die een concurrentieel nadeel met zich zal meebrengen voor de Belgische bedrijven.

Europa :

De basistekst in Europa is de Richtlijn 2000/31/EC inzake e-commerce alsook de richtlijn inzake het verwerken van persoonsgegevens in de electronische communicatiesector.

Wat de richtlijn e-commerce betreft die eind januari 2002 in Belgisch recht dient omgezet te worden, zijn er twee belangrijke punten die ik verder kort wens uiteen te zetten.

Enerzijds was er het debat rond de aansprakelijkheid van de ISP.

De richtlijn maakt een onderscheid tussen de ISP als de éénvoudige «carrier» en de ISP in een «hosting» rol.

que les artistes sont allés plaider leur dossier devant le Parlement européen.

Mais la directive a offert une sécurité juridique aux ISP : il faut que le copiage technique soit toléré.

Belgique :

En Belgique, le texte de base est la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins dans le contexte du développement de la société de l'information.

Le sénateur Monfils a déposé une proposition de loi visant à transposer la directive relative au copyright en droit belge.

c) **Commerce électronique : marketing direct par e-mail**

Depuis des années, on insiste sur l'importance de promouvoir le commerce électronique. Il est donc indispensable de trouver la meilleure solution pour les entreprises européennes et belges.

Comme on l'a vu, c'est là aussi qu'il faut situer le débat *opt-in/opt-out* relatif aux e-mails commerciaux.

Je répète qu'un règlement est actuellement en préparation en Belgique, lequel s'écarte de la réglementation européenne qui entraînera un préjudice concurrentiel aux entreprises belges.

Europe :

En Europe, les textes de base sont la directive 2000/31/EC relative au commerce électronique ainsi que la directive relative au traitement des données personnelles dans le secteur de la communication électronique.

Je tiens à développer brièvement deux points importants de la directive relative au commerce électronique qui doit être transposée en droit belge fin janvier 2002.

D'une part, il y a eu le débat relatif à la responsabilité des ISP.

La directive fait une distinction entre l'ISP en tant que simple « *carrier* » et l'ISP dans un rôle de « *hosting* ».

a) ISP als «carrier», «mere conduit»

In dat geval is de ISP niet aansprakelijk voor illegale inhoud indien:

– hij de transmissie/verzending niet initieert;
– hij de ontvanger van de verzending niet selecteert;
– hij de informatie die verzonden wordt, niet wijzigt.

Een voorbeeld is een klant die een MP3 downloadt via Napster; in dat geval is de ISP louter de carrier; de MP3 file staat niet op zijn server, maar op de computer van de klant.

b) ISP in de «hosting» rol

In dat geval is er een beperkte aansprakelijkheid voor de ISP in die zin dat hij niet aansprakelijk zal zijn:

– indien hij geen kennis heeft of kan hebben van de illegal inhoud die hij host;
– indien hij van zodra hij in kennis wordt gesteld van de illegale inhoud, onmiddellijk de nodige maatregelen neemt om de toegang tot de informatie te beperken.

In feite introduceert deze richtlijn de «Notice and Take Down Procedure» die sinds enige tijd gebruikt wordt in de Verenigde Staten.

Wat belangrijk is, is dat de ISP niet verplicht is om de inhoud pro-actief te screenen.

Het samenwerkingsprotocol dat ISPA op 28 mei 1999 met de Ministers van Telecommunicatie en Justitie heeft gesloten, is volledig in lijn met de e-commerce directive en is eigenlijk een voorloper in België.

Enerzijds was er de aansprakelijkheid van de ISP, anderzijds regelt deze richtlijn eveneens de toepasselijke wet in het kader van e-commerce en dit is de wet van het land van oorsprong, men hanteert dan ook het country-of-origin principe. Er zijn een aantal uitzonderingen zoals in het kader van het auteursrecht of contractuele aspecten in het kader van consumentencontracten.

België :

Op dit moment is er een wetsvoorstel in voorbereiding dat de Europese richtlijn e-commerce zal omzetten.

Een ander belangrijk element in de ontwikkeling van de electronisch handel is de erkenning van de digitale handtekening.

a) L'ISP simple porteur, « *mere conduit* », n'est pas responsable des contenus illégaux :

– s'il n'amorce pas la transmission/envoi ;
– s'il ne sélectionne pas le destinataire de l'envoi;
– s'il ne modifie pas les informations expédiées.

Prenons le cas d'un client qui charge un MP3 via Napster. Dans ce cas, l'ISP est simplement le *carrier*; le fichier MP3 n'est pas sur son serveur mais sur l'ordinateur du client.

b) Lorsque l'ISP est « hosting », sa responsabilité de l'ISP est limitée en ce sens qu'il ne sera pas responsable :

– s'il n'a pas ou ne peut avoir connaissance du contenu illégal qu'il héberge;
– si, dès qu'il est mis au courant du contenu illégal, il prend immédiatement les mesures qui s'imposent pour limiter l'accès aux informations.

En fait, cette directive introduit la *Notice and Take Down Procedure* utilisée depuis peu aux États-Unis.

Ce qui est très important, c'est que l'ISP n'a pas l'obligation d'afficher le contenu à l'écran de manière proactive.

Le protocole de coopération auquel a souscrit l'ISPA, le 28 mai 1999, ainsi que les ministres des Télécommunications et de la Justice, se situe tout à fait dans le droit fil de la directive relative au commerce électronique et est en fait un précurseur en Belgique.

D'une part, il y avait la responsabilité de l'ISP et, d'autre part, cette directive règle également la loi applicable dans le cadre du commerce électronique qui est la loi du pays d'origine; on manipule par conséquent le principe du *country-of-origin.* Il y a un certain nombre d'exceptions comme dans le cadre du droit d'auteur ou d'aspects contractuels dans le cadre des contrats de consommateurs.

Belgique :

Un projet de loi qui transposera la directive européenne relative au commerce électronique est actuellement en préparation.

La signature numérique est un autre élément important du développement du commerce électronique.

Europa :

De basistekst in Europa is de richtlijn in verband met de digitale handtekening 1999/93/EC.

4. *Besluit :*

Tot besluit wil ik u de volgende kerngedachten meegeven.

Internet in het algemeen, e-mail in het bijzonder is niets meer of niet minder dan een communicatiemiddel zoals éénder ander communicatiemiddel, de telefoon bijvoorbeeld. Dit betekent dat een dergelijk communicatiemiddel ingepast kan worden in de bestaande wetgeving. Zoals reeds gesteld, is de richtlijn inzake copyright directive daarvan een bewijs.

Er is echter één groot verschil, één bepaalde karakteristiek welke het internet onderscheidt van andere communicatiemiddelen. Het is grensoverschrijvend, het internet kent geen landsgrenzen. De world wide web is in één millieseconde over de hele wereld bereikbaar.

Een globale, mondiale aanpak is noodzakelijk.

Wat onze nationale wetgeving betreft, kunnen we besluiten dat de belangrijkste problemen inzake het internet aan bod komen of aan bod zullen komen in de nabije toekomst.

Ook al kan je het internet en e-mail beschouwen als een communicatiemiddel zoals elk ander, menen wij dat het belangrijk is dat de technische aspecten/beperkingen van de marktspelers in de internet sector in aanmerking worden genomen bij het opstellen van de diverse wetteksten.

Wetten zijn daar om de maatschappij te regelen en te beschermen, maar mogen op geen enkele wijze een maatschappij beperken in zijn ontwikkeling.

Een voorbeeld zal dit verduidelijken :

In het kader van de auteurswet moet de technische noodzaak van de proxy servers in beschouwing worden genomen. Zonder proxy is er geen internet meer.

Wat de aansprakelijkheden betreft is er één belangrijk punt dat éénvoudig verwoord kan worden als «don't shoot the ISP», maar «trust de ISP» of ook «don't shoot the messenger». Het is correct dat de ISP, als tussenpersoon steeds gemakkelijk te identificeren is, gemak-

Europe :

En Europe, le texte de base est la directive 1999/93/EC relative à la signature numérique.

4. *Conclusion :*

En conclusion, je voudrais vous livrer les réflexions suivantes.

L'internet en général et l'e-mail en particulier ne sont ni plus ni moins qu'un moyen de communication semblable à tout autre moyen de communication, comme le téléphone par exemple. Un tel moyen de communication peut dès lors être intégré dans la législation existante. Comme nous l'avons déjà dit, la directive sur les droits d'auteur en est la preuve.

Il existe toutefois une grande différence, une caractéristique précise qui distingue l'internet des autres moyens de communication. Il est transfrontalier, il ne connaît pas les frontières nationales. Le *world wide web* est accessible en une milliseconde dans le monde entier.

Une approche globale, mondiale s'impose.

Quant à notre législation nationale, nous pouvons conclure que les principaux problèmes concernant l'internet se posent et se poseront dans un futur proche.

Même si nous pouvons considérer l'internet et l'e-mail comme un moyen de communication comme un autre, nous estimons qu'il importe de tenir compte des aspects et des limites techniques des acteurs du marché dans le secteur de l'internet lors de l'élaboration des divers textes légaux.

Les lois sont là pour régler et protéger la société mais ne peuvent en aucune façon entraver son développement.

Un exemple éclairera ce point de vue :

La loi sur les droits d'auteur doit tenir compte de la nécessité technique des serveurs proxy ou serveurs mandataires. Sans serveur proxy, il n'y a plus d'internet.

Quant aux responsabilités, il faut relever un point capital qu'on peut formuler simplement en ces termes : «don't shoot the ISP» mais «trust the ISP» ou encore «don't shoot the messenger». Il est vrai qu'en tant qu'intermédiaire, le fournisseur d'accès à l'internet est tou-

kelijker dan een gebruiker vooral wanneer het om strafbare feiten gaat. Indien steeds meer verplichtingen op de ISP worden gelegd, heeft dit een financiële impact waardoor prijzen stijgen en alsdusdanig de ontwikkeling van de e-maatschappij in de weg zal staan. Dit is vanzelfsprekend de extreme maar realistische situatie. Ik verwijs in dat kader naar het Koninklijk Besluit in uitvoering van «de tapwet». Op dit moment werd het afluisteren van internet niet in dit Koninklijk Besluit opgenomen om twee belangrijke redenen: enerzijds bestaat er nog geen technisch pasklare oplossing; anderzijds betekent dit dat als een ISP dergelijke maatregelen op dit moment zou moeten treffen, dit hoge kosten met zich meebrengt, die spijtig genoeg voor een groot gedeelte door de ISP gedragen moeten worden. Het ziet er naar uit dat de investeringskosten in het algemeen in het kader van deze problematiek ten laste vallen van de operator. De impact van een dergelijke verplichting werd door ons geschat op 15 tot 20 mio euro voor alle ISPs in België.

Om het nog duidelijker te stellen, wil ik de volgende vergelijking maken: de autoproducenten investeren in de veiligheid van auto's, niet in de veiligheid van wegen, noch in politie. Dit komt toe aan de maatschappij «at large».

Om al deze redenen, meent ISPA, dat de wetgever een duidelijk en juist inzicht in het Internet gebeuren moet hebben. Wij zijn vanzelfsprekend steeds bereid u daarbij van dienst te zijn op welke wijze ook. Deze conferentie is daarvan een goed voorbeeld en ik wens jullie daarvoor nogmaals in naam van ISPA te bedanken.

Indien de wet een goede bescherming biedt alsook de ontwikkeling van de e-maatschapppij bewerkstelligt waarbij elke partij, gebruiker, ISP etc. aan bod komt op een harmonieuze wijze, beschouwen wij dit als een werkelijk success. In bepaalde gevallen kan de co-regulerende aanpak, zoals die op dit moment bestaat in het kader van illegale inhoud, doorgetrokken worden. Een belangrijk voordeel van dergelijke samenwerkingsprotocollen is dat zij op een redelijk eenvoudige wijze aangepast kunnen worden aan de snelle evolutie van het Internet.

jours facilement identifiable, plus facilement qu'un utilisateur, surtout lorsqu'il s'agit de faits délictueux. Si de plus en plus d'obligations lui sont imposées, cela a une incidence financière car les prix augmentent, ce qui entravera le développement de la société électronique. Il s'agit bien sûr de la situation extrême mais elle est réaliste. Dans ce cadre, je renvoie à l'arrêté royal pris en exécution de ce que nous avions coutume d'appeler la loi sur les écoutes téléphoniques. À ce moment-là, les écoutes sur internet n'ont pas été reprises dans l'arrêté royal pour deux raisons importantes : d'une part, il n'existe pas encore de solution prête à l'emploi et, d'autre part, si un fournisseur d'accès devait prendre de telles mesures à l'heure actuelle, il en résulterait des frais élevés qu'il devrait malheureusement largement supporter lui-même. Il semble que les coûts d'investissement en général soient, dans le cadre de cette problématique, à charge de l'opérateur. Nous avons estimé l'impact d'une telle obligation à 15 à 20 millions d'euros pour tous les fournisseurs d'accès actifs en Belgique.

Pour être encore plus précis, je voudrais faire la comparaison suivante : les constructeurs automobiles investissent dans la sécurité des voitures, non dans la sécurité des routes, ni dans la police. Ce devoir incombe à la société dans son ensemble.

Pour toutes ces raisons, l'ISPA estime que le législateur doit avoir une idée précise et exacte du phénomène de l'internet. Nous sommes bien sûr toujours disposés à offrir nos services à cet égard, de quelque manière que ce soit. La conférence d'aujourd'hui en est un bon exemple et je souhaite vous en remercier une fois encore au nom de l'ISPA.

Si la loi offre une bonne protection et favorise le développement de la société électronique, chacune des parties, utilisateur, fournisseur d'accès, etc., pouvant entrer en ligne de compte de manière harmonieuse, nous considérerons cela comme un véritable succès. L'approche corégulatrice telle qu'elle existe aujourd'hui dans le cadre du contenu illégal peut être appliquée dans certains cas. Un avantage important de tels protocoles de coopération est qu'ils peuvent être adaptés assez simplement à l'évolution rapide de l'internet.

E. E-mail en privacy, standpunt van de Commissie voor de bescherming van de persoonlijke levenssfeer : Uiteenzetting van de heer P. Thomas, voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer

Heren Voorzitters, Dames en Heren,

Ik ben zeer vereerd en tevreden om het woord te mogen nemen voor dit hoog gezelschap ter gelegenheid van dit Forum.

Uiteraard is het zo dat de Commissie zich, al dan niet op eigen initiatief, reeds meermaals over verschillende thema's van deze middag heeft kunnen uitspreken.

Bijvoorbeeld, betreffende Echelon. De Echelon problematiek staat vermeld op het programma van vandaag in verband met de veiligheidsaspecten.

Wel, de Commissie had reeds in 1998 alle informatie waarover zij beschikte aan de Minister van Justitie laten bezorgen, en dit op een vraag die de Minister haar gesteld had.

Zij heeft ook haar informaticus deskundige ter beschikking gesteld van het Vast Comité I om het in staat te stellen een verslag uit te brengen ter attentie van de Commissie belast met zijn parlementaire begeleiding.

Zij nam ook het initiatief een debat over Echelon te laten ontstaan binnen de werkgroep die op Europees niveau de vertegenwoordigers van de nationale privacy controle- en adviesautoriteiten samenbrengt.

.

Op 15 juni 2001 werd de voorzitter van de Commissie over deze problematiek gehoord door de Commissie belast met de parlementaire begeleiding van het Vast Comité I .

Na de gebeurtenissen van 11 september 2001 in New York plaatsten de vertegenwoordigers van de Belgische Privacycommissie het probleem op de agenda van voornoemde Europese werkgroep van de interceptie van telecommunicatieverkeer in het kader van militaire operaties buiten de Europese Unie, waaraan EU-landen evenwel deelnemen, met andere woorden Echelons op kleinere schaal. De bedoeling is zeker niet trachten te interfereren in politieke beslissingen en nog minder als het gaat om 's werelds veiligheid. Maar dat is het nu wel : het moeten politieke beslissingen zijn, genomen door democratische instellingen, en

E. Courrier électronique et la vie rivée, point de vue de la commission pour la protection de la vie privée : Expose de M. P. Thomas, president de la commission pour la Protection de la Vie privée

Messieurs les Présidents, mesdames et messieurs,

Je suis très honoré et heureux de pouvoir prendre la parole devant cette haute assemblée à l'occasion de ce forum.

La Commission a déjà pu se prononcer maintes fois, parfois de sa propre initiative, sur différents thèmes abordés cet après-midi.

Sur le système Echelon par exemple. La question Echelon figure au programme de ce jour dans le volet consacré aux aspects sécuritaires.

Or en 1998 déjà, la Commission avait transmis au ministre de la Justice toute l'information dont elle disposait et ce en réponse à une question qu'il lui avait posée.

Elle a également mis son expert informaticien à la disposition du Comité permanent de contrôle des services de renseignements et de sécurité afin de permettre à celui-ci de rédiger un rapport à l'attention de la Commission chargée de son suivi parlementaire.

Elle a aussi pris l'initiative de lancer un débat sur le système Echelon au sein du groupe de travail réunissant, au niveau européen, les représentants des autorités nationales chargées de contrôler le respect de la vie privée et de formuler des avis en la matière.

Le 15 juin 2001, le président de la Commission a été entendu au sujet de cette question par la Commission chargée du suivi parlementaire du Comité R.

Après les événements survenus à New York le 11 septembre 2001, les représentants de la Commission belge pour la protection de la vie privée ont inscrit à l'ordre du jour du groupe de travail européen précité le problème de l'interception de télécommunications dans le cadre d'opérations militaires menées en dehors de l'Union européenne avec la participation de pays de l'UE , autrement dit, de systèmes Echelon à plus petite échelle. L'objectif n'est certainement pas de tenter d'interférer dans les décisions politiques, d'autant moins lorsqu'il s'agit de la sécurité mondiale. Toutefois, il doit s'agir de décisions politiques prises par des institu-

niet enkel door de uitvoerende macht zoals initiatieven van politionele of militaire staffen ter plekke, buiten willen of weten van de betrokken parlementen. Dit initiatief zou opnieuw moeten leiden tot een gemeenschappelijk standpunt en een aanbeveling naar alle EU-regeringen toe of zelfs tot een behandeling door het Europees Parlement zelf, zoals dit al het geval is wat Echelon betreft.

Op 22 november 2000 heeft de Commissie in verband met e-commerce, op eigen initiatief een advies uitgebracht waarin gewezen werd op de juridische principes die toepasselijk zijn op «cookies» en op «spamming». De Commissie geeft in haar advies de voorkeur aan opt-in- boven opt-outmailing. De kwestie van de transmissie van data uit niet-EU-landen wordt eveneens behandeld conform de Europese richtlijn 95/46 van 24 oktober 1995. De transmissie van die data is krachtens deze richtlijn, en dus krachtens de wetgeving van elke EU-lidstaat, enkel toegestaan naar landen waar de gegevens op een even afdoende manier beschermd worden als in Europa.

Alleen : als het meer bepaald om de Verenigde Staten gaat, waar noch een vergelijkbare wetgeving, noch een gelijkwaardige commissie bestaat, rijst er een probleem.

De Europese richtlijn zegt dat de nationale commissies oordelen of de gegevens in kwestie al dan niet verzonden mogen worden, daarbij gebeurlijk steunend op contractuele bepalingen (zie bv. de zogenaamde «safe harbours», Amerikaanse bedrijven die met de Europese Commissie afspraken gemaakt hebben over respect van de privacy). Rest de vraag hoe klachten kunnen worden ingediend tegen misbruiken in een land waar er geen privacycommissie is …

Tot slot moet worden opgemerkt dat het ondertekenen van gedragscodes sterk wordt aangemoedigd. De Belgische Commissie heeft een werkgroep ingesteld waarin ze zich samen met de marketingsector over een aanpassing van de gedragscode van die sector aan de elektronische technologie wil buigen.

In verband met het toezicht door de werkgever op het gebruik van het computersysteem op het werk, heeft de Commissie zich op eigen initiatief twee keer over deze kwestie uitgesproken.

In haar advies van 3 april 2000 worden alle juridische teksten genoemd die op deze thematiek toepasselijk zijn in het kader van de arbeidsverhouding, en wordt, met betrekking tot de controle van de elektroni-

tions démocratiques et pas seulement par le pouvoir exécutif, comme certaines initiatives prises par des états-majors policiers ou militaires à l'insu des parlements concernés. Cette initiative devrait de nouveau conduire à un point de vue commun et à une recommandation de tous les gouvernements des pays de l'UE ou même à un examen au sein du Parlement européen lui-même, comme c'est déjà le cas pour le système Echelon.

En ce qui concerne le commerce électronique, la Commission a émis, le 22 novembre 2000, un avis d'initiative rappelant les principes juridiques applicables aux «cookies», au «spamming» et préconisant la solution de l'opt in de préférence à l'opt out. La question de la transmission des données recueillies dans des pays hors Union européenne est également traitée conformément à la Directive européenne 95/46 du 24 octobre 1995. Cette transmission n'est permise par la Directive, et donc par chacune des législations des pays membres de l'Union, que vers des pays disposant d'une protection des données équivalente à la protection en Europe.

Problème quand il s'agit, par exemple, du grand frère américain, qui n'a ni législation, ni commission équivalente.

La Directive européenne a voulu que les Commissions nationales apprécient si les données peuvent être transférées ou non, éventuellement sur base de dispositions contractuelles (comme les Safe harbors élaborés par certaines firmes US avec la Commission européenne). Reste la question des recours en cas d'abus dans un pays sans commission…

Enfin, des codes de conduite sont fortement encouragés. La Commission belge a pris l'initiative d'un groupe de travail avec le secteur marketing en vue d'adapter le code de conduite de ce secteur aux techniques électroniques.

En ce qui concerne la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail: la Commission s'est prononcée d'initiative à ce sujet à deux reprises.

L'avis du 3 avril 2000 rappelait l'ensemble des textes juridiques applicables en l'espèce dans le cadre de la relation de travail ainsi que les principes de transparence, de proportionnalité et de nécessité concernant

sche post en de door de werknemer bezochte websites, gewezen op de principes van transparantie, evenredigheid en noodzakelijkheid. Ik had het voorrecht Kamervoorzitter De Croo in hoogsteigen persoon dit advies te horen toelichten. Ik had het zelf niet beter gekund.

In een ander op eigen initiatief uitgebracht advies van 8 oktober 2001 werd, naar aanleiding van de indiening van een wetsvoorstel over deze problematiek door senator Destexhe, eerstgenoemd advies nog eens onder de aandacht gebracht.

U kan deze teksten eveneens raadplegen op de website van de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (http://www.privacy.fgov.be) of op de website van groep 29 van de Europese Commissie (http://www.europa.eu.int/comm/internal_market/fr/dataprot/index.htm).

Mijn bedoeling voor vandaag was dus enkel het werk van de Commissie wat toe te lichten, in het algemeen, en meer in het bijzonder aangaande de thema's van vandaag. Geen sprake dus van de documentatie die u gekregen heeft te ontleden, maar misschien wel er toe aan te zetten een nieuw Forum te organiseren, ditmaal speciaal toegewijd aan de problematiek e-mail of internet en de privacybescherming.

Zou dit de intentie kunnen zijn van het Parlement, zoals uitdrukkelijk gewenst en zelfs aangekondigd door de heer Voorzitter De Croo, staat de Commissie helemaal ter beschikking.

Mijnheer de voorzitter, beste vrienden, het is altijd moeilijk om de rol van socioloog te spelen na alle technische beschouwingen die hier aan bod zijn gekomen. De socioloog is degene die «een bijrol vertolkt» en het noodzakelijkerwijze moet hebben over meer algemene en minder technische aspecten en zijn werk moet trachten te doen, namelijk een kritische – wat niet wil zeggen vernietigende – visie op de uiteengezette problemen aanreiken en er op zo groot mogelijke schaal verslag over uitbrengen.

F. **De sociaal-economische impact van e-mail : Uiteenzetting van de Professor Claude Javeau (ULB):**

Volgens Steiner zouden wij vandaag met het internet de derde culturele revolutie doormaken. De eerste culturele revolutie was niet het schrift, zoals men doorgaans aanneemt, maar wel de uitvinding van de rol, toen de Egyptenaren zich ervan bewust geworden zijn

le contrôle du courrier électronique et des sites consultés par le travailleur. J'ai eu le privilège d'entendre cet avis présenté par M. le Président De Croo en personne. Je ne pourrais mieux faire.

Cet avis a été rappelé dans un autre avis d'initiative, émis le 8 octobre 2001, à l'occasion du dépôt d'une proposition de loi du Sénateur Destexhe, sur le sujet.

Enfin, tous ces textes sont consultables : tantôt sur le site de la Commission belge pour la protection de la vie privée : **http://www.privacy.fgov.be** ; tantôt sur celui du groupe 29 de la Commission européenne : http://www.europa.eu.int/comm/internal_market/fr/dataprot/index.htm

Mon intention aujourd'hui était donc seulement de présenter brièvement le travail de la Commission en général et plus particulièrement en ce qui concerne les thèmes abordés aujourd'hui. Il n'est donc pas question d'analyser la documentation que vous avez reçue mais peut-être d'inciter à organiser un nouveau forum, consacré cette fois spécifiquement à la problématique de l'e-mail ou de l'internet et à la protection de la vie privée.

Si telle pouvait être l'intention du Parlement, comme l'a souhaité ouvertement et même annoncé le président Herman De Croo, la Commission serait à son entière disposition.

Monsieur le président, chers amis, il est toujours difficile de jouer le rôle du sociologue après tant de considérations techniques. Le sociologue est celui qui vient en «vedette américaine» et doit nécessairement parler de choses plus générales, moins techniques, et essayer de faire son métier, c'est-à-dire proposer une vision critique — ce qui ne veut pas dire destructrice — des problèmes exposés et les rapporter à la plus grande totalité possible.

F. **Les répercussions socio-économiques du courrier électronique, exposé du Professeur Claude Javeau (ULB) :**

Selon Steiner, nous assisterions à l'heure actuelle avec l'Internet à la troisième révolution culturelle. La première révolution culturelle n'a pas été l'écriture, comme on le croit toujours, mais bien l'invention du rouleau, lorsque les Egyptiens se sont avisés que l'on

dat men ook op andere dingen dan stenen kon schrijven en dat wat op schrift stond bijgevolg kon worden overgedragen. De tweede culturele revolutie is te danken aan Gutenberg en de boekdrukkunst. De derde revolutie zou dan het internet zijn, dat de wijze waarop de mens zich tot de wereld verhoudt – trouwens via een wijziging van de manier waarop het woord zich tot de wereld verhoudt – beetje bij beetje grondig zal wijzigen.

Volgens Steiner betreft het een ware revolutie. Mijn vriend Dominique Volton van het CNRS is het daarmee niet eens ; voor hem is het louter een nieuwe vorm van individualisme. Misschien heeft Dominique nog niet ingezien dat het individualisme is veranderd. Het lijdt hoe dan ook geen twijfel dat in onze wereld de communicatie – of de «municatie» want vaak ontbreekt de «com» – de fysieke verplaatsing vervangt. Anders dan bij de telefoon, behalve wanneer men notities neemt, betreft het een vorm van communicatie die sporen nalaat op verscheidene plaatsen, die doorgaans niet kunnen worden gelokaliseerd.

Men moet die uitvinding opnieuw situeren in het allesomvattend kader van wat Heidegger «de onderwerping van de wereld door de techniek» noemt. De mens vervangt een wereld die door de natuur wordt gedomineerd door een wereld die door de machine wordt gedomineerd. Die door de machine gedomineerde wereld zal zorgen voor een wijziging van de betrekkingen tussen de mensen, van de verhoudingen tussen de mensen en wereld, en dat via een wijziging van de manier waarop het woord zich tot de wereld verhoudt. Om het op een zeer geleerde manier te zeggen , de «phusis» moet het afleggen tegen de «tekhnê» teneinde de logos te beheren. Er was met andere woorden in het begin de wereld van het woord dat zich verbreidde op de agora of het forum, dat nadien op schrift werd gesteld en zich verspreidde via het boek – dat wonderbaarlijk emancipatie-instrument. En vandaag worden wij geconfronteerd met een gefragmenteerde wereld : e-mail en internet zijn vormen van «traceerbare» en vereenvoudigde instantcommunicatie.

Ik vind het nuttig om even bij die drie begrippen te blijven stilstaan.

Vooreerst instantcommunicatie. Vanuit de hele wereld en op elk ogenblik kan men ons, met eventuele als attachments bijgevoegde documenten en de bijbehorende virussen, berichten toesturen en ons vragen die te beantwoorden. De tekst wordt een beeld op het scherm : in een wereld die door het beeld wordt gedomineerd, wordt zelfs de tekst een beeld of in zekere mate, een icoon!

pouvait écrire ailleurs que sur des pierres et ont ainsi permis le transport de l'écrit. La deuxième révolution culturelle est due à Gutenberg et à l'imprimerie. Et la troisième serait ainsi l'Internet qui, petit à petit, modifiera considérablement le rapport de l'homme au monde — à travers d'ailleurs la modification du rapport du mot au monde.

Steiner pense qu'il s'agit d'une révolution. Mon ami Dominique Volton du CNRS à Paris dit que non et considère que ce n'est qu'une nouvelle application de l'individualisme. Peut-être Dominique n'a-t-il pas vu que l'individualisme a changé. En tout cas, il est certain que dans notre monde, la communication — ou la «*munication*» car il manque souvent le «*com*» — supplante le déplacement physique. Dorénavant, à la différence du téléphone sauf si on prend note, il s'agira d'une communication qui laisse des traces à différents endroits que l'on ne peut généralement pas localiser.

On doit replacer cette invention dans le cadre global de ce que Heidegger a appelé «*l'arraisonnement du monde par la technique*». L'homme remplace un monde dominé par la nature par un monde dominé par la machine. Ce monde dominé par la machine va entraîner une modification des rapports entre les hommes, des rapports des hommes au monde, par la modification des rapports entre le mot et le monde. Pour le dire de manière très savante, le *phusis* cède à la *tekhnê* pour gérer le *logos*. Dit autrement, il y a d'abord eu le monde de la parole qui circulait sur l'agora ou le forum, qui a été ensuite écrite et a circulé dans le livre — prodigieux instrument d'émancipation. Et aujourd'hui, il y a un monde éclaté: l'e-mail et l'Internet sont des formes de communication instantanée, «traçable» et simplifiée.

Ces trois caractéristiques me semblent mériter une attention soutenue.

Tout d'abord, communication instantanée. Du monde entier, à tout moment, avec d'éventuels *attachements* de documents et les virus qui les accompagnent, nous pouvons être sollicités à recevoir un message et à en envoyer un en réponse. Le texte devient une image sur écran: dans un monde dominé par l'image, même le texte devient une image ou dans une certaine mesure, une icône!

Voorts gaat het om «traceerbare» communicatie : zij laat sporen na. Al degenen die de kwestie van de telefoontap hebben onderzocht, zullen wellicht nog meer moeilijkheden hebben met het onderzoek naar de «traceerbaarheid» van de berichten op het «web». Zij laat sporen na voor al wie er naar zoekt. Al die «Sherlock Holmes» die overal opduiken, zelfs tot in de kleine toestellen in onze kantoren!

Ten slotte gaat het ook om «vereenvoudigde» communicatie. Ik word almaar meer overspoeld door «e-mails» van studenten en plaats vraagtekens bij de vereenvoudigde taal die daarbij wordt gebruikt. Er wordt immers een heel andere taal gehanteerd die nauwer aanleunt bij de gesproken taal, met afkortingen, wat een vals gevoel van familiariteit in de hand werkt. De boodschappen die de heer Roth mij heeft toegezonden kon ik soms moeilijk ontcijferen – zoals «bav» voor «bien à vous». Zij doen soms wat denken aan de bizarre boodschappen die adolescenten via hun gsm uitwisselen : de zogenaamde «sms'jes» die opgesteld zijn in een zeer bizarre taal die zelfs ouders die bij de tijd zijn niet altijd kunnen begrijpen. Maar opgelet : die communicatie heeft niet enkel een ludieke dimensie; zij werkt ook een vals gevoel van familiariteit in de hand die de neiging heeft voorbij te gaan aan elke vorm van – functionele, natuurlijke of andere – hiërarchie, maar die de hiërarchie van de instrumentele deskundigheid niet vervangt.

Sommigen zullen er zich immers beter van bedienen dan anderen; sommigen zullen een aangepaste taal uitvinden en anderen, die van de technologie verstoken blijven, zullen voortdurend achterop blijven hinken omdat zij niet begrijpen waarover het precies gaat.

Daarbij komt nog het bestaan van «hyperlinks» die het mogelijk maken samengestelde berichten op te stellen waarbij geput kan worden uit een grote verscheidenheid van bronnen. Zo kan ik u morgen een bericht sturen met een stukje tekst van mezelf, passages uit het werk van Shakespeare, fragmenten uit de wetgeving, stukjes tekst van Jacques Mercier, stukjes van om het even welke reclameboodschap,… en het doen voorkomen alsof het een boodschap van mijzelf betreft, in een zodanige mengelmoes dat de verdedigers van de auteursrechten volledig het spoor bijster zullen raken!

Die samengestelde boodschappen zorgen ervoor dat wij ons nu bevinden in een soort van wazige wereld waar niemand nog uit wijs geraakt omdat de diverse grenzen tussen wat wordt gecreëerd, gereconstrueerd, geplagieerd, uitgevonden, verdraaid of vervalst zullen vervagen.

Ensuite, il s'agit d'une communication «traçable»: elle laisse des traces. Tous ceux qui se sont penchés sur les écoutes téléphoniques auront sans doute encore beaucoup plus de difficultés à se pencher sur la «traçabilité» des messages sur la «toile». Elle laisse des traces à l'usage de tous ceux qui en cherchent. Tous ces «Sherlock Holmes» qui sont en train de s'installer jusqu'à l'intérieur même des petites machines que nous avons sur nos bureaux!

Enfin, c'est en même temps une communication simplifiée. Etant de plus en plus inondé de «*courriel*» envoyé par mes étudiants, je suis fortement interpellé de constater l'utilisation d'un langage simplifié. Le langage est modifié: il se rapproche du langage parlé, avec des abréviations, créant ainsi une fausse familiarité. Les messages que m'a envoyés M. Roth m'ont parfois posé quelques problèmes de traduction — par exemple, «bav» pour «bien à vous». Cela rappelle un peu ces messages curieux que les adolescents s'envoient sur leur «G»: les «sms» écrits dans un langage très curieux que les parents, même au courant, ne parviennent pas à comprendre. Mais méfions-nous: ce n'est pas uniquement une dimension ludique; cela crée une fausse familiarité qui aurait tendance à passer au-dessus de toute hiérarchie, fonctionnelle, naturelle ou autre, mais qui ne remplace pas la hiérarchie des compétences instrumentales.

En effet, certains s'en serviront toujours mieux que d'autres; certains inventeront des langages appropriés; certains laisseront sur place les «démunis» de la technologie qui courront toujours après pour essayer de comprendre de quoi il s'agit.

Ajoutons à cela l'existence des «hyper-liens» qui permettent la constitution de messages composites à partir d'une multiplicité considérable de sources. Ainsi, je peux vous envoyer demain un message dans lequel il y a des morceaux de moi, des morceaux de Shakespeare, des morceaux du législateur, des morceaux de Jacques Mercier, des morceaux d'une publicité quelconque, … et le faire passer pour un message à moi dans un mélange tel que les défenseurs des droits d'auteurs vont y perdre non pas leur latin, mais leur «courriel»!

Cette constitution de messages composites fait que nous nous trouvons désormais dans une sorte de flou flexible au sein duquel un chat ne reconnaît plus ses jeunes parce que les différentes frontières entre ce qui est créé, recréé, plagié, inventé, détourné ou trafiqué ne sont plus très visibles.

In feite hebben internet en de bijbehorende e-mail in de menselijke communicatie voor een buitengewone paradox gezorgd.

Enerzijds onstaat er een soort van hyperindividualisering aangezien men ons op elk ogenblik in - zoals de vorige spreker het uitdrukte – onze «huiskamer» kan bereiken. Wij zijn niet langer beschermd tegen mogelijke indringers, behalve natuurlijk door de machine uit te schakelen, wat altijd mogelijk is, maar weinig mensen zetten hun draagbare telefoon af. Wij zijn in feite allemaal knechten geworden die men op elk moment kan opbellen. Er is dus sprake van een individualisering, maar die paradoxaal genoeg de anonimiteit in de hand werkt. Wie schrijft? Wie ontvangt? Wie verspreidt?

Daarnet werd duidelijk aangetoond dat ondanks alle beschermingsmaatregelen, mogelijke vervalsingen op het stuk van de verzending of de ontvangst nooit uitgesloten zijn. Ik kan iemand immers niet echt beletten over mijn schouder mee te lezen wat er op mijn scherm staat. En ik zal hoe dan ook nooit zeker weten wie mij dat bericht heeft gestuurd. Ik kan evenmin met zekerheid weten welke weg dat bericht heeft afgelegd en wie het voor of na mij heeft gelezen.

U zegt mij dat zulks mogelijk is met andere systemen. Uiteraard, maar hier krijgt dat een heel universele dimensie.

Een en ander kadert in de postmoderniteit. De postmoderniteit of wat men de gevorderde moderniteit noemt, bestaat erin de kernbegrippen van de moderniteit over te nemen, namelijk de beweging en de onzekerheid – wij leven in een wereld vol onzekerheden – waaraan men een specifieke reflexiviteit toevoegt, die van elk van ons kleine experts maakt op een bepaald gebied op grond van een deskundigheid die wij doorgaans uit de media halen en die dus niet altijd juist is omdat men een en ander niet volledig beheerst, zodanig dat degenen die niet over die deskundigheid beschikken dreigen te lijden onder wat Voorzitter De Croo daarnet het «neo-analfabetisme» heeft genoemd. De mensen die daarvan verstoken zullen blijven en die niet aan die specifieke reflexiviteit zullen kunnen deelnemen dreigen een nieuwe soort – ditmaal culturele – verstotenen te worden die de kloof tussen henzelf en die vorm van communicatie almaar groter zien worden.

Daarbij komt dat de virtualiteit het dreigt te halen op de realiteit – virtuele ontvanger en virtuele afzender kunnen naast de reële ontvanger en de reële afzender bestaan – een beetje zoals de pers. Het lijdt geen twij-

En fait, l'internet et l'e-mail qui se branche sur lui ont créé, dans la communication humaine, un paradoxe extraordinaire.

D'un côté, on a à faire à une espèce d'hyperindividualisation puisque nous pouvons être atteints à tout moment au cœur de notre foyer – tout à l'heure, le préopinant a parlé de «huiskamer». Nous ne sommes plus protégés contre une irruption possible, sauf évidemment en éteignant la machine, ce qui est toujours une possibilité, mais peu de gens éteignent leur téléphone portable. En fait, nous sommes tous devenus des domestiques que l'on peut appeler à tout moment. Donc, une individualisation mais qui a ce paradoxe d'engendrer l'anonymat. Qui écrit? Qui reçoit? Qui fait circuler?

On a bien montré tout à l'heure qu'en dépit de toutes les protections que l'on pouvait prendre, on n'est jamais à l'abri d'une falsification de l'expédition ou de la réception. Après tout, on ne peut réellement empêcher quelqu'un de lire mon écran par dessus mon épaule. Et, après tout, je ne serai jamais certain de la personne qui a envoyé le message. Je ne suis pas non plus certain des endroits par où il est passé et je ne serai d'ailleurs jamais certain des personnes qui l'auront lu avant ou après moi.

Vous me dites c'est possible dans d'autres systèmes. Bien sûr, mais celui-ci le rend particulièrement universel.

Il s'inscrit dans la postmodernité. La postmodernité ou ce qu'on appelle la surmodernité, la modernité avancée, consiste à reprendre les éléments fondamentaux de la modernité, c'est-à-dire le mouvement plus l'incertitude – nous sommes dans un monde d'incertitudes – auquel on ajoute une réflexivité spécifique, celle qui fait de chacun de nous des petits experts de quelque chose à partir d'une compétence qui nous vient généralement des médias, donc, qui n'est pas tout à fait juste, qui n'est pas tout à fait dominée, à telle enseigne que ceux qui ne bénéficient pas de ces expertises risquent de souffrir de ce que le Président De Croo a appelé tout à l'heure «le néo-analphabétisme». Les gens qui en seront exclus et qui ne pourront pas participer à cette réflexivité spécifique risquent de constituer une nouvelle espèce d'exclus, culturels cette fois, qui risquent d'être rejetés de plus en plus loin du monde de la communication.

Ajoutons à cela que la virtualité risque de l'emporter sur la réalité – destinataire virtuel et expéditeur virtuel peuvent cohabiter avec destinataire réel et expéditeur réel – un peu comme la presse. Quand on voit un jour-

fel dat een krant voor virtuele lezers is bestemd – de krant weet niet door wie ze wordt gelezen– en de mensen die de artikels in de krant ondertekenen kunnen ook virtuele journalisten zijn –agentschappen worden overgenomen, informatie wordt vervalst, enz.

Hier gaat het om een gepersonaliseerde krant die bij mij terechtkomt en waarvan ik nooit zal weten in hoeverre de berichten met de werkelijkheid overeenstemmen. Wij leven trouwens in een wereld waar de realiteit volledig in twijfel moet worden getrokken. Is men er echt zeker van dat Bin Laden bestaat of betreft het een nieuwe stunt van Walt Disney?

Welke gevaren kunnen daarin schuilen?

Het eerste gevaar is uiteraard dat van het almaar verder uiteenvallen van de maatschappij.

Ook de maatschappij is aan paradoxale tendensen onderworpen. Enerzijds gaat zij op in almaar grotere gehelen, waarvan de onlangs geïntroduceerde euro één van de symbolen is. Driehonderd miljoen Europeanen gebruiken nu dezelfde munt en blijken dat met een intelligentie te doen die de besluitvormers nooit hadden vermoed. Tegelijkertijd, zoals Jean-François Kahn in het jongste hoofdartikel van «Marianne» stelde, ontstaat er momenteel een soort tribalisme, een terugplooien op pseudo-gemeenschappen. Ik neem niet het voorbeeld van België, dat zou immers moeilijk zijn omdat het woord «gemeenschappen» hier bijzondere connotaties heeft, maar wel van Frankrijk, waar men Fransman is, maar ook almaar meer Bask die Baskisch spreekt, Bretoen die Bretoens spreekt, Elzasser die Elzassisch spreekt en daarbovenop, is men ook nog heteroseksueel of homoseksueel, atheïst of gelovig, men draagt een hoofddoek of men draagt er geen. Op die manier worden er kleine stammen gecreëerd die door de huidige communicatiemethoden als het ware dreigen te worden versterkt. Dat houdt risico's in, omdat de sociale samenhang zich beperkt tot een inflatoire communicatie via de technische onpersoonlijkheid, de onpersoonlijkheid van het toestel.

Dat is zeer mooi – persoonlijk heb ik die instrumenten altijd zeer lelijk gevonden – maar het heeft niet de schoonheid van een handschrift, zelfs al zijn het hanepoten, dat de expressie is van de persoon zoals die echt is in zijn grafologie, met zijn handtekening, de krabbels die hij of zij in de marge maakt. Het ene zal het andere nooit vervangen. Stel u een partituur van Johann Sebastian Bach voor die er zo zou uitzien. Dat zou geen Bach meer zijn. Dat systeem zal bovendien – en de wetgever lijkt daar oog voor te hebben – een hele reeks politionele of andere controles mogelijk

nal, il est certain que celui-ci est expédié à des lecteurs virtuels – le journal ne sait pas qui le lit - et les gens qui signent dans le journal peuvent aussi être des journalistes virtuels – reprise d'agence, traficotage d'informations, etc…

Ici, il s'agit d'un journal personnalisé qui arrive chez moi et dont je ne saurai jamais quel est le degré exact de réalité. Nous sommes d'ailleurs dans un monde dont la réalité devient tout à fait soupçonnable. Est-on vraiment certain que Ben Laden existe ou est-ce un nouveau coup de Walt Disney?

Quels sont les dangers que l'on peut voir?

Le premier danger est évidemment celui de l'éclatement de plus en plus prononcé du corps social.

Le corps social est, lui aussi, soumis à des tendances paradoxales. D'un côté, il se fond dans des ensembles de plus en plus grands, dont l'euro, que l'on vient d'introduire, est l'un des emblèmes. Nous sommes désormais trois cent millions d'européens à utiliser la même monnaie et cela, semble-t-il, avec une intelligence que ceux qui l'ont introduite n'avaient pas soupçonnée. En même temps, comme le signalait remarquablement Jean-François Kahn dans le dernier éditorial de «Marianne», nous sommes en train de connaître une espèce de tribalisme, de repli sur des pseudo-communautés. Pour ne pas prendre l'exemple de la Belgique parce que ce serait difficile, d'autant que le mot «communauté» a ici des sens bizarres, si nous prenons la France où on est Français mais où de plus en plus de Basques parlent basque, où de Bretons parlent breton, où d'Alsaciens parlent alsacien et, en plus de cela, on est hétérosexuel ou homosexuel, laïque ou religieux, on porte le foulard ou on ne le porte pas. Tout cela créant de petites unités tribales que, dans une certaine mesure, les modes actuels de communication risquent de renforcer. C'est un risque, le lien social se réduisant à une communication inflatoire via la froideur technique, la froideur de l'appareil.

C'est très joli – personnellement j'ai toujours trouvé ces instruments très vilains – mais cela n'a pas la beauté d'une écriture, même d'une écriture de cochon, où vous trouvez la personne telle qu'elle est en elle-même dans sa graphologie, avec sa signature, les petits dessins qu'elle peut faire dans la marge. Cela ne la remplacera jamais. Imaginez une partition de Jean-Sébastien Bach fabriquée avec ceci. Ce ne serait plus du Bach. En plus, ce système va permettre – et le législateur semble y être tout à fait attentif – une multiplicité de contrôles policiers ou autres soit par la publicité, la marchan-

maken, ofwel door de reclame, de merchandising, de uiteenlopende propaganda – ik wil er geen doekjes om winden – die ons dreigen op te sluiten in een keurslijf dat – herinner u de passage dienaangaande uit de eerste toespraak van de huidige Koning tijdens zijn eedaflegging – door Alexis de Tocqueville op het einde van «La démocratie en Amérique» (1835) zo goed werd beschreven. Het betrof als het ware een profetie. Ik verwijs naar die tekst die sindsdien de koninklijke goedkeuring heeft verkregen.

Het web vervangt het sociaal contract. Dat is het tweede punt waarmee ik wil eindigen. Dat punt heeft betrekking op de verhouding tussen de invoering van die nieuwe technologieën en de democratie zoals wij die voorstaan.

De democratie – en het is uiteraard niet aan parlementsleden dat ik moet uitleggen waarover het gaat – behelst het bestaan van een openbare plaats waar de diverse passies met elkaar in evenwicht worden gehouden. Eénieder heeft een passie, die zich vertaalt in een politiek programma en op de openbare plaats aanvaardt men dat die uiteenlopende passies onderling worden getoetst, eventueel met elkaar in botsing komen, zonder dat één ervan het recht heeft te beweren dat zij de enig mogelijke is.

U weet dat in een democratie twee plaatsen centraal staan, vooreerst *de agora* waar de mensen komen spreken over publieke, privé- en semi-privé aangelegenheden en daarnaast, wat men noemt de *basilica*, namelijk de plaats waar de assemblee beraadslaagt, stemt en beslissingen neemt, wat een lichamelijke, menselijke aanwezigheid impliceert van individuen die oog in oog met elkaar staan.

Thans dreigt de verspreiding van dit soort instrumenten – als men daar niet voor oplet natuurlijk – tot gevolg te hebben dat die openbare plaats volledig wordt geprivatiseerd.

De openbare plaats is grotendeels al tot een metafoor verworden maar bestaat nog altijd, met name in Parlementen, plaatsen waar men spreekt, en die, in bepaalde hypertechnocratische utopieën, dreigt te worden vervangen door die talloze kleine terminals die bij ons thuis zullen geïnstalleerd zijn, waaraan wij slechts van 's morgens tot s' avonds hoeven plaats te nemen en via welke men ons gewoon van alles en nog wat zal vragen.

Persoonlijk denk ik dat de democratie berust op een aantal plechtige rituelen waarvan de stemming wellicht het essentiële is.

De stemming, waaraan, zoals u weet, het merendeel van onze landgenoten met enige tegenzin deelneemt, is een plechtige daad die wij stellen door ons te verplaatsen – en dat is misschien de reden waarom de

dise, les propagandes diverses – je n'ai pas peur des gros mots – qui risquent de nous enfermer dans un carcan si bien décrit - rappelez-vous que cela a été un extrait du premier discours du Roi actuel lors de sa prestation de serment – par Alexis de Tocqueville dans le final de «La démocratie en Amérique» (1835). Prémonitoire. Je vous renvoie à ce texte qui a, depuis lors, reçu l'assentiment royal.

La toile remplace le contrat social. C'est le deuxième point sur lequel je voudrais terminer. C'est le point qui a trait au rapport entre la mise en place de ces nouvelles technologies et la démocratie telle que nous essayons de la connaître.

La démocratie – ce n'est évidemment pas à des parlementaires que je dois dire de quoi il s'agit – consiste en l'existence d'un espace public au sein duquel se compensent les passions singulières. Chacun a une passion qui s'exprime par un programme politique et, dans l'espace public, on accepte que ces différentes passions se rencontrent, éventuellement s'opposent, sans qu'aucune ait le droit de prétendre être la seule possible.

Vous savez que la démocratie se compose de deux endroits. D'abord un agora où les gens viennent parler de choses publiques, privées et semi-privées et, à côté, ce qu'on appelle la basilique qui est le lieu où l'assemblée délibère, vote et prend des décisions, ce qui implique une présence corporelle, humaine, de face à face des individus.

A l'heure actuelle, la diffusion d'instruments de ce genre – si on n'y prend garde bien entendu – risque de voir l'espace public se privatiser complètement.

L'espace public, en grande partie déjà réduit à une métaphore, mais qui existe encore, notamment dans des Parlements, des endroits où l'on parle, risque d'être, dans certaines utopies hypertechnocratiques, remplacé par cette multiplicité de petits terminaux que nous aurons chez nous, devant lesquels nous n'aurons plus qu'à rester assis du matin au soir et par lesquels nous pourrons simplement être appelés à répondre à des sollicitations diverses.

Personnellement, je crois que la démocratie repose sur une série de rituels solennels dont le vote est sans doute l'essentiel.

Le vote, auquel, vous le savez, la plupart de nos concitoyens se rendent en traînant les pieds, est un acte solennel que nous reproduisons en nous déplaçant – et c'est peut-être la raison pour laquelle le vote

elektronische stemming geen goed idee is. Op basis daarvan wordt er een nieuw sociaal contract gesloten en ondertekend. Dat is een metafoor, maar wel een sterke metafoor waarop alle democratische systemen stoelen. Fysiek, op de dag van de stemming, zoals later, tijdens de parlementaire debatten, de openbare plaats fysiek zichtbaar wordt.

Als men de bevraging via internet combineert met iets waar ik persoonlijk helemaal niet van hou, maar waar ik niettemin een specialist van ben, namelijk de opiniepeilingen, bevindt de burger zich niet meer op de openbare plaats en verliezen wij dat plechtig karakter. Wij bagatelliseren de politiek op een onherstelbare manier. Het volstaat dat een vraag wordt gesteld en wij zullen moeten antwoorden. Men zal ons misschien op de een of andere manier verplichten te antwoorden. Dat is in mijn ogen niet het beleid dat in een democratie moet worden gevoerd. Volgens mij komen in een democratie de mensen bijeen met een mandaat dat zij moeten uitoefenen en dat wij hen voor een beperkte tijd verlenen, na afloop waarvan zij rekenschap moeten afleggen. En nadien wordt dat mandaat al of niet vernieuwd.

Het is een droom. Dat systeem zou minder kosten. In plaats dat zes tot zeven miljoen Belgen of 200 miljoen Europeanen zich moeten verplaatsen, ondervraagt men om de twee weken 1500 burgers. Wil u dat het loon van de gedelegeerd-bestuurder van De Post wordt opgetrokken? Mogen universiteitsprofessoren meer verdienen? Ja! Wil u dat er vaker fora plaatsvinden? Ja! Maar het is niet enkel door te antwoorden op een ludieke of commerciële vraag of door te chatten dat de democratie vorm krijgt, zoniet dreigt de burger te verworden tot wat Copernicus van hem heeft willen maken – excuseer mij voor deze polemiek – en wat trouwens een stroom van protest heeft veroorzaakt, onder meer van mijzelf, namelijk een «cliënt». Wij zijn geen cliënten. Wij zijn de mede-eigenaars van het huis België en die mede-eigendom wordt niet ingevuld via elektronische boodschappen.

Tot slot zal ik u een zinnetje voorlezen van een van mijn eminente collega's, Luc Wilkin, professor aan de Solvay-handelsschool van de ULB, dat in Espace de liberté, tijdschrift van het Centre d'action laïque in juli 2001 werd gepubliceerd.

Hij zegt het volgende : «Het dominante vertoog op internet is een vertoog dat zichzelf als voor de hand liggend beschouwt en dat aanzet tot gedragingen waarvan men niet altijd de gevolgen inschat bij gebrek aan

électronique n'est pas une bonne idée. A partir de là se renégocie, se resigne le contrat social. C'est une métaphore mais une métaphore vive sur laquelle tous les systèmes démocratiques reposent. Physiquement, le jour du vote, comme plus tard, physiquement, le jour des débats parlementaires, l'espace public se donne à voir.

Si l'on combine la sollicitation par l'Internet à quelque chose que personnellement je n'aime pas du tout, et pourtant j'en suis un spécialiste, le sondage, le citoyen n'est plus dans l'espace public, et nous perdons cette solennité. Nous banalisons le politique de manière irrémédiable. Il suffit de poser une question et nous devrons répondre. Peut-être serons-nous obligés de répondre, d'une manière ou d'une autre. Je ne crois pas que ce soit cela la politique en démocratie. Je crois que la démocratie ce sont des gens qui se réunissent avec un mandat qu'ils doivent assumer, que nous leur donnons pour un temps limité et au bout duquel ils nous rendent compte. Et alors, nous les renouvelons ou nous ne les renouvelons pas.

C'est un rêve. Cela coûterait moins cher. Au lieu de faire déplacer six ou sept millions de belges ou deux cents millions d'européens, on en interroge 1500 tous les quinze jours. Voulez-vous encore augmenter le salaire de l'administrateur des postes? Voulez-vous augmenter le salaire des professeurs d'université? Oui! Voulez-vous que se tiennent plus souvent des forums? Oui! Mais ce n'est pas justement en répondant à une sollicitation ludique, commerciale ou à un échange de tchats que la démocratie s'installe sinon nous risquons de voir le citoyen se réduire à ce que Copernic a voulu faire de lui – excusez-moi cette polémique – et qui a fait dresser pas mal de boucliers, dont le mien, un «client». Nous ne sommes pas des clients. Nous sommes les copropriétaires de la maison Belgique et la copropriété ne se fait pas à travers des appareillages électroniques.

Pour terminer, je vais vous lire une petite phrase d'un de mes éminents collègues, Luc Wilkin, qui est professeur à l'École de commerce, dite Solvay à l'ULB, parue dans l'Espace de liberté, journal du centre d'action laïque, en juillet 2001.

Il dit ceci : «Le discours dominant sur l'Internet est un discours d'évidence qui impulse des comportements dont ceux qui les adoptent ne mesurent pas toujours les effets faute de repères ou d'analyse. Son usage

houvast of analyse. Een doordacht en verantwoord gebruik ervan berust op een analysevermogen waarbij, naast recht en techniek, een belangrijke rol is weggelegd voor deontologie en ethiek als onderzoeksdisciplines».

Ik dank u voor uw aandacht.

G. **Paneldebat**

De heer Peter Vanhoutte, voorzitter : Ik dank u voor deze hoogst interessante uiteenzetting.

Dan is het nu tijd om het debat te openen met de zaal. Er werden vele aspecten aangekaart. Tegenover u zit een panel van ter zake uiterst kundige mensen. Wie vragen wil stellen, krijgt het woord.

De heer Rudi Roth : Ik ben vermoedelijk het panellid dat juridisch het minst beslagen is. Ik verzoek u dan ook om, net als al mijn advocaten, mijn eventuele fouten door de vingers te zien.

Er is inderdaad een koninklijk besluit betreffende de telefoontap in de maak, ter aanvulling van de wet. Het ministerie van Telecommunicatie en dat van Justitie leggen er op dit moment de laatste hand aan. U moet immers weten dat de kabinetten in deze het heft in handen hebben.

Wij hopen dat dit koninklijk besluit eind januari, begin februari zal worden goedgekeurd. Volgens ons gaat het immers om de privacy op het werk. Hoewel wij op bepaalde vlakken met de politie samenwerken, zijn alle wettelijke voorwaarden nog niet helemaal duidelijk. Welke gegevens moeten we bewaren? Hoe lang moeten we ze bewaren? Mevrouw Mermans heeft hierover meer uitleg gegeven. Hier duikt nog een ander element op dat bij het probleem van de bescherming van de privacy komt. Het probleem van de telefoontap en controle wordt ook aangekaart, evenals onrechtstreeks dat van de privacy op het werk. Het gaat hier immers om het aftappen van telefoongesprekken en het opsporen van informatie, of dit nu bij een internetprovider of elders gebeurt. Dat kadert uiteraard in een strafrechtelijke procedure en vereist een normaal bevelschrift van een onderzoeksrechter.

Ik hoop hiermee een antwoord te hebben gegeven op een aantal van uw vragen.

De heer Thibault Verbiest, voorzitter van het Observatorium van de Rechten op het Internet: Mijnheer de voorzitter, ik zou graag een vraag stellen en een opmerking maken.

raisonné et responsable repose sur une capacité d'analyse dans laquelle la déontologie et l'éthique, comme disciplines de recherche, ont un rôle important à jouer au même titre que le droit et la technique».

Je vous remercie pour votre attention.

G. **Débat du panel**

M. Peter Vanhoutte, Président : Je vous remercie pour cet exposé très intéressant.

Nous allons maintenant ouvrir le débat avec la salle. De nombreux aspects ont été abordés. Vous avez devant vous un panel extrêmement compétent. Si vous voulez poser des questions, la parole vous appartient.

M. Rudi Roth : Je suis sans doute ici la personne qui possède le moins de connaissance d'ordre juridique. Vous excuserez donc, à l 'instar de tous mes avocats, d'éventuelles erreurs que je pourrais commettre.

Un arrêté royal sur les écoutes téléphoniques est effectivement en préparation pour compléter cette loi.. Il est actuellement finalisé par le ministère des Télécommunications et celui de la Justice. Il faut, en effet, savoir que cela se joue au niveau des cabinets.

Nous espérons que cet arrêté royal passera fin janvier, début février. En effet, selon nous, il en va de la sécurité dans le travail. Si nous coopérons dans certains domaines avec la police, toutes les conditions légales ne sont toutefois pas tout à fait précises. Quelles données doit-on garder? Combien de temps doit-on les garder? Mme Mermans a donné des explications à ce sujet. Il y a là un élément qui vient compléter le problème de la vie privée. Le problème des écoutes et de la surveillance est également évoqué ainsi qu'indirectement celui du travail. En effet, il s'agit-là d'écoutes ou de recherches d'informations que ce soit chez un fournisseur Internet ou ailleurs. Cela se situe bien entendu toujours dans un cadre pénal avec un juge d'instruction et les demandes normales.

J'espère ainsi avoir répondu à certaines de vos questions.

M. Thibault Verbiest, président de l'observatoire de l'Internet: Monsieur le président, je voudrais poser une question et formuler une remarque.

We hebben het uitgebreid gehad over cyber-controle, met andere woorden over de controle van elektronische berichten op het werk. Tijdens de gesprekken stond de bescherming van de privacy centraal. Dat is belangrijk, want de privacy op kantoor heeft een fundamentele juridische dimensie. Maar, tenzij ik me vergis, heb ik niets gehoord over mogelijke hervormingen van andere bepalingen uit ons wettenarsenaal die rechtstreeks betrekking hebben op cyber-controle, van de bepalingen uit het Strafwetboek en van de wet van 1991 op de hervorming van de overheidsbedrijven die de vertrouwelijkheid van elektronische correspondentie garanderen.

Aangezien wij ons hier in een parlementaire assemblee bevinden, wil ik opmerken dat ik persoonlijk van mening ben dat de hervorming van de regelgeving betreffende de bescherming van de privacy niet nodig is. De commissie voor de bescherming van de persoonlijke levenssfeer, waarvan de voorzitter hier vandaag tot ons groot genoegen het woord heeft genomen, heeft reeds een advies uitgebracht. Onder voorbehoud van de Europese hervormingen is het juridisch kader van de bescherming van de privacy vandaag voldoende afgebakend. Het fundamentele debat betreft echter de hervorming van het Strafwetboek en de wet van 1991 die, als we ze strikt toepassen, momenteel gewoonweg de wettelijkheid van elk elektronisch controlesysteem op het werk ondermijnen.

De heer Peter Vanhoutte, volksvertegenwoordiger (AGALEV-ECOLO): Betreffende het principe van de cyber-controle kan het koninklijk besluit, waarvan ik wel het bestaan ken maar niet de precieze tekst, het probleem niet oplossen. Hier zal het parlement werk van moeten maken. Dat lijkt mij absoluut noodzakelijk.

De heer Patrick Van Eecke: Goedenavond, ik ben Patrick Van Eecke van de universiteit van Leuven. Ik ben advocaat in Internetrecht. Ik heb een vraag voor de parlementsleden maar ook voor de vertegenwoordigers van ISPA.

Omwille van opsporingdoeleinden merk ik meer en meer dat de gerechtelijke autoriteiten medewerking eisen van Internet-toegangsleveranciers en aanhangende actoren. Daarmee gaan enorme kosten gepaard.

Lopen wij daarmee niet het risico dat alleen de grote spelers van toegangsdienstverlening tot het Internet overblijven en dat de kleine en middelgrote ondernemingen die toegang verlenen tot het Internet uit de boot vallen, omdat zij die infrastructurele aanpassingen niet kunnen doorvoeren?

On a beaucoup parlé de cyber-surveillance autrement dit de la surveillance des courriers électroniques sur le lieu de travail. On a également beaucoup axé la discussion sur la vie privée. C'est important car la vie privée au bureau est une dimension juridique fondamentale. Mais, sauf erreur de ma part, je n'ai pas entendu de développements sur la réforme d'autres dispositions de notre arsenal juridique concernant directement la cyber-surveillance, des dispositions issues du code pénal et de la loi de 1991 sur la réforme des entreprises publiques qui garantissent le secret des correspondances électroniques.

Comme nous nous trouvons dans une enceinte parlementaire, je voulais faire remarquer que la réforme de la vie privée ne me semble pas, à titre personnel, nécessaire. En effet, la commission pour la vie privée, dont le président nous a fait le plaisir d'intervenir aujourd'hui, a déjà rendu un avis. Par conséquent, le cadre juridique sur la vie privée, réserve faite des réformes européennes, est suffisamment balisé aujourd'hui. Par contre, le débat fondamental a trait à la réforme du code pénal et la loi de 1991 qui, lorsqu'on les applique de manière rigoureuse empêchent tout simplement la légalité de tout système de surveillance électronique sur le lieu de travail aujourd'hui.

M. Peter Vanhoutte, député (AGALEV-ECOLO): Sur le principe même de la cyber-surveillance, l'arrêté royal, dont je connais l'existence sans en avoir pris connaissance, ne pourra pas régler le problème. C'est le parlement qui devra s'en saisir. Cela me semble indispensable.

M. Patrick Van Eecke : Bonsoir, je suis Patrick Van Eecke de l'Université de Louvain. Je suis avocat, spécialisé en droit de l'internet. J'ai une question à adresser aux parlementaires mais aussi aux représentants de l'ISPA.

Je remarque de plus en plus que pour rechercher des délits, les autorités judiciaires exigent la collaboration de fournisseurs d'accès à l'internet et d'acteurs connexes. Cela entraîne des frais énormes.

Ne risquons-nous pas ainsi de ne voir subsister que les grands fournisseurs d'accès à l'internet et de voir disparaître les petites et moyennes entreprises qui ne seraient pas en mesure d'adapter leur infrastructure ?

Heren en dames parlementsleden, wordt er gedacht aan een of andere manier van bijvoorbeeld sponsoring voor kleinere operatoren, die op die manier toch zouden kunnen blijven overleven zonder dat alle gelden in de aanpassing van de infrastructuur geïnvesteerd moeten worden voor gerechtelijke opsporingsmethodes?

De heer P. Thomas, voorzitter van de commissie voor de bescherming van de persoonlijke levenssfeer: Mijnheer de voorzitter, nu mij daartoe de gelegenheid wordt geboden, neem ik graag het woord.

Eerst en vooral sta ik volledig achter de suggestie van mijn collega en voorzitter, de heer Verbiest, die het parlement aanspoort om zijn verantwoordelijkheid op zich te nemen en een en ander niet over te laten aan de uitvoerende macht, de Koning en de bevoegde ministers.

Ik wil de woorden van de heer Verbiest projecteren op een onderwerp dat niet werd aangesneden en dat even belangrijk is, want het begint met een ‘e’, wat staat voor ‘elektronisch’, en ik bedoel niet de ‘e’ van ‘e-commerce’, maar van ‘e-government’.

Dat thema houdt niet alleen verband met het technisch aspect, maar vooral met het leven van de burger en de goede werking van de diverse overheidsinstellingen.

Betreffende e-government worden heel wat plannen gemaakt. Er doen allerhande geruchten de ronde, hier en daar duiken allerlei ideeën op. Men heeft het over de elektronische handtekening, een portaalsite en nog veel meer. Er wordt over gesproken in bepaalde perskringen en in de wandelgangen en ik vrees dat men bij het parlement geen allesomvattend ontwerp zal indienen dat het parlement precies in staat moet stellen een algemeen standpunt in te nemen over het ontwerp in zijn geheel en niet stap voor stap over de afzonderlijke onderdelen ervan.

Volgens mij is het absoluut noodzakelijk dat het parlement een totaalvisie ontwikkelt en zijn eigen keuzes maakt, die eventueel door de regering zijn ingegeven of worden aangereikt. Maar die keuzes en beslissingen moeten van het parlement zelf komen en niet van de regering, die de ene of de andere maatregel druppelsgewijs zou opdringen, maatregel die als ze afzonderlijk wordt genomen, op weinig weerstand zou stuiten. Nee, er is meer nodig dan dat. Ten slotte ben ik zo vrij het voorstel van mijn collega, voorzitter Verbiest, nog te verruimen om u ertoe aan te zetten daar werk van te maken.

De heer Peter Vanhoutte, voorzitter : Mijnheer Thomas, ik ben het geheel met u eens.

Mesdames et messieurs les parlementaires, envisage-t-on, par exemple, de sponsoriser de l’une ou l’autre manière les plus petits opérateurs pour leur permettre de survivre sans devoir investir tous leurs moyens dans l’adaptation de l’infrastructure pour développer des méthodes d’investigations judiciaires ?

M. P. Thomas, président de la commission pour la Protection de la vie privée: Monsieur le président, je ne résisterai pas à la tentation de prononcer quelques mots, puisque l’occasion m’en est donnée.

Tout d’abord, j’appuie entièrement la suggestion que vous a faite mon collègue, M. le président Verbiest, pour inciter le parlement à prendre sa responsabilité et ne pas l’abandonner à l’Exécutif, au Roi ou aux ministres compétents.

Je voudrais transposer ce qui a été dit par M. Verbiest sur un thème qui n’a nullement été abordé et qui revêt toute son importance, puisqu’il commence par un «e» pour électronique et c’est le «e» non pas commerce mais le «e-government».

Ce thème concerne non seulement la technique mais surtout la vie du citoyen et la bonne marche des divers exécutifs.

Ce «e-government» fait l’objet de plusieurs projets. On entend des rumeurs, une esquisse par-ci, par-là, sur tantôt ceci, tantôt cela. On parle de signature électronique, d’un portail et d’autres choses. On en parle dans une certaine presse, dans les couloirs et je crains qu’on ne saisisse pas le parlement d’un projet tout à fait complet pour permettre à ce dernier de prendre une attitude globale et générale sur l’ensemble du projet et non pas successivement sur tel et tel volet.

Il est impératif, me semble-t-il que le parlement ait une vision globale et prenne des options qui sont les siennes, éventuellement initiées, suscitées par le gouvernement. Mais ces options, ces choix, ces décisions doivent émaner du parlement lui-même et non du gouvernement qui, par petites doses homéopathiques, vous distille, vous instille l’une ou l’autre mesure qui, prise séparément, serait aisément admise. Non, il faut davantage. Je me permets d’élargir encore la proposition de mon collègue, le président Verbiest, pour vous encourager à faire ce travail.

M. Peter Vanhoutte, président: Monsieur Thomas, je partage entièrement votre opinion.

Geachte collega's, ik dank u alle drie voor deze toelichting. Uit de onderscheiden uiteenzettingen blijkt dat het Parlement een specifieke opdracht te vervullen heeft die méér inhoudt dan het uitwerken van een technische of juridische regelgeving. Hier worden belangrijke vraagstukken, die rechtstreeks te maken hebben met de democratie en de persoonlijke levenssfeer, aan de orde gesteld. Het is onze taak op die kwesties in te gaan. Op dit colloquium werd het thema alvast ingeleid. Nu is het zaak het verder uit te diepen.

De heer Rudi Roth (ISPA): Ik dank Kamer en Senaat, en alle deelnemers aan dit colloquium. Wij hopen inderdaad dat er in het kielzog van dit forum nog andere activiteiten zullen worden georganiseerd. De heer Vanhoutte zal hier zo meteen nog op terugkomen. Wij zijn bereid volgend jaar opnieuw zo'n forumbijeenkomst te houden, over een meer specifieke thematiek. Wij wensen echter dat dat debat op uw initiatief op gang gebracht wordt.

Aangezien zowat iedereen met e-mail te maken krijgt, kon het debat van vandaag rekenen op een ruime belangstelling. Als we vandaag een debat hadden geopend over breedbandinternet, denk ik niet dat we ons in een grote opkomst hadden kunnen verheugen. E-mail is nu eenmaal een beter bekend fenomeen. Dat neemt echter niet weg dat het debat over breedbandinternet in België gevoerd moet worden. Het zal voor een andere keer zijn.

De heer Peter Vanhoutte, voorzitter : Zijn er nog vragen ?

In het Parlement hebben wij er alles aan gedaan om het debat op gang te brengen en aan de bevoegde commissie werd gevraagd om een debat te organiseren over e-governement, de nieuwe identiteitskaart en tal van initiatieven die tot doel hebben de benutting van informatica-infrastructuren op federaal niveau te optimaliseren, zoals dat eufemistisch heet. Er zijn veel vragen te stellen, met name over privacy.

Ik wil even terugkomen op de vraag die zonet gesteld is. Volgens mij is die vraag belangrijk. Anderzijds vind ik dat de overheid bijzonder terughoudend moet zijn voor de ondersteuning van deze of gene. Dat brengt ons namelijk in een straatje zonder einde.

Ik denk dat de gerechtelijke overheid erg terughoudend moet zijn in het opvragen van bepaalde informatie. Die maatregelen moeten volgens mij niet verder gaan. Soms heb ik de indruk dat de gerechtelijke instanties alle informatie willen bekomen, zoals de inhoud van de e-mails, wanneer en op welke wijze gecommuniceerd

Chers collègues, je vous remercie tous les trois pour cette intervention. Il résulte des différents exposés que le parlement a une mission particulière qui n'est pas simplement de prévoir une régulation technique ou juridique. Des questions importantes, qui touchent à la démocratie et à la vie privée, sont soulevées ici. Il nous appartient de les rencontrer. Ce colloque permet d'introduire le sujet. Il devra bien entendu être prolongé.

M. Rudi Roth (ISPA): Je remercie la Chambre et le Sénat, ainsi que tous les participants de ce colloque. Nous espérons effectivement qu'il sera suivi d'autres activités. M. Vanhoutte aura encore l'occasion d'en reparler. Nous sommes prêts à refaire cet exercice l'année prochaine, sur un débat plus pointu que celui d'aujourd'hui. Nous souhaitons que ce débat soit lancé à votre initiative.

Comme tout le monde est concerné par l'e-mail, le débat d'aujourd'hui intéressait bon nombre de gens. Si nous avions entamé un débat sur la large bande aujourd'hui, je ne pense pas que beaucoup de personnes seraient venues. L'e-mail est effectivement mieux connu. Cependant, le débat sur la large bande doit être ouvert en Belgique. Ce sera pour une autre fois.

M. Peter Vanhoutte, président : Y a-t-il encore d'autres questions ?

Au parlement, nous avons tout fait pour lancer le débat et avons demandé à la commission compétente d'organiser un débat sur l'administration électronique, la nouvelle carte d'identité et de nombreuses initiatives visant à optimiser l'utilisation des infrastructures informatiques au niveau fédéral, comme on le dit par euphémisme. Les questions sont nombreuses, notamment en ce qui concerne la vie privée.

Je voudrais revenir brièvement sur la question qui vient d'être posée. Selon moi, elle est importante. Il me semble par ailleurs que les autorités doivent être particulièrement réticentes à soutenir telle ou telle entreprise car cela déboucherait sur une impasse. .

Je pense que les autorités judiciaires doivent se montrer très réservées dans la demande de certaines informations. À mon sens, ces mesures ne doivent pas aller plus loin. J'ai parfois l'impression que les instances judiciaires veulent obtenir toute l'information, comme le contenu d'e-mails, et veulent savoir quand

is. Voor een onderzoeker is het natuurlijk erg aantrekkelijk om zo'n hele informatiepool vrij ter beschikking te krijgen. Met het oog op de privacy moet het Parlement zoeken naar een goed evenwicht tussen de vraag om informatie te verifiëren als er een bepaald misdrijf begaan zou zijn en het vrij ter beschikking stellen van informatie. Enkele opvragingen zullen strafrechtelijk gezien zeker noodzakelijk zijn. Ik ben er echter geen voorstander van om informatie en databases ter beschikking te houden zogauw gevraagd wordt om bepaalde informatie te onderzoeken. Ook De Post maakt geen kopie van elke langskomende brief om in een archief te steken, moest er ooit een onderzoek komen rond een bepaald thema. Ook de telefoondiensten doen dat niet. Voor zover ik mij de discussie in de Kamer herinner, hebben wij afgesproken dat de informatie voor de facturatie, die bewaard moeten worden wegens mogelijke bezwaren tegen de factuur, bewaard zou blijven gedurende een periode van minimum twaalf maanden. Niet méér informatie, ook niet minder. De minister heeft zich ertoe geëngageerd daarvan ook maar hoogstens twaalf maanden te maken. Verder gaan wij dus niet.

et de quelle manière se déroulent les communications. Pour un enquêteur, il est bien sûr très tentant de disposer librement d'un tel pool d'informations. Afin de protéger la vie privée, le parlement doit rechercher un bon équilibre entre la demande de vérification de l'information lorsqu'un certain délit est commis et la possibilité de disposer librement de l'information. Certaines demandes seront certes nécessaires du point de vue judiciaire. Je ne suis toutefois pas partisan de rendre l'information et les bases de données disponibles dès qu'une demande d'analyse de telle information est introduite. La Poste ne prend pas non plus une copie de chaque lettre qui passe par ses services pour en conserver la trace dans ses archives au cas où une enquête serait un jour menée sur un thème particulier. Les services téléphoniques ne le font pas davantage. Pour autant que je me rappelle la discussion à la Chambre, nous avons convenu que l'information destinée à la facturation, qui doit être conservée en raison des réclamations pouvant éventuellement être introduites contre la facture, serait conservée pendant une période de douze mois au moins. Il ne faut conserver ni plus ni moins d'informations. Le ministre s'est engagé à porter ce délai à douze mois maximum. Nous n'allons donc pas au-delà.

Er zijn geen bijkomende vragen meer.

Il n'y a plus d'autres questions.

Ik heb nog twee mededelingen.

J'ai encore deux communications à faire.

Ten eerste, het verslag van dit colloquium zal in de commissie voor Wetenschappelijke en Technologische Vraagstukken van de Kamer worden ingebracht als initiatiefrapport. Op basis van het debat van vandaag zullen wij in de commissie een aantal aanbevelingen trachten te formuleren, die in de Kamer opgenomen zullen worden.

D'une part, le compte rendu de ce colloque sera déposé à la Commission chargée des Questions scientifiques et technologiques de la Chambre comme rapport d'initiative. Sur la base du débat d'aujourd'hui, nous tenterons de formuler en commission quelques recommandations qui seront reprises à la Chambre.

Ten tweede, als u nog vragen zou hebben, kunt u daarmee terecht op een Nederlandstalig en een Franstalig e-mailadres dat wij vanaf morgen ter beschikking zullen stellen. Wij leven nu eenmaal in een tijdperk van Informatica- en Communicatietechnologie. Het zou vreemd zijn als u uw vragen alleen maar door een schrijven of een telefoonbericht naar de Kamer kwijt zou kunnen.

D'autre part, si vous souhaitiez encore poser des questions, vous pouvez les adresser par courrier électronique à une adresse e-mail francophone ou néerlandophone que nous mettrons à votre disposition. Nous vivons à une époque caractérisée par la technologie de l'information et de la communication. Il serait étrange que vous ne puissiez poser vos questions que par courrier postal ou par téléphone.

Het gaat om het volgende Nederlandstalig adres en de Franstalige tegenhanger voor de Kamer en het adres voor de Senaat:

ispaforum@dekamer.be
ispaforum@lachambre.be
ispaforum@senate.be

Les adresses francophone et néerlandophone de la Chambre et l'adresse du Sénat sont les suivantes :

ispaforum@lachambre.be
ispaforum@dekamer.be
ispaforum@senate.be

Via die adressen kunt u bijkomende vragen, bedenkingen twijfels kwijt. Wij hopen dat wij dat initiatief in de

Vous pouvez, via ces adresses, faire part des questions que vous vous posez encore, de vos réflexions,

toekomst verder kunnen uitbreiden tot een heus discussieforum voor parlementairen en geïnteresseerde technici, zodat de discussie on line gevoerd zal kunnen worden.

Dan rest mij nog de panelleden, die de onderscheiden aspecten van e-mail aan de hand van de gekozen thema's voortreffelijk hebben ingeleid, hartelijk te bedanken.

Slotwoord:

De heer Moens, Senator (sp.A): Geachte collega's, dames en heren, op deze forumbijeenkomst werd overduidelijk aangetoond hoezeer de werkmethoden en –instrumenten waarvan wij ons elke dag bedienen, geëvolueerd zijn en verder blijven evolueren.

Tegelijk worden de uitdagingen die vandaag onontkoombaar op de Belgische en Europese wetgever afkomen, scherp in het licht gesteld. Naast de bio-ethiek en de nieuwe economie vormen ook de nieuwe communicatiemiddelen een voor onze beschaving kenschetsend geworden maatschappelijk issue.

De snelle technische vooruitgang doet ons aloude, vast verankerde rechtsstelsel wankelen. Ik denk hier onder meer aan de nieuwe criminaliteitsvormen die ontstaan zijn, en aan het vrijwaren van het vertrouwelijke karakter van de elektronische post. Die ontwikkelingen nopen ons ertoe ons over nieuwe materies te buigen, na te denken over de rol van de wetgever ten aanzien van die voortdurende evolutie, en te innoveren.

De internationale dimensie van die verschijnselen biedt weliswaar waardevol vergelijkingsmateriaal, maar verzwaart tegelijk ook de taak van de wetgever. Die opdracht is des te zwaarder daar de technologische ontwikkeling, ongeacht de kwaliteit en het snelle verloop van het wetgevend werk, de wetgever steevast een stap voor blijft.

Wij danken de vereniging van internetaanbieders, de voorzitter van de Privacycommissie, en professor Javeau voor hun commentaar en toelichting op deze studiedag.

Ik durf aan te nemen dat voor de enkelingen onder u die nog niet de status van internaut genieten, de elektronische post in al zijn aspecten tenminste wat minder virtueel zal zijn.Voorts twijfel ik er niet aan of ieder onder u bij het behandelen van e-mailberichten voortaan

de vos doutes. Nous espérons que nous pourrons développer cette initiative à l'avenir pour en faire un véritable forum de discussion pour les parlementaires et les techniciens intéressés, de manière à permettre la discussion en ligne.

Il me reste à remercier très chaleureusement les membres du panel.

Conclusion:

M. Moens, Sénateur (sp.A): Chers collègues, mesdames et messieurs, l'initiative d'aujourd'hui illustre suffisamment combien les méthodes et les outils de travail dont nous nous servons quotidiennement ont évolué et continuent à évoluer.

En même temps, elles mettent en exergue les défis actuels que les législateurs, belge et européen doivent impérativement relever. En sus de la bioéthique et de la nouvelle économie, les nouveaux moyens de communication constituent en effet des enjeux de société cruciaux par lesquels notre civilisation se définit d'ores et déjà.

Le progrès technique rapide ébranle le système juridique solidement établi depuis très longtemps. Je me réfère entre autres exemples aux nouveaux types de délits qui sont commis, ainsi qu'à l'organisation et au maintien de la confidentialité du courrier électronique. Ces évolutions nous contraignent donc à étudier de nouvelles matières, à réfléchir au rôle du législateur par rapport à ces développements en mutation constante et à innover.

Le caractère international de ces phénomènes nous fournit certes de précieux outils de comparaison mais complique en même temps la tâche du législateur. Celle-ci est d'autant plus ardue que, quelle que soit la qualité et la célérité du travail législatif, les développements technologiques lui dament à chaque fois le pion.

Nous exprimons notre reconnaissance à l'association des fournisseurs de services informatiques, au président de la commission de la vie privée et au professeur Javeau pour les commentaires et les explications fournies tout au long de cette journée d'étude.

J'ose croire que pour les rares personnes parmi vous qui n'ont pas encore le statut d'internaute, le courrier électronique dans tous ses aspects sera au moins devenu un peu moins virtuel. Je ne doute pas par ailleurs qu'en traitant ses e-mails, chacun d'entre vous soit dé-

nog meer dan vroeger bewust zal zijn van de veiligheidsaspecten en risico's die hierbij aan de orde zijn.

Ik hoop dat het initiatief van vandaag slechts een begin is, en dat er volgend jaar opnieuw een dergelijk forum kan worden gehouden. Ook de federale overheid doet trouwens een duit in het zakje, onder meer met het door het ministerie van Economische Zaken, onder leiding van minister Picqué ingestelde Observatorium van de Rechten op het Internet.

Dames en heren, vooraleer af te sluiten wens ik u allen te danken voor uw belangstelling en medewerking tot het welslagen van het forum.Ik wens inzonderheid u, mijnheer Vanhoutte, te feliciteren. U hebt het idee voor de organisatie van het forum gelanceerd en u hebt het in samenwerking met ISPA concreet gestalte gegeven.

Ik dank ook de heer Istasse, die het debat met de hem eigen minzaamheid en kunde geleid heeft.

Ik nodig u allen uit de gedachtewisseling op een informele manier voort te zetten, tijdens de receptie waarop ik u bij deze inviteer.

De heer Peter Vanhoutte, voorzitter : Ik dank u, mijnheer Moens.

Ik heb nog een laatste verzoek. U heeft een evaluatieformulier ontvangen. Aangezien wij in het kader van het parlementaire werk een follow-up van dit colloquium beloofd hebben, willen wij u vragen dit formulier in te vullen, want die informatie zal ons zeker van dienst zijn. Ik nodig u uit op de receptie, en dank u voor uw aandacht.

sormais plus conscient qu'auparavant des aspects de sécurité et des risques en jeu.

Je souhaite que l'initiative d'aujourd'hui ne soit qu'un point de départ et qu'elle puisse être réitérée l'année prochaine. Elle côtoie celles organisées par les autorités fédérales parmi lesquelles je relève l'Observatoire internet organisé par le ministre de l'Economie, M. Picqué.

Mesdames, messieurs, avant de conclure, je voudrais vous remercier tous pour l'intérêt que vous avez porté à ce forum et pour votre collaboration à sa réussite. Je tiens en particulier à vous féliciter, Monsieur Vanhoutte. C'est vous qui avez lancé l'idée de l'organisation de ce forum et qui l'avez concrétisée en collaboration avec l'ISPA.

Je remercie également M. Istasse pour la conduite des débats. Vous avez assumé cette responsabilité avec l'amabilité et l'adresse qui sont les vôtres.

Je vous invite tous à prolonger les échanges, de façon informelle cette fois, au cours de la réception à laquelle je vous convie.

M. Peter Vanhoutte, président: Je vous remercie, monsieur Moens.

Je formule une dernière demande. Vous avez reçu un formulaire d'évaluation. Comme nous avons promis un suivi à ce colloque et également au cours des travaux parlementaires, nous vous demandons de remplir ce formulaire car cela nous sera très utile.Je vous convie à la réception et vous remercie de votre attention.

Lijst van de deelnemers/ Liste des participants

1. Parlementsleden – Membres des assemblées

1.1.Federale Assemblees – Assemblées fédérales :

Herman DE CROO, Voorzitter van de Kamer van volksvertegenwoordigers
Armand DE DECKER, Président du Sénat

Ludwig CALUWÉ, Gemeenschapssenator
Simonne CREYF, Kamerlid
Alain DESTEXHE, Sénateur
François ROELANTS du VIVIER, Sénateur
André GEENS, Senator
Zoë GENOT, députée
Gérard GOBERT, Membre de la Chambre
Jean-François ISTASSE, Sénateur
Anne-Marie LIZIN, Sénatrice
Jean-Pierre MALMENDIER, Sénateur
Guy MOENS, Senator
Fatma PEHLIVAN, Senatrice
Joke SCHAUVLIEGE, Kamerlid
Erika THIJS, Senatrice
Peter VANHOUTTE, Kamerlid
Vincent VAN QUICKENBORNE, Senator
Gerda VAN STEENBERGE, Senatrice
Wim VERREYCKEN, Senator
Geert VERSNICK, Kamerlid

1.2.Vlaams Parlement :

Carl DECALUWÉ, Vlaams volksvertegenwoordiger
Peter DE RIDDER, Vlaams volksvertegenwoordiger
Cis SCHEPENS, Vlaams volksvertegenwoordiger

1.3.Parlement Wallon (PW) et/ou Parlement de la Communauté française (PCF) :

C. ANCION, député PW et PCF
Patrick AVRIL, député PW et PCF
André BAILLY, député PCF
Michel LEBRUN, député PW et PCF
Annie SERVAIS, députée PW et PCF

2. Federale regering – Gouvernement Fédéral :

– Joost LAGA, vertegenwoordiger van de minister van Telecommunicatie en Overheidsbedrijven en Participaties
– Christophe VAN VAERENBERGH, vertegenwoordiger van de minister van Justitie

3. Overige federale instanties – Autres Instances Fédérales:

– P. THOMAS, Président de la commission pour la Protection de la vie privée - Voorzitter van de commissie voor de Bescherming van de Persoonlijke Levenssfeer
– Thibault VERBIEST, Président de l'Observatoire des Droits de l'Internet - Voorzitter van het Observatorium van de Rechten op het Internet

4. Politieke fracties – Groupes politiques :

4.1. Federale Assemblees – Assemblées fédérales :

VLD :
– Gerda PELOSIE (Kamer)
– Christophe PEETERS (Kamer)

CD&V :

– Kristof HEYNDRIKX (Kamer)

Agalev-Ecolo :
– Danny VENUS (Kamer)
– Christel VERHAS (Kamer)

PS :
– Joëlle KAPOMPOLE (Chambre)

MR :
– Xavier BAESELEN (Chambre)
– Hervé BECHOUX (Chambre)
– C. Lejeune de SCHIERVEL (CCF)

VB :
– Arnaud COLLIER (Kamer)

SP.A :
– Steven PATTYN (Kamer)
– Martine VAN RYCKEGEM (Kamer)

CDH :
– Anne SACRÉ-MIKOLAJCZAK (Chambre)

VU&ID :
– Karl VANLOUWE (Kamer)

5. Diensten van de Kamer – Services de la Chambre :

Lut AERTS (Dienst Documentatie en Archief)
Jean-François BAUDUIN (Service de traduction des Documents parlementaires)
Etienne BAUSIER (Service des Affaires Générales)
An DE FOER (dienst Personeel)
Xavier DEBROUX (Service Juridique)
Christophe DEFOSSA (Service du Compte Rendu Analytique)
Gerda DEKERK (Bibliotheek)
Luc DE LOY VERMEULEN (Dienst Documentatie en Archief)
Jan DELTOUR (Wetgevend Secretariaat)

Yves DELVAUX (Service des Affaires Générales)
Idès DE PELSEMAEKER (Commissiedienst)
André GRENACS (Service Juridique)
Thierry HANNAERT (Service Informatique)
Luc HOSTE (Dienst Vertaling van de Beknopte Verslagen)
Roeland JANSOONE (Secretariaat-generaal)
Inge JANSSENS (Dienst van de Algemene Zaken)
Ronald MEES (Dienst Integraal Verslag)
Pierre MOTYL, ICT Manager
Robert MYTTENAERE, adjunct-griffier, directeur-generaal van de wetgevende diensten
Pierre PEETERS (Service Informatique)
Martin PELEMAN (Commissiedienst)
Ralph RAIGLOT (Service Informatique)
Paul SARENS (Bibliotheek)
Marie-Anne SNOECK (Service de traduction des Comptes rendus analytiques)
Freddy TOMICKI (Service Informatique)
Patrick VAN HOOF (Service de traduction des Documents parlementaires)
Geert VAN RENTERGHEM (Dienst Algemene Zaken)
Bernard VANSTEELANDT (Bibliothèque)
Eddy VASTMANS (Service de traduction des Comptes rendus analytiques)
Michel WETTACH (Secretariat législatif)

6. Diensten van de Senaat – Services du Sénat :

Erik ADAM (Dienst Wetsevaluatie)
Ward BIJL (Dienst Vergadering)
L. BLONDEEL (Dienst Verslaglegging)
Koen BRYNAERT (Commissiedienst)
Thibaut CARDON DE LICHTBUER (service Protocole)
Roger DE VRIENDT (Informaticadienst)
Y. HANOTIAU (Juridische dienst)
Patrick PEREMANS (dienst Protocol)
Hans VANHEVELE (Commissiedienst)
E. WILLEMS (Service Informatique)

7. Diensten van het Vlaams Parlement :

Robby DEBOELPAEP, dienst Informatica

8. Services du Conseil de la Région Bruxelles-Capitale – Diensten van de Raad van het Brussels Hoofdstedelijke Gewest :

Henri CAERS, service du secretariat général

9. Services du parlement de la Communauté française :

Philippe DI NUNZIO, Service des Relations interparlementaires
Viviane GÉRARD, coordinatrice de la Cellule Internet
Christine MALOLEPSZY, service du Bâtiment, de l'Infrastructure et de l'Informatique

10. ISPA

Maria-Pia BONNE (ISPA Belgium)
Pascale DE JONCKHEERE (Belgacom/Skynet)
Saskia MERMANS (Belgacom/Skynet)
Pieter RABAU (ISPA Belgium)
Rudi ROTH (ISPA Belgium)
Carlos VAN NUNEN (Planet Internet)
Bart VANSEVENANT (Ubizen)

11. Andere :

Robby BERLOZNIK, Vlaams Instituut voor Wetenschappelijke en Technologische Aspecten (VIWTA)
Claude JAVEAU, Professeur à l'ULB
Michèle LAHAYE, Manager Institutional Relations - De Post
Flip PETILLION, advocaat
Patrick VAN EECKE, advocaat, ICRI
Walter VAN WOLPUTTE, Manager Institutional Relations - De Post