2 - 392/3

SÉNAT DE BELGIQUE

SESSION DE 1999-2000

28 JUIN 2000

Projet de loi relative à la criminalité informatique

Procédure d'évocation

RAPPORT

FAIT AU NOM
DE LA COMMISSION
DE LA JUSTICE
PAR M. **ISTASSE**
ET MME **KAÇAR**

La commission de la Justice a examiné le projet de loi qui vous est soumis au cours de ses réunions des 14, 20, 21 et 28 juin 2000, en présence du ministre de la Justice.

I. PROCÉDURE

Le présent projet de loi, qui relève de la procédure bicamérale facultative, a été adopté à l'unanimité par

Ont participé aux travaux de la commission:

1. Membres effectifs: M. Dubié, président; Mmes de Bethune, de T'Serclaes, Leduc, Lindekens, Nyssens, M. Ramoudt, Mme Taelman, M. Vandenberghe et M. Istasse et Mme Kaçar, rapporteurs.

2. Membres suppléants: M. Daif, Mme Laloy, M. Moens, Mmes Vanlerberghe et Van Riet.

3. Autre sénateur: M. Van Quickenborne.

Voir:

Documents du Sénat:

2-392 - 1999/2000:

Nº 1: Projet transmis par la Chambre des représentants.

Nº 2: Amendements.

BELGISCHE SENAAT

ZITTING 1999-2000

28 JUNI 2000

Wetsontwerp inzake informaticacriminaliteit

Evocatieprocedure

VERSLAG

NAMENS DE COMMISSIE VOOR
DE JUSTITIE
UITGEBRACHT
DOOR DE HEER **ISTASSE**
EN MEVROUW **KAÇAR**

De commissie voor de Justitie heeft dit wetsontwerp besproken tijdens haar vergaderingen van 14, 20, 21 en 28 juni 2000, in aanwezigheid van de minister van Justitie.

I. PROCEDURE

Onderhavig optioneel bicameraal wetsontwerp werd door de Kamer van volksvertegenwoordigers

Aan de werkzaamheden van de commissie hebben deelgenomen:

1. Vaste leden: de heer Dubié, voorzitter; de dames de Bethune, de T'Serclaes, Leduc, Lindekens, Nyssens, de heer Ramoudt, mevrouw Taelman, de heer Vandenberghe en de heer Istasse en mevrouw Kaçar, rapporteurs.

2. Plaatsvervangers: de heer Daif, mevrouw Laloy, de heer Moens, de dames Vanlerberghe en Van Riet.

3. Andere senator: de heer Van Quickenborne.

Zie:

Stukken van de Senaat:

2-392 - 1999/2000:

Nr. 1: Ontwerp overgezonden door de Kamer van volksvertegenwoordigers.

Nr. 2: Amendementen.

la Chambre des représentants le 30 mars 2000 et évoqué le 28 avril 2000 à la demande de 37 sénateurs (*Bulletin du greffe* nº 23 du 28 avril 2000).

Le délai d'examen s'achève le vendredi 14 juillet 2000, la commission parlementaire de concertation ayant décidé de le prolonger de 9 jours, le 22 juin 2000 (bulletin des travaux, nº 11).

II. EXPOSÉ INTRODUCTIF DU MINISTRE DE LA JUSTICE

L'objectif du présent projet de loi est de proposer, à la lumière de la situation internationale, un certain nombre de démarches concrètes afin de fournir aux acteurs de la justice les instruments juridiques adéquats pour lutter contre la criminalité sur les autoroutes de l'information. À cet égard, certaines modifications du droit pénal matériel et du droit de la procédure pénale sont envisagées, le principe de base étant que le niveau de protection pénale qui prévaut actuellement à l'égard d'une série de biens juridiques, doit également être maintenu dans le contexte de la technologie de l'information. En outre, des dispositions adéquates sont créées pour des nouveaux intérêts qui méritent protection.

Les récents événements ont en effet démontré à suffisance que, dans l'optique des intérêts de l'autorité, mais également des entreprises et des particuliers, la protection des réseaux d'un point de vue pénal doit constituer une priorité politique majeure qui requiert une intervention urgente sur le plan législatif.

Il est tenté dans le projet de loi d'adapter l'arsenal légal des dispositions pénales et les moyens prévus dans le droit de procédure pénale aux besoins d'une lutte efficace contre la criminalité relative à la technologie de l'information, et ce sous deux angles :

— on cherche à se conformer à la structure existante du Code pénal et du Code d'instruction criminelle sans y apporter de profondes réformes structurelles;

— concernant l'introduction de nouveaux délits, il faut s'interroger sur l'incrimination de certains abus en matière de technologie de l'information afin d'éviter une criminalisation excessive.

À la lumière de ce qui précède, le projet de loi vise principalement à garantir, y compris dans le contexte de la technologie de l'information, deux intérêts juridiques traditionnellement protégés, à savoir la foi publique et le patrimoine, surtout en raison du doute qui règne à cet égard au niveau de la doctrine et de la jurisprudence.

C'est la raison pour laquelle de nouvelles dispositions relatives au faux en informatique et à la fraude

eenparig aangenomen op 30 maart 2000, en geëvoceerd op 28 april 2000 op verzoek van 37 senatoren (*Griffiebulletin* nr. 23 van 28 april 2000).

De onderzoekstermijn loopt ten einde op vrijdag 14 juli 2000, na beslissing tot verlenging met 9 dagen door de parlementaire overlegcommissie op 22 juni 2000 (overzicht van de werkzaamheden nr. 11).

II. INLEIDENDE UITEENZETTING VAN DE MINISTER VAN JUSTITIE

Het ontwerp van wet beoogt, in het licht van de internationale stand van zaken, een aantal concrete stappen te nemen om de actoren van de justitie de adequate juridische instrumenten aan te reiken om de criminaliteit op de informatiesnelweg te kunnen bestrijden. In dat verband worden een aantal wijzigingen van het materieel strafrecht en het strafprocesrecht voorzien. Het uitgangspunt hierbij is dat het strafrechtelijke beschermingsniveau dat thans ten aanzien van een aantal rechtsgoederen bestaat, ook in de context van de informatietechnologie moet worden gehandhaafd. Bovendien worden voor nieuwe beschermwaardige belangen adequate bepalingen gecreëerd.

De recente gebeurtenissen hebben immers ten overvloede aangetoond dat de strafrechtelijke bescherming van de informaticanetwerken zowel in het licht van de belangen van de overheid, de bedrijven en de particulieren een belangrijke beleidsprioriteit moet zijn die een dringend wetgevend optreden noodzakelijk maakt.

In het ontwerp wordt betracht het wettelijk arsenaal aan strafbepalingen en de middelen voorzien in het strafprocesrecht aan te passen aan de noden van een effectieve bestrijding van criminaliteit die verband houdt met de informatietechnologie, en dit vanuit een dubbele invalshoek :

— er wordt aansluiting gezocht bij de bestaande structuur van het Strafwetboek en het Wetboek van Strafvordering, zonder hier ingrijpende structurele hervormingen in door te voeren;

— inzake het invoeren van nieuwe misdrijven wordt de strafwaardigheid van misbruiken inzake de informatietechnologie in rekening gebracht, teneinde overcriminalisering te vermijden.

In het licht van het voorgaande streeft het ontwerp er vooreerst naar om twee centrale traditionele beschermde rechtsbelangen, de openbare trouw en het vermogen, ook in een informatietechnologiecontext te waarborgen, niet in het minst omwille van de twijfel die in dat verband in doctrine en rechtspraak heerst.

Er worden derhalve nieuwe bepalingen inzake valsheid in informatica en informaticabedrog inge-

informatique sont insérées dans les chapitres du Code pénal qui portent sur les intérêts juridiques précités, sans toutefois toucher à la structure de ces chapitres ni à leurs dispositions.

Dans de très nombreux cas, les infractions punissables commises en matière de confidentialité, d'intégrité et de disponibilité des systèmes informatiques et des données qu'ils permettent de stocker, de traiter ou de transmettre ne peuvent être assimilées en tant que telles à des infractions contre des intérêts juridiques existants sans faire violence à la réalité concrète et juridique. Il est dès lors inséré au livre II du Code pénal un titre nouveau visant essentiellement à réprimer l'accès illicite, ainsi que le sabotage informatique et le sabotage de données.

Un certain nombre de nouveautés sont insérées dans le Code d'instruction criminelle en ce qui concerne les actes d'information et d'instruction dans le contexte informatique. Il s'agit essentiellement de dispositions relatives à la saisie de données, à la recherche sur réseau, à des obligations de collaboration particulières dans un contexte informatique ainsi qu'à l'adaptation des modalités d'interception des télécommunications.

Enfin, la législation sur les télécommunications est également adaptée afin de permettre au Roi de préciser les obligations d'identification et de conservation à l'égard des fournisseurs de services de télécommunications, en ce qui concerne l'utilisation des services de télécommunications. Le non-respect de ces obligations est sanctionné pénalement.

Étant donné que le projet de loi relatif à la criminalité informatique et le projet de loi relatif à la signature électronique traitent tous deux du problème du faux en informatique, le présent projet de loi est présenté et cosigné par le ministre de la Justice, le ministre des Télécommunications et des Entreprises et Participations publiques et le ministre de l'Économie.

Le ministre souligne l'importance du projet qui est soumis à l'approbation des sénateurs.

Électronique et informatique pénètrent toujours plus loin dans notre quotidien et ont bouleversé radicalement notre cadre de vie.

L'ordinateur est partout et son utilisation est devenue banale.

Ce qui devient aussi banal, c'est la multiplication des réseaux et leur interconnexion à un point tel que l'on distingue difficilement l'ordinateur du réseau.

Les moyens de communication actuels constituent une immense toile d'araignée qui couvre la planète entière. L'exemple le plus frappant, c'est bien évidemment internet.

voegd in de hoofdstukken van het Strafwetboek die op de voormelde rechtsbelangen betrekking hebben, zonder evenwel te raken aan de opbouw van die hoofdstukken en de bepalingen daarvan.

De strafwaardige inbreuken op de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, als zodanig kunnen in zeer veel gevallen niet herleid worden tot inbreuken op bestaande rechtsbelangen, zonder de feitelijke en juridische realiteit geweld aan te doen. Daarom word hiervoor een nieuwe titel in boek II van het Strafwetboek ingevoegd dat in essentie de ongeoorloofde toegang, evenals computer- en datasabotage beoogt te beteugelen.

In het Wetboek van Strafvordering worden een aantal vernieuwingen ingevoerd inzake opsporings- en onderzoekshandelingen in een geïnformatiseerde context. In essentie betreft het hier bepalingen inzake databeslag, netwerkzoeking, bijzondere medewerkingsverplichtingen in een geïnformatiseerde omgeving, en een aanpassing van de modaliteiten van het onderscheppen van telecommunicatie.

Tenslotte wordt ook de telecommunicatiewetgeving aangepast teneinde de Koning toe te laten bepaalde identificatieverplichtingen en bewaringsverplichtingen inzake het gebruik van telecommunicatiediensten ten aanzien van de dienstenverstrekkers van telecommunicatiediensten te preciseren. Het niet-respecteren van deze verplichtingen wordt strafrechtelijk gesanctioneerd.

Gezien de gemeenschappelijke problematiek betreffende de valsheid in informatica tussen het wetsontwerp inzake informaticacriminaliteit en dat inzake de digitale handtekening, wordt onderhavig ontwerp voorgedragen en medeondertekend door de minister van Justitie, de minister van Telecommunicatie en Overheidsbedrijven en Participaties en de minister van Economie.

De minister onderstreept het belang van het wetsontwerp dat hier wordt voorgelegd.

Elektronica en informatica dringen steeds meer ons dagelijkse leven binnen en hebben onze leefomgeving radicaal veranderd.

De computer is alomtegenwoordig en men maakt er zonder veel ophef gebruik van.

Wat ook dagelijkse kost is geworden is de toename van de netwerken en hun onderlinge verbinding, in die mate zelfs dat men de computer amper nog van het netwerk kan onderscheiden.

De huidige communicatiemiddelen vormen een reusachtig web dat de hele planeet beslaat. Het meest voor de hand liggende voorbeeld hiervan is natuurlijk het internet.

Les échanges sur ces réseaux sont permanents, les transactions s'effectuent à la vitesse électronique et les notions d'espace et de temps disparaissent au profit d'une réalité virtuelle, universelle et permanente.

Ce nouvel espace constitue une force extraordinaire de dialogue, d'échanges et de progrès.

Ce nouvel espace présente malheureusement une formidable vulnérabilité.

Face à l'usage normal voire quasi obligatoire de l'environnement informatique, il faut constater aussi l'émergence d'utilisations frauduleuses ou criminelles de l'outil informatique.

Ces utilisations sont d'autant plus dangereuses que les vulnérabilités sont accrues et que, dans une mesure très importante, le fonctionnement, l'économie, voire l'existence même de nos sociétés peuvent être gravement menacés.

Il faut assurer la viabilité du nouvel ordre numérique qui se crée et auquel on ne peut échapper.

Le droit pénal et le droit de la procédure pénale doivent intégrer parfaitement cette évolution pour continuer à assurer la pérennité des valeurs qui doivent être protégées.

Internet soumet tant le droit pénal que le droit de la procédure pénale à rude épreuve comme le soulignait en 1997 M. l'avocat général émérite Vandemeulebroecke(1).

Pour permettre aux magistrats d'affronter l'épreuve et de fournir ainsi une réponse aux conséquences pénales de l'émergence d'un nouvel ordre numérique, le gouvernement a déposé ce projet de loi en créant également une distinction importante: l'informatique peut constituer un moyen de commettre des infractions classiques mais elle peut être aussi le but de la criminalité.

En ce qui concerne le Code pénal

De manière générale, les infractions citées ci-après sont punies d'une amende de 26 à 200 000 francs (× 200) et/ou d'un emprisonnement de 3 mois à 5 ans.

Ces peines sont doublées si les infractions sont commises dans les 5 ans après une première condamnation pour les mêmes faits.

(1) Oscar Vandemeulebroecke, «Le droit pénal et la procédure pénale confrontés à internet» in *Internet sous le regard du droit*, Éditions du jeune barreau de Bruxelles, 1997, p. 151 et suivantes.

Er zijn voortdurend uitwisselingen op de netwerken, er worden transacties uitgevoerd met elektronische snelheid en de noties van tijd en ruimte verdwijnen om plaats te maken voor de virtuele, universele en permanente realiteit.

Deze nieuwe ruimte biedt ongekende mogelijkheden tot dialoog, uitwisseling en vooruitgang.

Deze nieuwe ruimte heeft echter ook een zeer zwak punt.

Samen met het gewone, quasi ingeburgerde gebruik van de informatica, zijn er ook frauduleuze en misdadige praktijken ontstaan met betrekking tot de informatica.

Deze praktijken zijn des te gevaarlijker omdat de kwetsbaarheid van de netwerken vrij groot is geworden en de dagelijkse werking, de economie en het bestaan zelf van onze samenleving hierdoor zwaar in het gedrang kunnen komen.

Men moet ervoor zorgen dat het nieuwe digitale systeem dat is ontstaan en waaraan men niet meer kan ontsnappen, levensvatbaar blijft.

Het strafrecht en het strafprocesrecht dienen volledig aangepast te worden aan deze ontwikkelingen om het voortbestaan te verzekeren van de waarden die wij in bescherming nemen.

Zoals emeritus advocaat-generaal Vandemeulebroecke(1) het in 1997 onderstreepte, stelt het Internet zowel het strafrecht als het strafprocesrecht voor een zware taak.

Om de magistraten in staat te stellen deze taak te volbrengen en zo een antwoord te bieden op de strafrechtelijke gevolgen van het nieuwe digitale systeem, heeft de regering dit wetsontwerp ingediend, waarbij tevens een belangrijk onderscheid is gemaakt: de informatica kan een middel zijn om klassieke strafbare feiten te begaan, maar kan ook het doel zelf van het misdrijf zijn.

Wat betreft het Strafwetboek

In het algemeen kan worden gesteld dat de hierna genoemde inbreuken worden bestraft met geldboetes gaande van 26 tot 200 000 frank (× 200) en/of met een gevangenisstraf tussen de 3 maanden en de 5 jaar.

Deze straffen worden verdubbeld indien ze worden begaan binnen de 5 jaar na een eerste veroordeling wegens eenzelfde feit.

(1) Oscar Vandemeulebroecke, «Le droit pénal et la procédure pénale confrontés à internet», in «*internet sous le regard du droit*», Éditions du jeune barreau de Bruxelles, 1997, blz. 151 en volgende.

I. Faux en informatique

Par faux en informatique, on entend la falsification, par le biais de manipulation de données, de données informatiques juridiquement pertinentes, par exemple :

— la falsification et/ou la contrefaçon de cartes de crédit, les faux en matière de contrats numériques lorsque les données juridiquement pertinentes ne sont plus imprimées sur papier, ni signées à la main;

— l'utilisation de données fausses.

La tentative de faux en informatique sera également punie.

II. Fraude informatique

Par fraude informatique, on entend la fraude réalisée sur ordinateur. Exemples :

— l'utilisation d'une carte de crédit volée pour retirer de l'argent d'un distributeur automatique;

— le dépassement illicite du crédit octroyé par sa propre carte de crédit;

— l'introduction d'instructions de programmation permettant d'obtenir à la suite de certaines transactions d'autres résultats en vue d'un avantage financier illicite;

— le détournement à des fins lucratives de fichiers ou de programmes informatiques confiés dans un but spécifique.

La tentative de fraude informatique est également punissable.

Cette disposition est dissociée de l'article 496 du Code pénal (l'escroquerie) étant donné que la fraude informatique concerne des manipulations illicites de données à l'égard d'une machine tandis que l'escroquerie vise essentiellement des actes frauduleux qui trompent la confiance de personnes.

III. Accès non autorisé tant par les insiders que par les outsiders

Cela englobe le « hacking ».

Une distinction est faite entre le « hacking » réalisé par des personnes externes à l'organisation et le « hacking » réalisé par des personnes qui ont en principe accès à une partie du réseau.

Exemple de la première catégorie : contourner le dispositif de sécurité d'un réseau fermé par le biais de l'infrastructure de télécommunication publique et accéder ainsi au système.

I. Valsheid in informatica

Hieronder wordt verstaan via datamanipulatie vervalsen van juridisch relevante computergegevens, bijvoorbeeld :

— vervalsen en/of namaken van kredietkaarten, valsheid inzake digitale contracten waar de juridisch relevante documenten niet meer op papier worden geprint en de manu worden ondertekend;

— gebruik van valse gegevens.

De poging tot valsheid in informatica wordt eveneens strafbaar gesteld.

II. Informaticabedrog

Hieronder wordt verstaan de gerealiseerde computerfraude. Voorbeelden van de gevallen die geviseerd worden zijn :

— gebruik van een gestolen kredietkaart om geld uit een automatische biljettenverdeler te halen;

— onrechtmatig overschrijden van het krediet van zijn eigen kredietkaart;

— invoeren van programma-instructies waardoor bepaalde verrichtingen een ander resultaat opleveren met het oog op het bekomen van een onrechtmatig financieel voordeel;

— verduisteren met winstbejag van bestanden of programma's die men enkel voor een welbepaald doel toevertrouwd heeft gekregen.

De poging tot informaticabedrog wordt eveneens strafbaar gesteld.

Deze bepalingen wordt losgekoppeld van artikel 496 van het Strafwetboek (de oplichting) aangezien computerfraude ongeoorloofde manipulaties betreft van data ten aanzien van een machine en oplichting in essentie bedrieglijke handelingen viseert die het vertrouwen van « personen » schenden.

III. Ongeoorloofde toegang zowel door outsiders als door insiders

Dit omvat de zogenaamde « hacking ».

Er wordt een bewust onderscheid gemaakt tussen de hacking die gebeurt door mensen van buiten de organisatie en hacking door mensen die principieel toegang hebben tot een deel van het netwerk.

Als voorbeeld van het eerste : via de openbare telecominfrastructuur de beveiliging van een gesloten netwerk omzeilen en zich aldus toegang verschaffen tot het systeem.

Exemple de la deuxième catégorie: pénétrer dans des parties du réseau interne d'une entreprise sans y être habilité, afin de causer des dommages ou de commercialiser certaines données pour son propre compte.

Les «outsiders» sont passibles d'une peine lorsqu'ils savent qu'ils ne sont pas habilités à accéder au système ou à y rester. Lorsque l'infraction a lieu dans une intention frauduleuse, une peine plus lourde est prévue.

Pour les «insiders», le seuil d'incrimination est plus élevé. La transgression du niveau d'autorisation accordé doit se faire dans un but délibéré de nuire, notamment dans un but lucratif illicite ou dans une intention malveillante.

Le fait d'accéder simplement de manière illégitime à des parties du système doit être abordé par des mécanismes moins énergiques (par exemple, des sanctions internes).

De plus, un certain nombre d'actes consécutifs au «hacking» sont punissables sous la forme de circonstances aggravantes de l'infraction de base, sous ses deux variantes, notamment:

1. la soustraction de données à la suite du «hacking», par exemple le vol de secrets industriels dans le cadre de l'espionnage industriel;

2. l'abus de la capacité d'un ordinateur dans lequel la personne s'est introduite de manière illicite, c'est-à dire l'utilisation de la capacité du système causant une diminution temporaire des capacités d'utilisation des autres utilisateurs, le «vol de temps»;

3. le fait de causer des dommages, intentionnellement ou non, après le «hacking».

Autre acte consécutif dorénavant punissable, le «recel» des données obtenues par le biais du «hacking». Étant donné que, traditionnellement, le recel ne concerne que des biens matériels, cette disposition est surtout importante dans le contexte de l'espionnage industriel.

De plus, la personne qui charge une autre personne d'effectuer un «hacking» ou qui l'y incite est passible de peines plus sévères que celle qui commet effectivement l'acte. La raison en est la suivante: auparavant, le «hacking» constituait généralement pour les jeunes «fous de l'informatique» une façon de passer le temps tandis qu'aujourd'hui des criminels professionnels ont recours à ces personnes pour mettre leurs plans à exécution.

Vu la gravité des comportements, le montant de la peine prévu pour la tentative est le même que celui prévu pour l'infraction en tant que telle. Prenons comme exemple l'essai automatisé de mots de passe où l'auteur s'intéresse davantage à l'obtention du

Als voorbeeld van het tweede: in delen van een intern bedrijfsnetwerk binnendringen zonder daartoe de bevoegdheid te hebben, teneinde schade te berokkenen of bepaalde data voor eigen rekening te commercialiseren.

Buitenstaanders zijn strafbaar indien ze weten dat zij onbevoegd in het systeem komen of blijven. Wanneer de inbreuk plaatsvindt met bedrieglijk opzet wordt een zwaardere straf voorzien.

Voor insiders wordt de strafbaarheidsdrempel hoger gelegd. Het overschrijden van het verleende autorisatieniveau moet plaatsvinden met een bijzonder opzet, namelijk onrechtmatig winstbejag of kwaadwillige bedoelingen.

Het louter onrechtmatig betreden van delen van het systeem moet via minder ingrijpende mechanismen (zoals interne sancties) worden aangepakt.

Bovendien worden ook een aantal gevolghandelingen van de hacking strafbaar gesteld, onder de vorm van verzwarende omstandigheden bij het basismisdrijf in zijn beide varianten, inzonderheid:

1. het ontvreemden van gegevens naar aanleiding van het hacken, bijvoorbeeld het stelen van industriële geheimen in het kader van bedrijfsspionage;

2. het misbruik maken van de capaciteit van de computer waar de persoon ongeoorloofd is binnengedrongen: het benutten van de capaciteit van het systeem waardoor de mogelijkheden van andere gebruikers tijdelijk beperkt worden, de zogenaamde «tijdsdiefstal»;

3. het al dan niet gewild toebrengen van schade na de hacking.

Een andere gevolghandeling die wordt strafbaar gesteld, is het «helen» van de naar aanleiding van de hacking bekomen gegevens. Aangezien het misdrijf heling traditioneel enkel materiële voorwerpen kan betreffen, is deze bepaling vooral binnen de context van spionagebestrijding belangrijk.

Bovendien wordt het opdracht geven of het aanzetten tot hacking zwaarder gestraft dan degene die het misdrijf effectief uitvoert. De reden hiervoor is dat, waar vroeger hacking in veel gevallen een tijdverdrijf was voor jonge computerfreaks, thans professionele criminelen dergelijke personen inschakelen om hun plannen uit te voeren.

Gezien de ernst van de gedragingen wordt wat de poging betreft, dezelfde strafmaat voorzien als voor het voltooide misdrijf. Nemen we hierbij als voorbeeld het geautomatiseerd uitproberen van paswoorden, waarbij de dader eerder geïnteresseerd is in het

code d'accès qu'au cambriolage effectif du système informatique.

IV. Le sabotage de données et le sabotage informatique

Les dispositions actuelles du Code pénal visent uniquement la destruction et l'endommagement de biens matériels. L'endommagement de hardware est donc punissable en tant que tel, mais la détérioration de données n'est pas visée.

Les nouvelles dispositions comblent cette lacune.

Concernant les adaptations sur le plan de la procédure pénale

Dans ce domaine, un certain nombre d'innovations sont introduites sur le plan des actes d'information et d'instruction dans le contexte informatique.

I. La saisie de données informatiques

La saisie des données pertinentes pour l'instruction, qui sont stockées, traitées ou transmises via un système informatique, peut se dérouler complètement selon les procédures traditionnelles, pour autant qu'elle s'accompagne de la saisie du support matériel (par exemple, l'ordinateur, les disques optiques, les disquettes, etc.).

La situation est différente lorsque l'autorité judiciaire veut uniquement disposer des données sans en saisir les supports ou le système.

Les nouvelles règles particulières en matière de saisie des données peuvent être résumées comme suit :

1. En principe, les données pertinentes sont copiées sur des supports des autorités. Il est possible d'utiliser les supports mis à la disposition des personnes habilitées à utiliser le système dans deux cas spécifiques uniquement, à savoir en cas d'urgence ou en cas de problèmes techniques.

2. En principe, l'accès aux données figurant sur le système informatique examiné ou sur les supports présents sur place est bloqué (par exemple, par cryptage).

Cette manière de procéder permet d'aborder le mieux la situation de la saisie classique. Il peut toutefois être décidé de ne pas bloquer les données dans leur intégralité ou en partie afin de ne pas compromettre la continuité du fonctionnement d'un système ou d'une organisation.

Dans deux cas, le blocage des données peut être remplacé par l'effacement, notamment :

1. lorsque le procureur du Roi estime que les données portent atteinte à l'ordre public ou aux bonnes mœurs (par exemple, en cas de pornographie enfantine et de tracts racistes);

bekomen van de toegangscode op zich dan in het effectief binnenbreken in de computer.

IV. Data- en computersabotage

De huidige bepalingen van ons strafrecht viseren enkel de vernieling en beschadiging met betrekking tot tastbare voorwerpen. Beschadiging aan hardware wordt als dusdanig strafbaar gesteld, doch de beschadiging van data wordt hierbij niet geviseerd.

De nieuwe bepalingen vullen dit tekort op.

Wat betreft de wijzigingen op het vlak van het strafprocesrecht

Hier worden een aantal vernieuwingen ingevoerd inzake opsporings- en onderzoekshandelingen binnen een geïnformatiseerde context.

I. Het databeslag

De inbeslagneming van voor het strafonderzoek relevante gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, kan volledig volgens de traditionele procedures verlopen zolang dit gepaard gaat met de inbeslagneming van de materiële drager (bijvoorbeeld de computer, optische schijven, diskettes, enz.).

Als de gerechtelijke overheid enkel wil beschikken over de data, zonder inbeslagneming van de dragers of het systeem, is de situatie verschillend.

De nieuwe bijzondere regels inzake databeslag kunnen als volgt worden samengevat :

1. In principe worden de relevante gegevens gekopieerd op dragers van de overheid. Enkel in twee specifieke gevallen, meer bepaald bij dringendheid of bij technische problemen kunnen dragers die ter beschikking staan van personen bevoegd voor het gebruik van het systeem, worden aangewend.

2. In principe wordt de toegang tot deze gegevens in het onderzochte informaticasysteem of op ter plaatse aanwezige dragers bovendien geblokkeerd (bijvoorbeeld door encryptie).

Op die manier benadert men het dichtst de situatie van een klassieke inbeslagneming. Er kan evenwel beslist worden om gegevens of een deel daarvan niet te blokkeren om reden van het niet in het gedrang brengen van de continuïteit van de werking van een systeem of organisatie.

In twee gevallen kan het blokkeren van de gegevens worden vervangen door het wissen ervan, namelijk :

1. wanneer de procureur des Konings de gegevens strijdig acht met de openbare orde of goede zeden (bijvoorbeeld kinderporno, racistische pamfletten);

2. lorsque le procureur du Roi estime que les données comportent un risque d'endommagement (par exemple, des virus informatiques).

Dans ces cas, une copie sera faite en vue de l'enquête judiciaire.

II. Le blocage

Lorsque copier n'est pas possible (pour des raisons de complexité ou de volume), les données seront uniquement bloquées, ce qui revient en fait à une sorte d'apposition des scellés.

III. Obligation d'information

Il existe une obligation d'information à l'égard du responsable du système informatique, laquelle constitue une garantie générale. Un résumé des opérations exécutées à l'égard des données est communiqué au responsable. En effet, un inventaire exhaustif n'est souvent pas réaliste dans un environnement informatisé.

Tous les moyens *ad hoc* doivent être appliqués pour garantir l'intégrité et la confidentialité des données susmentionnées. Cela vaut également pour leur conservation dans les greffes.

IV. Une nouvelle disposition porte également sur la recherche sur réseau

Lorsqu'un juge d'instruction effectue une recherche dans un système informatique, il peut étendre cette recherche à un système informatique qui se trouve dans un autre lieu que celui sur lequel s'exécute la recherche, en respectant un certain nombre de conditions.

La mesure doit d'abord être nécessaire pour la recherche de la vérité. En outre, il faut qu'il y ait un risque de perdre des éléments de preuve sans cette extension ou que le juge d'instruction estime que d'autres mesures (par exemple, plusieurs mandats d'arrêt) sont disproportionnées.

Il appartient au juge d'instruction d'apprécier les choses en toute équité.

On ne peut étendre pareille recherche que si cela s'avère nécessaire dans le cadre d'une affaire pénale concrète dont est chargé un juge d'instruction.

L'exercice de cette compétence est limité par le niveau d'accès des personnes autorisées à utiliser le système informatique faisant l'objet de cette recherche.

2. wanneer de procureur des Konings meent dat de gegevens een risico voor schade opleveren (bijvoorbeeld computervirussen).

In deze gevallen zal enkel een kopie worden genomen met het oog op het strafonderzoek.

II. Blokkering

Wanneer kopiëren niet mogelijk is (complexiteit, omvangrijkheid) worden de gegevens enkel geblokkeerd, wat in feite neerkomt op een variant van verzegeling.

III. Informatieverplichting

Als algemene waarborg is er een informatieverplichting ten aanzien van degene die verantwoordelijk is voor het informaticasysteem. Daarbij wordt een samenvatting meegedeeld van de operaties die ten aanzien van de gegevens werden uitgevoerd. Een uitputtende inventaris is immers in een geïnformatiseerde omgeving vaak niet realistisch.

Ook dienen alle passende middelen te worden aangewend om de integriteit en de vertrouwelijkheid van voornoemde gegevens te waarborgen. *Idem dito* voor de bewaring ervan ter griffie.

IV. Een nieuwe bepaling heeft betrekking op de netwerkzoeking

Wanneer een onderzoeksrechter een zoeking verricht in een informaticasysteem, kan hij deze zoeking uitbreiden naar een informaticasysteem dat zich op een andere plaats bevindt dan daar waar deze zoeking plaatsvindt, met inachtneming van een aantal voorwaarden.

De maatregel moet vooreerst noodzakelijk zijn voor de waarheidsvinding en bovendien moet er een risico bestaan dat zonder deze uitbreiding bewijselementen verloren gaan of moet de onderzoeksrechter van oordeel zijn dat andere maatregelen (bijvoorbeeld meerdere huiszoekingsbevelen) disproportioneel zijn.

Het komt aan de onderzoeksrechter toe om dit in alle redelijkheid te beoordelen.

Ook mag een dergelijke zoeking enkel uitgebreid worden in zover dit noodzakelijk is in het kader van de concrete strafzaak waarmee de onderzoeksrechter gelast is.

De grens voor het uitoefenen van deze nieuwe bevoegdheid wordt gevormd door de toegangsbevoegdheid van de personen die bevoegd zijn voor het gebruik van het informaticasysteem dat het voorwerp uitmaakt van de zoeking.

Par ailleurs, la connexion technique via les réseaux doit avoir un caractère permanent et stable et ne peut être purement occasionnelle.

En outre, lorsqu'il s'avère que des données pertinentes ne se trouvent pas sur le territoire belge, celles-ci peuvent uniquement être copiées. Dans ce cas particulier, le juge d'instruction est tenu, par le biais du ministère public, d'en avertir immédiatement le ministère de la Justice qui informera les autorités compétentes de l'État concerné, lorsque ce dernier peut être raisonnablement désigné.

V. Obligations de coopération

Dans un contexte de hautes technologies évoluant très rapidement, dans lequel les autorités ne disposent souvent pas de l'expertise suffisante ou dans lequel des experts sont moins disponibles, il est indispensable que l'on puisse obliger des personnes qui connaissent le système informatique à examiner ou qui possèdent une certaine expertise dans certains de ses aspects (par exemple en matière de protection ou de cryptage), d'assister les autorités judiciaires.

Deux types d'obligations sont prévues en l'espèce :

1. l'obligation d'information à l'égard du juge d'instruction pour des personnes ayant une connaissance particulière de certains aspects spécifiques de l'informatique;

2. l'obligation d'information à l'égard du juge d'instruction pour certaines personnes en vue de l'exécution de certaines opérations (par exemple, faire fonctionner un ordinateur, rechercher certains fichiers).

L'obligation de rechercher certaines données ne peut toutefois pas être imposée aux suspects.

VI. Respect du secret de l'instruction

Afin de protéger le secret de l'instruction dans cette matière, les personnes qui prennent connaissance de la mesure ou qui doivent y apporter leur collaboration, sont tenues au secret.

Pour garantir cette obligation, le non-respect des obligations prévues ainsi que toute entrave à une instruction relative à un système informatique seront sanctionnés pénalement.

VII. Responsabilité du dommage causé

Les citoyens qui, dans le cadre de cette disposition, sont obligés de participer à une enquête criminelle,

Bovendien dient de technische verbinding via de netwerken een element van permanentie en stabiliteit in te houden en mag niet louter occasioneel zijn.

Bovendien, wanneer blijkt dat relevante gegevens zich niet op het grondgebied van het Rijk bevinden, worden deze enkel gekopieerd. In dit bijzonder geval is de onderzoeksrechter verplicht, via het openbaar ministerie, onverwijld hiervan mededeling te doen aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze bepaald kan worden.

V. Medewerkingsverplichtingen

Immers, in een snel evoluerende hoogtechnologische context, waar de overheid zelf vaak niet over voldoende expertise beschikt of deskundigen in mindere mate beschikbaar zijn, is het onontbeerlijk om personen die het te onderzoeken informaticasysteem kennen of over een bijzondere expertise beschikken inzake zekere deelaspecten (bijvoorbeeld inzake beveiliging of encryptie) te kunnen verplichten de gerechtelijke overheid bij te staan.

Hiertoe wordt in twee soorten medewerkingsverplichtingen voorzien :

1. informatieverplichting ten aanzien van de onderzoeksrechter voor personen die over een bijzondere kennis beschikken inzake specifieke technische aspecten van informatica;

2. de verplichting ten aanzien van de onderzoeksrechter voor bepaalde personen om zekere operaties uit te voeren (bijvoorbeeld het doen functioneren van de computer, het opvragen van bepaalde files ...).

De verplichting om bepaalde data te zoeken kan evenwel niet worden opgelegd aan de verdachte.

VI. Geheimhoudingsverplichting

Om het geheim van het onderzoek in deze materie te beschermen, wordt een geheimhoudingsverplichting ingevoerd voor de personen die kennis krijgen van de maatregel of die hun medewerking moeten verlenen.

Om de afdwingbaarheid hiervan te garanderen wordt de niet-naleving van de voorziene verplichtingen, evenals het hinderen van het onderzoek in een informaticasysteem, strafrechtelijk gesanctioneerd.

VII. Verantwoordelijkheid voor de toegebrachte schade

De burgers die in het kader van deze bepaling verplicht worden mee te werken aan een strafrechtelijk

peuvent endommager des systèmes ou des données informatiques.

Il ne serait pas raisonnable de tenir ces personnes pour civilement responsables, sauf en cas de dommages intentionnels. C'est la raison pour laquelle il est explicitement prévu que l'État sera responsable du dommage non intentionnel causé dans le cadre du respect de l'obligation de collaborer.

Le projet de loi vise également à adapter le régime des écoutes de télécommunications par les services judiciaires. Trois modifications sont apportées :

1. La liste des infractions autorisant une mesure de mise sur écoute est élargie aux infractions existantes dans le domaine de l'écoute des télécommunications, aux nouvelles infractions de faux en informatique et de fraude informatique, ainsi qu'au « hacking », au sabotage informatique et au sabotage de données.

2. Les obligations particulières de collaboration précitées s'appliquent également, par définition, à l'interception de télécommunications.

3. Les techniques de protection et de verrouillage actuellement disponibles peuvent être utilisées par des autorités judiciaires pour garantir la confidentialité et l'intégrité des matériels d'écoute (qui seront de plus en plus souvent numériques), y compris les modalités de conservation au greffe.

Dans ce cadre, il convient d'examiner les possibilités offertes par la signature digitale. Pour ce qui est de l'avenir, la technologie informatique offrira également des possibilités en matière de transcription et éventuellement de traduction. C'est la raison pour laquelle le projet de loi crée en principe la possibilité de les utiliser, tout en tenant compte du fait que l'introduction de ces applications ne se fera pas dans un avenir proche.

C'est pourquoi il appartiendra au Roi de déterminer les modalités « spécifiques » ainsi que la date d'application.

Enfin, le projet de loi prévoit plusieurs modifications de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

Les nouvelles obligations imposées aux fournisseurs de services, à préciser par le Roi, concernent le non-respect de l'obligation d'identification relative à l'utilisation de services de télécommunication.

Dans ce cadre, les fournisseurs de services de télécommunication devront prendre des mesures structurelles permettant, d'une part, de retrouver les données d'appel (origine, destination, localisation, durée, etc.)

onderzoek, kunnen hierbij schade veroorzaken aan informaticasystemen of data.

Het zou onredelijk zijn dat deze personen hiervoor burgerlijk aansprakelijk gesteld zouden worden, tenzij zij opzettelijk schade zouden berokkenen. Daarom wordt expliciet voorzien dat de Staat aansprakelijk is voor onopzettelijk toegebrachte schade in het kader van het nakomen van de medewerkingsverplichting.

Het wetsontwerp beoogt eveneens een aanpassing van de modaliteiten van het regime van het gerechtelijk onderscheppen van telecommunicatie. Drie wijzigingen worden doorgevoerd.

1. De lijst van misdrijven waarvoor een tapmaatregel mogelijk is wordt uitgebreid met de bestaande misdrijven inzake het aftappen van telecommunicatie, met de nieuwe delicten valsheid in informatica en informaticabedrog, evenals de nieuwe delicten *hacking* en computer- en datasabotage.

2. De bijzondere medewerkingsverplichtingen, zoals hiervoor reeds aangehaald, worden per definitie ook ingevoerd inzake het onderscheppen van telecommunicatie.

3. De beveiligings- en versleutelingstechnieken die thans beschikbaar zijn, kunnen ook door de gerechtelijke overheid worden aangewend om de vertrouwelijkheid en de integriteit van tapmateriaal (dat meer en meer digitaal zal worden) te waarborgen, met inbegrip van de bewaringsmodaliteiten op de griffie.

Hierbij kan meer bepaald gedacht worden aan de mogelijkheden die de digitale handtekening biedt. Naar de toekomst toe zal de informatietechnologie ook inzake de transcriptie en de eventuele vertaling mogelijkheden bieden. Het wetsontwerp schept daarom de principiële mogelijkheid om hiervan gebruik te maken, maar houdt er tegelijk rekening mee dat de implementatie hiervan enige tijd zal vergen.

Om die reden wordt het bepalen van de « specifieke » modaliteiten en de datum van toepassing gedelegeerd aan de Koning.

Uiteindelijk voorziet het wetsontwerp in een aantal wijzigingen van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven.

De nieuwe verplichtingen voor de dienstenverstrekkers die door de Koning zullen moeten worden gepreciseerd, hebben betrekking op het niet-nakomen van de identificatieverplichting inzake gebruik van telecommunicatiediensten.

In dit verband zullen de verstrekkers van telecommunicatiediensten structurele maatregelen moeten nemen om, enerzijds, de oproepgegevens (oorsprong, bestemming, lokalisatie, duur, enz.) van telecommu-

de télécommunications et, d'autre part, d'identifier les utilisateurs proposant les données au public et de conserver les informations.

Si dans ce cadre on a opté pour le terme « données d'appel », c'est parce que dans le contexte des réseaux informatiques, on utilise non seulement des numéros de téléphone traditionnels mais également des adresses internet.

Il s'agit en tout premier lieu des connexions entre l'utilisateur et le fournisseur d'accès (accessprovider).

Toutefois, dans certains cas, il peut être intéressant pour le magistrat compétent de pouvoir contrôler les adresses internet contactées.

Il appartiendra au Roi de déterminer les types d'opérateurs de réseaux de télécommunication et de services de télécommunication auxquels cette obligation s'appliquera.

Il appartiendra également au Roi de promulger des mesures spécifiques en vertu desquelles les fournisseurs d'accès à internet seront tenus de conserver certaines données dans des cas exceptionnels et en fonction de la technologie dont ils peuvent raisonnablement disposer.

Outre cette obligation imposée aux fournisseurs de télécommunications, dont le non-respect est sanctionné pénalement, il est également prévu que les données à conserver seront, sur le plan technique, suffisamment protégées du point de vue de la confidentialité et de l'intégrité.

Voilà ainsi exposé le contenu du projet de loi contre la criminalité informatique.

Le Sénat a évoqué le projet de loi afin de pouvoir analyser la matière.

Depuis l'adoption du projet de loi par la Chambre, des événements nouveaux sont intervenus notamment la diffusion mondiale de virus informatique au nom charmant mais dévastateur.

Le projet de loi tel qu'adopté permettait de rencontrer de telles situations.

III. DISCUSSION GÉNÉRALE

A. Questions et observations des membres

Un membre souligne l'importance du projet de loi en discussion. Même si ce qui reste du délai est plutôt court, il mérite un examen approfondi.

Nul doute que chacun souhaite qu'Internet puisse se développer dans les meilleures conditions. L'internet est en effet un élément très important de

nicatie te kunnen achterhalen en, anderzijds, gebruikers die informatie aan het publiek aanbieden, te kunnen identificeren en deze inlichtingen te bewaren.

Hiertoe wordt het begrip « oproepgegevens » gebruikt, omdat in de context van computernetwerken niet louter met traditionele telefoonnummers wordt gewerkt, maar bijvoorbeeld ook met internetadressen.

In een eerste instantie worden de verbindingen tussen de gebruiker en de accessprovider geviseerd.

Niettemin kan het in bepaalde gevallen voor de bevoegde magistraat ook nuttig zijn om precies te kunnen nagaan welke internetadressen werden gecontacteerd.

Het is de Koning die zal bepalen op welke types van operatoren van telecommunicatienetwerken en telecommunicatiediensten deze verplichting betrekking heeft.

De mogelijkheid werd tevens opengelaten om de Koning toe te laten specifieke maatregelen uit te vaardigen om bijvoorbeeld internetproviders te verplichten bepaalde informatie te bewaren in uitzonderlijke gevallen en in functie van de technologie waarover zij redelijkerwijze kunnen beschikken.

Naast deze strafrechtelijk gesanctioneerde verplichting voor de verstrekkers van telecommunicatiediensten wordt tevens voorzien dat de gegevens die zij zullen moeten bewaren, technisch afdoende worden beveiligd vanuit het oogpunt van confidentialiteit en integriteit.

Dit is dus wat er in het wetsontwerp inzake informaticacriminaliteit staat.

De Senaat heeft het wetsontwerp geëvoceerd om zich in het onderwerp te kunnen verdiepen.

Sinds het wetsontwerp in de Kamer is aangenomen, zijn er nieuwe gebeurtenissen geweest, zoals de wereldwijde verspreiding van een computervirus met een charmante naam maar met zeer kwalijke gevolgen.

Het wetsontwerp zoals het is aangenomen kan een oplossing bieden voor dergelijke situaties.

III. ALGEMENE BESPREKING

A. Vragen en opmerkingen van de leden

Een lid onderstreept het belang van het voorliggend wetsontwerp. Ofschoon de resterende onderzoekstermijn nogal kort is, verdient het ontwerp een grondig onderzoek.

Iedereen wenst ongetwijfeld dat de ontwikkeling van het internet zich in de beste omstandigheden kan ontplooien. Internet is immers een zeer belangrijk

notre société de l'information et il va de soi que son développement est freiné par l'attitude de certains pirates informatiques et autres saboteurs, et notamment par la criminalité internationale qui peut s'organiser sur les réseaux informatiques.

La sécurité de l'usage est requise pour que l'on puisse favoriser le développement de l'informatique et de l'internet.

Bien que le volet économique du développement ne soit pas négligeable, d'autres éléments doivent être retenus dans le développement des applications d'internet et dans l'ouverture vers une nouvelle société de l'information.

Compte tenu de ces évolutions, on peut affirmer que le Code pénal est dépassé. En effet, au moment de sa rédaction, il n'était pas encore question d'informatique. On est donc souvent confronté à des problèmes réels auxquels il n'est pas toujours possible de trouver une solution (*cf.* le développement de réseaux pédophiles sur l'internet et celui de sites web à caractère raciste ou fasciste).

On peut réagir de deux manières. Il y a, d'une part, la tendance américaine, qui vise principalement à protéger le réseau. Le contenu des réseaux ne vient qu'à la seconde place. Pour stimuler le développement de l'internet, on veille à ce que les réseaux soient protégés contre les virus et les pirates informatiques. La deuxième attitude a un caractère plus européen: on préconise une surveillance et une réglementation, non seulement au niveau de l'utilisation des réseaux, mais aussi en ce qui concerne leur contenu.

Le projet de loi à l'examen se rattache plutôt au deuxième point de vue.

Par ailleurs, il faut se demander si le projet n'est pas déjà dépassé compte tenu de l'évolution très rapide de l'informatique. L'intervenant fait référence au sommet du G8 à Paris, auquel assistaient non seulement les autorités concernées, mais aussi les principaux acteurs privés (Microsoft, etc.). Quels ont été les résultats de ce sommet?

Une commissaire souligne la complexité de cet aspect nouveau des réseaux de communication. La criminalité s'inscrit toujours très naturellement dans toute nouvelle évolution des technologies, et sous des formes très différentes (virus, copie des réseaux). Il existe donc une multitude de possibilités de développer des réseaux criminels dès que des moyens de communication plus modernes sont développés échappant au contrôle des pouvoirs publics. Une réglementation nationale n'est pas suffisante pour éliminer cette criminalité. De plus, les criminels chercheront des systèmes pour échapper à cette réglementation. Le texte doit être suffisamment général pour permettre de répondre aux évolutions et pour éviter

element in onze informatiemaatschappij, en de ontwikkeling ervan wordt uiteraard geremd door de houding van sommige hackers, saboteurs, enz., namelijk door de internationale criminaliteit die zich op computernetwerken kan organiseren.

Om de ontwikkeling van de informatica en het internet te bevorderen is een veilig gebruik daarvan noodzakelijk.

Hoewel de economische gevolgen niet te verwaarlozen zijn, moet men bij de ontwikkeling van de Internettoepassingen en bij de groei naar een nieuwe informatiesamenleving rekening houden met andere elementen.

Gelet op deze evoluties, kan men stellen dat het Strafwetboek verouderd is. Bij de redactie van het Strafwetboek was er immers nog geen sprake van informatica. Aldus heeft men vaak te kampen met reële problemen waar er niet altijd een antwoord voor te vinden is (zie de ontwikkeling van pedofilienetwerken via internet, de ontwikkeling van racistische websites of de ontwikkeling van het fascisme via websites).

Er zijn twee mogelijke reacties. Enerzijds is er de Amerikaanse strekking die voornamelijk de bescherming van het netwerk beoogt. De inhoud van de netwerken komt hierbij op de tweede plaats. Om de ontwikkeling van internet te stimuleren, zorgt men ervoor dat de netwerken worden beschermd tegen virussen en hackers. Een tweede visie is meer Europees getint, waarbij een beheersing en reglementering wordt vooropgesteld niet alleen op het vlak van het gebruik van de netwerken, maar ook op het vlak van de inhoud van de netwerken.

Het voorliggende wetsontwerp sluit nader aan bij het tweede standpunt.

Voorts rijst de vraag of het wetsontwerp niet reeds voorbijgestreefd is, gezien de zeer snelle evolutie van de informatica. Spreker verwijst naar de top van Parijs van de G8, waar niet alleen de betrokken overheden, maar ook de voornaamste private actoren aanwezig waren (Microsoft, enz.). Wat waren de resultaten van deze top?

Een commissielid merkt op dat deze nieuwe gedaante van de communicatienetwerken complex is. De misdaad sluit altijd op zeer natuurlijke wijze aan bij elke nieuwe ontwikkeling van de technologieën en neemt daarbij zeer uiteenlopende vormen aan (virussen, kopiëren van netwerken). Er bestaan dus enorm veel mogelijkheden om criminele netwerken uit te bouwen zodra nog modernere communicatiemiddelen tot ontwikkeling komen die aan de controle van de overheid ontsnappen. Om deze criminaliteit uit te schakelen is een nationale regelgeving niet voldoende. Bovendien zullen de misdadigers systemen zoeken om aan deze regelgeving te ontkomen. De tekst moet algemeen genoeg zijn om op de ontwikkelingen te

qu'il soit immédiatement dépassé. Il paraît également indispensable que le texte s'inscrive dans les évolutions au niveau européen et international.

L'exposé du ministre à la Chambre mentionnait que le projet de loi s'était largement inspiré des travaux menés au sein de l'OCDE et du Conseil de l'Europe. Comment le projet se situe-t-il par rapport aux travaux des partenaires européens ? Y a-t-il des directives européennes en la matière ? Le projet s'inscrit-il dans un projet européen en la matière ? Quelles sont les règles qui ont été élaborées en cette matière au sein de l'OCDE et du Conseil de l'Europe ?

L'intervenante souligne l'importance du contrôle que les pouvoirs publics doivent pouvoir exercer sur des réseaux. Il importe de veiller à ce que le développement des réseaux commerciaux puisse s'effectuer en toute sécurité (voir le projet sur la signature électronique et sur la sécurité des paiements).

La question se pose de savoir s'il est possible de légiférer en cette matière. Le projet ne risque-t-il pas d'être rapidement dépassé ? Les règles générales de base ne sont-elles pas suffisantes ? L'intervenante s'interroge quant à l'articulation de ce projet par rapport à la loi sur la protection de la vie privée. Quelle est la compatibilité au niveau pénal de ce projet avec le projet concernant la protection des données sensibles ?

Une disposition du projet mentionne de manière très générale le principe de l'atteinte aux bonnes mœurs et à l'ordre public. Cela est-il suffisant ? Il existe déjà des dispositions, par exemple en matière de pornographie enfantine, applicables au réseau internet. Il faut éviter d'avoir des dispositions allant dans le sens contraire.

En ce qui concerne les sanctions prévues, l'intervenante s'interroge sur les peines de prison. La saisie des moyens utilisés lui semble une sanction plus adéquate. Il y a une multiplicité de types de criminalité qui demandent probablement des approches différentes (virus, *hackers*, pornographie). Le projet est-il adapté et n'entre-t-il pas en contradiction avec les lois existantes ?

Un membre s'interroge sur la conservation des données, et plus particulièrement sur la définition des services de télécommunication. Qu'intègre-t-on dans ces services ? Le projet mentionne les opérateurs de réseaux de télécommunication et les fournisseurs de services de télécommunication. Quelle est la définition précise d'un fournisseur ? Qu'en est-il d'une téléphonie centrale dans un hôtel ? Une définition extensible d'un service de télécommunication aboutit à une conservation de n'importe quelle communication qui part d'un endroit quelconque.

Le délai de conservation de 12 mois semble poser problème pour les opérateurs de télécommunication

kunnen inspelen en om te vermijden dat de regels onmiddellijk achterhaald zijn. Ook moet de tekst aansluiten op de ontwikkelingen die zich op Europees en internationaal vlak afspelen.

De minister vermeldde in zijn uiteenzetting in de Kamer dat het wetsontwerp in ruime mate teruggaat op de werkzaamheden binnen de OESO en binnen de Raad van Europa. Welk verband bestaat er tussen dit ontwerp en de werkzaamheden van de Europese partners ? Bestaan er terzake Europese richtlijnen ? Sluit het ontwerp aan bij een Europees ontwerp terzake ? Welke regels zijn op dat vlak opgesteld door de OESO en door de Raad van Europa ?

Spreekster merkt op dat het belangrijk is dat de overheid toezicht kan uitoefenen op netwerken. Men moet ervoor zorgen dat de handelsnetwerken in alle veiligheid ontwikkeld kunnen worden (zie het wetsontwerp op de elektronische handtekening en op de veiligheid van het betalingsverkeer).

De vraag rijst of het op dit vlak mogelijk is wetgevend werk te verrichten. Bestaat het gevaar niet dat het ontwerp vlug achterhaald is ? Zijn algemene basisregels niet voldoende ? Spreekster vraagt zich af op welke wijze dit ontwerp zich verhoudt tot de wet ter bescherming van de persoonlijke levenssfeer. Stemt dit ontwerp in het strafrechtelijke domein overeen met het ontwerp inzake de bescherming van gevoelige gegevens ?

Een bepaling van het ontwerp vermeldt in zeer algemene bewoordingen het principe van de aantasting van de goede zeden en van de openbare orde. Is dat voldoende ? Er bestaan reeds regels, bijvoorbeeld inzake kinderporno, die van toepassing zijn op het internet. Men moet voorkomen dat men regels krijgt die hiertegen ingaan.

Wat de voorgestelde straffen betreft, heeft spreekster vragen bij de gevangenisstraffen. De inbeslagname van de gebruikte middelen lijkt haar een meer passende straf. Er zijn vele soorten van criminaliteit die waarschijnlijk een uiteenlopende aanpak vereisen (virussen, *hackers*, pornografie). Is het ontwerp aangepast en is het niet in strijd met de bestaande wetten ?

Een lid heeft vragen bij de bewaring van de gegevens en in het bijzonder bij de omschrijving van de telecommunicatiediensten. Wat verstaat men onder die diensten? Het ontwerp vermeldt de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten. Wat is de precieze definitie van een verstrekker? Geldt dat ook voor een telefooncentrale in een hotel? Een rekbare definitie van een telecommunicatiedienst leidt tot het bewaren van eender welke communicatie die uitgaat van onverschillig welke plaats.

De bewaringstermijn van 12 maanden lijkt problemen op te leveren voor de operatoren van telecommu-

(coût, etc.). L'intervenant soulève également un problème à ce sujet en ce qui concerne la protection de la vie privée. Pendant un an toutes les activités du citoyen seront conservées. Ceci est extrêmement lourd au niveau de la vie privée. Le citoyen n'a aucune garantie en ce qui concerne l'utilisation de ces données.

Enfin, l'intervenant renvoie à l'avis du Conseil d'État. Il est curieux de fixer un délai minimum. Le projet de loi ne fixe pas de maximum de la durée de conservation.

Une commissaire souhaite déposer un amendement visant à remplacer, à l'article 14, 1º, les mots « ne peut jamais être inférieur à 12 mois » par les mots « ne peut être supérieur à 12 mois ». Le délai minimal d'un an lui semble trop long. Il représente une charge trop importante pour l'opérateur. (*cf. infra* — discussion des articles).

L'intervenante est d'avis que le projet sur la criminalité informatique forme un vaste ensemble avec les projets sur la signature électronique et l'activité des autorités de certification agréées en vue de l'utilisation de signatures digitales. Qu'en est-il de ces deux projets ?

L'intervenante s'interroge sur la nécessité de prévoir des règles particulières pour les saisies du matériel informatique. En quoi ces dispositions particulières sont-elles nécessaires par rapport au droit ordinaire des saisies et des confiscations ? Visent-elles simplement à protéger les personnes qui toucheraient au matériel contre les dommages qu'elles causeraient à ce matériel ?

Le projet de loi à l'examen prévoit également des dispositions particulières sur le respect du secret de l'instruction. En quoi constituent-elles une dérogation aux principes généraux ?

L'intervenante renvoie ensuite à l'avis de la Commission de la protection de la vie privée. Le projet est-il conforme aux attentes de cette commission ?

Un sénateur se réjouit de ce que l'on ait enfin un débat sur l'internet et la société de l'information. On sait que la Belgique accuse un retard énorme en matière de commerce, de gouvernement et de justice électroniques (quoique sur ce dernier plan, on ait lancé récemment des expériences comme la publication de jurisprudence sur l'internet). La Belgique est un des derniers pays d'Europe à adopter une loi sur la criminalité informatique. Il est important d'avoir une bonne législation, car la confiance est le facteur clé de la réussite ou de l'échec du commerce électronique et du développement de l'internet.

L'intervenant fait une observation préliminaire concernant les travaux de la Chambre. On peut cons-

nicatienetwerken (kostprijs, enz.). Spreker vermeldt eveneens een probleem in dit verband dat betrekking heeft op de bescherming van de persoonlijke levenssfeer. Alle activiteiten van de burger zullen gedurende een jaar bewaard blijven. Daarmee wordt een zeer zware druk uitgeoefend op de privacy. De burger heeft geen enkele waarborg in verband met het gebruik van deze gegevens.

Spreker verwijst ten slotte naar het advies van de Raad van State. Het is vreemd dat men een minimale bewaartermijn vaststelt. Het wetsontwerp bepaalt geen maximumduur voor de bewaring.

Een commissielid wenst een amendement in te dienen dat ertoe strekt in artikel 14, 1º, de woorden « mag nooit minder zijn dan 12 maanden » te vervangen door de woorden « mag niet meer zijn dan 12 maanden ». De minimumtermijn van een jaar lijkt haar te lang. Het is een te zware last voor de operator (*cf. infra* — artikelsgewijze bespreking).

Spreekster is van mening dat het ontwerp op de computercriminaliteit één groot geheel vormt met de ontwerpen op de elektronische handtekening en de werking van de certificatiedienstverleners met het oog op het gebruik van elektronische handtekeningen. Hoever staat het met die twee ontwerpen ?

Spreekster vraagt zich af of het noodzakelijk is bijzondere regels te bepalen voor de inbeslagneming van computeruitrusting. In hoeverre zijn die bijzondere bepalingen noodzakelijk rekening houdend met het gewone beslag- en verbeurdverklaringsrecht ? Is het gewoon de bedoeling de personen die aan de apparatuur komen, te beschermen tegen de schade die zij aan die apparatuur zouden toebrengen ?

Het voorliggende ontwerp bepaalt eveneens bijzondere regels om het geheim van het gerechtelijk onderzoek te waarborgen. In hoeverre wijken deze regels af van de algemene beginselen ?

Spreekster verwijst ten slotte naar het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Stemt het ontwerp overeen met de verwachtingen van die commissie ?

Een senator verheugt zich over het feit dat er eindelijk een debat op gang komt met betrekking tot het internet en de informatiemaatschappij. Het is bekend dat België een enorme achterstand vertoont op het vlak van de e-commerce, de e-government en e-justice (hoewel op dit laatste vlak recente experimenten zijn op gang gebracht, zoals de publicatie van rechtspraak op het internet). België is een van de laatste landen in Europa om een wet betreffende de informaticacriminaliteit in te voeren. Een goede wetgeving is belangrijk, aangezien het vertrouwen het kernvraagstuk is van het al dan niet slagen van de e-commerce en de ontwikkeling van het internet.

Een voorafgaande opmerking betreft de werkzaamheden in de Kamer. Het is opvallend dat in het

tater, de manière frappante, que trois parties sont impliquées dans le projet de loi, à savoir les services de police (recherche des délits), la Commission pour la protection de la vie privée (problème du respect de celle-ci) et les fournisseurs d'accès à l'internet (articles 9 et 14). Alors que le projet impose à ces derniers une obligation de collaboration et de conservation des données, ils n'ont pas été associés aux discussions à la Chambre. Le sénateur propose donc d'entendre des représentants de l'organisation fédérative des fournisseurs d'accès à l'internet (ISPA). Ces gens se posent en effet une série de questions ponctuelles au sujet du délai de conservation et des coûts qui résulteront du projet de loi.

Sa deuxième remarque préliminaire concerne la philosophie de la loi en projet. Celle-ci est fondée sur deux principes importants. Le premier transpose la notion de vol dans les nouvelles technologies de l'information. On considère que « ce qui est interdit hors ligne l'est également en ligne ». Le deuxième principe pose clairement que le droit pénal doit rester *l'ultimum remedium*. Compte tenu de ces principes, il est surprenant que le projet passe rapidement sur la définition et l'établissement des éléments constitutifs des nouveaux délits. On peut ainsi citer le fait que dans nombre de définitions de délits, on se contente du dol général. L'intervenant renvoie à ce sujet aux diverses interventions du président de la commission de la Justice de la Chambre.

À un moment donné, on a comparé le piratage informatique au délit de vol. Toutefois, parmi les éléments constitutifs du vol figure également l'intention frauduleuse, alors que le dol général suffit pour le piratage informatique. Le fait de se contenter du dol ne nuit-il pas à la philosophie du projet de loi (en ligne = hors ligne).

En ce qui concerne l'*ultimum remedium*, l'intervenant déplore que le projet de loi ne dise pas qu'il existe divers types de pirates. C'est qu'il faut faire une distinction entre, d'une part, ceux qui font des expériences sur l'internet et, d'autre part, ceux qui s'adonnent, sur l'internet, au piratage informatique à des fins nuisibles et criminelles. Le projet de loi semble les mettre tous dans le même panier. L'on aurait pu prévoir plusieurs degrés d'incrimination ou introduire une série de sanctions alternatives pour les formes moins coupables de piratage informatique. Cela aurait permis de fixer de véritables sanctions pour les pirates criminels dont l'intention est de s'approprier un avantage patrimonial. Il y a un problème du fait qu'il est difficile de définir le piratage informatique. Aux termes du projet de loi, le piratage informatique consiste à accéder à des systèmes informatiques. Un article paru dans *Le Vif-L'Express* du 2 juin critique le caractère imprécis de la disposition qui définit le piratage informatique

wetsontwerp drie partijen zijn betrokken, met name de politiediensten (opsporing van de misdrijven), de Commissie voor de bescherming van de private levenssfeer (vraagstuk van de privacy) en de internetproviders (artikelen 9 en 14). Hoewel het ontwerp aan deze laatste partij een plicht van medewerking en bewaring van gegevens oplegt, kwam zij niet aan bod bij de besprekingen in de Kamer. Aldus stelt de senator voor de overkoepelende organisatie van de internetproviders (ISPA) te horen. Deze mensen hebben immers een aantal punctuele vragen in verband met de bewaringstermijn en de kosten ten gevolge van het wetsontwerp.

Een tweede voorafgaande opmerking betreft de filosofie van het wetsontwerp. Deze is gestoeld op twee belangrijke principes. Een eerste principe transponeert het begrip diefstal in de nieuwe informaticatechnologieën. Er wordt gesteld dat « wat *off-line* niet mag, *on-line* ook niet mag ». Een tweede uitgangspunt stelt duidelijk dat de strafwet het *ultimum remedium* moet blijven. Gelet op deze principes, is het wel opmerkelijk dat het wetsontwerp vrij licht gaat over het definiëren en het vastleggen van de constitutieve bestanddelen van de nieuwe misdrijven. Zo kan men het feit aanhalen dat men zich in heel wat misdrijfomschrijvingen beperkt tot het algemeen opzet. Spreker verwijst terzake naar de verscheidene tussenkomsten van de voorzitter van de commissie voor de Justitie in de Kamer.

Op een bepaald ogenblik werd de *hacking* vergeleken met het misdrijf van diefstal. In de constitutieve elementen van diefstal zit echter het element van bedrieglijk opzet, terwijl voor hacking het algemeen opzet volstaat. Wordt de filosofie van het ontwerp *(on-line = off-line)* niet geschaad door het volstaan van het element van algemeen opzet ?

Wat betreft het *ultimum remedium,* betreurt spreker dat in het wetsontwerp niet werd ingeschreven dat er verscheidene soorten hackers bestaan. Er moet immers een onderscheid worden gemaakt tussen enerzijds mensen die experimenteren op het internet en anderzijds personen die met schadelijke en criminele bedoelingen op het internet hacken. Het wetsontwerp lijkt iedereen over dezelfde kam te scheren. Men had verschillende trappen van strafwaardigheid kunnen inbouwen of men had een aantal alternatieve sancties kunnen inbouwen met betrekking tot een minder schuldige vorm van *hacking.* Er zouden dan echte sancties kunnen worden bepaald voor de criminele hackers die de intentie hebben vermogensvoordeel op te strijken. De moeilijkheid bestaat erin *hacking* te definiëren. Het wetsontwerp bepaalt *hacking* als zijnde « zich toegang verschaffen tot informaticasystemen ». Een artikel van 2 juni in *Le Vif-L'express* hekelt de vaagheid van de bepaling die hacking definieert als zijnde zich toegang te verschaffen tot een

comme le fait de s'ouvrir un accès à un système informatique (une législation floue, floue, floue, ...).

L'intervenant conclut qu'il est difficile de retrouver dans les dispositions citées, ce qui constitue le point de départ de la loi, à savoir le souci d'arriver à une égalité de traitement du *off-line* et du *on-line* et l'*ultimum remedium* dans la loi pénale, parce que tout le monde est traité sur le même pied et que l'on recourt trop rapidement et trop expressément à une peine. En cas de vol, par exemple, il existe une gradation sous la forme du *joyriding*. Pourquoi n'a-t-on pas prévu en l'occurrence que celui qui s'adonne au piratage informatique sans produire aucun effet nuisible, sans se procurer un avantage patrimonial, peut être assimilé à un *joyrider*?

Une troisième remarque concerne le repérage des auteurs. Le ministre a mis en évidence la nécessité d'une législation en la matière et il a expliqué que la loi en projet aurait été suffisamment efficace pour s'attaquer au virus *I love you*. Comment s'y serait-on pris? Aurait-on repéré les auteurs philippins par une recherche sur le réseau ou aurait-on considéré aussi que ceux qui ont répandu le virus chez nous sont des criminels potentiels? Avait-on l'intention d'assimiler les personnes qui ont propagé les virus à des criminels potentiels? Le Conseil d'État a dit clairement qu'en définissant unilatéralement dans une loi des moyens permettant d'accomplir des actes de recherche à l'étranger, l'on contreviendrait aux règles du droit pénal actuel, si bien que les moyens de preuve générés pourraient être irréguliers.

Une membre s'interroge sur l'adéquation du type de sanctions que le projet de loi en discussion maintient en vigueur. Elle a l'impression que les peines proposées sont inappropriées.

Comment peut-on réagir contre les sites internet racistes et contre des propos personnels racistes transmis par courrier électronique?

S'agissant du délai de conservation visé à l'article 14 du projet, l'intervenante se dit favorable au maintien du délai de 12 mois qui permet de mieux garantir les droits de la victime. En Grande-Bretagne, le délai est de 18 mois.

Un autre membre renvoie à l'avis critique du Conseil d'État concernant le projet de loi initial. Dans quelle mesure a-t-on ou n'a-t-on pas tenu compte de ses diverses observations? Celles-ci portaient principalement sur la compétence territoriale du législateur et du pouvoir judiciaire (pp. 44-45) et l'application du principe d'égalité (pourquoi ne reprend-on pas, pour ce qui est des délits informatiques, les conditions spécifiques qui doivent être remplies en ce qui concerne le délit de droit commun).

Une commissaire s'interroge sur la nécessité de prévoir des incriminations spécifiques, dès que l'outil

informaticasysteem *(une législation floue, floue, floue ...).*

Spreker besluit dat het uitgangspunt van de wet, namelijk een gelijke behandeling van *off-line* en *on-line*, en het *ultimum remedium* in de strafwet, moeilijk terug te vinden is in de vermelde bepalingen, omdat alle personen over dezelfde kam worden geschoren en men al te snel en uitdrukkelijk grijpt naar een aantal straffen. Bij diefstal bijvoorbeeld bestaat er een gradatie als joyriding. Waarom heeft men hier dan niet gesteld dat degene die hackt zonder een schadelijk effect, zonder zich een vermogensvoordeel te verschaffen, kan worden gelijkgesteld met een joyrider?

Een derde bemerking betreft de opsporing van daders. De minister heeft de nood aan wetgeving aangetoond en uitgelegd dat de wet in ontwerp afdoende zou zijn geweest bij de aanpak van het *I love you*-virus. Hoe zou dit dan worden aangepakt? Zou men de personen in de Filippijnen via de netwerkzoeking hebben opgespoord of worden ook de personen die het virus hier verder hebben verspreid beschouwd als potentiële criminelen? Was het de bedoeling ook de mensen die de virussen hebben *geforwarded* als potentiële criminelen te beschouwen? De Raad van State stelde duidelijk dat het eenzijdig vastleggen in een wet van middelen om opsporingsdaden te stellen in het buitenland een inbreuk zou vormen op het thans gekende strafrecht, wat dan onregelmatige bewijsmiddelen zou kunnen opleveren.

Een lid heeft vragen met betrekking tot de adequaatheid van de strafmiddelen die in het voorliggende wetsontwerp worden gehandhaafd. Zij heeft de indruk dat de voorgestelde straffen niet adequaat zijn.

Hoe kan worden gereageerd op racistische websites en persoonlijke racistische uitingen via e-mail?

Betreffende de bewaringstermijn bepaald in artikel 14 van het ontwerp, verklaart spreekster zich voorstander van het behoud van de termijn van minstens 12 maanden. Aldus kunnen de rechten van het slachtoffer beter worden gewaarborgd. In Groot-Brittannië bedraagt de termijn 18 maanden.

Een ander lid verwijst naar het kritisch advies van de Raad van State bij het oorspronkelijke wetsontwerp. Op welke wijze is men aan die diverse opmerkingen al dan niet tegemoetgekomen? De opmerkingen hielden voornamelijk verband met de territoriale bevoegdheid van de wetgever en de rechterlijke macht (blz. 44-45), en de toepassing van het gelijkheidsbeginsel (waarom zijn de specifieke vereisten van het gemeenrechtelijk delict niet terug te vinden in het computerdelict?).

Een commissielid vraagt zich af of specifieke strafbaarstellingen nodig zijn, alleen omdat gebruik wordt

informatique est utilisé; les infractions (faux en écriture etc.) semblent valables quel que soit l'outil utilisé. Faut-il dès lors prévoir d'autres dispositions, sauf en ce qui concerne la responsabilité de ceux qui mettent le réseau à disposition? L'intervenante cite l'exemple de la pornographie enfantine. L'article 383*bis* du Code pénal est utilisé dans le cadre de la poursuite des délits en matière de pornographie enfantine. Cette matière réprime la fabrication et la possession des images. Les bandes dessinées et les images de synthèse avec des enfants sont également visées. Pourquoi ne pas garder les incriminations de type général qui pourraient s'appliquer quel que soit le moyen?

Un sénateur croit pouvoir conclure de certaines déclarations de fournisseurs d'accès que la police judiciaire réclame déjà régulièrement la communication de numéros IP, et ce, sur la base d'un mandat qui les y autorise. Sur la base de quelle disposition légale peut-elle demander les données internet visées à l'article 14?

Un membre est d'avis que la législation actuelle donne déjà les moyens nécessaires pour répondre à des délits de pédophilie, de racisme ou de fascisme. Ce ne sont pas là de bons exemples pour illustrer la nécessité de légiférer. Par contre, ils illustrent le souci européen de contrôle du contenu. La nécessité de légiférer se situe surtout sur le plan des délits propres à la technique informatique (pénétration ou sabotage des réseaux, etc.).

Une commissaire souligne l'intérêt économique d'Internet, qui est plus qu'un réseau de communication. Les utilisateurs veulent vendre et acheter par l'internet. Il faut donc que les données soient fiables et que les personnes puissent acheter en toute sécurité. Il existe incontestablement une demande de sécurisation au niveau mondial de la part des opérateurs économiques et financiers. Ceci implique une possibilité de sensibilisation, non seulement pour les données économiques. L'intervenante souligne le besoin de sécurisation sur le plan économique. Cette inquiétude freine le commerce électronique.

D'où la nécessité du projet de loi relatif à la signature électronique.

Un commissaire demande quelles sont les garanties dont on dispose quand on transmet le numéro de sa carte de crédit par l'internet. L'intéressé ne peut-il pas utiliser ce numéro des fins impropres?

Un sénateur souligne que la situation peut varier en fonction de la firme qui émet la carte. Une banque peut être plus souple qu'une autre. La directive sur le commerce électronique et le projet de loi relatif à la signature électronique pourraient apporter une solution. Le problème en question se pose parfois aussi dans le monde de la téléphonie (transmission d'un numéro de carte Visa par téléphone). La banque élec-

gemaakt van informatica. De bestaande strafbaarstellingen (valsheid in geschrifte, enz.) lijken bruikbaar ongeacht het gebruikte instrument. Is er dan nog nood aan andere bepalingen dan die over de verantwoordelijkheid van degenen die het netwerk ter beschikking stellen? Spreekster geeft het voorbeeld van de kinderporno. Bij de vervolging van misdrijven inzake kinderporno wordt artikel 383*bis* van het Strafwetboek gebruikt. Dat artikel bestraft het vervaardigen en het bezit van afbeeldingen. Ook strips of samengestelde afbeeldingen met kinderen vallen daaronder. Waarom niet de algemene strafbaarstellingen behouden die toepasbaar zijn ongeacht het middel?

Een senator meent te hebben vernomen van de internetproviders dat de gerechtelijke politie reeds vandaag geregeld IP-nummers opvraagt, aan de hand van een bevel. Op welke wettelijke basis kunnen zij zich beroepen om deze internetgegevens bedoeld in artikel 14 op te vragen?

Een lid vindt dat de huidige wetgeving de nodige middelen biedt om misdrijven inzake pedofilie, racisme of fascisme te bestraffen. Het is niet op dat vlak dat een wetgevend optreden nodig is. Het illustreert wel de drang die in Europa bestaat om de inhoud van de sites te controleren. Wetgevend optreden is vooral nodig voor de misdrijven die eigen zijn aan de informaticatechniek (binnenbreken of saboteren van netwerken, enz.).

Een commissielid benadrukt het economisch belang van het internet, dat meer is dan een communicatienetwerk. De gebruikers willen kopen en verkopen via internet. De gegevens moeten dus betrouwbaar zijn opdat mensen in alle veiligheid kunnen kopen. Wereldwijd vragen de economische en financiële operatoren onweerlegbaar om meer beveiliging. Spreekster benadrukt de nood aan meer beveiliging op economisch vlak aangezien het gevoel van onveiligheid de elektronische handel afremt.

Daarom is het wetsontwerp betreffende de elektronische handtekening noodzakelijk.

Een lid vraagt welke garantie men heeft als men via internet het nummer van zijn kredietkaart doorgeeft. Kan de betrokkene dit nummer dan niet aanwenden voor andere doeleinden?

Een senator vestigt de aandacht op het feit dat de situatie kan verschillen naargelang de firma die de kaart uitgeeft. De ene bank is flexibeler dan de andere. De richtlijn op E-commerce en het wetsontwerp met betrekking tot de elektronische handtekening zouden een oplossing vormen. Dit probleem rijst ook wel reeds in de telefonische wereld (doorgeven van visakaartnummer via de telefoon). E-bank zou

tronique pourrait constituer une solution dans la mesure où elle transmettrait les données en tant qu'intermédiaire.

Un commissaire fait valoir que l'on peut pour diverses raisons demander à un client de communiquer téléphoniquement le numéro de sa carte Visa. On peut le faire notamment pour vérifier si la carte en question n'est pas une carte recherchée ou volée et si le client est suffisamment solvable. L'intervenant souligne par ailleurs que le fournisseur n'est sûr de rien tant que le client n'a pas signé pour que le paiement puisse être effectué. Le client a même encore la possibilité d'émettre une contestation après avoir signé (par exemple lorsqu'il a signé sans compléter la case réservée à l'unité monétaire).

B. Réponse du ministre

Le ministre confirme qu'il y avait effectivement deux manières de réagir face aux problèmes que pose l'usage de l'informatique. La voie américaine n'a pas été retenue, vu que le principe de maîtrise du contenu lui semble plus préoccupant que la protection du réseau.

Il y a donc une différence entre les pays européens dès lors que certains de ces pays ont opté pour le système américain et d'autres, pour le système européen (surtout les pays anglo-saxons).

On a soulevé la question de l'évaluation du projet de loi. N'est-il pas d'ores et déjà dépassé ? Le ministre répond négativement. Le groupe de travail qui a été mis sur pied lors de l'apparition du virus *I love you* est arrivé à la constatation que la loi en projet aurait pu offrir une réponse appropriée.

Les résultats du sommet de Paris du G8 n'ont en effet pas été particulièrement diffusés auprès du public, mais les pays participants de l'Union européenne leur ont cependant donné la répercussion nécessaire.

Le problème, qui subsiste d'ailleurs dans le monde entier, est que les pays doivent de toute urgence changer de mentalité sur la question de leur souveraineté nationale. D'autre part, on observe au cours des réunions des ministres de la Justice et de l'Intérieur, une évolution favorable considérable dans plusieurs pays européens. Le projet de loi à l'examen présente en effet beaucoup de similitudes avec les systèmes qui existent en France et aux Pays-Bas. Il s'impose absolument d'arriver à une uniformisation au niveau européen.

Le ministre précise qu'il n'y a pas de directive européenne en matière de criminalité informatique. Cela s'explique par le fait que cette matière relève du troisième pilier, pour lequel il n'existe encore aucune

een oplossing vormen, waarbij de bank dan als een tussenpersoon de gegevens doorgeeft.

Een lid oppert dat er verschillende redenen zijn waarom men de klant verzoekt het nummer van zijn visakaart door te bellen. Men kan hierdoor nakijken of het niet gaat om een gezochte of gestolen kaart en of de klant voldoende kredietwaardig is. Verder onderstreept het lid dat de leverancier geen poot heeft om op te staan zolang de klant niet heeft getekend om de betaling uit te voeren. De klant heeft zelfs nog mogelijkheid om te betwisten, nadat hij heeft getekend (bijvoorbeeld wanneer hij heeft getekend zonder de munteenheid in te vullen).

B. Antwoord van de minister

De minister antwoordt dat men inderdaad kan reageren op twee manieren op de problemen die rijzen in verband met het computergebruik. De Amerikaanse oplossing is niet gevolgd, aangezien de minister meer belang hecht aan de controle op de inhoud dan aan de bescherming van het netwerk.

Er is aldus een onderscheid tussen de Europese landen, omdat de enen eerder voor het Amerikaanse systeem, en de anderen dan weer voor het Europese systeem hebben geopteerd (voornamelijk de Angelsaksische landen).

De vraag werd gesteld naar de evaluatie van het wetsontwerp. Is het wetsontwerp niet reeds voorbijgestreefd? De minister antwoordt ontkennend. De werkgroep die werd opgericht naar aanleiding van het *I love you*-virus, kwam tot de vaststelling dat de wet in ontwerp een passend antwoord had kunnen bieden.

De resultaten van de top van Parijs van de G8 werden inderdaad niet erg verspreid onder het publiek, maar de 4 landen van de Europese Unie die hieraan hebben deelgenomen, zorgden wel voor de nodige repercussie.

Het probleem, dat trouwens in de gehele wereld blijft bestaan, is dat de landen dringend hun mentaliteit moeten herzien inzake nationale soevereiniteit. Anderzijds merkt men wel, tijdens de vergaderingen van de ministers van Justitie en van Binnenlandse Zaken, dat er een aanzienlijke gunstige evolutie plaatsheeft in verschillende Europese landen. Het voorliggende wetsontwerp vertoont immers veel gelijkenis met de bestaande systemen in Frankrijk en Nederland. Uniformisering op het Europees vlak zou absoluut noodzakelijk zijn.

De minister verduidelijkt dat op het vlak van informaticacriminaliteit geen Europese richtlijnen bestaan. Dit verklaart zich wegens het feit dat deze materie behoort tot de derde zuil, waarover nog geen

directive. Si des directives sont édictées à l'avenir, on pourra parvenir très rapidement à une unification européenne. Le projet de loi à l'examen s'est cependant basé sur les résolutions du Conseil de l'Europe.

En ce qui concerne la concordance entre le présent projet de loi et la loi relative à la protection de la vie privée, le ministre répond que la Commission de la protection de la vie privée a été entendue à la Chambre. On a tenu compte de l'avis qu'elle a émis à cette occasion et le projet initial a été amendé dans ce sens.

En ce qui concerne l'ordre public et les bonnes mœurs, le ministre précise que l'on a retenu ces notions afin de disposer de la plus grande souplesse possible. Ce qui relève aujourd'hui de l'ordre public, n'en relèvera peut-être plus demain. La notion de bonnes mœurs évolue elle aussi en permanence. Le pouvoir judiciaire disposera donc d'une marge d'appréciation.

Une peine d'emprisonnement peut sembler disproportionnée pour certains. Elle est néanmoins prévue de la même manière dans tous les pays européens. De plus, il y a aussi d'autres possibilités telles que les amendes, la saisie, la confiscation, etc. Cet arsenal permet donc de réagir de la manière la plus adéquate possible à une situation en constante mutation.

En ce qui concerne le contenu des notions d'opérateur et de fournisseur, le ministre renvoie aux résolutions du Conseil de l'Europe. C'est ainsi que Belgacom est avant tout opérateur et que « Skynet » est par exemple surtout prestataire de services. Le ministre ne juge pas opportun de définir ces notions.

Le délai de conservation de 12 mois fait en effet l'objet de manœuvres de lobbying. Le ministre est convaincu de la nécessité de prévoir un délai minimum. On peut également prévoir éventuellement un délai maximum. Les pays qui nous entourent ont également prévu un délai d'environ un an.

Le ministre peut comprendre qu'il faille affiner la notion de protection de la vie privée.

En ce qui concerne le projet de loi relatif à la signature électronique, le ministre déclare que le sujet est en cours de discussion à la Chambre par le biais d'un amendement du gouvernement à une proposition de M. Geert Bourgeois (voir la proposition de loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire (doc. Chambre, n^{os} 50-38/1 à 7). Cette proposition de loi permet aux avocats de communiquer plus facilement dans le cadre d'une procédure judiciaire, par exemple en déposant des conclusions par e-mail. La validité de ces actes est toutefois subordonnée à l'utilisation d'une signature électronique.

richtlijnen bestaan. Indien er in de toekomst richtlijnen zullen komen, zal een Europese unificatie zeer snel kunnen worden bereikt. Nochtans baseerde het voorliggende wetsontwerp zich wel op de resoluties van de Raad van Europa.

Wat betreft de concordantie van het voorliggend wetsontwerp met de wet met betrekking tot de bescherming van het privé-leven, antwoordt de minister dat de Commissie voor de bescherming van de private levenssfeer werd gehoord in de Kamer. Er werd rekening gehouden met het advies dat daaruit voortvloeide en het initiële ontwerp werd in die zin geamendeerd.

Met betrekking tot de openbare orde en de goede zeden, verduidelijkt de minister dat deze begrippen werden weerhouden om over een zo groot mogelijke soepelheid te beschikken. Wat vandaag van openbare orde is, is dit morgen misschien niet meer. Ook het begrip goede zeden is onderhevig aan een constante evolutie. De rechterlijke macht beschikt aldus over een marge van appreciatie.

De gevangenisstraf kan voor sommigen buiten proportie lijken. Nochtans wordt deze straf in alle Europese landen op dezelfde wijze bepaald. Bovendien bestaan er ook andere mogelijkheden, zoals de geldboeten, het beslag, verbeurdverklaring, enz. Aldus wordt de mogelijkheid geboden op de meest adequate manier te reageren op een toestand die aan constante wijziging onderhevig is.

Met betrekking tot de inhoud van de begrippen « operatoren » en « leveranciers ... » verwijst de minister naar de resoluties van de Raad van Europa. Zo is Belgacom in de eerste plaats operator en is « Skynet » bijvoorbeeld vooral dienstenverstrekker. Het lijkt de minister niet opportuun deze begrippen te definiëren.

De bewaringstermijn van 12 maanden is inderdaad voorwerp van lobbying. De minister is er van overtuigd dat een minimumtermijn dient te worden bepaald. Eventueel kan ook een maximumtermijn worden voorzien. Ook de ons omringende landen bepalen een termijn van ongeveer een jaar.

De minister kan begrijpen dat de bescherming van het privé-leven zou moeten worden verfijnd.

Met betrekking tot het wetsontwerp over de elektronische handtekening, verklaart de minister dat dit, bij wijze van regeringsamendement op een wetsvoorstel van de heer Geert Bourgeois, in de Kamer ter bespreking voorligt (zie wetsvoorstel tot introductie van nieuwe telecommunicatiemiddelen in de gerechtelijke en de buitengerechtelijke procedure (zie Stuk Kamer, nrs. 50-38/1 tot 7). Dit wetsvoorstel geeft de mogelijkheid aan de advocaten gemakkelijker te communiceren binnen een gerechtelijke procedure, bijvoorbeeld door het neerleggen van besluiten per e-mail. Uiteraard kunnen deze handelingen slechts geldigheid bezitten als zij kunnen worden ondertekend door een elektronische handtekening.

Cette signature électronique peut se présenter de différentes manières (suite de chiffres, scannage de signature, etc.). Le problème est qu'il est plus aisé de reproduire ou de copier une signature électronique qu'une signature manuscrite. Il n'est pas certain qu'un juge puisse assimiler une suite de chiffres à une signature au sens du Code pénal actuel. C'est pour cette raison que le système du faux en informatique (copiage facilité) doit être prévu.

Le projet de loi concernant les activités de certification des signatures électroniques prévoit qu'un tiers de confiance peut agréer ou donner une bonne fin de l'utilisation de la signature. Il se pose un problème au regard du droit européen. On peut difficilement imaginer de confier à quelques personnes déterminées la capacité d'agréer seules ces signatures électroniques (liberté d'activités); une mise en parallèle avec les règles européennes doit se faire. Ce deuxième projet est donc moins avancé à l'heure actuelle.

À propos des règles particulières concernant la saisie et la confiscation, le ministre souligne les aspects suivants. Une première particularité concerne la possibilité que l'on doit avoir de saisir des données informatiques, qui ne se présentent pas nécessairement sous la forme de photographies ou d'autres supports matériels. La loi en projet est donc assez vague sur ce point, puisqu'elle doit pouvoir tenir compte des évolutions ultérieures.

Un deuxième aspect important concerne le matériel. L'ordinateur peut être un moyen de commettre une infraction. Cet ordinateur peut par exemple se trouver dans un réseau d'une entreprise. Le moyen utilisé pour commettre une infraction peut être saisi; la saisie d'un ordinateur qui se trouve dans un réseau peut poser des problèmes pour d'autres personnes qui ne sont pas concernées.

Faut-il pouvoir saisir un ensemble ou une particularité, un élément individualisé? Faut-il tout saisir ou simplement empêcher un accès? Les dispositions particulières sont donc une réponse à une donnée technique, notamment la mise en réseau de l'ensemble des ordinateurs.

Une autre particularité est que la personne qui se sert de l'ordinateur pour commettre une infraction, n'est pas nécessairement le propriétaire du matériel. Faut-il alors bloquer tout le système ou en retirer simplement une partie? Ces spécificités sont dues au développement technologique actuel, qui font une autre manière d'appréhender la commission d'infractions et la saisie des moyens qui servent à commettre une infraction.

De elektronische handtekening kan verschillende vormen aannemen (cijferreeks, scannen van de handtekening, enz.). Het probleem is dat een elektronische handtekening makkelijker kan worden nagemaakt of gekopieerd dan een geschreven handtekening. Het is niet zeker dat een rechter een cijferreeks kan beschouwen als een handtekening in de zin van het huidige Strafwetboek. Daarom moet het systeem van valsheid in informatica (makkelijker te kopiëren) ingevoerd worden.

Het wetsontwerp betreffende de werking van de certificatiedienstverleners met het oog op het gebruik van elektronische handtekeningen bepaalt dat een derde-vertrouwenspersoon de handtekening kan erkennen of het gebruik ervan beëindigen. Hier rijst een probleem ten opzichte van het Europees recht. Vanwege het vrij verrichten van diensten kan men de bevoegdheid om de elektronische handtekeningen te erkennen moeilijk alleen aan bepaalde personen toekennen; dit moet dus in overeenstemming worden gebracht met de Europese regelgeving. Het tweede ontwerp is op dit ogenblik dus minder vergevorderd.

Met betrekking tot de bijzondere regels voor beslag en verbeurdverklaring, verwijst de minister naar volgende aspecten. Een eerste bijzonderheid is dat men de mogelijkheid moet hebben beslag te leggen op informaticagegevens, die niet noodzakelijk de vorm hebben van foto's of andere materiële dragers. Daarom is de wet in ontwerp ook vaag op dit punt. Zij wil immers tegemoetkomen aan alle verdere evolutie.

Een tweede belangrijk aspect is de apparatuur. Een computer kan een middel zijn om een misdrijf te plegen. Deze computer kan bijvoorbeeld deel uitmaken van het netwerk van een onderneming. Het middel dat wordt gebruikt om het misdrijf te plegen kan in beslag worden genomen; de inbeslagneming van een computer die tot een netwerk behoort, kan problemen opleveren voor andere personen die niets met het misdrijf te maken hebben.

Moet men een geheel in beslag kunnen nemen of een welbepaald onderdeel? Moet men alles in beslag nemen of alleen de toegang afsluiten? De bijzondere bepalingen zijn dus een antwoord op een technisch gegeven, namelijk het opnemen van de computers in een netwerk.

Een ander probleem is dat de persoon die de computer gebruikt om een misdrijf te plegen, niet noodzakelijk de eigenaar daarvan is. Moet het systeem dan geblokkeerd worden of een onderdeel eruit verwijderd? Deze specifieke problemen zijn een gevolg van de huidige technologische ontwikkelingen, die een andere aanpak nodig maken van misdrijven en van de daarbijhorende inbeslagneming van de middelen die hebben gediend om het misdrijf te plegen.

Le ministre n'est pas d'accord avec la remarque selon laquelle le projet de loi porterait des règles dérogatoires à propos du secret de l'instruction.

Les règles s'appliquent. Le fait de pouvoir faire une perquisition dans un réseau n'implique pas la possibilité pour l'enquêteur d'utiliser ces informations. Le principe du secret de l'instruction est établi et ne varie pas.

Un membre a demandé quel était l'avis de la Commission de la vie privée. Un représentant de cette commission a été entendu par la commission de la Justice de la Chambre.

Leur avis n'était pas négatif par rapport au projet de loi, et n'appelait pas d'autres observations qu'une prise en compte dans le cadre de l'élaboration de l'arrêté royal d'exécution.

Un arrêté d'exécution sera, en effet, nécessaire pour déterminer quelles sont les données que les opérateurs doivent conserver. Dès que cet arrêté sera élaboré, la Commission pour la protection de la vie privée rendra un avis.

En ce qui concerne la condition du dol général ou de l'intention frauduleuse pour les différentes infractions, le ministre répond qu'on a établi un parallèle avec les infractions ordinaires (faux en écriture, fraude); pour ce qui est du respect du principe d'égalité concernant les faux en écriture, on a suivi l'avis du Conseil d'État.

À propos du *hacking*, le ministre peut confirmer qu'il s'agit d'un délit *sui generis* tout à fait nouveau. Les différentes possibilités de *hacking* sont retenues à l'article 6.

Pour ce qui est des sanctions, le ministre constate qu'elles sont conformes aux sanctions applicables aux infractions ordinaires. Le juge peut toutefois décider d'infliger une sanction alternative (interdiction générale ou limitée d'utiliser un ordinateur).

Le ministre souligne qu'il ne peut souscrire au contenu de l'article paru dans la *Le vif-L'express* et qui taxe le projet d'imprécision.

À propos du virus *I love you*, le ministre relève que, s'il a pu se répandre si rapidement sur toute la planète, c'est parce qu'il a été transmis par l'intermédiaire de Microsoft et a ainsi pu toucher 95% des internautes. Si la loi à l'examen avait déjà existé, elle aurait permis aux victimes de déposer plainte pour sabotage. Dans les circonstances actuelles, les victimes ont été forcées de recourir à une procédure civile, qui ne peut malheureusement rien donner, vu que ce dommage n'est pas couvert, à l'heure actuelle, par les compagnies d'assurances.

On a posé la question de savoir s'il était possible de punir les délits racistes commis par le biais d'Internet. Les dispositions existantes de la loi Moureaux

De minister kan niet akkoord gaan met de opmerking dat het wetsontwerp afwijkende regels zou bepalen in verband met het geheim van het onderzoek.

De regels moeten worden toegepast. Een zoeking in een netwerk naar aanleiding van een huiszoeking impliceert niet dat de onderzoeker die informatie kan gebruiken. Het beginsel van het geheim van het onderzoek staat vast en daarvan wordt niet afgeweken.

Een lid vroeg naar het advies van de Commissie ter bescherming van de persoonlijke levenssfeer. De commissie werd gehoord in de commissie voor de Justitie van de Kamer.

Het advies van die commissie over het wetsontwerp was niet negatief. Er werd alleen opgemerkt dat met het advies rekening moet worden gehouden bij het opstellen van het uitvoeringsbesluit.

Inderdaad zal een uitvoeringsbesluit noodzakelijk zijn om vast te leggen welke gegevens de operatoren moeten bewaren. Dan zal de Commissie voor de bescherming van de persoonlijke levenssfeer een advies uitbrengen.

Met betrekking tot de problematiek van de vereiste van algemeen opzet of bedrieglijk opzet in verband met de verschillende misdrijven, antwoordt de minister dat hier een parallel werd getrokken met de gewone misdrijven (valsheid in geschrifte, bedrog); in verband met de eerbiediging van het gelijkheidsbeginsel in verband met de valsheid in geschrifte, werd het advies van de Raad van State gevolgd.

Met betrekking tot *hacking*, kan de minister bevestigen dat dit een volledig nieuw misdrijf is «*sui generis*». In artikel 6 werden de verschillende mogelijkheden van *hacking* in overweging genomen.

Wat de sancties betreft, stelt de minister vast dat deze gelijklopend zijn met de sancties toepasselijk bij de gewone misdrijven. De rechter kan echter beslissen een alternatieve sanctie op te leggen (algemeen of beperkt verbod voor het gebruik van een computer).

De minister merkt op dat hij niet kan instemmen met de inhoud van het in *Le vif-L'express* verschenen artikel dat het ontwerp van vaagheid verwijt.

Met betrekking tot het *I love you*-virus merkt de minister op dat dit virus zich zo vlug over de gehele wereld heeft kunnen verspreiden dankzij het feit dat het verspreid werd via Microsoft en aldus 95% van de internetgebruikers kon bereiken. Indien deze wet reeds zou hebben bestaan, zou dit de slachtoffers hebben toegelaten klacht in te dienen wegens sabotage. Nu werden de slachtoffers ertoe gedwongen zich te beroepen op een burgerlijke procedure, die helaas niets uithaalt, gezien deze schade thans niet wordt gedekt door de verzekeringsmaatschappijen.

De vraag rees naar de mogelijkheid om racistische misdrijven die gepleegd worden via internet aan te pakken. Hierop zijn de bestaande bepalingen van de

s'appliquent en l'espèce, dès lors que l'infraction est la même quoique commise par un moyen nouveau, l'ordinateur.

Un membre a posé des questions concernant l'avis du Conseil d'État. On a tenu compte des observations relatives au principe d'égalité. Pour ce qui est de la compétence territoriale, le ministre estime qu'une collaboration internationale est absolument nécessaire sur le plan de la criminalité informatique.

Pour ce qui concerne la compétence territoriale, l'avis du Conseil d'État n'a pas été suivi dans la mesure où les données techniques auxquelles les enquêteurs sont confrontés sont telles qu'il faut permettre de dépasser les limites d'un territoire et d'adopter une conception plus souple.

Le ministre explique ensuite que la nécessité du faux et de la fraude informatique peuvent se justifier par le fait que deux comportements sont visés. D'une part, il y a les infractions commises au moyen d'un ordinateur et, d'autre part, il y a les infractions qui sont commises contre un système informatique. À l'heure actuelle, les infractions commises contre un système informatique ne sont pas suffisamment protégées en Belgique. En ce qui concerne les infractions commises au moyen d'un ordinateur, l'intervenant renvoie à ses propos concernant la signature électronique. En ce qui concerne l'escroquerie informatique, le représentant souligne la particularité d'une personne qui trompe une machine. L'escroquerie dans le Code pénal actuel concerne une personne qui trompe une autre personne. Il s'agit donc d'une autre logique. De plus, il faut prendre en considération que le droit pénal s'interprète de manière restrictive.

Le ministre déclare qu'il est exact que l'utilisation d'une carte de crédit sur l'internet n'est pas tout à fait sûre.

Le ministre renvoie à un tableau qui représente l'ensemble des points connectés sur l'Internet lorsqu'une demande est envoyée.

Cela peut concerner 80 000 ordinateurs. Une communication du Sénat vers la Chambre peut passer par Paris, Washington, Tokyo, etc. Un nombre important de personnes peut donc intervenir sur le réseau. La particularité d'internet est de permettre le développement d'une structure décentralisée. On passe donc par un ensemble d'endroits. Le tout est de localiser ces endroits.

Ce qui intéresse les autorités judiciaires, ce n'est pas d'imposer des obligations très fortes aux opérateurs.

Les difficultés rencontrées par les *Computer Crime Units* se situent au niveau de se trouver face à une personne qui est victime d'une infraction (par exemple menace de mort par courrier électronique). Il est

wet-Moureaux van toepassing. Het misdrijf is immers hetzelfde, ook al wordt het via een nieuw middel, de computer, gepleegd.

Een lid had vragen met betrekking tot het advies van de Raad van State. De opmerkingen met betrekking tot het gelijkheidsbeginsel kregen navolging. Met betrekking tot de territoriale bevoegdheid, is de minister van oordeel dat internationale samenwerking op het vlak van informaticacriminaliteit absoluut noodzakelijk is.

Wat de territoriale bevoegdheid betreft werd het advies van de Raad van State niet gevolgd daar de technische gegevens waarmee de onderzoekers geconfronteerd worden van die aard zijn dat het mogelijk moet zijn de grenzen van een grondgebied te overschrijden en een soepelere houding aan te nemen.

De minister legt vervolgens uit dat de nood aan twee begrippen, namelijk valsheid in informatica en informaticabedrog, gewettigd kan zijn omdat er twee gedragsvormen beoogd worden. In eerste instantie zijn er de misdrijven die gepleegd worden met behulp van een computer en vervolgens zijn er de misdrijven die gepleegd worden tegen een computersysteem. Thans zijn de overtredingen gepleegd tegen een computersysteem in België onvoldoende beschermd. Wat de misdrijven betreft die gepleegd zijn met behulp van een computer, verwijst spreker naar zijn betoog over de elektronische handtekening. Wat het informaticabedrog betreft, wijst de vertegenwoordiger op het bijzonder geval van een persoon die een machine bedriegt. In het Strafwetboek slaat bedrog steeds op een persoon die een andere persoon bedriegt. Het gaat dus om een andere logica. Daarenboven moet in overweging genomen worden dat het strafrecht steeds restrictief geïnterpreteerd wordt.

De minister legt uit dat het gebruik van een kredietkaart op internet inderdaad niet helemaal veilig is.

De minister verwijst naar een tabel die alle op internet aangesloten punten weergeeft wanneer een verzoek wordt verstuurd.

Daarbij kunnen 80 000 computers betrokken zijn. Een boodschap van de Senaat aan de Kamer kan via Parijs, Washington, Tokio, enz. de Kamer bereiken. Er kan dus een groot aantal personen op het net tussenbeide komen. Kenmerkend voor het internet is dat het mogelijk is een gedecentraliseerde structuur te ontwikkelen. Er worden dus tal van plaatsen aangedaan. Het probleem rijst die plaatsen te lokaliseren.

Het is niet de bedoeling van de gerechtelijke autoriteiten strenge verplichtingen op te leggen aan de operatoren.

Geconfronteerd worden met een persoon die het slachtoffer is van een misdrijf (bijvoorbeeld doodsbedreiging per e-mail) behoort tot het soort moeilijkheden waarmee de *computer crime units* te maken

difficile de retrouver la personne qui a envoyé le courrier électronique, vu qu'il faut alors retracer l'ensemble du parcours à travers une masse d'ordinateurs. Au moment où la personne dépose plainte, il est actuellement trop tard de retracer les données (certains opérateurs respectent une durée de conservation de 8 jours).

Des membres ayant fait remarquer que cet exemple n'est pas bien choisi et que le même problème se pose lorsque les menaces de mort sont lancées à partir d'une cabine téléphonique, le ministre répond que l'on peut localiser cette dernière. Il est certain en tout cas que les délais de conservation ne sont pas suffisamment longs. On se trouve en fait en présence d'un nouveau délai de prescription, fixé par les opérateurs; l'action publique doit s'éteindre après un délai d'environ deux mois, parce que les données nécessaires à la preuve ne sont plus disponibles. La question est de savoir si le délai de conservation de 12 mois est suffisant. Doit-on prévoir un délai maximum de 12 mois ou un délai minimum de 12 mois ?

On peut en débattre, mais il faut se rappeler qu'en matière pénale, le délai de prescription est en principe de 5 ans. Il faut trouver un équilibre. Il n'est pas question de permettre aux fournisseurs d'accès à Internet d'imposer les délais et de ne garder que les données qui pourraient éventuellement servir à défendre leurs propres intérêts. Le gouvernement aurait éventuellement pu proposer un autre délai. Un certain consensus s'est toutefois dégagé autour du délai de 12 mois.

Le problème qui se pose est un problème de traçabilité. Si les autorités judiciaires ne peuvent pas suivre et refaire le parcours dans un délai raisonnable, il s'agit d'un empêchement d'agir correctement vis-à-vis d'un moyen qui sert à commettre des infractions.

C. Répliques des membres

Un membre souhaiterait avoir des précisions à propos de la saisie. Comment peut-on saisir des données ? Il est, en effet, très facile de les copier. Quel est donc l'intérêt de la saisie ?

Le ministre répond que l'on aurait effectivement pu prévoir que les dispositions actuelles sur la saisie s'appliquent dans le contexte informatique. On a cependant estimé qu'en raison de la spécificité du secteur et de la diversité des cas de figure, il serait indiqué, sinon nécessaire pour la sécurité juridique, d'avoir une approche diversifiée de la question.

Dans certains cas, il suffira effectivement de saisir des disquettes, ou même des copies de sauvegarde. Dans d'autres cas (par exemple, en matière de pornographie infantile), cela ne sera cependant pas suffisant.

krijgen. Het is moeilijk de persoon die de e-mail verstuurd heeft, op te sporen omdat daarvoor een spoor gevolgd moet worden dat via een groot aantal computers loopt. Op het ogenblik waarop de persoon klacht indient, is het te laat om de gegevens op te sporen (sommige operatoren nemen een bewaringstermijn van 8 dagen in acht).

Op de opmerkingen dat dit voorbeeld niet goed is gekozen en dat hetzelfde probleem rijst bij het uiten van doodsbedreigingen vanuit een telefooncel, antwoordt de minister dat een telefooncel te lokaliseren is. Het staat in ieder geval vast dat de bewaringstermijnen niet lang genoeg zijn. In feite komt dit neer op een nieuwe verjaringstermijn, die wordt vastgesteld door de operatoren; de strafvordering dient te vervallen na een termijn van ongeveer twee maanden, aangezien de gegevens voor bewijs niet meer beschikbaar zijn. De vraag rijst wel of de bewaringstermijn van 12 maanden voldoende is. Moet men maximaal 12 maanden of minimaal 12 maanden vaststellen ?

Hierover kan een debat plaatsvinden. Men moet wel rekening houden met het feit dat de verjaringstermijn in strafzaken in principe vijf jaar bedraagt. Men moet een evenwicht vinden. Het is niet de bedoeling dat de internetproviders de termijnen opleggen en slechts de gegevens bewaren ter eventuele verdediging van hun eigen belangen. De regering zou eventueel een andere termijn hebben kunnen voorstellen. De termijn van 12 maanden werd echter gedragen door een zekere consensus.

Het probleem dat hier rijst, is een probleem van opsporing. Indien de gerechtelijke autoriteiten de afgelegde weg niet binnen een redelijke termijn kunnen volgen en overdoen, kan er niet correct worden opgetreden ten aanzien van een middel dat dient om misdrijven te plegen.

C. Replieken van de leden

Een lid wenst nadere informatie over het beslag. Hoe kan men beslag leggen op gegevens ? Deze kunnen immers zeer makkelijk worden gekopieerd. Waar zit dan het belang van het beslag ?

De minister antwoordt dat men inderdaad had kunnen stellen dat de huidige bepalingen over inbeslagneming zouden van toepassing zijn in de informaticacontext. Men heeft echter geoordeeld dat de context hier vrij specifiek is en dat er diverse casusgevallen zijn, waarbij het aangewezen is, zo niet noodzakelijk omwille van reden van rechtszekerheid, om een gediversifieerde aanpak te hebben.

In bepaalde gevallen zal het inderdaad volstaan om diskettes in beslag te nemen, of ook de back-ups. Er zijn andere situaties (bijvoorbeeld kinderpornografie) waar dit echter niet volstaat.

Les possibilités de copie sont effectivement une des caractéristiques de la technologie informatique. À l'impossible nul n'est tenu. Il se peut très bien que l'on ait stocké des copies des informations dans son ordinateur. Ce problème est insoluble. Par le présent projet de loi, on se borne à réaliser ce qui peut l'être.

Une membre a l'impression que tout le monde est d'accord pour qu'un délai soit imposé aux fournisseurs d'accès. L'intervenante renvoie au passage du rapport de la Chambre concernant l'audition des représentants des services de police (doc. Chambre, nº 50-213/4, pp. 42 et suivantes). Il arrive que sur les «*chatlines*», l'activité soit telle que si les conversations se poursuivent, les données qui y figuraient sont écrasées; est-il techniquement possible de sauvergarder les données dans un tel cas?

Si l'on opte pour un délai plus long que celui des pays voisins (quels délais dans quels pays), ne risque-t-on pas alors de voir les fournisseurs d'accès à internet conserver ailleurs leurs données?

À la Chambre, on a cité l'exemple de «America On Line», qui conserve ses données aux États-Unis. Il faudra alors nécessairement faire appel à l'aide juridique internationale. N'est-il donc pas préférable d'imposer un délai plus court?

Un membre fait remarquer que les données relatives aux paiements électroniques (par exemple par carte de crédit aux stations-service) sont conservées pendant quelque temps. Quel est le délai de conservation de ces données par les organismes financiers? Jusqu'à quand peut-on remonter en cas d'enquête judiciaire?

L'intervenante estime aussi que la personne qui veut commettre un acte criminel utilisera d'autres moyens si une loi existe. Le citoyen honnête pourra véritablement être suivi à la trace grâce aux moyens électroniques (voir aussi la carte d'identité sociale). Les criminels éviteront d'utiliser tous les moyens susceptibles de les trahir.

Un sénateur estime que le problème du délai de conservation mérite que l'on s'y attarde. Il est important que l'on entende les fournisseurs d'accès à internet, étant donné qu'ils conservent déjà des données à l'heure actuelle. Ce délai varie. Il serait intéressant de savoir quelles sont les conditions de conservation et quelles données sont conservées précisément. L'intervenant souligne que le coût constitue leur principale objection à l'encontre d'un délai de conservation trop long. La police judiciaire peut aujourd'hui déjà demander les numéros à Belgacom (écoutes téléphoniques). Quel est le délai de conservation dans le cas de Belgacom? Les autorités belges reçoivent une facture de Belgacom à partir du moment où celle-ci reçoit une demande de transmission de données (arti-

Dat er mogelijkheden zijn tot kopie is uiteraard eigen aan de informatietechnologie. Men kan enkel doen wat haalbaar is. Het is perfect mogelijk dat men kopieën heeft van de informatie gestockeerd in zijn computer. Dit probleem is onoplosbaar. Het wetsontwerp poogt enkel het haalbare te realiseren.

Een lid heeft de indruk dat iedereen akkoord gaat met het feit dat een termijn wordt opgelegd aan de providers. Spreekster verwijst naar het verslag van de Kamer over de hoorzitting met de politiediensten (Stuk Kamer, nr. 50-213/4, blz. 42 en volgende). Op de *chatlines* is de activiteit op sommige momenten zodanig groot dat door het verderzetten van de gesprekken de gegevens die er voordien reeds opgestonden worden vernietigd; is het dan technisch mogelijk de gegevens te bewaren?

Indien men de termijn lang gaat houden in vergelijking met de omliggende landen (welke termijnen in welke landen) bestaat dan niet het risico dat de internetproviders hun gegevens elders gaan bewaren?

In de Kamer werd het voorbeeld aangehaald van «America On Line» die zijn gegevens in de VS bewaart. Dan zal men noodzakelijkerwijze een beroep moeten doen op internationale rechtshulp. Kan men niet beter besluiten tot het opleggen van een minder lange termijn?

Een lid merkt op dat de elektronische betalingen (bijvoorbeeld per kredietkaart aan benzinepompen) bewaard worden gedurende enige tijd. Welk is deze termijn van bewaring door de financiële instellingen? Hoelang kan een gerechtelijk onderzoek teruggaan?

Tevens is spreekster van oordeel dat de persoon die een criminele daad wil stellen, andere middelen zal aanwenden indien er een wet bestaat. De eerlijke burger kan men werkelijk op de voet volgen via de elektronische middelen (zie ook SIS-kaart). De criminelen zullen alle middelen die hen kunnen verraden vermijden.

Een senator is van oordeel dat de problematiek van de bewaringstermijn een discussie verdient. Het is belangrijk de internetproviders te horen, aangezien zij ook vandaag reeds gegevens bijhouden. Deze termijn varieert. Het zou interessant zijn te weten hoe zij dit doen en welke gegevens zij precies bijhouden. Spreker onderstreept dat de problematiek van de kostprijs determinerend is bij hun bezwaar tegen een te lange bewaringstermijn. De gerechtelijke politie kan vandaag reeds nummers opvragen bij Belgacom (telefoontap). Welke is de bewaringstermijn voor Belgacom? Belgacom factureert de Belgische overheid op het ogenblik dat zij een vraag krijgt om gegevens door te spelen (artikel 109*ter* van de Telecomwet). Indien de providers het personeel dat de gegevens ter

cle 109*ter* de la loi sur les télécommunications). Si les fournisseurs d'accès peuvent facturer le travail réalisé par le personnel qui met les données à disposition, ainsi que le délai, le débat sera plus ouvert.

En ce qui concerne l'obligation de conservation, et le fait que les fournisseurs d'accès pourraient s'établir ailleurs, l'intervenant renvoie à la disposition qui prévoit que la conservation doit avoir lieu dans les frontières du Royaume. La question se pose de savoir si cette disposition est conforme à la législation européenne (liberté de circulation des capitaux, liberté de circulation des biens). Peut-on obliger une société à conserver systématiquement les données sur place ?

Vient encore la remarque du ministre selon laquelle un délai de conservation trop court donnerait aux fournisseurs d'accès à Internet la possibilité d'instaurer un nouveau délai de prescription. Dans la logique des choses, cela signifierait qu'il faille alors porter le délai de conservation à 5 ans. Telle n'est cependant pas la tendance européenne. Une discussion avec les fournisseurs d'accès sur le coût pourrait apporter une réponse aux questions qui se posent.

Un membre estime qu'il serait intéressant de savoir quel est le délai de conservation proposé par la *National Computer Crime Unit.*

Le ministre répond que ses représentants pouvaient marquer leur accord sur un délai d'un an. Ils n'ont cependant pas été entendus sur la question spécifique du délai de conservation.

En ce qui concerne le délai de conservation des données afférentes aux paiements électroniques, le représentant du ministre ne peut donner aucune réponse, même pas en ce qui concerne Belgacom.

Un membre attire l'attention sur le fait que la criminalité informatique porte sur des délits qui revêtent généralement un caractère transfrontalier. Comment détermine-t-on quel est le droit pénal matériel qui est applicable (voir droit international privé) ?

Un autre membre demande quelles sont les règles applicables à un adolescent de quatorze ans qui copie de la musique pour son usage personnel ou à des fins commerciales. La loi en question est-elle applicable ?

Quelles sanctions peut-on infliger à un site iranien qui explique comment fabriquer des bombes ?

Le ministre répond que le droit international privé n'est pas applicable à la criminalité informatique, celle-ci relevant du droit pénal. On pourrait éventuellement concevoir un droit privé européen pour ce qui est de la signature électronique (voir directive).

MP3 est un logiciel qui permet d'écouter des supports audiovisuels sur internet. On peut écouter et enregistrer à des fins privés. Il y a une infraction dès qu'il y a commercialisation, vu que les droits d'auteur ne sont pas respectés. L'infraction existe s'il y a des

beschikking stelt mogen factureren, alsook de termijn, zal het debat vlotter verlopen.

In verband met de bewaringsplicht, en het feit dat providers zich elders zullen vestigen, verwijst spreker naar de bepaling die voorziet dat de bewaringsplicht moet uitgevoerd worden binnen de grenzen van het Rijk. De vraag rijst of dit conform de Europese wetgeving is (vrijheid van kapitaal, vrij verkeer van goederen). Kan men een bedrijf verplichten telkens de gegevens ter plaatse te houden ?

Een laatste punt betreft de opmerking van de minister dat een te korte bewaringstermijn aan de internetprovider de kans zou verschaffen een nieuwe verjaringstermijn in te voeren. Als men consequent wil zijn, betekent dit dat men dan de bewaringstermijn zou moeten brengen op vijf jaar. Dit is echter niet de Europese tendens. Een gesprek met de providers over de kostprijs zou een antwoord kunnen verschaffen op de gestelde vragen.

Een lid is van oordeel dat het interessant zou zijn te weten welke bewaringstermijn wordt vooropgesteld door de *National Computer Crime Unit*.

De minister antwoordt dat zij konden akkoord gaan met een termijn van een jaar. Zij werden echter niet over de specifieke problematiek van de bewaringstermijn gehoord.

Wat betreft de bewaringstermijn van gegevens van elektronische betaling, kan de vertegenwoordiger van de minister geen antwoord geven, ook niet wat Belgacom betreft.

Een lid vestigt de aandacht op het feit dat informaticacriminaliteit een misdrijf betreft dat meestal over de grenzen wordt gepleegd. Hoe wordt bepaald welke materiële strafwet van toepassing is (zie IPR) ?

Een ander lid vraagt welke regelen van toepassing zijn op een 14-jarige die muziek kopieert voor zichzelf of om commerciële doeleinden. Is de betreffende wet van toepassing ?

Welke sanctie kan men toepassen op een Iranese website die meldt hoe men bommen moet maken ?

De minister antwoordt dat IPR niet toepasselijk is op de informaticacriminaliteit, die in het domein van het strafrecht valt. Eventueel kan een Europees privaatrecht worden uitgedacht in verband met de digitale handtekening (zie richtlijn).

MP3 is software die het mogelijk maakt audiovisuele dragers op internet te beluisteren. Men kan die dragers beluisteren en de informatie registreren voor privé-doeleinden. Er is sprake van een misdrijf zodra dit voor handelsdoeleinden gebeurt omdat er geen

sites qui commercialisent des œuvres piratées ou copiées au moyen de MP3.

La loi de 1994 sur les droits d'auteur est applicable. Il s'agit d'un autre contexte, protégé par la loi sur les droits d'auteur.

En ce qui concerne les attentats à la bombe, le ministre renvoie aux règles applicables en matière de pornographie enfantine. On peut dire que les dispositions pénales en la matière s'appliquent dans la même mesure à un tel comportement sur internet; tout comportement punissable dans le monde « papier » est punissable dans la même mesure sur internet. On maintient un parallélisme maximal. Le droit international privé n'est pas applicable en l'espèce. Lorsqu'il s'agit d'un site web à l'étranger, il faut tenir compte de la charge culturelle des délits, par exemple, le racisme qui est permis aux États-Unis au nom de la liberté d'expression, mais qui est interdit chez nous. Se pose en effet la question du point de rattachement territorial. Il s'agit d'une question de fait, qui consiste à savoir à quel moment ce point de rattachement est présent. Les solutions liées au droit international privé ne sont pas réalistes à court terme, bien que l'on tente d'arriver à une harmonisation (Conseil de l'Europe), principalement sur le plan des délits (surtout pour ce qui est du *hacking*). L'harmonisation sur le plan des délits va de pair avec une amélioration de la coopération internationale, dans le sens d'une délivrance plus rapide des commissions rogatoires, d'une modernisation des techniques de recherche, etc. (*hard core cyber crime offences*).

En ce qui concerne la base juridique relative à la consultation des données, il faut distinguer deux points.

Il y a, d'une part, les techniques de recherche spécifiques, les mesures d'enquête qui sont actuellement prévues par le Code d'instruction criminelle (articles 46*bis* et 88*bis* du Code d'instruction criminelle, à savoir la consultation des données de télécommunications, des données d'abonnés, etc.). Cette législation a été adaptée récemment (en 1998) afin de rendre neutre du point de vue technologique la terminologie des dispositions qui était fortement axée sur la téléphonie traditionnelle. On parle de télécommunications. Les mesures de recherche existent donc déjà et peuvent être appliquées.

Le problème auquel on est confronté et qui est à l'origine de l'obligation spécifique de conservation est le cas de figure dans lequel les magistrats interrogent un fournisseur d'accès et que celui-ci n'est plus en possession des données. On peut affirmer que les règles relatives au délai de conservation sont insérées afin de garantir l'efficacité de certaines mesures d'enquête et de recherche actuellement inscrites dans le Code d'instruction criminelle.

auteursrechten betaald worden. Er is een misdrijf indien bepaalde sites illegaal gekopieerde werken met behulp van MP3 in de handel brengen.

De wet van 1994 op de auteursrechten is van toepassing. Het gaat hier om een andere context, die beschermd wordt door de wet op de auteursrechten.

Wat betreft bomaanslagen, verwijst de minister naar de toestand inzake kinderpornografie. Men kan zeggen dat de strafrechtelijke bepalingen terzake in dezelfde mate toepasselijk zijn op dergelijk gedrag op het internet; een bepaald gedrag dat in de papieren wereld strafbaar is, is in dezelfde mate strafbaar als het op internet gebeurt. Een maximaal parallellisme wordt gehandhaafd. Het IPR is niet ter zake. Als het gaat om een website in het buitenland moet men rekening houden met de cultuurgeladenheid van de misdrijven (zie racisme: in de VS: vrijheid van meningsuiting, bij ons verboden). Daar rijst inderdaad de vraag naar het territoriaal aanknopingspunt. Het is een feitenkwestie op welk moment dit aanwezig is. IPR-oplossingen zijn op korte termijn niet realistisch. Men poogt wel te komen tot (Raad van Europa) harmonisering voornamelijk op het vlak van de misdrijven (zie voornamelijk *hacking*). Aan de harmonisering op het vlak van de misdrijven wordt verbeterde internationale samenwerking gekoppeld in de zin van versnelde rogatoire commissies, nieuwe opsporingstechnieken, enz. (*hard core cyber crime offences*).

Met betrekking tot de juridische grondslag over het opvragen van gegevens is het van belang twee zaken te onderscheiden.

Enerzijds heeft men de specifieke opsporingstechnieken, onderzoeksmaatregelen die thans voorzien zijn in het Wetboek van strafvordering (artikel 46*bis* en 88*bis* van het Wetboek van strafvordering, met name het opvragen van telecommunicatiegegevens; abonneegegevens, enz.). Die wetgeving is recent (in 1998) aangepast om de terminologie in de bepalingen die zeer sterk was toegespitst op de traditionele telefoon technologieneutraal te maken. Men spreekt over telecommunicatie. De opsporingsmaatregelen bestaan dus nu reeds en kunnen nu worden toegepast.

Het probleem waarmee men wordt geconfronteerd en waarvoor de specifieke bewaringsplicht op de proppen komt, is het geval waar de magistraten een provider bevragen en de providers de gegevens niet meer bezitten. Men kan stellen dat de regels met betrekking tot de bewaringstermijn worden ingevoegd om de effectiviteit van bepaalde thans in het Wetboek van strafvordering voorziene onderzoeks- en opsporingsmaatregelen te garanderen.

Une membre fait référence au trafic de drogue organisé au niveau international, bien que cette activité se situe dans la sphère privée. Il semble bon à l'intervenante que l'on inscrive dans les textes un point de rattachement territorial. Cela serait tout bénéfice pour la sécurité juridique.

Un sénateur renvoie au principe du «traitement en ligne = traitement hors ligne». D'une part, on fait la comparaison avec le vol et le faux en écriture et, d'autre part, le *hacking* est qualifié de nouveau délit. On ne fait la comparaison que lorsque cela arrange; cette comparaison devrait toujours être faite, surtout en ce qui concerne les éléments constitutifs. Le vol a pour élément constitutif une intention frauduleuse. Le faux en écritures a pour élément constitutif le dol spécial. En ce qui concerne le faux en informatique et le *hacking*, le dol général suffit tout à coup. Le Conseil d'État a souligné à plusieurs reprises les risques de violation du principe d'égalité. À cela s'ajoute que l'on s'écarte du principe de base. L'on n'aperçoit toujours pas pour quelles raisons les éléments constitutifs du vol, à savoir le dol spécial, ne sont pas utilisés dans la définition du délit de *hacking* ou de *hacking* informatique. Il y a là un manque de cohérence.

Le ministre répond qu'il y a une grande différence entre le vol et le *hacking*. Ces éléments sont différents. Il n'y a aucune comparaison possible.

Le *hacking* consiste à s'introduire dans un système, il ne s'agit pas nécessairement de voler des données; on peut s'y introduire et s'y maintenir sans autres agissements illicites. Le *hacking* peut plutôt être comparé à une violation d'un réseau.

Un membre se demande s'il ne s'agit pas en l'occurrence d'un problème de mentalité. Il arrive fréquemment que les juges n'osent pas aller jusqu'au bout et appliquer les dispositions existantes au monde de l'informatique.

Le ministre précise que le projet de loi vise à combattre trois catégories de délit:

Premièrement, il y a les délits liés au racisme, à la xénophobie, à la pornographie, etc., dont on constate qu'ils sont de même nature si ce n'est que le moyen d'expression diffère. On ne modifie en rien la manière dont ils sont punis. Les dispositions en la matière sont formulées de manière neutre, du point de vue de la technologie, et sont manifestement applicables.

Il y a en outre le faux en écritures et l'escroquerie. Il est clair qu'un doute existe tant dans la jurisprudence que dans la doctrine. Dans un tel cas, on donne la priorité à la sécurité juridique. Afin de souligner clairement que le dol spécial prévu à l'article 193 est également applicable, on a amendé le texte sur le faux en écritures par rapport au projet initial.

Een lid verwijst naar drugshandel, die internationaal wordt geregeld, ook al bevindt dit zich in de private sfeer. Het lijkt spreekster goed een territoriaal aanknopingspunt in de teksten in te schrijven. Dit komt de rechtszekerheid ten goede.

Een senator verwijst naar het uitgangspunt «*on-line* = *off-line*-behandeling». Enerzijds wordt de vergelijking gemaakt met diefstal en valsheid in geschrifte, anderzijds wordt *hacking* als een nieuw misdrijf bestempeld. Men vergelijkt enkel als het goed uitkomt; de vergelijking zou steeds moet worden getrokken, zeker wat betreft de constitutieve bestanddelen. Diefstal heeft bedrieglijk opzet als constitutief bestanddeel. Valsheid in geschrifte heeft bijzonder opzet als constitutief bestanddeel. Wat de valsheid in informatica en de *hacking* betreft volstaat plots het algemeen opzet. De Raad van State heeft telkenmale gewezen op de eventuele schending van het gelijkheidsbeginsel; daarbovenop komt dat men afwijkt van het uitgangspunt. Het blijft volkomen onduidelijk waarom men de constitutieve elementen van diefstal, respectievelijk bijzonder opzet, niet hanteert in het definiëren van het misdrijf van *hacking*, respectievelijk in *informaticahacking*. Er is een gebrek aan consistentie.

De minister antwoordt dat er een groot verschil bestaat tussen diefstal en *hacking*. De elementen zijn verschillend. Er is geen vergelijking mogelijk.

Hacking komt neer op binnendringen in een systeem. Het gaat niet noodzakelijk om diefstal van de gegevens; men kan in een systeem binnendringen en daar blijven zonder verdere ongeoorloofde handelingen. *Hacking* is eerder te vergelijken met het kraken van een netwerk.

Een lid vraagt zich af of het hier niet een probleem van mentaliteit betreft. De rechters durven vaak niet tot het uiterste gaan en de bestaande bepalingen toepassen op de informaticawereld.

De minister verduidelijkt dat het wetsontwerp is uitgegaan van drie categorieën van delicten:

Ten eerste zijn er de delicten van racisme, xenofobie, pornografie, enz. waarbij men stelt dat de delicten dezelfde zijn, maar enkel het medium verschilt. Men raakt niet aan de bestraffing ervan. De bepalingen terzake zijn technologieneutraal geformuleerd en zijn duidelijk toepasselijk.

Verder zijn er de valsheid in geschrifte en oplichting. Daar is het duidelijk dat twijfel bestaat zowel in jurisprudentie als doctrine. In zulk geval wordt de knoop doorgehakt in het voordeel van de rechtszekerheid. Om duidelijk te stellen dat het bijzonder opzet van artikel 193 eveneens toepasselijk is, is de tekst over de valsheid in geschrifte geamendeerd ten opzichte van het oorspronkelijke ontwerp.

Les éléments actuels constitutifs du faux en écritures, y compris l'intention de frauder et le préjudice potentiel, ont donc aussi été intégrés dans le texte (voir les articles 2 et 3). Le texte actuel a été totalement adapté, en ce qui concerne les éléments constitutifs, aux dispositions existantes en matière de faux en écritures. Pour ce qui est de la fraude informatique, il convient de se demander si l'on peut tromper une machine ou non.

Le troisième type de délits sont ceux touchant à la confidentialité et à la disponibilité des systèmes informatiques et des données. À cet égard, on s'en est tenu au consensus existant au niveau international. Il faut en quelque sorte établir une analogie avec les dispositions existantes (aux Pays-Bas par exemple, on parle de violation de l'ordinateur par analogie à la violation de domicile), mais on peut par ailleurs prévoir clairement que le *hacking* n'est pas du vol. Il peut d'ailleurs y avoir *hacking* sans que la moindre donnée ait été dérobée. On a choisi, dans le cas du *hacking* et du sabotage, d'indiquer qu'il s'agit de nouveaux intérêts juridiques en pleine expansion nécessitant une protection *sui generis.* Ce serait faire offense à la réalité que de les assimiler à des délits traditionnels.

Un membre demande si ce raisonnement participe du consensus qui existe au sein du Conseil de l'Europe. S'il n'y a pas le moindre consensus au niveau international, cela n'a que peu d'utilité.

Le ministre renvoie à la recommandation de 1989 du Conseil de l'Europe relative au droit pénal matériel. Cette recommandation est aujourd'hui partiellement dépassée. Et tel est même le cas de la recommandation sur laquelle on s'est basé pour le droit de la procédure pénale. Depuis 1997, un comité d'experts travaille au sein du Conseil de l'Europe à l'élaboration d'un projet de convention en matière de criminalité informatique. On essaie ainsi de parvenir à un consensus et à une certaine harmonisation en matière de délits.

Si l'on envisage le *hacking* séparément, un sénateur se demande si certaines formes de *hacking* pourraient ne pas être condamnables. Certaines formes de *hacking* ne sont pas malveillantes et n'appellent donc pas de sanction.

En ce qui concerne la discussion sur les faux en écritures, le ministre a fait état de la concordance et du parallélisme des éléments constitutifs qu'apporterait l'amendement de M. Erdman. Selon l'intervenant, ce n'est pas exact (l'article 193 parle de l'intention frauduleuse alors qu'à l'article 210*bis*, celle-ci n'est pas mentionnée expressément); il n'y a pas d'uniformité entre ces deux articles.

Le ministre répond que la structure du chapitre relatif au faux en écritures est complexe. Les éléments constitutifs visés à l'article 193 reviennent pour les diverses variantes prévues aux sections 1, 2, 2*bis* et 3,

De bestaande constitutieve elementen voor de valsheid in geschrifte, met inbegrip van het bedrieglijk opzet en het potentiële nadeel, zijn derhalve ook geïntegreerd (zie artikelen 2 en 3). De huidige tekst is in termen van constitutieve elementen volledig gealigneerd met de bestaande bepalingen over schriftvervalsing. Voor informaticabedrog rijst de vraag of men al dan niet een machine kan bedriegen.

De derde categorie betreft de misdrijven tegen de vertrouwelijkheid, beschikbaarheid van informaticasystemen en gegevens. Hiervoor werd de internationale consensus nagevolgd. Er is ergens een parallel te trekken met de bestaande bepalingen (zie in Nederland spreekt men in analogie met de huisvredebreuk over computervredebreuk), maar anderzijds kan men stellen dat *hacking* duidelijk geen diefstal is. Er kan trouwens *hacking* zijn zonder dat er iets wordt weggenomen. Bij *hacking* en sabotage werd de keuze gemaakt te stellen dat het om nieuwe zich ontwikkelende rechtsbelangen gaat die een *sui generis* bescherming noodzakelijk maken. Men zou hier de realiteit geweld aandoen door deze te assimileren met traditionele misdrijven.

Een lid vraagt of deze redenering de consensus wegdraagt van de Raad van Europa. Als er geen enkele consensus bestaat op internationaal vlak, heeft dit weinig nut.

De minister verwijst naar de aanbeveling van 1989 van de Raad van Europa die het materiële strafrecht betreft. Deze aanbeveling is thans gedeeltelijk voorbijgestreefd. Zelfs de aanbeveling die als basis diende voor het strafprocesrecht is reeds ten dele voorbijgestreefd. Sinds 1997 is er een comité van experten werkzaam in de schoot van de Raad van Europa om een ontwerp van overeenkomst op te stellen inzake informaticacriminaliteit. Aldus probeert men tot een consensus te komen en tot harmonisering van de misdrijven.

Indien de discussie van *hacking* autonoom wordt gevoerd, vraagt een senator zich af of bepaalde vormen van *hacking* niet strafwaardig kunnen zijn. Bepaalde vormen van *hacking* zijn niet kwaadaardig en behoeven geen bestraffing.

Wat betreft de discussie valsheid in geschrifte, verwees de minister naar de overeenstemming en de gelijklopendheid van de constitutieve elementen door het amendement van de heer Erdman. Volgens spreker is dit onjuist (artikel 193 spreekt over het bedrieglijk opzet, terwijl artikel 210*bis* het bedrieglijk opzet niet expliciet vermeldt); er is geen uniformiteit tussen deze artikelen.

De minister verwijst naar de ingewikkelde structuur van het hoofdstuk over de valsheid in geschrifte. De constitutieve elementen als bepaald in artikel 193 komen terug voor de verschillende varianten, voor-

et donc aussi pour l'article 210*bis*. Il y a donc une modification par rapport au projet initial.

Un sénateur en conclut que le dol général ne suffit que pour le *hacking* (article 6). Pourquoi le dol général suffit-il en l'occurrence et ne requiert-on pas l'intention frauduleuse ?

Le ministre répond que le *hacking* est en fait considéré comme une sorte de délit préparatoire qui peut se présenter à des degrés divers. La peine portée à l'article 550*bis*, § 1er, est aussi beaucoup moins sévère que celle qui réprime le faux en informatique ou la fraude. À mesure que le degré de *hacking* augmente, les peines maximales s'alourdissent. On fait une distinction entre les diverses catégories de *hackers* en fonction de la gravité de l'abus.

Plusieurs membres estiment que l'article 550*bis*, § 3, proposé, n'est pas tout à fait clair.

Un sénateur se réfère à l'article 550*bis*, § 3, 2º, qui constitue une circonstance aggravante. Est-il possible de faire du *hacking* sans faire usage d'un système informatique ?

Un membre relève que beaucoup de jeunes cherchent à découvrir où se situent les limites. On prend automatiquement connaissance des données et on se retrouve tout aussi automatiquement en situation de circonstance aggravante.

Un sénateur a l'impression qu'en légiférant de manière trop stricte, on pénaliserait toute forme de curiosité qui se manifesterait sur l'internet, sans intention méchante.

Le ministre répond que la disposition doit se lire dans la logique de l'article. Le § 3 cerne le cas où l'on s'introduit dans un système alors qu'on n'y est pas autorisé, pour ensuite utiliser celui-ci.

Un membre estime que l'on peut compter sur la sagesse des juges.

Étant donné que plusieurs questions se posent, principalement à propos de la conservation des données, la commission décide d'organiser une audition de représentants de l'ISPA (*Internet Service Providers Association*) et de la NCCU (*National Computer Crime Unit*).

D. Audition de représentants de la cellule *National Computer Crime Unit* de la police judiciaire, de la *Computer Crime Unit* du parquet de Bruxelles et d'ISPA Belgium (*Internet Service Providers Association*)

M. Olivier van Cutsem (ISPA Belgium) explique que l'ISPA est une fédération de fournisseurs d'accès à internet en Belgique. Elle regroupe également des sociétés qui s'occupent de webdesign, c'est-à-dire la

zien in afdeling 1, 2, 2*bis*, en afdeling 3, dus ook voor artikel 210*bis*. Er is dus een wijziging ten opzichte van het oorspronkelijk ontwerp.

Een senator besluit dat enkel voor de *hacking* het algemeen opzet volstaat (artikel 6). Waarom volstaat het algemeen opzet hier en is er niet de vereiste van bedrieglijk opzet ?

De minister antwoordt dat *hacking* eigenlijk wordt beschouwd als een soort voorbereidend delict dat in verschillende gradaties kan voorkomen. Ook de strafmaat in artikel 550*bis*, § 1, is veel lager dan de strafmaat voor valsheid in informatica of bedrog. Naarmate de situatie van *hacking* zwaarder is, heeft men zwaardere maximumstraffen. Er wordt een differentiatie gemaakt tussen verschillende categorieën van *hackers* naargelang de ernst van het misbruik.

Verscheidene leden zijn van oordeel dat het voorgestelde artikel 550*bis*, § 3, niet helemaal duidelijk is.

Een senator verwijst naar artikel 550*bis*, § 3, 2º », welk een verzwarende omstandigheid uitmaakt. Bestaat er mogelijkheid te *hacken* zonder gebruik te maken van een computersysteem ?

Een lid wijst op het probleem dat veel jongeren uitzoeken waar de grenzen zijn; men neemt automatisch kennis van de gegevens waardoor men automatisch in de verzwarende omstandigheid zit.

Een senator heeft de indruk dat men door al te strikte wetgeving elke vorm van nieuwsgierigheid op het internet zonder schadelijke bedoelingen bestraft.

De minister antwoordt dat de bepaling moet worden gelezen in de logica van het artikel. Paragraaf 3 bepaalt de situatie waarbij men binnendringt als niet-gerechtigde in een systeem en er is een daaropvolgend gebruik van het systeem.

Een lid is van oordeel dat kan worden gerekend op de wijsheid van de rechters.

Aangezien verscheidene vragen rijzen, voornamelijk over de bewaring van de gegevens, besluit de commissie een hoorzitting te organiseren met ISPA (*Internet Service Providers Association*) en vertegenwoordigers van de NCCU (*National Computer Crime Unit*).

D. Hoorzitting met vertegenwoordipers van de *National Computer Crime* van de gerechtelijke politie, de *Computer Crime Unit* bij het parket te Brussel, en ISPA Belgium (*Internet Service Providers Association*)

De heer Olivier van Cutsem (ISPA Belgium) legt uit dat ISPA een vereniging is van internetproviders in België. Zij biedt ook onderdak aan bedrijven die zich bezighouden met webdesign, dat wil zeggen het ont-

création des sites internet, ainsi que des sociétés spécialisées en consultance en matière d'internet. C'est une fédération ouverte à tous les acteurs en Belgique du monde de l'internet.

L'ISPA représente plus de 90 % du marché des fournisseurs d'accès à internet en Belgique. La plateforme ISPA est donc vraiment représentative. Une des missions de l'ISPA est également de promouvoir l'utilisation de l'internet et de favoriser le développement de la société d'information.

Internet ne se fait pas sans les réseaux et les opérateurs de réseaux en Belgique, que ce soit Belgacom, BT, Worldcom ou un autre. Le message que l'intervenant fera passer à leur égard est que, ce qui est dit dans le cadre de son exposé est en majeure partie partagé par les opérateurs de réseaux.

Au moment de l'affaire Dutroux, en août 1996, les professionnels ont pris connaissance de la nécessité d'avoir un code de déontologie et de coopérer avec les autorités judiciaires. Un code de déontologie a été créé par l'ISPA en collaboration avec l'IBPT, l'Institut belge des postes et télécommunications, et avec le ministère de la Justice. Chaque membre de l'ISPA doit souscrire à ce code. C'est une sorte d'autorégulation qui a été mise en place. En 1999, un protocole de collaboration avec le ministre de la Justice et le ministre des Télécommunications a été signé. Ce protocole vise à combattre les actes illicites sur internet et principalement les infractions pénales.

L'intervenant explique que les coûts pour les fournisseurs d'accès à internet et les fournisseurs de services quant à la conservation des données, seront dans l'avenir de plus en plus importants. Il faut donc veiller à ne pas imposer des obligations supplémentaires à ces fournisseurs de services, ce qui aurait pour effet désastreux de les obliger à procéder à des investissements trop lourds et trop importants, et de mettre en péril leur activité.

Plus on met d'entraves au développement des entreprises et de leurs activités commerciales sur internet, moins d'entreprises voudront se lancer sur internet. Le but est de travailler ensemble et de manière constructive pour limiter et réduire ce nombre d'entraves et ne pas en créer de nouvelles. Le risque est clairement identifié, à savoir un risque de délocalisation des activités économiques.

L'ISPA, avec les autorités judiciaires, a mis en place un système de corégulation, un système de « travailler ensemble ». Cette collaboration existe déjà et les membres de la *National Computer Crime Unit* ne le démentiront pas.

L'ISPA et les fournisseurs d'accès à internet en général collaborent déjà avec les autorités judiciaires et avec les autorités publiques en Belgique, afin de promouvoir l'internet mais également d'avoir un internet *« safe »*, sûr, propre, sans comportement illicite.

werpen van internetsites, alsmede aan bedrijven die gespecialiseerd zijn in internetconsultance. Het is een vereniging die openstaat voor al wie in België actief is in de internetwereld.

ISPA vertegenwoordigt meer dan 90% van de markt van internetproviders in België en is dus werkelijk representatief. Een van de taken van ISPA is ook het gebruik van het internet en de ontwikkeling van de informatiemaatschappij bevorderen.

Zonder de netwerken en de Belgische netwerkoperatoren, ongeacht of dat nu Belgacom, BT, Worldcom of andere zijn, is er geen internet. Spreker merkt op dat de netwerkoperatoren het grotendeels eens zijn met wat in het kader van zijn uiteenzetting is gezegd.

Ten tijde van de Dutroux-zaak in augustus 1996 hebben de vakmensen beseft dat er nood was aan een deontologische code en aan samenwerking met de gerechtelijke autoriteiten. ISPA heeft die deontologische code opgesteld in samenwerking met het BIPT en met het ministerie van Justitie. Elk lid van ISPA moet die code onderschrijven. Er is dus een vorm van zelfregulering. In 1999 werd een samenwerkingsprotocol gesloten met de minister van Justitie en de minister van Telecommunicatie. Dat protocol wil de ongeoorloofde handelingen op internet bestrijden en vooral de misdrijven.

Spreker verklaart dat de kosten voor de internetproviders en de dienstverleners op het gebied van de gegevensbewaring in de toekomst zullen toenemen. Men moet er dus voor zorgen dat aan die dienstverleners geen bijkomende verplichtingen worden opgelegd; het rampzalig gevolg daarvan zou immers zijn dat zij verplicht worden tot te grote en te zware investeringen waardoor hun activiteit in gevaar komt.

Hoe meer hinderpalen bedrijven moeten overwinnen om hun commerciële activiteiten op het internet te ontwikkelen, hoe minder bedrijven op het internet aanwezig zullen willen zijn. Het is de bedoeling constructief samen te werken om het aantal hinderpalen te beperken en er vooral geen nieuwe bij te maken. Het risico is duidelijk, namelijk een verschuiving van de economische activiteit.

ISPA heeft met de gerechtelijke autoriteiten een coreguleringssysteem ingevoerd, een soort samenwerkingsmodel. Die samenwerking bestaat nu al en de leden van de *National Computer Crime Unit* zullen dit niet loochenen.

ISPA en de internetproviders in het algemeen werken in België reeds met de gerechtelijke autoriteiten samen en ook met de overheid teneinde het internet te promoten maar dan wel een veilig en schoon internet, waar ongeoorloofd gedrag geweerd wordt.

Cet aspect des choses doit être développé et il faut se pencher sur le projet de loi relative à la criminalité informatique qui, dans sa version actuelle, risque de soulever quelques questions et de poser quelques problèmes.

M. Geert Glas (ISPA) déclare vouloir se pencher brièvement sur les aspects juridiques et économiques liés aux six points suivants: la définition de la notion de «données d'appel», le coût d'enregistrement, la durée de conservation, les instances auxquelles les informations doivent être communiquées, le coût de transmission des informations et la conservation territoriale.

Définition de la notion de «données d'appel»

— L'adresse internet (IP), le début de la connexion (log-in) et la fin de la connexion (log-out) sont déjà stockés automatiquement dans des fichiers temporaires. Les fournisseurs d'accès à internet (FAI) se disent disposés à poursuivre cette pratique de manière constructive.

— Les choses se compliquent si l'on englobe dans la définition de la notion de «données d'appel»: le nom d'utilisateur (*user name*) et l'identification de la ligne de l'appelant (*caller line identification*-CLI). Ces données sont parfois conservées temporairement mais cela n'est pas toujours faisable techniquement.

— Si les «données d'appel» englobent plus que l'IP, le log-in et le log-out, on se trouve confronté à de graves problèmes techniques et sur le plan de la protection de la vie privée.

Coût de l'enregistrement des données d'appel

— Ce coût est considérable sur un marché qui connaît une croissance exponentielle (+ 90 % durant les quatre derniers mois selon la dernière étude de marché en date).

— Ce coût sera répercuté sur l'utilisateur.

— Une obligation d'enregistrement et de conservation trop poussée constituerait un frein au développement de la société de l'information.

Durée de conservation

— Le projet prévoit une durée de conservation d'«au moins douze mois».

— La durée de conservation fait augmenter le coût de manière exponentielle.

— Les pays voisins de la Belgique appliquent un délai de trois mois.

— L'ISPA propose de limiter le délai de conservation à un maximum de six mois.

Dit aspect van de zaak moet nader onderzocht worden en men moet zich buigen over het wetsontwerp inzake informaticacriminaliteit, dat in zijn huidige versie enkele vragen en problemen kan doen rijzen.

De heer Geert Glas (ISPA) stipt aan kort aandacht te willen besteden vanuit juridisch en economisch oogpunt aan volgende zes punten: de omschrijving van het woord «oproepgegevens», de kost van de registratie, de duur van de bewaringsplicht, aan wie moeten inlichtingen verschaft worden, de kost van de verschaffing van inlichtingen en de territoriale bewaringsplicht.

Omschrijving van het begrip «oproepgegevens»

— Nu reeds worden het internet adres (IP), begin van de verbinding (log-in) en einde van de verbinding (log-out) steeds tijdelijk bijgehouden. De ISP's geven hun constructieve bereidheid te kennen tot het verderzetten van deze praktijk.

— Het wordt moeilijker wanneer men onder oproepgegevens ook gaat verstaan: de gebruikersnaam (*user name*) en *caller line identification* (CLI). Deze worden soms tijdelijk bijgehouden maar dit is niet altijd technisch mogelijk.

— Indien «oproepgegevens» meer omvat dan IP, log-in en log-out, rijzen er ernstige technische en privacy-problemen.

Kost registratie oproepgegevens

— Deze kost wordt aanzienlijk in een exponentieel groeiende markt (+ 90 % over vier maanden in laatste marktstudie).

— Deze kost zal doorgerekend worden aan de gebruiker.

— Al te uitgebreide registratie- en bewaringsverplichting vormt een rem op de ontwikkeling van de informatiemaatschappij.

Duur bewaringsplicht

— Het ontwerp bepaalt een bewaringstermijn van «minimum twaalf maanden».

— De duur van de bewaringsplicht doet de kost exponentieel stijgen.

— België omringende landen hanteren een termijn van drie maanden.

— ISPA stelt voor de bewaringstermijn te beperken tot maximum zes maanden.

À quelles instances les FAI doivent-ils communiquer des informations ?

— Interaction, transparence, spécialisation et efficacité.

— Relation existante entre les FAI et la *National Computer Crime Unit* (NCCU).

— L'ISPA propose que les demandes soient centralisées et formulées par la NCCU.

Coût de la communication des informations

— Surcoût réel compte tenu du personnel nécessaire (24 h/24 h), des logiciels et du matériel requis.

— Le coût est proportionnel à la vitesse, à l'ampleur du processus, etc.

— Le coût spécifique de la communication des informations doit être supporté par l'instance demandeuse et ne doit pas être répercuté sur tous les utilisateurs de l'internet (par analogie avec les demandes de renseignements relatives aux communications téléphoniques, qui sont adressées à Belgacom).

Conservation territoriale

— Le projet dispose que «la conservation doit s'effectuer à l'intérieur des limites du territoire du Royaume».

— Cette obligation est en porte-à-faux avec la réalité économique et la recherche d'efficacité.

— Cette règle est contestable sur le plan du droit de la concurrence.

— Il existe actuellement une coopération constructive entre les FAI et les pouvoirs publics, sans conservation territoriale.

Une membre souhaite revenir sur le fait que, d'après les intervenants précédents, il est techniquement difficile de conserver davantage que les données IP. En est-il vraiment ainsi? L'intervenante fait la comparaison avec une facture téléphonique qui mentionne les heures de début et de fin des communications. Où est le problème?

M. van Cutsem répond que, pour la facture téléphonique, il y a un log-in qui est la composition du numéro de téléphone ainsi que l'heure de début et de fin de la conversation téléphonique. Ainsi, un autre opérateur peut déterminer combien de temps a duré la conversation. Le contenu de la conversation n'est pas connu. Il en va de même pour internet. Actuellement, on peut savoir quels utilisateurs se connectent à quel moment et à quel moment ils se déconnectent. Au lieu d'un numéro de téléphone, une adresse IP est conservée.

Un membre pose deux questions au sujet de l'adresse IP. On conserve temporairement le log-in et le log-out. Serait-il possible de préciser comment on

Aan wie moeten de ISP's inlichtingen verschaffen ?

— Wisselwerking transparantie, specialisatie en efficiëntie.

— Bestaande relatie tussen ISP's en *National Computer Crime Unit* (NCCU).

— ISPA stelt voor de verzoeken via NCCU te centraliseren en te formuleren.

Kost verschaffen inlichtingen

— Daadwerkelijke meerkost gezien vereiste menselijke inzet (24/24 uur), software en hardware.

— De kost staat in verhouding met snelheid, omvang van het proces, ...

— De specifieke kost van het verschaffen van inlichtingen dient gedragen te worden door de verzoekende instantie en niet afgewenteld te worden op alle internet gebruikers (analogie met verzoeken aan Belgacom om inlichtingen omtrent gesprekken).

Territorialiteit bewaringsplicht

— Het ontwerp bepaalt dat de «bewaringsplicht moet worden uitgevoerd binnen de grenzen van het Rijk».

— Dit staat haaks op economische realiteit en op efficiëntieverzuchting.

— Dit is mededelingsrechtelijk aanvechtbaar.

— Thans bestaat een constructieve samenwerking tussen ISP's en overheid zonder territoriale bewaringsplicht.

Een lid wenst in te gaan op het feit dat het volgens de voorgaande sprekers technisch zeer moeilijk is om meer dan het IP-gegeven te bewaren. Is dat zo? Spreekster maakt de vergelijking met een telefoonfactuur waarbij de in-bel en de out-bel geregistreerd staan. Waar zit de moeilijkheid?

De heer van Cutsem antwoordt dat een log-in op de telefoonrekening de vorming van het telefoonnummer is alsmede het begin- en einduur van het telefoongesprek. Een andere operator kan aldus bepalen hoe lang het gesprek geduurd heeft. De inhoud van het gesprek is niet gekend. Hetzelfde geldt voor internet. Thans kan men te weten komen welke gebruikers op welk ogenblik met elkaar in verbinding treden en op welk ogenblik zij die verbinding verbreken. In plaats van een telefoonnummer wordt een IP-adres bewaard.

Een lid stelt twee vragen in verband met het IP-adres. De log-in en de log-uit worden tijdelijk bijgehouden. Kan dit meer concreet worden omschreven?

procède concrètement? Qu'entend-on par temporairement? La durée varie-t-elle d'un fournisseur d'accès à l'autre ou bien évolue-t-on dans le sens d'une normalisation? Les intervenants affirment que, dans les pays voisins de la Belgique, la durée de conservation est de trois mois. Quels sont ces pays? Y a-t-il aussi des pays qui appliquent d'autres délais? Dispose-t-on de données à ce sujet?

M. Glas répond que les pays voisins où le délai est de trois mois sont les Pays-Bas, la France et l'Allemagne. En Belgique, les délais appliqués varient d'un FAI à l'autre. Certains ont pour règle d'appliquer un délai de conservation de un à deux mois seulement alors que d'autres appliquent un délai plus long. Il est équitable de dire que, pour la plupart des FAI, le délai minimum de 12 mois qui est prévu dans la loi en projet est déjà plus long que le délai qu'ils appliquent actuellement.

Un membre souligne que, selon l'ISPA, une obligation d'enregistrement et de conservation trop étendue entraverait le développement de la société de l'information et que le coût de cette obligation devrait être imputé à l'utilisateur. Le poids de cet inconvénient est-il proportionnel à la croissance importante de la criminalité sur internet? Fait-on bien de ne prendre en considération que les avantages de la croissance? Ne devrait-on pas, à terme, tenter d'endiguer quelque peu cette criminalité et, au besoin, d'en freiner le développement? L'intervenant craint que la criminalité ne puisse se développer aussi vite sinon plus vite que la société de l'information elle-même.

Une deuxième question concerne la «territorialité» de l'obligation de conservation. Selon la NCCU, l'obligation de conservation doit être mise en œuvre à l'intérieur des frontières du Royaume. Est-ce à dire que l'on n'aura plus aucune prise sur ce qui se trouve chez les fournisseurs d'accès étrangers? Pourtant, certains pourraient facilement se servir d'un système basé en Iran par exemple, pour se livrer à des pratiques malhonnêtes.

En ce qui concerne la conservation à l'intérieur des frontières du Royaume, M. Verbeeren (*National Computer Crime Unit*) renvoie à l'exemple de Compuserve. Cet opérateur belge conserve ses «logins» aux Pays-Bas. Chaque fois que l'on a besoin d'une donnée ou d'un renseignement, on doit passer par une demande d'entraide judiciaire internationale, ce qui ralentit évidemment le déroulement de la procédure. Les affaires de ce genre entraînent des difficultés lorsque les logins en question ne sont pas conservés à l'intérieur des frontières du Royaume.

M. Luc Beirens (gendarmerie-AREA) ajoute que la loi est applicable, non seulement aux FAI qui sont affiliés à l'ISPA, mais aussi à tous les autres FAI. Les organisations criminelles peuvent devenir elles-mêmes des FAI. Elles ne s'affilieront bien sûr pas à

Wat is tijdelijk? Verschilt dit van provider tot provider of is er een standaardisatie aan de gang? Wat de duur van de bewaringsplicht betreft stellen de sprekers dat die in de België omringende landen drie maanden is. Welke landen zijn dat? Zijn er ook landen die een andere termijn hanteren? Bestaan daar gegevens over?

De heer Glas antwoordt dat de omringende landen waar de termijn drie maanden bedraagt, Nederland, Frankrijk en Duitsland zijn. De praktijk die thans in België wordt gebruikt is afhankelijk van ISP tot ISP. Sommigen hebben terzake een praktijk van een bewaringstermijn van slechts één à twee maanden en anderen hanteren een langere termijn. Het is fair te zeggen dat de in het voorliggende ontwerp voorgestelde minimumtermijn van 12 maanden, voor de meeste ISP's een verlenging is van de termijn die zij heden hanteren.

Een lid stipt aan dat ISPA stelt dat een al te uitgebreide registratie- en bewaringsverplichting een rem zou zijn op de ontwikkeling van de informatiemaatschappij en dat de kost zou moeten worden doorgerekend aan de gebruiker. Weegt dit op tegen de grote groei van criminaliteit op het net? Is dit evenredig? Is het goed enkel de baten van de groei te zien? Moet men op termijn niet eerder proberen om de criminaliteit op dat gebied wat in te perken en misschien die groei desnoods wat te vertragen? Spreker vreest dat de criminaliteit misschien wel even vlug zoniet nog vlugger zou kunnen groeien dan de informatiemaatschappij.

Een tweede vraag betreft de «territorialiteit» van de bewaringsplicht. NCCU stelt dat de bewaringsplicht moet worden uitgevoerd binnen de grenzen van het Rijk. Wil dit zeggen dat men op al hetgeen bij buitenlandse providers zit geen vat meer heeft? Nochtans kan een systeem in Iran bijvoorbeeld perfect de basis zijn van mensen die zich willen bezighouden met malafide praktijken.

De heer Verbeeren (*National Computer Crime Unit*) verwijst, wat betreft de bewaring binnen de grenzen van het Rijk, naar het voorbeeld van Compuserve. Deze Belgische operator bewaart zijn logins in Nederland. Wanneer men een gegeven, een inlichting, nodig heeft, heeft men een internationaal rechtshulpverzoek nodig. Dit vertraagt zeker de procedure. Dergelijke zaken leiden tot moeilijkheden als die logins niet binnen de grenzen van het Rijk worden bewaard.

De heer Luc Beirens (rijkswacht-BOGO) voegt hieraan toe dat de wet niet enkel slaat op ISP's die aangesloten zijn bij ISPA, maar op alle ISP's. Criminele organisaties kunnen zelf ISP worden. Zij zullen niet aansluiten bij ISPA maar het zijn juist die ISP's die

l'ISPA, mais il n'en reste pas moins que ce sont ces FAI-là dont il faut s'occuper dans le cadre de la lutte contre la criminalité organisée.

Certaines firmes tentent d'échapper à toutes sortes de dispositions légales en s'établissant dans des «refuges», plus précisément dans de petites îles de l'Océan pacifique, où la législation est peu élaborée. Cette pratique entrave considérablement la lutte contre la criminalité. Il va de soi que, quand un pays est seul à instaurer une législation donnée, le risque existe de voir les criminels se déplacer vers les pays voisins. Il y a lieu dès lors d'élaborer une réglementation applicable dans le contexte européen.

M. Glas répond que les FAI ont évidemment le moins intérêt à ce que des faits criminels soient commis sur ou par l'intermédiaire de l'internet. Tout le monde se trouve dans le même camp. D'ailleurs, un FAI est un fournisseur de services à valeur ajoutée qui doit être enregistré auprès de l'IBPT. Le problème de la territorialité de l'obligation de conservation concerne uniquement l'emplacement physique du serveur. Il n'a donc rien à voir avec le fait que les FAI peuvent avoir sans difficulté, dans chaque pays — et donc également en Belgique —, une personne qui fait office de point de contact pour l'autorité publique. On peut comprendre qu'il est normal que l'autorité ne doive pas se déplacer vers l'étranger pour y obtenir l'information qu'elle désire. Chaque FAI établi en Belgique aura évidemment chez nous une personne à qui l'établissement pourra remettre les informations. La seule question à se poser est celle de savoir si cela signifie *ipso facto* que les données doivent se trouver physiquement sur le territoire belge. On peut craindre que certains FAI de taille modeste, pour lesquels il est économiquement plus rentable de stocker les données relatives aux Pays-Bas, au Luxembourg et à la France, sur un seul serveur situé au Luxembourg, n'éprouvent des difficultés économiques si la législation les obligeait à disposer en Belgique d'un serveur distinct pour y stocker les données belges. Il semble parfaitement possible de prévoir que le FAI doit avoir, en Belgique, une personne à qui toute demande pourrait être soumise, et qui aurait la faculté d'aller chercher les informations *de facto*, sans doute dans la plupart des cas sur un serveur situé en France, aux Pays-Bas ou au Luxembourg.

Le ministre soulève que, en ce qui concerne la durée de conservation des données, l'ISPA a mis en garde contre des obligations trop lourdes impliquant d'importants investissements qui pourraient mettre en péril leurs activités et peut-être les inciter à se délocaliser. Les FAI demandent également pour des raisons d'économie de ne pas avoir à conserver ces données sur le territoire du Royaume.

Le ministre a le sentiment que, dès maintenant, sans que la loi ne soit effectivement entrée en vigueur et in het kader van de bestrijding van de georganiseerde criminaliteit moeten aangepakt worden.

Bepaalde firma's trachten te ontglippen aan allerlei wettelijke bepalingen door zich op *«save heavens»* te gaan vestigen — dat zijn kleine eilandjes in de Stille Oceaan — waar weinig wetgeving bestaat. Daardoor wordt de bestrijding van de criminaliteit sterk bemoeilijkt. Als men uiteraard als enig land een wetgeving gaat instellen loopt men het risico dat criminelen naar de nabije landen uitwijken. Er moet een regelgeving uitgewerkt worden in Europees verband.

De heer Glas antwoordt dat de ISP's er natuurlijk het minst mee gebaat zijn dat er zich op en rond het internet criminele feiten zouden voordoen. Iedereen staat aan dezelfde kant. Trouwens, als ISP is men een leverancier van diensten met een toegevoegde waarde die geregistreerd moet zijn bij het BIPT. Het probleem van de territorialiteit van de bewaringsplicht heeft enkel te maken met de plaats waar de server zich fysisch bevindt en heeft niets te maken met het feit dat de ISP's geen enkel probleem hebben om in ieder land — dus ook in België — iemand te hebben die het contactpunt, het aanspreekpunt is voor de overheid. Het valt te begrijpen dat de overheid zich niet naar het buitenland dient te verplaatsen om daar informatie te krijgen. Iedere ISP in België zal uiteraard in België een aanspreekpunt hebben waar de instelling de informatie neerlegt. De enige vraag is of dat ook betekent dat de gegevens zich fysisch op het Belgisch grondgebied moeten bevinden. De vrees bestaat dat bepaalde kleinere ISP's voor wie het economisch efficiënter zou zijn om de gegevens van Nederland, Luxemburg en Frankrijk te bundelen in één server die in Luxemburg staat, het economisch moeilijker zullen krijgen omdat ze door deze wetgeving verplicht zullen worden om in België een aparte server te hebben voor de Belgische data. Het lijkt perfect haalbaar te stellen dat de ISP in België iemand dient te hebben bij wie alle vragen worden neergelegd, maar die persoon moet de vrijheid hebben om dan de informatie *de facto* te gaan ophalen on-line, waarschijnlijk in de server die dan in Frankrijk, Nederland of Luxemburg staat.

De minister merkt op dat, wat de bewaartermijn van de gegevens betreft, ISPA gewaarschuwd heeft voor te zware verplichtingen die te grote investeringen impliceren, waardoor de activiteit van dienstverlener een riskante onderneming wordt, wat de betrokkenen er misschien toe aanzet die activiteit te verplaatsen. Om economische redenen vragen zij ook dat ze niet verplicht zouden worden die gegevens op het grondgebied van het Rijk te bewaren.

De minister heeft de indruk dat de ISP's nu al om economische redenen hun activiteit dreigen te ver-

sans que l'on n'impose des charges trop lourdes, les FAI ont déjà tendance à la délocalisation au nom de raisons économiques.

Le gouvernement et le ministre de la Justice n'entendent en aucune manière imposer des conditions trop lourdes, parce que d'une manière ou d'une autre, ils en subiront les conséquences.

M. Verbeeren explique que la *National Computer Crime Unit* (NCCU) se situe dans le prolongement des *Computer Crime Units*. En 1992, la police judiciaire a décidé, avec l'accord du ministre de la Justice, de créer, pour chaque cour d'appel, une *Computer Crime Unit* qui aurait deux objectifs. Le premier objectif consiste à agir efficacement contre la criminalité informatique et le deuxième à fournir une aide lors d'enquêtes effectuées dans des environnements automatisés. À partir de 1992, on a essayé de lutter de la manière la plus efficace possible contre la criminalité informatique avec les moyens qu'offre le Code pénal. Si, lors de perquisitions, on découvre des ordinateurs et des systèmes informatiques, des collègues des CCU apportent leur aide pour la recherche et la reproduction des données utiles à l'enquête.

En 1997, on a créé, dans le prolongement de ces *Computer Crime Units* régionales, la *National Computer Crime Unit*. En plus d'une série de tâches de formation et de gestion budgétaire, la NCCU est chargée d'une mission importante, à savoir l'exploitation d'un bureau de notification judiciaire. Celui-ci a été créé en décembre 1996 par le ministre de la Justice, dans le but de rechercher la pornographie enfantine sur l'internet.

En concertation avec la Justice, les Télécommunications, l'ISPA et la NCCU, un protocole de collaboration a été signé aux termes duquel le bureau de notification pour la pornographie enfantine a été transformé en un bureau de notification judiciaire central, qui a compétence pour toutes les informations illégales et nuisibles présentes sur l'internet. Ce protocole prévoit un certain nombre de procédures auxquelles les fournisseurs d'accès à l'internet doivent se conformer. Tout se déroule bien. On est encore confronté à beaucoup de pornographie enfantine, mais plus l'internet se développe, plus l'éventail des infractions s'y élargit: droits d'auteur, racisme, *hacking*, pratiques commerciales déloyales. Toutes les incriminations que l'on trouve dans le Code pénal ou dans les législations particulières se retrouvent également sur l'internet. La collaboration avec l'ISPA et ses membres est très bonne; lorsqu'on a besoin d'informations de la part des fournisseurs d'accès à l'internet, la NCCU les obtient facilement. De nombreuses plaintes concernent le *hacking*, c'est-à-dire l'accès non autorisé aux ordinateurs. Ces plaintes

plaatsen, zelfs zonder dat er een wet is en zonder dat al te zware lasten worden opgelegd.

De regering en de minister van Justitie zijn geenszins voornemens te strenge voorwaarden te stellen omdat zij daarvan op een of andere manier toch de gevolgen zullen dragen.

De heer Verbeeren preciseert dat het *National Computer Crime Unit* (NCCU) een voortzetting is van de *Computer Crime Unit*. In 1992 besliste de gerechtelijke politie met goedkeuring van de minister van Justitie om per hof van beroep een computer crime unit op te richten met twee doelstellingen. Ten eerste, efficiënt optreden tegen de computercriminaliteit en ten tweede het verlenen van een assistentie tijdens of bij onderzoekingen in geautomatiseerde omgevingen. Vanaf 1992 werd met de voorhanden zijnde middelen in het Strafwetboek getracht de computercriminaliteit op de meest efficiënte manier te bestrijden. Tijdens huiszoekingen waar computers en informaticasystemen aangetroffen worden, verlenen collega's van de CCU's hun bijstand voor het opsporen en vastleggen van gegevens nuttig voor het onderzoek.

In 1997 werd in voortzetting van die regionale computer crime units, de *National Computer Crime Unit* opgericht. Naast een reeks taken van opleiding en budgetbeheer heeft de NCCU één belangrijke missie, namelijk de exploitatie van een gerechtelijk meldpunt. Dit werd in december 1996 door de minister van Justitie opgericht, met het oog op het opsporen van kinderpornografie op het internet.

In overleg met Justitie, Telecommunicatie, ISPA en NCUU werd een samenwerkingsprotocol ondertekend waarbij het meldpunt kinderpornografie werd omgedoopt in een centraal gerechtelijk meldpunt bevoegd voor alle illegale en schadelijke informatie op het internet. In dat protocol zijn een aantal procedures voorzien waaraan de Internet Providers zich moeten houden. Dat loopt goed. Men wordt nog altijd geconfronteerd met veel kinderpornografie maar hoe meer het internet zich ontwikkelt, hoe groter de waaier van verschillende misdrijven op het internet: auteursrechten, racisme, *hacking*, oneerlijke handelspraktijken. Alle incriminaties die men kan terugvinden in het Strafwetboek of de bijzondere wetgeving vindt men ook terug op het internet. Er is een zeer goede samenwerking met ISPA en haar leden en wanneer er inlichtingen nodig zijn bij de Internetproviders dan verkrijgt het NCCU die ook op een vlotte manier. Er komen veel klachten over *hacking*, dit wil zeggen het binnendringen in de computers. Deze klachten worden eerder behandeld door de regionale CCU's. Dit is de reden waarom spreker aan

sont plutôt traitées par les CCU régionales. C'est la raison pour laquelle l'intervenant a demandé à un de ses collègues, M. Olivier Bogaert, d'être présent, ici, devant la commission.

La NCCU a en théorie huit membres du personnel à sa disposition (une personne est temporairement absente). Cinq membres du personnel sont issus du monde judiciaire, deux membres sont issus du civil, dont un juriste et un informaticien. La mission finale concernant l'exploitation — 24 heures sur 24 — du bureau de notification judiciaire nécessite trois personnes.

M. Luc Beirens est à la tête de l'équipe AREA, Assistance et recherche dans les environnements automatisés. Cette équipe comprend six personnes et fait partie du Bureau central de recherches. Elle existe depuis 1995 et a essentiellement les mêmes missions que les *Computer Crime Units*. Depuis l'entrée en vigueur de la directive concernant la spécialisation des divers services de police, le volet criminalité informatique a été attribué à la police judiciaire. La cellule AREA n'intervient qu'en matière de criminalité informatique spécifique, lorsqu'elle y est requise par le magistrat du parquet ou par le juge d'instruction. Si tel n'est pas encore le cas, elle essaye de transmettre la question ou la notification relative à la criminalité informatique à la *Computer Crime Unit* régionale ou à la *National Computer Crime Unit*. La cellule intervient essentiellement dans le cas d'enquêtes dans des environnements informatisés lorsqu'il s'agit de criminalité traditionnelle. Celle-ci couvre tous les domaines, à savoir l'identification des personnes qui ont transmis des messages relatifs au trafic des stupéfiants, les disparitions, les escroqueries, la pornographie enfantine, etc. La cellule AREA est une unité nationale qui prête toujours assistance à la BSR locale ou à une brigade.

Une commissaire s'interroge sur le sens d'une éventuelle législation, si les autres pays, du moins les pays européens, ne travaillent pas de la même manière. On a évoqué les problèmes de délocalisation, mais il est évident que la criminalité informatique opère hors frontières. L'intervenante souhaiterait savoir en quoi ceci répond à la préoccupation de terrain, notamment en ce qui concerne la lutte contre la criminalité. À part des incriminations spécifiques, l'informatique n'est qu'un moyen qu'on utilise tout comme le téléphone ou d'autres moyens de transmission d'informations. Toutes les incriminations du Code pénal peuvent évidemment s'appliquer en tant que telles.

Par ailleurs, il semble qu'on entre très en détail sur un certain nombre d'incriminations qui pourraient, plus que de permettre la poursuite de la criminalité informatique, entrer dans le champ de la vie privée. L'intervenante renvoie à un exemple extrêmement précis à propos de l'utilisation de fichiers, en matière de fichiers d'élèves en Communauté française; il y a lieu de trouver un équilibre entre la légitime préoccu-

een van zijn collega's, de heer Olivier Bogaert, gevraagd heeft om hier aanwezig te zijn.

Wat de personeelsbezetting betreft, werkt de NCCU in theorie met acht personen (een persoon is tijdelijk afwezig). Er zijn vijf gerechtelijke en twee burgerlijke personeelsleden, waarvan een jurist en een informaticus. De uiteindelijke missie in verband met het exploiteren — 24 op 24 uur — van het gerechtelijk meldpunt vergt drie personeelsleden.

De heer Luc Beirens staat aan het hoofd van het BOGO-team, Bijstand en Opsporingen in Geautomatiseerde Omgevingen (*Assistance et Recherche dans les Environnements Automatisés* (AREA). Dit team bestaat uit zes personen en is ondergebracht in het Centraal Bureau voor opsporingen. Het bestaat sinds 1995 en heeft hoofdzakelijk dezelfde taken als de *Computer Crime Units*. Sinds de specialisatierichtlijn tussen de politiediensten, is de computercriminaliteit toegekend aan de gerechtelijke politie. BOGO komt enkel tussenbeide in de specifieke computercriminaliteit, als zij door de parketmagistraat of door de onderzoeksrechter gevorderd worden. Is dat nog niet het geval dan trachten zij de vraag of de melding in verband met de computercriminaliteit door te spelen naar de bevoegde regionale of naar de nationale computer crime unit. Hoofdzakelijk doen zij tussenkomsten voor onderzoekingen in computeromgevingen wat betreft de traditionele criminaliteit. Dit strekt zich uit in alle domeinen, namelijk identificatie van mensen die berichten in verband met drugshandel verzonden hebben, verdwijningen, oplichtingen, kinderpornografie, enz. BOGO is een nationale eenheid die altijd bijstand verleent aan lokale BOB of een brigade.

Een commissielid vraagt zich af of een eventuele wetgeving zin heeft als andere landen, en dan vooral de Europese landen, niet op dezelfde manier tewerk gaan. Men heeft gesproken over verplaatsing van activiteiten, maar het is evident dat de informaticacriminaliteit geen grenzen kent. Spreekster vraagt zich af of dit tegemoetkomt aan de werkelijke noden, met name wat de strijd tegen de criminaliteit betreft. Afgezien van de specifieke strafbaarstellingen, is informatica maar een middel dat net als de telefoon en andere middelen wordt gebruikt voor het verzenden van informatie. Alle strafbaarstellingen uit het Strafwetboek kunnen uiteraard als zodanig worden toegepast.

Bovendien gaat men heel gedetailleerd in op een aantal strafbaarstellingen die niet zozeer de vervolging van informaticacriminaliteit bevorderen, als wel binnendringen in het privé-leven. Spreekster verwijst naar een zeer specifiek voorbeeld inzake het gebruik van gegevensbestanden, met name de leerlingenbestanden in de Franse Gemeenschap. Daarom moet worden gestreefd naar een evenwicht tussen de legi-

pation de poursuivre la criminalité informatique et la protection de la vie privée. En quoi ceci est-il une amélioration pour pouvoir traquer les criminels informatiques ?

L'intervenante cite l'exemple de la pornographie enfantine qui est une spécialité de la *National Computer Crime Unit*. Celle-ci surveille le réseau et tente de trouver les personnes qui mettent sur celui-ci ce type de délit comme on peut le faire par le biais de journaux spécialisés ou autres. Évidemment, en général, ces personnes n'opèrent pas en Belgique. Par quels moyens arrivera-t-on à traquer cette criminalité informatique ? Le projet de loi va-t-il résoudre ce problème ?

M. Verbeeren répond qu'en fait, la pornographie enfantine est une incrimination indifférente au média utilisé. C'est un exemple d'article du Code pénal qui est en réalité applicable à n'importe quel média. Certains délits informatiques comme le vol de données ne relèvent pas des incriminations prévues. Le Code pénal suppose une chose tangible que l'on prend. C'est pourquoi il est nécessaire de prévoir une incrimination spécifique en ce qui concerne le vol de données informatisées.

L'évolution rapide de l'internet n'est toutefois pas une raison pour se résigner devant cette situation. On est confronté à des problèmes internationaux dans d'autres domaines de la criminalité également et pourtant, il y a bel et bien une politique pénale en matière de drogue et de criminalité organisée. Il y aura toujours des paradis où les criminels pourront plus ou moins se réfugier. C'est une réalité dont il faut tenir compte, mais on ne doit pas s'y résigner pour autant.

M. Coenraets (juriste attaché à la NCCU) souhaite revenir un instant au débat concernant le délai de conservation. Les pays voisins de la Belgique sont en train de revoir leur législation en matière de criminalité informatique. Il est exact que la plupart des pays préconisent un délai de conservation de trois mois, mais on constate une tendance à reconsidérer ce délai pour le porter à un an. C'est le cas en Allemagne, aux Pays-Bas, au Danemark et en Suède et cela nous a été confirmé par téléphone par les différentes équipes informatiques de ces pays. L'intervenant estime qu'il serait surtout utile d'examiner de plus près les initiatives législatives prévues dans ces pays. Au sein du Conseil de l'Europe également, on élabore une réglementation visant à harmoniser la situation entre les différents pays. Un des articles de cette réglementation prévoit aussi que chaque État membre est tenu de veiller à la conservation des données et à leur transmission immédiate à la première demande des services de police. Rien n'est dit sur l'imputation des frais que cela entraînera. Il paraît évident qu'ils devront être pris en charge par les entreprises mêmes.

tieme wens om de informaticacriminaliteit te vervolgen enerzijds en het privé-leven te beschermen anderzijds. In welk opzicht kan de informaticacriminaliteit hierdoor beter worden opgespoord ?

Spreekster geeft het voorbeeld van de kinderporno, waarin de *« National Computer Crime Unit »* is gespecialiseerd. De NCCU controleert het net en tracht de personen op te sporen die dit type van misdrijf plegen op het net (zoals dat ook kan gebeuren via gespecialiseerde tijdschriften en andere). Meestal opereren deze personen niet vanuit België. Hoe zal men deze vorm van informaticacriminaliteit opsporen ? Zal het wetsontwerp dit probleem oplossen ?

De heer Verbeeren antwoordt dat kinderpornografie een incriminatie is die eigenlijk media-onafhankelijk is. Dat is een voorbeeld van een artikel van het Strafwetboek dat eigenlijk toepasbaar is op gelijk welk medium. Een aantal informaticamisdrijven vallen niet onder de voorziene incriminaties, bijvoorbeeld diefstal van gegevens. Het Strafwetboek veronderstelt iets tastbaars dat men wegneemt. Daarom is er nood aan een specifieke incriminatie in verband met diefstal van computerdata.

Maar het is niet omdat het internet snel evolueert dat men zich bij de situatie moet neerleggen. In andere criminaliteitsdomeinen bestaan ook internationale problemen en toch is er een strafrechterlijk beleid in verband met drugs en georganiseerde criminaliteit. Er zullen altijd paradijzen bestaan waar men zich min of meer kan verstoppen. Dat is de realiteit waarmee men rekening moet houden, maar men moet er zich daarom niet bij neerleggen.

De heer Coenraets (jurist binnen de NCCU) wenst nog even terug te komen op de discussie in verband met de bewaartermijn. De verschillende landen die België omringen herzien hun wetgeving op het gebied van de computercriminaliteit. Het is inderdaad zo dat de meeste landen een bewaartermijn van drie maanden voorop stellen. Nochtans is er een tendens tot herziening naar een termijn van een jaar toe. Dat is zowel voor Duitsland, Nederland, Denemarken als Zweden het geval en dit werd telefonisch bevestigd door de verschillende computerteams uit die landen. Spreker is van mening dat het vooral nuttig is om de wetgevende initiatieven in die landen eens van nabij te bekijken. Binnen de Raad van Europa is men ook bezig met een regelgeving te ontwikkelen om een harmonisatie te creëren tussen de verschillende landen. In één van die artikelen stelt men ook dat elke lidstaat verplicht is om te voorzien in een bewaring van de communicatiedata en een onmiddellijke overzending van de data op het eerste verzoek van de politiediensten. Er wordt niets vermeld over wie de kosten moet dragen. Het lijkt evident dat de bedrijven zelf deze kost moeten dragen.

M. Olivier Bogaert (CCU de Bruxelles) soulève qu'il y a un paradoxe dans les propos des FAI. Ils mettent en avant les coûts considérables de la conservation des données, mais il faut également attirer l'attention sur l'évolution technologique des supports de conservation. Les volumes de conservation doublent tous les six mois à peu près pour un support et un volume déterminés à des coûts constants, c'est-à-dire pour une somme déterminée. L'intervenant relève également le fait que les opérateurs développent la gratuité de l'internet et incitent un plus grand nombre à la connexion gratuite, mais se plaignent simultanément du coût de la conservation des données. Des explications à ce sujet sont nécessaires.

Un commissaire pose la question de savoir si le coût de conservation des données peut être évalué. A-t-on une idée, par exemple, du montant que représente un mois de conservation ou d'archivage des données ?

L'intervenant s'étonne que, du côté de l'ISPA, ce soit le seul point soulevé dans cette audition. N'y a-t-il pas d'autres points dans ce projet de loi qui pourraient les intéresser ? Qu'en est-il en particulier de la régulation du contenu ? L'intervenant cite le cas de Yahoo Incorporated, qui a refusé l'application d'un jugement intervenu en France et ayant trait à la vente d'objets nazis sur son site. Ce sont là des questions qui devraient interpeller l'ISPA en Belgique. L'intervenant souhaite savoir si l'ISPA a des correspondances internationales, qui pourraient éventuellement permettre d'avoir une ouverture plus grande.

Une seconde question s'adresse aux autorités judiciaires et à la gendarmerie. L'article 6 du projet de loi érige en infraction le fait de se trouver de façon non autorisée sur un site. Va-t-on trop loin ? A-t-on les moyens judiciaires et autres de rechercher ces infractions avant même de penser à les sanctionner ?

Le ministre a déclaré que, si la Belgique avait disposé de cette loi au moment de l'apparition du virus *I love you*, il y aurait eu d'autres moyens, et en particulier d'autres moyens d'indemnisation des victimes de ce virus. Quelle est l'opinion de la NCCU à ce sujet ?

M. Olivier van Cutsem répond que, pour les coûts de stockage des données *login, logout* et adresses IP, Skynet a prévu pour cette année un budget total d'environ deux millions. M. Bogaert dit que les moyens de stockage coûtent de moins en moins cher et que, tous les six mois, leur prix diminue de moitié.

Actuellement, on trouve des cd-rom chez nos revendeurs au prix de 56 francs/pièce. Ce n'est pas le cd-rom ou le médium de stockage qui coûte cher, c'est toute l'ingénierie et les machines qui permettent de consulter et de réconcilier toutes ces données qui sont onéreuses. L'estimation donnée est valable pour 2000

De heer Olivier Bogaert (CCU van Brussel) wijst op een paradox in de verklaringen van de ISP. Zij beweren dat het bewaren van gegevens veel geld kost, maar houden er geen rekening mee dat de ondersteuningsprogramma's daarvoor een technologische ontwikkeling hebben ondergaan. Om de zes maanden ongeveer verdubbelt het aantal gegevens dat een bewaringsprogramma tegen dezelfde prijs aankan. Spreker wijst er eveneens op dat de operatoren de gratis toegang tot het internet bevorderen maar tegelijk klagen over de prijs van de bewaring van de gegevens. Dit moet nader worden toegelicht.

Een commissielid vraagt of de kosten voor de bewaring van gegevens kunnen worden geschat. Heeft men er bijvoorbeeld een idee van hoeveel het kost om gegevens een maand te bewaren ?

Spreker verbaast zich erover dat de ISPA het tijdens de hoorzitting alleen daarover heeft gehad. Waren er geen andere aspecten van het wetsontwerp die hen interesseerden ? Hoe zit het met de inhoud van de sites ? Spreker noemt het geval van Yahoo Incorporated, dat weigerde om de uitspraak van een Frans gerecht in verband met de verkoop van nazivoorwerpen op een site, toe te passen. Deze kwesties gaan de ISPA in België rechtstreeks aan. Spreker wil weten of de ISPA internationale contacten heeft die meer openheid toestaan.

Een tweede vraag is gericht tot de gerechtelijke instanties en de rijkswacht. Artikel 6 van het wetsontwerp maakt van de ongeoorloofde aanwezigheid op een site een misdrijf. Gaat dat niet te ver ? Zijn de nodige gerechtelijke en andere middelen wel voorhanden om deze misdrijven op te sporen, laat staan te bestraffen ?

De minister heeft gezegd dat als deze wet in België had bestaan toen het *I love you*-virus opdook, er meer mogelijkheden zouden zijn geweest met name om de slachtoffers te vergoeden. Wat denkt de NCCU hierover ?

De heer Olivier van Cutsem antwoordt dat Skynet dit jaar ongeveer twee miljoen heeft uitgetrokken om de *login*- en *logout*-gegevens en de IP-adressen te bewaren. De heer Bogaert zegt dat het bewaren van gegevens steeds minder duur wordt en dat de kosten om het half jaar met de helft verminderen.

Thans vindt men bij de verkopers cd-rom's tegen de prijs van 56 frank per stuk. Het is niet de cd-rom of het opslagmedium dat duur is maar de engineering en de machines die het mogelijk maken al die gegevens te raadplegen. De gegeven raming is geldig voor 2000. Wel moet er rekening mee gehouden worden dat het

mais sachant que le nombre de connexions internet va croissant. Cela aura pour conséquence d'augmenter le budget.

Concernant le contenu sur internet, l'intervenant explique être confronté par exemple à des violations des droits d'auteur. Actuellement, cela ne pose pas un problème majeur en ce qui concerne le respect des droits des tiers puisque la législation existante peut y être transposée.

Une commissaire posait la question de l'opportunité de cette loi en faisant la balance entre le respect de la vie privée et la lutte contre la criminalité informatique. L'intervenant est d'avis que les représentants de la gendarmerie et de la police judiciaire ont bien relevé le fait que les infractions qui seraient incriminées par cette loi sont de nouveaux types d'infractions; de nos jours, rien n'est prévu pour le faux en écritures informatique, ni pour les actes de piratage ou de *hacking*. Il cite l'exemple très médiatique de Red Attack qui est poursuivi par Skynet. Une plainte au pénal a été déposée non pour le fait qu'il ait attaqué les serveurs de Skynet mais parce qu'il a distribué ces informations au public. Si une loi avait été disponible en matière de criminalité informatique, cette personne aurait également pu être poursuivie pour piratage.

Un membre soulève que l'évaluation du coût de conservation était de l'ordre de deux millions. Il serait utile de connaître le chiffre d'affaires de l'entreprise pour pouvoir se faire une idée de ce que cela représente.

M. Olivier van Cutsem répond que, pour l'instant, le chiffre d'affaires dépasse les 500 millions. Donc, cela fait 0,5 %. Il n'y a pas de bénéfice, l'entreprise est en perte.

Le membre pose la question de savoir comment la société assure sa rentabilité.

M. Glas répond qu'il n'y a évidemment ni miracle ni secret à ce sujet. Ceux qui prônent le libre accès à l'internet ne le font pas pour des raisons philanthropiques, mais parce qu'ils ont ou escomptent d'autres formes de revenus. Il y a deux principales sources de revenus. La première est le produit des publicités — les bannières — parfois aussi les revenus liés au fait que, lorsque quelqu'un clique sur l'une des bannières, il est conduit sur le site d'un des annonceurs. La deuxième source est la rétribution que l'on perçoit de l'opérateur de télécommunications pour chaque communication téléphonique.

En réponse à la remarque formulée, l'intervenant tient encore à ajouter que l'ISPA est demandeur par rapport à la loi en projet parce que l'on constate que certains faits se produisent, comme le piratage informatique, l'escroquerie aux mots de passe,

aantal internetaansluitingen zal toenemen. Dat zal een stijging van het budget ten gevolge hebben.

In verband met de inhoud op het internet legt spreker uit dat bijvoorbeeld de auteursrechten geschonden worden. Voor het respecteren van de rechten van derden doet dit thans geen grote problemen rijzen aangezien de bestaande wetgeving kan worden toegepast.

Een commissielid vroeg zich af of deze wet wel wenselijk was, waarbij de eerbiediging van de persoonlijke levenssfeer werd afgewogen tegen de strijd tegen de cybercriminaliteit. Spreker is van mening dat de vertegenwoordigers van de rijkswacht en de gerechtelijke politie er duidelijk op gewezen hebben dat de misdrijven die door deze wet strafbaar worden gesteld, nieuwe soorten van misdrijven zijn; thans is er niets bepaald voor schriftvervalsing in informatica noch voor computerkraak of *hacking*. Hij haalt het voorbeeld aan van Red Attack waaraan in de media veel aandacht werd besteed. Red Attack wordt vervolgd door Skynet. Red Attack wordt strafrechtelijk vervolgd niet omdat hij de server van Skynet heeft aangevallen maar omdat de verkregen informatie onder het publiek verspreid werd. Was er op dat ogenblik een wet inzake informaticacriminaliteit geweest, dan had men die persoon ook kunnen vervolgen wegens computerkraak.

Een lid merkt op dat de bewaringskosten geraamd werden op 2 miljoen. Het zou nuttig zijn de omzet van het bedrijf te kennen om een idee te krijgen van wat bovenvermeld cijfer vertegenwoordigt.

De heer Olivier van Cutsem antwoordt dat de omzet thans meer dan 500 miljoen bedraagt. Het gaat dus om 0,5 %. Er wordt geen winst gemaakt. Het bedrijf lijdt verlies.

Het lid vraagt hoe het bedrijf rendabel kan blijven.

De heer Glas antwoordt dat er natuurlijk geen mirakels noch geheimen daaromtrent zijn. De mensen die vrije toegang tot het internet voorstaan, doen dat niet uit filantropie maar doen dat omwille van het feit dat zij andere vormen van inkomsten hebben of verhopen. Er zijn twee belangrijke vormen van inkomsten. Ten eerste de inkomsten uit advertenties — de banners — soms ook inkomsten uit het feit dat wanneer men klikt op één van die banners men naar de website gaat van één van de adverteerders. Ten tweede, de retributie die men krijgt van de Telecomoperator per telefoonverbinding.

In antwoord op de opmerking wil spreker nog toevoegen dat ISPA vragende partij is opdat deze wet wordt aangenomen omdat men vaststelt dat zich een aantal feiten voordoen zoals de hacking, paswoordenzwendel, het inbrengen van virussen, het mani-

l'introduction de virus, la manipulation de données, etc. En tant que juriste, il faut être très créatif pour trouver une parade dans le Code pénal actuel. L'intervenant renvoie à la vieille affaire Bistel, dans laquelle on avait poursuivi l'intéressé pour vol d'électricité. L'ISPA est partie prenante pour que les autorités soient à même de s'attaquer à un certain nombre de phénomènes nouveaux.

Il va de soi que l'ISPA se préoccupe aussi du contenu. Elle souligne l'existence d'un point d'appui judiciaire. Toute observation sur le contenu parvenant aujourd'hui à un membre de l'ISPA est prise au sérieux et rapportée. Mais une importante tâche incombe également aux FAI, car on ne peut pas donner suite à toute demande de fermeture du site d'un tiers; les FAI ont donc fort à faire pour signaler que : « Nous avons bien reçu votre requête; nous prendrons contact avec notre abonné et lui demanderons ce qui se passe. » On le fait avec beaucoup de sérieux et il y a toujours eu *a fortiori* en Belgique un respect pour les décisions du parquet comme des tribunaux civils. On a toujours donné suite — bon gré, mal gré — aux condamnations du tribunal ordonnant de fermer l'accès à un site. Quant à savoir si cela éradique le problème, c'est une autre histoire.

M. Beirens veut réagir à la question d'un membre concernant l'incrimination du simple fait de pénétrer dans l'ordinateur.

Les pirates informatiques tentent souvent à différentes reprises de pénétrer dans le système sans faire de dégâts. Suit alors souvent un échange de mots de passe, comme l'a expliqué le représentant de l'ISPA. On a donc déchiffré le code d'accès sans toucher au système et on est parvenu de l'une ou l'autre façon à connaître le moyen d'y pénétrer. C'est une sorte d'acte préparatoire. On garde cette information et on va l'utiliser comme monnaie d'échange pour pénétrer dans d'autres systèmes. Il faut pouvoir distinguer avec quelqu'un qui s'est retrouvé par accident à l'intérieur du site ou d'un ordinateur, mais lorsqu'il n'y a pas intention de nuire, cela ressort de l'enquête. Mais s'il s'agit effectivement d'un acte préparatoire en vue de pénétrer dans un système, cela vaut la peine d'incriminer ce fait. Il appartient bien entendu à la commission de se prononcer à ce sujet.

Le plus souvent, la victime constate, certes, qu'il y a eu un problème, mais cela ne doit pas empêcher d'incriminer certains faits. On constate souvent une infraction chez une seule personne et, en examinant le matériel informatique de l'auteur, on constate qu'il a pénétré dans d'autres sites. Ces données sont alors effectivement utilisées comme monnaie d'échange et transmises à d'autres pirates.

puleren van data, enz. Als jurist moet men zeer creatief zijn om er in het huidige Strafwetboek iets op te vinden. Spreker verwijst naar de oude Bistel-zaak waar men toen de man heeft vervolgd wegens diefstal van elektriciteit. ISPA is vragende partij opdat de overheid in staat zou zijn om een aantal nieuwe fenomenen aan te pakken.

Uiteraard is ISPA ook bezorgd over de inhoud. ISPA wijst op het bestaan van het gerechtelijk meldpunt. Elke opmerking die een lid van ISPA vandaag krijgt over inhoud wordt au serieux genomen en gerapporteerd. Maar op de ISP's rust ook een belangrijke taak want men kan geen gevolg geven aan ieder verzoek tot het afsluiten van de site van een derde, dus de ISP's hebben veel werk om te melden: « We hebben uw verzoek goed ontvangen; we zullen contact opnemen met onze abonnee en vragen wat er aan de hand is. » Men doet dat heel ernstig en er is in België *a fortiori* altijd respect geweest voor de uitspraken zowel van het parket als van de burgerlijke rechtbanken en men heeft — graag of niet graag — altijd gevolg gegeven aan veroordelingen door de rechtbank om de toegang tot een site af te sluiten. Of dat het probleem uitroeit is een andere vraag.

De heer Beirens wil reageren op de vraag van een lid in verband met het strafbaar stellen van het enkele feit van binnen te dringen in de computer.

Hackers proberen vaak verschillende malen om in het systeem binnen te dringen zonder schade toe te brengen. Daarna komt er dikwijls een ruilhandel van paswoorden op gang, zoals de vertegenwoordiger van ISPA meegedeeld heeft. Dus zonder dat men in het systeem ook maar iets gedaan heeft, heeft men de toegangscode ontcijferd of is men op één of andere manier te weten gekomen hoe men in een systeem moet binnendringen. Het is een soort voorbereidende handeling. Men houdt die informatie bij en gaat ze gebruiken als een soort pasmunt om in andere systemen binnen te dringen. Men moet een onderscheid kunnen maken tussen degene die per ongeluk op een site of een computer terecht gekomen is, maar als er geen kwaad opzet mee gemoeid is, blijkt dat uit het onderzoek. Als het inderdaad een voorbereidende handeling is om in een systeem binnen te dringen, is het toch wel de moeite waard om dat feit strafbaar te stellen. Het is natuurlijk aan de commissie om daarover te oordelen.

Meestal stelt het slachtoffer wel vast dat er een probleem is geweest, maar dat belet niet dat men bepaalde zaken strafbaar kan stellen. Men stelt dikwijls een inbreuk vast bij één persoon en als men het informaticamateriaal van de dader gaat onderzoeken, ziet men dat hij op andere sites is binnengedrongen. Die gegevens worden dan inderdaad als ruilhandel gebruikt en worden doorgegeven aan andere hackers.

M. Bogaert réplique que l'information au départ d'une enquête vient des ingénieurs-systèmes des sociétés ou des universités qui reçoivent la visite des pirates. Sans entrer dans les détails, l'intervenant dit que le serveur Web du Bureau du Plan a été visité par des pirates informatiques ce qui implique une certaine inquiétude dans la mesure où il y a des données qui peuvent s'avérer confidentielles, en matière d'exportation pour la Belgique.

Au sujet de la durée de la conservation des données, l'intervenant est d'avis que le délai de douze mois est un minimum. D'après la demande de l'ISPA, cela devrait être un maximum. En fait, il faut savoir comment se déroule une enquête. À partir du moment où une personne, une société ou une institution prend conscience qu'elle a eu la visite d'un pirate informatique, que des données la concernant ont été divulguées ou qu'elle fait l'objet, par exemple, d'un harcèlement téléphonique à la suite de la création sur un site de rencontre d'un faux profil, il faut qu'elle parvienne dans un premier temps à localiser la source de ses tracas.

Elle se rend généralement dans le bureau de gendarmerie ou de police le plus proche pour déposer plainte et pour signaler qu'elle a été victime d'un pirate informatique. Elle se trouve généralement confrontée à un agent de police ou à un gendarme qui n'a pas spécialement l'habitude de ce problème. Consciencieusement, il actera la plainte qui sera transmise au parquet. Le parquet se retrouve confronté à un problème qui n'est pas encore particulièrement courant en matière judiciaire. Le dossier sera alors transmis au parquet de Bruxelles en demandant que la CCU de Bruxelles prenne en charge l'enquête.

Entre le moment où la personne a constaté l'infraction et le moment où la CCU a connaissance du dossier, une période de trois ou quatre mois peut s'écouler en raison du fonctionnement de l'institution judiciaire à l'heure actuelle. L'institution judiciaire se plaint en permanence de manquer de moyens, ce qui joue également en matière informatique. Si les moyens existaient et si le nombre de personnes qui enquêtent dans le domaine informatique était plus élevé, on pourrait travailler plus vite.

Dès que la CCU dispose des informations concernant le délit commis, ils demandent, par l'intermédiaire du parquet, au fournisseur d'accès de leur identifier le numéro IP de la machine qui était connectée à l'ordinateur qui a subi cette infraction. Puis, ils essayent de remonter jusqu'à l'auteur de ce délit. Il n'y a pas forcément un seul opérateur. À ce niveau-là, la collaboration est parfaite.

Il peut y avoir eu plusieurs intermédiaires et si Skynet donne une information qui renvoie à un autre opérateur, la même demande sera faite auprès de ce nouvel opérateur. En fonction des moyens dont on

De heer Bogaert antwoordt dat de informatie bij het begin van een onderzoek komt van de systeemingenieurs van de bedrijven of de universiteiten die bezoek krijgen van de krakers. Zonder in detail te willen treden, merkt spreker op dat de webserver van het Planbureau computerkrakers op bezoek heeft gekregen. Dit geeft aanleiding tot enige ongerustheid daar bepaalde gegevens vertrouwelijk kunnen zijn, bijvoorbeeld die inzake uitvoer voor België.

Wat de bewaartermijn voor gegevens betreft, is spreker van mening dat twaalf maanden een minimum is. ISPA vraagt dat dit een maximumtermijn zou zijn. Eigenlijk moet men weten hoe een onderzoek verloopt. Zodra een persoon, een bedrijf of een instelling beseft dat iemand in het computersysteem is binnengedrongen, dat persoonlijke gegevens verspreid worden of dat die persoon bijvoorbeeld het slachtoffer wordt van hijgtelefoons nadat over hem een vals profiel werd verspreid op een site met contactadvertenties, moet in een eerste fase de bron van alle ellende gelokaliseerd kunnen worden.

De betrokkene klopt gewoonlijk aan bij het dichtstbijgelegen rijkswacht- of politiebureau om er klacht in te dienen en om er mee te delen dat hij het slachtoffer is geworden van een computerkraker. De politieagent of rijkswachter die niet noodzakelijk vertrouwd is met dit soort problemen, zal plichtsgetrouw de klacht noteren en doorspelen aan het parket. Ook het parket wordt geconfronteerd met een probleem dat niet erg gebruikelijk is in gerechtelijke kringen. Het dossier zal worden overgezonden aan het parket van Brussel met het verzoek dat de CCU van Brussel zich met het onderzoek bezighoudt.

Tussen het ogenblik waarop de betrokkene het misdrijf heeft vastgesteld en het ogenblik waarop de CCU kennis neemt van het dossier, kan een periode van drie tot vier maanden liggen naar gelang van de snelle of minder snelle werking van het gerecht. Het gerecht klaagt voortdurend over een gebrek aan middelen en dat geldt ook op informaticagebied. Indien de middelen voorhanden waren en er meer onderzoekers waren op het gebied van de informaticacriminaliteit, dan zou er sneller kunnen worden gewerkt.

Zodra de CCU beschikt over de informatie betreffende het gepleegde misdrijf, wordt via het parket bij de internetprovider het IP-nummer opgevraagd van de machine die verbonden was met de computer die het slachtoffer van dit misdrijf geworden is. Vervolgens wordt gepoogd op te klimmen tot de dader van het misdrijf. Er is niet noodzakelijk één enkele operator. Op dat niveau is de samenwerking perfect.

Er kunnen verschillende tussenpersonen geweest zijn en indien Skynet informatie verstrekt die verwijst naar een andere operator, wordt hetzelfde verzoek gericht tot die nieuwe operator. Naar gelang van de

dispose et en fonction de l'évolution technologique, la durée d'un an est tout à fait acceptable pour permettre d'obtenir l'identification de l'auteur avec une quasi certitude.

Le ministre précise que la première version du projet présentée à la Chambre par le gouvernement ne précisait aucune durée. On pensait pouvoir régler le problème par arrêté royal et c'est au cours des débats en commission de la Justice que le député Verherstraeten a dépose un amendement qui a reçu un soutien unanime. Le ministre s'est rallié à cet amendement, se disant qu'on aurait peut-être pu se trouver dans une situation intenable en exigant un délai de conservation qui soit identique à celui de la prescription de l'action publique. Le gouvernement n'a soulevé aucune objection lorsqu'on a fait cette proposition. L'amendement de Mme Nyssens tend à remplacer le mot «minimum» par «maximum». Les autorités doivent encore pouvoir mener une enquête tout en respectant l'équilibre entre l'enquête pénale, la protection de certaines valeurs et le respect de la vie privée.

M. Olivier van Cutsem confirme qu'il va de soi qu'une collaboration est souhaitable dans le but de poursuivre les actes pénalement répréhensibles. Concernant la question de la rapidité et de la poursuite des infractions pénales, l'intervenant annonce qu'il a été décidé avec le ministère de la Justice que l'ISPA allait entreprendre des formations pour les magistrats instructeurs. Celles-ci pourraient également être envisagées au niveau des *Computer Crime Unit* et éventuellement concerner d'autres membres des autorités judiciaires afin de leur assurer une formation sur le plan de la technologie.

D'autre part, l'intervenant tient à signaler que Belgacom avait déjà entrepris ce genre de démarche, il y a plus d'un an, en organisant des formations destinées aux juges d'instruction non seulement pour tout ce qui concernait les aspects purement télécom mais également pour les aspects internet. Il est persuadé qu'une bonne formation et une prise de conscience de l'existence de ce nouveau type de délit, pourraient permettre de réduire les délais dans des sections locales de la *Computer Crime Unit* ou de la gendarmerie; il y va de leur intérêt mais aussi de celui du justiciable.

L'intervenant s'étonne des exemples étrangers de douze mois alors que les trois mois dont disposent le Danemark, les Pays-Bas et l'Allemagne semblent tout à fait suffisants pour pouvoir demander des informations aux ISP. À son avis, six mois paraît être un délai tout à fait correct pour entamer et demander des informations aux fournisseurs d'accès. Ce délai leur donnera également la possibilité de conserver ces données dans des conditions qui économiquement ne les pénalisent pas et qui ne pénalisent pas le client final.

middelen waarover men beschikt en van de technologische ontwikkelingen, kan het makkelijk één jaar duren om de dader nagenoeg met zekerheid te identificeren.

De minister preciseert dat de eerste versie van het ontwerp, zoals het in de Kamer door de regering is ingediend, in geen enkele termijn voorzag. Men was toen nog de mening toegedaan dat het probleem geregeld kon worden bij koninklijk besluit; tijdens de bespreking in de commissie voor de Justitie heeft kamerlid Verherstraeten een amendement ingediend dat door iedereen gesteund werd. De minister heeft zich achter dit amendement geschaard omdat hij van mening was dat het allicht niet haalbaar was een bewaartermijn te eisen die overstemde met die voor de verjaring van de strafvordering. De regering had geen enkel bezwaar toen dit voorstel werd gedaan. Het amendement van mevrouw Nyssens strekt ertoe het woord «minimum» te vervangen door het woord «maximum». Er moet nog een onderzoek kunnen worden verricht met inachtneming van het evenwicht tussen strafonderzoek, bescherming van bepaalde waarden en eerbiediging van de persoonlijke levenssfeer.

De heer Olivier van Cutsem bevestigt dat samenwerking uiteraard wenselijk is om strafbare feiten te kunnen vervolgen. Wat de snelheid betreft waarmee die feiten worden vervolgd, kondigt spreker aan dat in overleg met het ministerie van Justitie besloten werd dat ISPA opleidingen voor onderzoeksmagistraten zal organiseren. Er zouden eveneens opleidingen kunnen worden gegeven aan de leden van de *Computer Crime Unit* en ook andere leden van de gerechtelijke autoriteiten zouden voor een opleiding op het gebied van de technologie in aanmerking kunnen komen.

Spreker wijst erop dat Belgacom reeds meer dan een jaar geleden die stap gezet heeft en opleidingen heeft georganiseerd voor onderzoeksrechters, niet alleen over de aspecten van de telecommunicatie maar ook over die van het internet. Hij is ervan overtuigd dat een degelijke opleiding en een bewustwording van het bestaan van dit soort misdrijven de termijnen in de lokale afdelingen van de *Computer Crime Unit* of van de rijkswacht drastisch kunnen inkorten. Het is in het belang van die afdelingen maar ook in het belang van de rechtzoekende.

Spreker is verbaasd over de buitenlandse voorbeelden waar twaalf maanden geldt, terwijl de drie maanden waarover Denemarken, Nederland en Duitsland beschikken, ruim voldoende blijken om informatie te vragen aan de ISP's. Zijns inziens lijkt een termijn van zes maanden correct om informatie op te vragen bij de providers. Die termijn zal hen ook de mogelijkheid geven om die gegevens te bewaren op een economisch verantwoorde wijze zonder de eindklant te benadelen.

Le ministre précise que le service formation des magistrats du ministère de la Justice organise effectivement un ensemble de cours; l'ISPA y est invitée tout comme la NCCU et d'autres membres. Cette formation est assurée par le ministère de la Justice sous la présidence d'un magistrat. Les magistrats sont bien conscients des problèmes et entendent mettre à leur disposition tous les outils nécessaires.

Un sénateur évoque la problématique de la conservation, pour ce qui est du territoire et du coût de la conservation. Après avoir entendu l'exposé de la *National Computer Crime Unit* et des CCU qui y sont rattachées, il lui semble que les délais qu'elles préconisent sont en fait dictés par leur manque d'effectif. Le message à l'autorité devrait alors être que c'est là qu'il faut investir pour renforcer la position des intéressés, l'améliorer et accélérer le travail de recherche. Il n'est pas possible d'adapter le délai de conservation chaque fois que le manque d'effectif s'aggrave ou se réduit. Ce serait tirer une mauvaise conclusion. En ce qui concerne le délai de conservation, il faut partir d'une sorte de «*bench marking*». Regardons l'Europe, les tendances européennes. On parle d'un délai de trois mois dans les pays voisins. On parle d'une harmonisation européenne qui irait vers les six mois. L'intervenant ne voit pas très bien pourquoi on instaurerait en l'espèce un délai double, voire quadruple, qui serait, de surcroît, un minimum de douze mois. Il faut trouver le juste milieu, et un délai de six mois pourrait constituer un bon compromis.

En ce qui concerne le problème du coût de la conservation, l'intervenant fait une comparaison avec les Pays-Bas, où l'on examine actuellement une proposition de loi visant à modifier certaines choses sur le plan de la criminalité informatique. Il existe là-bas une loi relative au «tarif en matière pénale», prévoyant que les pouvoirs publics rémunérent les personnes étrangères à la police qui collaborent dans le cadre d'une mesure d'écoute téléphonique. Dans notre pays, cela relève davantage du droit coutumier. Selon Belgacom, s'il y a fourniture de prestations, il peut aussi y avoir facture. Il semblerait que l'on ait déjà dit à maintes fois que le problème des frais pourrait se régler par arrêté royal. On n'y est toujours pas parvenu jusqu'à présent. Peut-être tient-on ici l'occasion idéale de régler le problème une fois pour toutes, de sorte que le facteur coût auquel sont confrontés les fournisseurs d'accès internet tombe en partie et qu'il leur soit aussi plus facile de conserver ces données pendant un délai dépassant peut-être trois mois. Aux Pays-Bas, on paie 50 florins au fournisseur d'accès par donnée demandée.

Enfin, en ce qui concerne le territoire sur lequel les données doivent être conservées, on peut dire qu'il est nécessaire que la police dispose de tous les moyens

De minister preciseert dat de dienst opleiding van magistraten van het ministerie van Justitie inderdaad een aantal cursussen organiseert; ISPA en de NCCU worden hiervoor uitgenodigd alsook andere leden. Die opleiding wordt aangeboden door het ministerie van Justitie onder het voorzitterschap van een magistraat. De magistraten zijn zich wel degelijk bewust van de problemen en willen alle noodzakelijke hulpmiddelen tot hun beschikking hebben.

Een senator maakt een opmerking in verband met de bewaringsproblematiek, met betrekking tot het grondgebied en de kost van bewaring. Gelet op de uiteenzetting van de *National Computer Crime Unit* en de verbonden CCU's lijkt het hem dat de termijn die zij voorstellen eigenlijk ingegeven is door hun onderbezetting. De boodschap naar de overheid zou dan moeten zijn dat daar een investering moet worden gedaan om die mensen te versterken, te verbeteren en het opsporingswerk te doen versnellen. Het mag niet zijn dat telkens wanneer de onderbezetting groter wordt of minder groot wordt, de bewaringstermijn wordt aangepast. Dat zou een verkeerde gevolgtrekking zijn. Wat betreft de bewaringstermijn, moet men uitgaan van een soort «*bench marking*». Men moet kijken naar Europa, de Europese tendensen. Men spreekt van een termijn van drie maanden in de buurlanden. Men spreekt van een Europese harmonisatie gaande in de richting van zes maanden. Spreker ziet niet goed in waarom men hier dan een dubbele of zelfs een vierdubbele termijn zou inbouwen in de wet met dan nog een minimum van twaalf maanden. Men moet de gulden middenweg vinden en zes maanden zouden een goed compromis kunnen vormen.

Met betrekking tot de problematiek van de kosten voor het bewaren maakt spreker de vergelijking met Nederland waar momenteel een wetsvoorstel wordt besproken om een en ander te wijzigen op het vlak van computercriminaliteit. Daar bestaat een wet «tarief op strafzaken» die erin voorziet dat mensen — buitenstaanders van politie die meewerken naar aanleiding van een aftapmaatregel — betaald worden door de overheid. Bij ons is dat meer een gewoonterecht. Belgacom vindt dat als er prestaties worden geleverd, er ook facturen mogen zijn. Men heeft blijkbaar al herhaaldelijk gesteld dat de kostenproblematiek zou te regelen zijn via een koninklijk besluit. Men is er tot nu toe nog niet in geslaagd. Misschien is dit het perfecte ogenblik om dit voor goed te regelen zodanig dat het element van de kostprijs waarmee de mensen van de ISP's worden geconfronteerd, voor een stuk wegvalt en dat het voor hen ook gemakkelijker wordt om die gegevens misschien langer dan drie maanden bij te houden. In Nederland betaalt men aan de provider 50 gulden per gegeven dat wordt opgevraagd.

Ten slotte, wat betreft het territorium waar de gegevens moeten worden bewaard, kan men hier stellen dat het noodzakelijk is dat het arsenaal voor de

possibles pour rechercher toutes les infractions. Il existe toujours des accords internationaux, une souveraineté et d'autres contraintes de ce genre. Si l'on souhaite changer quelque chose à cela, il faudra le faire en accord avec d'autres États. Nous ne pouvons faire cavalier seul en la matière ou prendre des mesures contraires aux accords internationaux. Le point de vue adopté aux Pays-Bas par rapport à cette proposition de loi est également très clair. La disposition selon laquelle les données doivent être conservées sur notre territoire est contraire aux règles de la liberté de marché et du marché intérieur européen. Les FAI implantés à l'heure actuelle en Belgique et qui conservent des données dans notre pays n'ont vraisemblablement pas l'intention de déménager.

politie zo groot mogelijk is om alle misdrijven op te sporen. Er bestaan nog altijd internationale afspraken; er bestaat nog altijd een soevereiniteit en dergelijke meer. Wil men daar iets aan veranderen, dan moet dat in samenspraak zijn met andere Staten. Wij kunnen op dat vlak niet het voortouw nemen of dingen vastleggen die ingaan tegen internationale afspraken. Met betrekking tot dat wetsvoorstel wordt in Nederland ook heel duidelijk stelling genomen. De bepaling waarbij gesteld wordt dat de gegevens op ons grondgebied moeten worden gehouden, gaat in tegen de regels van de vrije markt en de interne markt in Europa. Het is waarschijnlijk niet de bedoeling van de ISP's die vandaag in België zitten en die gegevens hier behouden, te verhuizen.

Un certain nombre de FAI, tels Compuserve, AOL et d'autres, conservent probablement ces données dans d'autres pays d'Europe et devraient faire des frais supplémentaires pour se conformer à la loi et transférer physiquement des données dans notre pays. Il est à espérer que l'on trouve une solution intermédiaire dans le sens indiqué par M. Glas.

Er zijn een aantal ISP's, zoals Compuserve, AOL en zo, die gegevens waarschijnlijk op andere plaatsen in Europa houden en die een supplementaire kost zouden moeten doen om op basis van die wet gegevens fysiek naar hier te moeten brengen. Hopelijk vindt men daar toch een tussenoplossing in de richting van hetgeen de heer Glas heeft gezegd.

L'intervenant se pose encore un certain nombre de questions qui concernent spécifiquement le travail de recherche qui se fait actuellement sur l'internet. Un point qui est souvent évoqué mais dont on n'a pas encore dit grand-chose concerne les données d'appel : la lecture des courriers électroniques. Les services judiciaires font-ils appel aux FAI ou à d'autres intermédiaires pour obtenir les adresses de courrier électronique auxquelles des données sont transférées ou pour en vérifier le contenu ? Dans l'affirmative, sur quelle base légale le font-ils ?

Spreker heeft nog een aantal vragen specifiek in verband met het recherchewerk dat momenteel op het internet gebeurt. Een punt dat dikwijls aan bod komt maar waar nog heel weinig over gezegd is, is in verband met de oproepgegevens: e-mails lezen. Doen de gerechtelijke diensten beroep op ISP's of andere tussenpersonen om e-mailadressen te hebben waar gegevens naartoe worden gestuurd of de inhoud na te gaan ? Als zij dit doen, op welke wettelijke grond baseren zij zich ?

Une deuxième question concerne le pseudo-achat et l'infiltration. Les services de la police judiciaire infiltrent-ils parfois certains réseaux et achètent-ils éventuellement certaines choses, des photos, etc. ? Aux Pays-Bas, il existe une réglementation concernant l'infiltration et le pseudo-achat. Prépare-t-on une réglementation similaire en Belgique ?

Een tweede vraag betreft de pseudo-koop en infiltratie. Infiltreren de diensten van de gerechtelijke politie soms in bepaalde netwerken waarbij zij eventueel dingen aankopen, foto's en dergelijke meer ? In Nederland bestaat een regeling op de infiltratie en op de pseudo-koop. Wordt hier aan gewerkt ?

La dernière question concerne le problème du nazisme. Selon un préopinant, le problème que Yahoo a connu en France était lié au nazisme. Quels sont les attaches nécessaires pour pouvoir dire que l'on est fondé à poursuivre une infraction déterminée, qualifiée comme telle dans notre Code pénal ? Si le Ku Klux Klan, aux États-Unis, formule un certain nombre d'observations racistes qui sont contraires aux dispositions de notre loi relative à la luttre contre le racisme, mais qui se trouvent sur un serveur étranger, les services judiciaires prennent-ils des mesures ou obligent-ils les logiciels de navigation belges qui renvoient à ces sites à supprimer les liens vers ceux-ci ?

Het laatste punt betreft de problematiek van het nazisme. Het komt een voorgaande spreker voor dat het probleem van Yahoo in Frankrijk het nazisme was. Welke zijn de voldoende aanknopingspunten om te zeggen dat voor een bepaald misdrijf dat bepaald is in ons Strafwetboek, grond bestaat om te vervolgen ? Als er vanuit de Ku Klux Klan in de Verenigde Staten een aantal racistische opmerkingen worden gemaakt die contra onze wet op de racismebestrijding zijn, maar die op een buitenlandse server staan, ondernemen de gerechtelijke diensten dan stappen of verplichten zij Belgische zoekrobotten die verwijzen naar die sites om dergelijke links weg te halen ?

M. Verbeeren répond qu'il y a, dans le Code pénal, des dispositions relatives au contenu pour des infractions traditionnelles comme la pornographie enfan-

De heer Verbeeren antwoordt dat wetsbepalingen bestaan in het Strafwetboek in verband met de inhoud, voor traditionele misdrijven zoals kinderpor-

tine, le racisme, les atteintes au droit d'auteur. Si la NCCU est informée de l'existence d'une littérature révisionniste, proposée en Belgique par une entreprise commerciale belge ou par un ressortissant belge («l'acte est lié à la Belgique»), ou est amenée à faire des constatations de ce type, alors elle intervient. Elle dresse ensuite procès-verbal comme pour les autres constatations d'infractions qui sont transmises au parquet. Par contre, si l'information de cette entreprise commerciale belge diffuse par l'intermédiaire de fournisseurs situés à l'étranger, la NCCU n'a aucun pouvoir. Il appartient alors au parquet, au magistrat qui mène l'enquête, de prendre les mesures qui s'imposent. Cela ne s'est pas encore produit.

Il est exact que l'on peut trouver beaucoup d'informations sur des contenus illégaux de toute sorte au moyen de logiciels de navigation comme Altavista ou Yahoo. On se sert en fin de compte de l'infrastructure du fournisseur d'accès pour exécuter certaines missions de recherche. Cette discussion va très loin et sort peut-être du débat sur le projet à l'examen. Pour ce qui est de l'information disponible sur le *World Wide Web*, la responsabilité éventuelle pourrait incomber au fournisseur d'accès. La situation est tout à fait différente lorsqu'il s'agit par exemple de groupes de nouvelles où l'information est présente physiquement sur les serveurs de nouvelles des fournisseurs d'accès. Dans l'esprit du protocole d'accord, le bureau de notification judiciaire et les fournisseurs d'accès ont de bons contacts et collaborent bien. Lorsqu'on constate, dans ces groupes de nouvelles, qu'il y a de la pornographie enfantine, on le signale aux fournisseurs d'accès. Ceux-ci sont alors censés être informés de la présence de matériel illégal. Si une plainte venait ensuite encore à être déposée concernant l'offre de ce genre de matériel illégal, la responsabilité des fournisseurs d'accès pourraient être engagée sur le plan judiciaire.

La technique des pseudo-achats et les techniques similaires sont utilisées effectivement dans d'autres pays et y sont même plus développées qu'en Belgique. L'on s'y livre, à propos de ces techniques, à des exercices de réflexion qui n'ont toutefois encore abouti à rien de concret. Le problème majeur vient de ce que, pour presque tous les sites contenant de la pornographie enfantine, par exemple, les paiements, doivent être effectués au moyen d'une carte Visa. Il en résulte un problème de technique financière, étant donné que les services de la NCCU ne disposent pas d'une carte Visa.

M. Vandenberghe (NCCU) dit avoir l'impression qu'il y a un malentendu en l'espèce. Les sénateurs donnent parfois à penser que, pour eux, les membres des CCU sont des superflics, mais tel n'est pas leur avis. Ils se bornent à utiliser tous les moyens légaux, ce qui revient finalement à traduire en justice ceux qui se sont rendus coupables de l'une ou l'autre infraction. Lorsque des fautes de procédures ont été commises

nografie, racisme, inbreuken op auteursrechten. Als NCCU op de hoogte is of vaststellingen moet doen in verband met revisionistische lectuur die in België wordt aangeboden door een Belgische handelsonderneming, door een Belgische onderdaan («het is België gelinkt»), dan treedt zij op. Vervolgens stellen zij een proces-verbaal op zoals in andere vaststellingen van misdrijven die aan het parket worden overgemaakt. Daarentegen, als die informatie van die Belgische handelsonderneming via providers in het buitenland staat, dan hebben zij daar geen enkele bevoegdheid over. Het is dan aan het parket, aan de magistraat die het onderzoek leidt om verdere stappen te doen. Dit is nog niet gebeurd.

Het is inderdaad juist dat heel wat informatie kan gevonden worden over allerhande illegale inhoud via zoekmachines zoals «Altavista» of «Yahoo». Uiteindelijk wordt de infrastructuur van de internetprovider aangewend om bepaalde zoekopdrachten uit te voeren. Deze discussie gaat zeer ver en valt misschien buiten het debat over het ontwerp. Inzake informatie die op het *World Wide Web* staat, zou de eventuele aansprakelijkheid bij de internetprovider kunnen liggen. Het is heel anders wanneer het bijvoorbeeld nieuwsgroepen betreft, waar fysiek de informatie op de newsservers van de providers aanwezig zijn. Overeenkomstig het samenwerkingsprotocol zijn er goede contacten en werkwijzen tussen het gerechtelijk meldpunt en de providers. Wanneer in die nieuwsgroepen kinderpornografie wordt aangetroffen, wordt dit gemeld aan de internetproviders. Zij zijn dan verondersteld op de hoogte te zijn van de aanwezigheid van illegaal materiaal. Wanneer er dan nog een klacht zou binnenkomen over het aanbieden van dergelijke illegaal materiaal, dan zouden zij op gerechtelijk vlak mede aansprakelijk kunnen worden gesteld.

De pseudo-koop en dergelijke zijn zaken die inderdaad in andere landen gebeuren en ook meer uitgebouwd zijn dan hier in België. Er zijn daar denkoefeningen over bezig die nog niet concreet zijn. Het grootste probleem ligt daarbij dat, bijvoorbeeld voor een site met kinderporno, bijna in alle gevallen de betaling dient te geschieden met een Visa-kaart. Daar ligt een financieel technisch probleem, namelijk dat de diensten van de NCCU niet beschikken over een Visa-kaart.

De heer Vandenberghe (NCCU) heeft de indruk dat het hier om een misverstand gaat. De senatoren geven soms de indruk te denken dat de CCU *super cybercops* zijn. Dat is het dus niet. Zij beperken zich tot het gebruik van alle wettelijke middelen. Uiteindelijk vertaalt het resultaat zich in het voor de rechtbank brengen van iemand die zich schuldig heeft gemaakt aan enig misdrijf. Als op het vlak van de procedure

lors de la recherche de faits commis, il est impossible de mener la procédure à bonne fin. L'objectif n'est assurément pas de travailler dans l'illégalité. Les CCU utilisent toutes les voies légales pour arriver à traduire quelqu'un en justice en recourant à des moyens honnêtes et loyaux. Toutes les opérations, qu'elles soient menées au niveau national en question ou au niveau judiciaire se déroulent en principe toujours sous le contrôle du magistrat national.

M. Beirens répond à la question relative à la lecture des messages électroniques. Il déclare que jusqu'à présent, on n'a intercepté aucun message électronique sur aucune base. Un jour, on est allé, muni d'un mandat de perquisition, retirer un message électronique qui était resté chez un fournisseur d'accès, du fait que le destinataire n'utilisait plus son abonnement. L'on s'est rendu alors, avec un mandat de perquisition, chez le fournisseur d'accès chez qui était encore stocké le message électronique d'un des suspects dans l'affaire en question, qui n'avait toutefois plus de compte actif chez ledit fournisseur. C'est le seul cas d'interception d'un message électronique dont l'intervenant a connaissance. En ce qui concerne l'éventuelle application de la loi sur les écoutes, l'intervenant note que, pour lui, le message électronique est tout bonnement un message qui circule; le considérer comme une communication ne posera donc guère de problèmes.

M. Coenraerts déclare que la question se pose évidemment de savoir s'il faut ranger les messages électroniques parmi les lettres classiques ou non. La jurisprudence n'a pas encore vraiment répondu à cette question. Par souci de prudence, on applique actuellement pour ce qui est du secret des messages électroniques, les règles relatives au secret des lettres. Si l'on veut prendre connaissance d'un message électronique au cours d'une perquisition, on pourra le saisir s'il se trouve sur un support. On ne voit pas encore clairement si la loi sur les écoutes est applicable ou non en l'espèce; tout dépendra de l'applicabilité ou non des règles relatives au secret des lettres. Il n'existe pas encore de jurisprudence à ce sujet.

M. Bogaert a l'impression qu'une partie de la question semblait porter sur l'identification de l'auteur d'un e-mail. En fait, il faut savoir que l'on peut consulter par une simple manipulation de son logiciel, le nom et le numéro de l'ensemble des machines qui ont été traversées par le message à partir du moment où il est envoyé jusqu'au moment où il est arrivé. Nous avons la possibilité de savoir à partir de quelle machine ce message a été envoyé et, donc de la même manière à partir du moment où nous disposons d'un réquisitoire, d'obtenir du fournisseur d'accès, chez qui est hébergée la boîte aux lettres de l'expéditeur, l'identité de cet expéditeur.

Le ministre souligne que l'écoute téléphonique ou l'ouverture du courrier ne peut se faire que moyennant l'intervention d'un juge d'instruction. Donc, il

fouten werden gemaakt bij het achterhalen van gepleegde zaken, dan kan de procedure niet tot een goed einde gebracht worden. Het is zeker niet de bedoeling illegaal te werken. De CCU wenden alle wettelijke middelen aan, om op een eerlijke en oprechte manier iemand voor de rechtbank te brengen. Alle operaties — zowel op nationaal als op gerechtelijk vlak — gebeuren in principe altijd onder controle van de nationale magistraat.

De heer Beirens antwoordt op de vraag in verband met het lezen van e-mail. Spreker legt uit dat zij tot op heden nog geen e-mail hebben onderschept, op welke basis dan ook. Eens is er met een huiszoekingsbevel de e-mail opgehaald bij een provider waar de e-mail achtergebleven was van een persoon die zijn abonnement niet meer gebruikte. Op dat moment is men met een huiszoekingsbevel bij de provider gegaan waar de e-mail nog opgeslagen was van één van de verdachten in de zaak, maar die geen actieve account meer had bij die provider. Dit is het enige geval waarvan spreker op dit ogenblik kennis heeft, waarbij men een e-mail onderschept heeft. Wat de eventuele toepassing van de «tapwet» betreft, meent spreker dat e-mail gewoon een bericht is dat onderweg is; er zullen dus weinig problemen zijn om dit als communicatie te gaan beschouwen.

De heer Coenraets verduidelijkt dat de vraag natuurlijk rijst of men e-mail laat vallen onder de klassieke brief of niet. Die vraag is nog altijd niet echt opgelost door de rechtspraak. Voorzichtigheidshalve past men momenteel dezelfde regels toe als voor het briefgeheim. Als men tijdens een huiszoeking een e-mail wil inkijken, kan men overgaan tot een inbeslagname, als dat zich op een drager bevindt. Of de tapwet van toepassing is of niet is nog niet duidelijk; dit is afhankelijk van het feit of men dit al dan niet onder een briefgeheim laat vallen. Op dit vlak is er nog geen rechtspraak.

De heer Bogaert heeft de indruk dat een deel van de vraag ging over de identificatie van de schrijver van een e-mail. De software maakt het mogelijk de naam en het nummer te achterhalen van alle computers waar de boodschap doorheen is gegaan vanaf de verzending tot de aankomst. Wij kunnen achterhalen vanuit welke computer de boodschap is gestuurd en, als we over een vordering beschikken kunnen we aan de provider bij wie de verzender zijn brievenbus heeft, de identiteit van die verzender opvragen.

De minister benadrukt dat de telefoontap of het openen van brieven alleen kan gebeuren op bevel van de onderzoeksrechter. De politiediensten kunnen dit

n'y aura jamais une intervention directe et immédiate des forces de police sans la couverture ou l'autorisation d'un juge d'instruction.

M. Geert Derre, attaché à la NCCU-Bruxelles, souhaite revenir sur la question du délai de conservation proposé qui est d'un an. Pour fixer ce délai, l'on s'est basé sur la manière dont les choses ont évolué dans les pays voisins. L'on doit faire face en Europe et dans le monde entier à une criminalité informatique par la voie de l'internet. La Belgique reçoit également des commissions rogatoires venant d'autres pays pour procéder à l'identification de données TCP-IP. Ils doivent rester dans les limites de ces commissions rogatoires, qui prennent bien sûr beaucoup de temps. Il est fort possible, lorsque le délai est trop restreint, que les commissions rogatoires ne puissent pas être exécutées, simplement parce que les choses ne vont pas assez vite chez nous. Il existe une solidarité internationale en Europe, et c'est un facteur très important. Si l'on envisageait de prévoir un délai de trois mois, les données TCP-IP en question n'existeraient plus étant donné que le délai serait déjà arrivé à expiration. Il se pourrait, dans ce cas, que nous soyons par exemple confrontés, en Belgique, à une personne qui diffuse de la pornographie enfantine et que nous ne soyons pas à même d'aider le BKA. Or, la lutte contre la pornographie enfantine est prioritaire en Belgique.

Une commissaire pose la question de savoir si l'ISPA regroupe l'ensemble des fournisseurs ? Belgacom, par exemple, fait-il partie de cette association et soutient-il les mêmes thèses ?

Un des orateurs a parlé de la convention du Conseil de l'Europe sur le sujet. Ce projet de loi est-il en harmonie complète et est-il une transposition de ce texte ?

Il est vrai qu'un article paru dans *Le Vif-L'Express* trouvait que la formulation des infractions dans le projet de loi était particulièrement large et floue. En lisant le projet de loi et l'article du *Vif-L'Express* et en particulier l'article 6, § 5, et l'article 7, § 4, il y avait des exemples qui expliquaient que n'importe quel citoyen même bien intentionné pouvait tomber sous la sanction pénale prévue par les articles.

Le libellé des infractions, telles qu'elles sont prévues par le projet de loi, permet-il de travailler avec une précision suffisante afin de pouvoir déceler toutes les infractions visées, ou y a-t-il des libellés excessivement larges qui, avec une interprétation pas suffisamment restrictive, pourraient faire en sorte que de braves citoyens tombent sous le coup de la loi pénale ?

M. Olivier van Cutsem répond que l'ISPA représente la grande majorité des ISP en Belgique et entre autres l'ensemble des membres de l'ISPA couvre 90 % des parts du marché de l'internet en Belgique.

nooit onmiddellijk en rechtstreeks doen zonder machtiging van de onderzoeksrechter.

De heer Geert Derre, verbonden aan het NCCU-Brussel, wenst terug te komen op de voorgestelde bewaringstermijn van één jaar. Om die termijn vast te stellen baseert men zich op de evoluties in onze buurlanden. Via internet wordt men in Europa, in gans de wereld, geconfronteerd met informaticacriminaliteit. Van andere landen ontvangt ook België rogatoire commissies met betrekking tot identificaties van TCP-IP-gegevens. Zij moeten zich houden aan die rogatoire commissies die natuurlijk heel wat tijd in beslag nemen. Indien de termijn te beperkt is, is het goed mogelijk dat de rogatoire commissies niet kunnen worden uitgevoerd omdat men in België achterwege blijft. Er heerst in Europa een solidariteit op internationaal vlak en dit is een zeer belangrijke factor. Indien men een termijn van drie maanden zou overwegen dan bestaan die TCP-IP-gegevens niet meer, want de drie maanden zijn al overschreden. In dat geval zouden we in België geconfronteerd worden met bijvoorbeeld een persoon die kinderpornografie verspreidt en we zouden niet in staat zijn om het BKA te helpen. Nochtans is in België de strijd tegen kinderpornografie prioritair.

Een commissielid vraagt of alle providers lid zijn van de ISPA. Maakt Belgacom bijvoorbeeld deel uit van deze vereniging en deelt het dezelfde principes ?

Een van de sprekers had het over het verdrag van de Raad van Europa hierover. Is dit wetsontwerp in overeenstemming daarmee en is het een omzetting van die tekst ?

Volgens een artikel in *«Le Vif-L'Express»* is de formulering van de misdrijven in het wetsontwerp te ruim en te vaag. *«Le Vif-L'Express»* gaf vooral in verband met artikel 6, § 5, en artikel 7, § 4, voorbeelden waaruit bleek dat elke brave burger de straffen kan oplopen waarin deze artikelen voorzien.

Zijn de misdrijven in het wetsontwerp voldoende precies geformuleerd opdat de bedoelde misdrijven precies kunnen worden opgespoord of zijn sommige ervan te ruim gedefinieerd zodat brave burgers het slachtoffer kunnen worden van een te ruime interpretatie van de strafwet ?

De heer Olivier van Cutsem antwoordt dat de ISPA de meerderheid van de ISP's in België vertegenwoordigt en dat de leden van de ISPA 90 % van de aandelen van de internetmarkt in België in handen hebben.

Concernant la participation de Belgacom à l'ISPA: Belgacom ne fait pas partie de l'ISPA puisque Belgacom n'est pas fournisseur d'accès à internet. C'est Skynet, une filiale de Belgacom, qui est membre de l'ISPA.

M. Coenraets souligne que le projet du Conseil de l'Europe ne donne qu'une définition générale de la conservation, et que cette définition doit encore être complétée par les États membres. En vue d'une harmonisation, le projet dispose que les États membres doivent prévoir une obligation de conserver sans délai les données communiquées, indépendamment de la réponse à la question de savoir si un ou plusieurs fournisseurs d'accès sont impliqués et s'il y a ou non complicité. Les autorités sont tenues de communiquer lesdites données aux services de police qui les leur demandent. Le projet comprend également des articles consacrés à la coopération internationale, qui disposent que l'État membre à qui une demande est faite doit prendre les mesures appropriées pour conserver effectivement les données visées, et ce, conformément à sa législation.

Cela revient à dire que le législateur doit tenir compte des demandes d'aide juridique qui prennent nécessairement le temps requis. Ces demandes sont complexes, surtout dans les cas de piratage informatique où nous avons affaire non plus à des amateurs, mais à des pirates spécialisés qui se sont mis au service de la criminalité organisée. Comme, dans un tel cas, il y a vite plusieurs pays impliqués, une période de trois à six mois ne suffit plus. Le projet tient compte d'éléments complexes de ce genre. Notre législation doit être adaptée à l'évolution des choses.

Un membre renvoie à l'observation de M. Van Cutsem relative au délai de conservation, selon laquelle ce délai est de trois mois dans les pays voisins de la Belgique. L'intervenante dit aussi avoir appris qu'en Grande-Bretagne, qui n'est pas un pays limitrophe, ce délai est de dix-huit mois. En est-il bien ainsi?

Ce qui importe, c'est l'applicabilité de la loi. Si l'on peut garantir que la loi pourra être appliquée effectivement au bout de six mois, c'est une bonne chose. Si la garantie que ce sera possible dans les six mois, n'est pas réelle, la loi risque d'être vidée de sa substance. Il est absurde de voter en Belgique une loi qui ne pourra pas être appliquée en raison des éléments invoqués par les membres de la NCCU.

Le présent projet de loi prévoit une conservation de douze mois. Comment procède-t-on dans les pays où ce délai de conservation n'est que de trois mois? Peut-être y applique-t-on une méthode plus efficace? Est-ce en harmonie avec le point de vue du Conseil de l'Europe?

M. Van Cutsem a aussi parlé d'une sorte de centralisation des centres de conservation au niveau du Benelux. Existe-t-il déjà quelque chose de tel à l'heure

Belgacom maakt geen deel uit van de ISPA omdat het geen internetprovider is. Skynet, een dochteronderneming van Belgacom, is wel lid van de ISPA.

De heer Coenraets vestigt de aandacht op het feit dat, wat betreft het bewaren, het ontwerp van de Raad van Europa enkel een algemene omschrijving geeft die nog door de lidstaten moet worden ingevuld. Met het oog op harmonisatie bepaalt het ontwerp dat de lidstaten moeten voorzien in een verplichting tot het onverwijld bewaren van de communicatiedata ongeacht de betrokkenheid van één of meerdere providers, ongeacht de compliciteit. De overheid is verplicht die data aan de politiediensten die erom verzoeken, bekend te maken. In het ontwerp zijn ook artikelen gewijd aan de internationale samenwerking, waarin bepaald wordt dat de aangezochte lidstaat de gepaste middelen dient te nemen teneinde de geviseerde data ook daadwerkelijk te bewaren, dit in overeenstemming met zijn wetgeving.

Het komt erop neer dat de wetgever dient rekening te houden met rechtshulpverzoeken die de nodige tijd in beslag nemen. Deze zijn complex vooral op het vlak van *hacking*gevallen waar we niet meer met amateurs te maken hebben, maar wel met gespecialiseerde *hackers* die in dienst staan van de georganiseerde misdaad. In dat laatste geval zijn er snel meerdere landen betrokken en volstaat een periode van drie à zes maanden niet meer. Het ontwerp houdt met dergelijke complexe zaken rekening. Onze wetgeving moet hieraan worden aangepast.

Een lid verwijst naar de opmerking van de heer Van Cutsem over de bewaringstermijn, namelijk dat deze in de ons omringende landen drie maanden bedraagt. Spreekster had nochtans vernomen dat Groot-Brittannië, weliswaar niet direct aangrenzend, over een termijn beschikt van achttien maanden. Is dit juist?

Wat van belang is, is de toepasbaarheid van de wet. Indien men kan garanderen dat binnen zes maanden de wet wel degelijk zou kunnen worden toegepast, is dit des te beter. Indien die garantie, dat dit binnen de zes maanden kan gebeuren, niet reëel is, dan bestaat het gevaar dat de wet zou worden uitgehold. Het heeft geen zin om in België een wet te stemmen, die niet kan toegepast worden, dit om de redenen die aangebracht werden door de leden van het NCCU.

In het voorliggend wetsontwerp wordt een bewaringstermijn van twaalf maanden vooropgesteld. Hoe werken de landen die over drie maanden beschikken? Misschien hebben zij een andere werkmethode die efficiënter is? Is dit in harmonie met de Raad van Europa?

De heer Van Cutsem heeft ook gesproken over een soort Benelux-centralisatie van bewaarcentra. Bestaat dit al op dit ogenblik? Iedereen is het eens dat de

actuelle ? Tout le monde s'accorde à reconnaître que la criminalité informatique n'a pas de frontières. Associer les trois pays du Benelux est certes un début, mais cela ne suffira pas. Il faudra opérer dans une perspective plus large.

M. Coenraets estime qu'il serait utile, dans le cadre de la discussion, d'une part, d'aller s'informer dans d'autres pays à propos des initiatives législatives qui y ont été prises en ce qui concerne les délais de conservation, et de faire une réelle analyse du rapport coût/profit pour les ISP.

Le membre dit partager cet avis d'autant plus que l'on cite, en l'occurrence, l'exemple d'un pays qui applique un délai de trois mois, sans savoir comment ces trois mois sont utilisés.

Une autre commissaire pose la question de savoir combien de temps Belgacom conserve actuellement ses données téléphoniques pour des enquêtes judiciaires ?

M. Van Cutsem ne peut répondre à cette question. Il peut cependant avouer que la loi, telle qu'elle sera votée, s'appliquera aussi bien aux foyers qui ont accès à internet qu'à tous les opérateurs de télécommunications, Belgacom y compris.

M. Bogaert explique que Belgacom a une cellule à Libramont qui est en charge de l'exploitation des données qui font suite à la demande des autorités judiciaires et travaille à deux niveaux. L'ensemble des centraux téléphoniques conserve les données pendant une durée déterminée d'à peu près six mois. Durant cette période, les données sont lisibles et disponibles instantanément sans autre forme de manipulation.

Ensuite, les données sont stockées et comprimées sous forme de bandes magnétiques à grande capacité. À partir de ce moment-là, l'exploitation des données et des bandes magnétiques devient une opération plus longue et plus coûteuse.

Un sénateur demande s'ils peuvent facturer leurs services et, si oui, à hauteur de quel montant ? Que comprend le coût constant, hormis les frais de mise en route, la capacité du personnel, les machines nécessaires ? Peut-il aussi être intégré dans la facture initiale ?

Le ministre répond affirmativement. Ce coût fait partie des frais de justice, d'écoutes téléphoniques, etc. et le ministre de la Justice est tenu de les payer.

Un membre fait remarquer que les opérateurs invoquent le problème du coût de l'opération, alors qu'il n'est pas à leur charge.

M. Van Cutsem répond que seuls les coûts de traitement de la demande sont payés à Belgacom. Ce n'est pas l'infrastructure qui est nécessaire pour répondre à la demande.

Le ministre souligne qu'en ce qui concerne l'exécution des écoutes téléphoniques, une réponse

informatiecriminaliteit over alle grenzen bestaat. Enkel die drie landen hierbij betrekken is een begin maar wellicht is dit onvoldoende. We moeten ruimer gaan werken.

M. Coenraets is van oordeel, dat het in het belang van de discussie nuttig is om in andere landen te gaan kijken naar hun wetgevende initiatieven wat betreft de bewaartermijnen, en dat er een echte kostenbatenanalyse in hoofde van de ISP's gemaakt wordt.

Het lid stemt hiermee in omdat hier een voorbeeld aangehaald wordt van een land dat drie maanden als termijn hanteert, maar men weet niet hoe die drie maanden worden ingevuld.

Een ander commissielid vraagt hoelang Belgacom de telefonische gegevens bewaart voor de gerechtelijke onderzoeken.

De heer Van Cutsem kan deze vraag niet beantwoorden. Als deze wet zo wordt goedgekeurd, zal zij net zo goed van toepassing zijn op gezinnen die toegang hebben tot het internet als op de telecommunicatie-operatoren, met inbegrip van Belgacom.

De heer Bogaert verklaart dat Belgacom te Libramont een cel heeft die belast is met de exploitatie van de door de gerechtelijke instanties opgevraagde gegevens en die op twee niveaus werkt. Alle telefooncentrales bewaren de gegevens gedurende een bepaalde periode van ongeveer zes maanden. Tijdens deze periode zijn de gegevens leesbaar en onmiddellijk beschikbaar zonder andere vorm van bewerking.

Vervolgens worden de gegevens opgeslagen en gecomprimeerd in de vorm van magneetbanden met een hoge capaciteit. Vanaf dat ogenblik wordt de exploitatie van de gegevens en de magneetbanden een langere en duurdere operatie.

Een senator vraagt of zij hun diensten kunnen factureren en ten bedrage van hoeveel. Wat omvat de vaste kostprijs, uitgenomen de opstartkost, capaciteit van personeel, machines om dat te verwerken, kan dat eventueel ook initieel gefactureerd worden ?

De minister antwoordt bevestigend. Deze kostprijs maakt deel uit van de gerechtskosten, telefoontap enz., en de minister van Justitie is verplicht om dit te betalen.

Een lid merkt op dat de operatoren het probleem van de kostprijs van de operatie aanhalen terwijl ze die kosten niet moeten dragen.

De heer Van Cutsem antwoordt dat alleen de kosten voor de verwerking van het verzoek aan Belgacom betaald worden, niet de infrastructuur die nodig is om het verzoek te beantwoorden.

De minister merkt op dat voor het verrichten van de telefoontap een antwoord moet worden gevonden

devrait être apportée via un arrêté royal. Les demandes de remboursement pour des missions accomplies doivent être payées. Les factures sont taxées soit par le juge d'instruction, soit par le procureur ou le procureur général et les services du ministère n'ont d'autres possibilités que de payer. Par un arrêté royal, on obtiendra une base uniforme qui permettrait de savoir et de planifier. Les enquêteurs doivent pouvoir recourir à tous les moyens qui sont prévus par la loi et d'un autre côté, il faut une juste rémunération des opérateurs, à qui on demande effectivement leur intervention.

M. Glas note qu'en ce qui concerne le délai, l'ISPA soutient que la seule norme est que le coût de la conservation sera en tout cas répercuté d'une manière ou d'une autre sur l'utilisateur de l'internet et que le délai doit correspondre en fait au délai nécessaire pour conduire l'instruction d'une manière normale et efficace. Il est à craindre que les ISP et, partant, l'utilisateur, seront les dindons de la farce, en raison d'un manque d'effectifs ou d'investissements à d'autres niveaux.

Ensuite, l'intervenant confirme que plusieurs ISP qui déploient leurs activités en Belgique et qui sont agréés par l'OBPT, collaborent avec la NCCU en lui transmettant des données, bien que la base de données contenant les données belges ne soit pas située en Belgique. Dans ce sens, l'adoption du texte à l'examen signifierait que plusieurs ISP agréés qui ont des points de contact seront contraints de s'organiser autrement sur le plan économique qu'ils ne le font aujourd'hui.

Une commissaire pose la question de savoir sur quelle base légale des renseignements qui ne sont pas stockés en Belgique sont transmis.

M. Glas répond que les ISP ont accepté, par le protocole d'accord, de se comporter vis-à-vis des autorités comme des citoyens responsables. Chacun a intérêt à ce que les abus soient combattus et, à cet égard, la question n'est pas de savoir s'il y a une base légale qui impose de donner suite à ces demandes.On donne volontiers suite à ces demandes indépendamment de toute base légale parce que cela fait l'objet du protocole d'accord et on en bénéficie en tant que ISP.

M. Beirens dit avoir l'impression que l'on peut stocker toutes ces données à des fins de facturation. C'est sans doute, sur cette base-là que les ISP conservent leurs données. Mais en fait, c'est leur problème.

Un intervenant fait observer à propos de la territorialité que l'on ne peut pas en arriver à une situation où une commission rogatoire est nécessaire lorsque les données sont stockées à l'étranger. L'enjeu principal est en fait la rapidité avec laquelle ces données peuvent être obtenues.

door middel van een koninklijk besluit. De verzoeken tot terugbetaling voor uitgevoerde taken moeten betaald worden. De facturen worden begroot door de onderzoeksrechter, of door de procureur of de procureur-generaal en de diensten van het ministerie hebben geen andere mogelijkheid dan te betalen. Door een koninklijk besluit krijgt men een eenvormige basis om de kostprijs beter te kennen en te plannen. De speurders moeten gebruik kunnen maken van alle wettelijk bepaalde middelen en anderzijds moeten de operatoren van wie effectief medewerking wordt gevraagd, een billijke vergoeding krijgen.

De heer Glas oppert dat, wat de termijn betreft, ISPA voorhoudt dat de enige norm is dat de bewaring hoe dan ook een kost is die op een of andere manier zal afgewenteld worden op de gebruiker van het internet en dat de termijn eigenlijk deze zou moeten zijn die men nodig heeft om op een normale, efficiënte wijze het onderzoek te verrichten. De vrees bestaat dat de ISP's maar dus ook de gebruiker het kind van de rekening zullen worden van een gebrek aan bestaffing of investering, die op andere niveaus bestaan.

Ten tweede bevestigt spreker dat er een aantal ISP's in België actief zijn, erkend door BPT, die samenwerken met het NCCU en die dus gegevens verstrekken aan het NCCU, maar waarvan de database wat die Belgische gegevens betreft, zich niet in dit land bevinden. In die zin zou het aannemen van deze tekst betekenen dat een aantal ISP's, die erkend zijn, die aansprekingspunten hebben, verplicht worden om zich economisch op een andere wijze te organiseren dan zij vandaag de dag doen.

Een commissielid stelt de vraag aan de hand van welke rechtsgrond inlichtingen die niet in België opgeslagen zijn, naar België doorgezonden worden.

De heer Glas antwoordt dat de ISP's door het protocolakkoord aanvaard hebben zich ten aanzien van de overheid te gedragen als verantwoordelijke burgers. Iedereen heeft er belang bij dat misbruiken bestreden worden en de vraag in dit verband is niet of er een rechtsgrond bestaat voor het beantwoorden van het verzoek. Men gaat graag in op deze verzoeken, los van elke rechtsgrond, omdat dit bepaald is door het protocolakkoord, en als ISP heeft men daar baat bij.

De heer Beirens heeft de indruk dat het voor facturatiedoeleinden toegelaten is om al die gegevens op te slaan. Dit vormt waarschijnlijk de basis waarop de ISP's hun gegevens bijhouden. Maar eigenlijk is dat hun zaak.

Een opmerking over die territorialiteit is dat men niet mag komen tot de situatie waarbij, indien die gegevens in het buitenland opgeslagen worden, een rogatoire opdracht noodzakelijk zou zijn. Het gaat eigenlijk over de snelheid waarmee de gegevens kunnen worden opgevraagd.

Il a déjà eu des contacts avec Interpol en ce qui concerne les grands fournisseurs d'accès tels que AOL. Lorsque l'on a besoin des données en question, on peut toujours aller les chercher en Amérique. La réponse est très simple, mais cette solution est à éviter. Il faut que les intéressés s'engagent à fournir les données en Belgique. Le plus important, c'est que l'on ne doive pas envoyer en Amérique une commission rogatoire chargée de réunir des informations sur une personne qui a établi en Belgique une connexion internet avec une autre personne qui propose ses services en Belgique.

Si quelqu'un entre en liaison en Belgique avec un fournisseur d'accès internet, ces données devraient être disponibles en Belgique.

M. Glas a le sentiment d'être sur la même longueur d'onde. Le plus important, c'est que ces données existent, qu'elles soient protégées, et qu'elles puissent être consultées rapidement et efficacement. Les gens de l'ISPA sont disposés à aller chercher eux-mêmes ces données à l'étranger. À propos des commissions rogatoires, il est clair qu'il ne s'agit plus de quelqu'un que l'on envoie; au XXIème siècle, cela se passe bien entendu on-line et on va chercher les données dans la banque de données à Luxembourg ou n'importe où ailleurs. Tout ce qu'ils demandent, c'est d'avoir le droit de stocker ces données en dehors des frontières du pays. Le texte actuel dit que la conservation doit se faire à l'intérieur des frontières du Royaume. Ils interprètent ce texte — peut-être à tort — comme signifiant que la banque de données doit, physiquement aussi, se trouver en Belgique.

Selon M. Coenraets, il est indispensable, en vue de la procédure, de disposer de dispositions claires. Ce n'est pas parce qu'une entreprise a un représentant en Belgique, qu'on peut aller chercher les données à l'étranger. Ces données sont soumises à la loi sur la vie privée du pays en question. Il n'est donc pas toujours logique que d'autres pays puissent, comme cela, sortir des données d'un dossier sans passer par l'une ou l'autre procédure, rien qu'en comptant sur la collaboration volontaire d'un fournisseur d'accès. Il en va exactement de même que pour l'identification du titulaire d'une adresse internet. Un fournisseur d'accès peut communiquer volontairement ces données, mais cela n'empêche pas que nous devrons nous adresser à un procureur pour obtenir la requête indispensable à la procédure prescrite. Il en va de même pour les données qui se trouvent à l'étranger: une base légale est nécessaire.

M. Verbeeren peut se rallier à ces propos. Si l'on prend la situation inverse, qu'il s'agisse d'un fournisseur d'accès belge conservant en Belgique les adresses de la communication de données et que celles-ci soient demandées par sa filiale située à l'étranger, le FAI belge aussi sera soumis à la réglementation belge sur la conservation et la protection des données. On

Er zijn al contacten met Interpol geweest, wat betreft de grote providers als AOL. Als men die gegevens nodig heeft, mag men ze altijd in Amerika gaan halen. Dit antwoord is heel simpel, maar dit moet worden vermeden. Men moet zich engageren om die in België af te leveren. Het belangrijkste is om niet met een rogatoire opdracht naar Amerika te moeten gaan voor iemand die in België een internetverbinding gelegd heeft naar iemand die in België zijn diensten aanbiedt.

Als een persoon in België zich verbindt met een internetprovider, dan zouden die gegevens in België moeten beschikbaar zijn.

De heer Glas heeft de indruk op dezelfde golflengte te zitten. Het belangrijkste is dat die gegevens bestaan, beschermd zijn, snel en efficiënt raadpleegbaar zijn. Zij zijn bereid zelf die gegevens te gaan halen uit het buitenland. Wat betreft de rogatoire commissies is het duidelijk dat het niet meer gaat over iemand die gestuurd wordt; dit gebeurt uiteraard in de 21e eeuw on-line, die gegevens worden uit de databank in Luxemburg of om het even waar gehaald. Zij vragen enkel het recht om die gegevens te stockeren buiten de landsgrenzen. De huidige tekst zegt nu: de bewaargevingsplicht moet worden uitgeoefend binnen de grenzen van het Rijk. Zij interpreteren deze tekst misschien ten onrechte — als een verplichting om ook fysiek het databestand in België te gaan houden.

De heer Coenraets is van oordeel dat het, met het oog op de procedure, onontbeerlijk is te beschikken over duidelijke bepalingen. Het is niet omdat er in België een vertegenwoordiger van een onderneming is, dat daarom de gegevens vanuit het buitenland gehaald kunnen worden. Die gegevens zijn onderhavig aan de wet op de privacy in dat land. Daarom is het niet altijd logisch dat uit een dossiermap andere landen zomaar gegevens kunnen halen, zonder toepassing van een of andere procedure, louter op basis van de bereidwillige medewerking van een provider. Het is net zoals met de identificatie van iemand die een internetadres bezit. Een provider kan die gegevens op een bereidwillige basis meedelen maar dat neemt daarom niet weg dat wij via een procureur moeten gaan om een vordering te bekomen die nodig is voor de noodzakelijke procedure. Hetzelfde geldt voor de gegevens die zich in het buitenland bevinden, waarvoor een wettelijke basis nodig is.

De heer Verbeeren kan hiermee instemmen. Indien men de situatie zou omdraaien en het betreft een Belgische ISP waarvan de gegevens over de datacommunicatie hier bewaard worden, en dat deze gegevens door het dochterbedrijf in het buitenland zouden opgevraagd worden, dan ook is de Belgische ISP onderworpen aan de Belgische regelgeving inzake data-

ne peut pas comme cela transférer des données sans autre formalité.

Une commissaire soulève le problème suivant. Quand il y aura des opérateurs de téléphone qui ne seront plus belges — on est dans une libre concurrence — on pourra avoir son abonnement de téléphone par un opérateur français. Comment pourra-t-on procéder à des enquêtes judiciaires? La situation semble effectivement complexe. La base territoriale est importante et le droit a été conçu de cette manière; et il est vrai que pour la régularité des preuves, on ne peut pas aller chercher à l'étranger n'importe quel élément. Ce qui nous pose problème, c'est qu'on a le sentiment qu'en Europe, chacun s'acharne avec sa petite loi à solutionner ce problème, alors que tous les opérateurs sont internationaux. On est à l'âge de la pierre dans nos lois, alors qu'on est à l'âge des satellites à l'autre niveau. La bonne voie à suivre est difficile à trouver et on a le sentiment que ceci est déjà dépassé avant même qu'on ne l'ait voté. Ceci explique la perplexité de la commission.

Le ministre n'est pas convaincu du fait qu'il faut inventer quelque chose. Il faudrait peut-être appliquer ce que l'on demande depuis bientôt 40 ans en matière d'entraide judiciaire internationale, et que l'on ait effectivement un système qui fonctionne correctement et rapidement. En ce qui concerne le problème d'accès à des données et de leur conservation, l'intervenant peut donner un exemple tout à fait frappant. Si une personne commet en Belgique une fraude fiscale et qu'elle détient un compte bancaire à l'étranger, on va devoir demander des renseignements à ce pays, relativement proche, qui nous répondra pratiquement au bout de trois ans que l'argent qui était sur le compte a été transféré 500 kilomètres plus loin. Que va faire le magistrat recevant l'information? Il va envoyer une nouvelle commission rogatoire dans ce pays, pour apprendre au bout de cinq ans que l'argent a été transféré dans un autre pays qui se trouve près de la Côte d'Azur. Et lorsqu'il aura fait le tour avec trois commissions rogatoires, il refermera son dossier parce que la prescription sera atteinte.

En ce qui concerne les données à conserver, l'intervenant est d'avis que chacun peut se rallier au fait qu'il faut conserver les éléments essentiels qui ne peuvent pas porter atteinte au respect de la vie privée. On doit pouvoir disposer de ces données et on doit pouvoir les suivre. Un délai de 12 mois est proposé, en vue de permettre aux autorités judiciaires et aux enquêteurs d'avoir la certitude que, s'ils commencent une enquête sur base de cette loi, ils pourront la terminer. L'intervenant renvoie au nouvel article 21*ter* du Code de procédure pénale (doc. Sénat, nº 2-279). Ce qui ne devrait pas pouvoir arriver ici, c'est qu'on n'ait pas la capacité d'aller le plus vite possible, le plus loin possible dans la recherche des informations.

bewaring en databescherming. Men kan niet zo maar gegevens transfereren.

Een commissielid haalt het volgende probleem aan. Wanneer er telefoonoperatoren zullen zijn die niet meer Belgisch zijn — we bevinden ons in een vrije markt — kan men zijn telefoonabonnement nemen bij een Franse operator. Hoe zal men gerechtelijke onderzoeken kunnen verrichten? De toestand lijkt inderdaad complex. De territoriale basis is belangrijk en het recht is zo opgevat: en het is waar dat men voor de regelmatigheid van de bewijsvoering niet zomaar elk gegeven in het buitenland kan gaan zoeken. Wij ondervinden het als een probleem dat iedereen in Europa blijkbaar met zijn eigen wetje hardnekkig het probleem tracht op te lossen terwijl de operatoren internationaal zijn. Met onze wetgeving zitten we nog in het steentijdperk terwijl men op een ander vlak in het tijdperk van de satellieten zit. Het is moeilijk om de juiste weg te vinden en men heeft het gevoel dat de tekst reeds achterhaald is nog voordat de wet is goedgekeurd. Dat verklaart waarom de commissie het noorden kwijt is.

De minister is er niet van overtuigd dat men iets moet uitvinden. Men moet misschien toepassen wat men gedurende weldra veertig jaar vraagt inzake internationale gerechtelijke bijstand, men moet effectief een systeem hebben dat correct en snel werkt. Wat het probleem van de toegang tot gegevens en hun bewaring betreft, kan spreker een zeer frappant voorbeeld geven. Indien een persoon zich in België schuldig maakt aan belastingfraude en een bankrekening in het buitenland bezit, zal men inlichtingen moeten vragen aan dat relatief dichtbij gelegen land, dat ons na bijna drie jaar zal antwoorden dat het geld dat op de rekening stond, 500 kilometer verder gebracht is. Wat zal de magistraat doen die de informatie ontvangt? Hij zal een nieuwe rogatoire commissie naar dat land sturen en na vijf jaar vernemen dat het geld overgebracht is naar een ander land dat dichtbij de Côte d'Azur ligt. En na drie rogatoire commissies zal hij zijn dossier sluiten omdat er verjaring is.

Wat de te bewaren gegevens betreft, is spreker van mening dat iedereen kan instemmen met de verplichting tot het bewaren van de belangrijke gegevens voor zover hiermee geen afbreuk wordt gedaan aan de persoonlijke levenssfeer. Men moet over deze gegevens kunnen beschikken en moet ze kunnen volgen. Een termijn van 12 maanden wordt voorgesteld om de gerechtelijke instanties en de speurders zekerheid te verschaffen dat ze een onderzoek dat ze op grond van deze wet starten, kunnen afwerken. Spreker verwijst naar het nieuwe artikel 21*ter* van het Wetboek van strafvordering (Stuk Senaat, nr. 2-279). Wat hier niet mag gebeuren, is dat men onvoldoende slagkracht heeft om zo snel mogelijk op te treden, om zo ver mogelijk te gaan in het speuren naar informatie.

Le texte ne semble pas dépassé, ni en ce qui concerne les incriminations, ni en ce qui concerne la coopération judiciaire. Le texte forme la base d'une coopération normale. Une commissaire avait évoqué la compatibilité entre ce projet de loi et le projet de convention du Conseil de l'Europe. Ce projet n'est toujours pas finalisé, non pas parce que le droit matériel pose problème, mais parce que le droit de la procédure pénale pose problème. Elle peut s'expliquer par l'invitation des États-Unis aux débats du Conseil de l'Europe. L'intervenant se réfère aux exemples de AOL ou Compuserve, qui conservent les données en Virginie. Et si AOL et Compuserve avaient l'audace de dire aux autorités belges: «nous vous remettons directement les données parce qu'on est bien conscient de la nécessité ou de l'importance qu'elles représentent pour vous», elles se mettraient à dos les autorités américaines. Les Américains, se rendant compte que la plupart des bases de données importantes sont conservées chez eux, n'ont pas envie d'être obligés de répondre aux demandes de coopération judiciaire internationales. Et là se situe effectivement le problème, qui ne peut pas être résolu à travers une loi, voire un traité. Il s'agit d'une question de mentalité.

Certains États, au niveau européen, sont prêts à s'engager dans une coopération avancée. Des structures ont été développées et une nouvelle convention va être ratifiée entre les 15 États membres pour permettre une plus grande efficacité en matière d'entraide judiciaire pour les écoutes téléphoniques de GSM. La communication peut être relayée par une antenne GSM qui se trouve en dehors du territoire belge, alors que la communication se fait entre deux personnes qui se trouvent sur le territoire belge. L'opérateur peut être français ou luxembourgeois. L'État français va vous répondre qu'il ne sert que d'intermédiaire. La question qui s'est posée au sein de l'Union européenne est de savoir si l'État intermédiaire, au nom de sa souveraineté, peut bloquer l'échange d'informations entre des autorités qui se trouvent sur un même territoire. La réponse a été négative. Il y a donc des structures relativement souples qui peuvent se mettre en place. Et on peut très bien imaginer qu'à l'avenir, ces mêmes structures se mettent en place au sein des 15 États membres pour s'attaquer au problème de la fraude informatique.

En ce qui concerne les incriminations, il a été évoqué en début de réunion la question de savoir si les magistrats pouvaient faire preuve d'imagination. Certains magistrats sont prêts à faire preuve d'imagination, mais il faut tenir compte de l'interprétation restrictive du droit pénal; là se trouve un peu la limite de l'imagination.

Pour ce qui est de la coopération judiciaire, l'État belge est de bonne volonté. Malheureusement, à travers un projet de loi, on ne parviendra pas à

De tekst lijkt niet achterhaald, noch wat de strafbaarstellingen, noch wat de gerechtelijke samenwerking betreft. De tekst vormt de basis voor een normale samenwerking. Een commissielid heeft vragen gesteld over de bestaanbaarheid van dit wetsontwerp en het ontwerp van verdrag van de Raad van Europa. Dat ontwerp is nog altijd niet afgewerkt, niet omdat het materiële recht problemen oproept maar omdat het strafvorderingsrecht problemen meebrengt. Een verklaring daarvoor is de uitnodiging aan de Verenigde Staten om deel te nemen aan de debatten van de Raad van Europa. Spreker verwijst naar de voorbeelden van AOL of Compuserve die de gegevens in Virginia bewaren. En indien AOL en Compuserve de moed hadden om de gegevens onmiddellijk te bezorgen aan de Belgische overheid omdat ze er zich van bewust zijn dat deze gegevens voor ons belangrijk zijn, dan zouden ze de Amerikaanse overheid tegen zich in het harnas jagen. De Amerikanen, die beseffen dat de meeste belangrijke gegegensbanken bij hen bewaard worden, hebben geen zin om gehoor te geven aan verzoeken tot internationale gerechtelijke samenwerking. En daar schuilt in de grond het probleem, dat niet door middel van een wet of zelfs door een verdrag opgelost kan worden. Het is een kwestie van mentaliteit.

Sommige Staten zijn bereid om op Europees vlak een gevorderde samenwerking aan te gaan. Er zijn structuren ontwikkeld en een nieuw verdrag tussen de 15 lidstaten zal geratificeerd worden om inzake rechtshulp nog doeltreffender te kunnen optreden voor het aftappen van GSM's. Het gesprek kan opgevangen worden door een GSM-antenne die zich buiten het Belgische grondgebied bevindt, terwijl het gevoerd wordt tussen twee personen die zich op het Belgische grondgebied bevinden. De operator kan Frans of Luxemburgs zijn. De Franse Staat zal antwoorden dat hij slechts als tussenpersoon optreedt. Binnen de Europese Unie is de vraag gerezen of de Staat die als tussenpersoon optreedt, in naam van zijn soevereiniteit de uitwisseling van gegevens kan blokkeren tussen overheden die zich op een zelfde grondgebied bevinden. Hier is een ontkennend antwoord op gegeven. Er kunnen dus relatief soepele structuren opgezet worden. En men kan zich zeer goed inbeelden dat deze zelfde structuren in de toekomst in de 15 lidstaten opgezet worden om het probleem van de computermisdaad aan te pakken.

Wat de strafbaarstellingen betreft, is bij de aanvang van de vergadering de vraag gesteld of de magistraten enige verbeelding aan de dag kunnen leggen. Sommige magistraten zijn bereid hun verbeelding te laten werken maar men moet rekening houden met de restrictieve interpretatie van het strafrecht die de verbeelding toch wel een beetje beperkt.

Wat de samenwerking tussen gerechten betreft, is de Belgische Staat van goede wil. Een wetsontwerp zal een land er echter niet zomaar van overtuigen dat

convaincre quelque pays que ce soit de changer de mentalité. C'est au niveau international que cela doit se faire. Le projet à l'examen, s'il peut être adopté, donnera peut-être une chance aux représentants du gouvernement belge lors des négociations au Conseil de l'Europe de dire: « Nous avons effectivement franchi un pas mais vous nous mettez dans l'impossibilité d'appliquer la loi. »

M. Beirens revient un instant au problème des données qui doivent être stockées. L'ISPA laisse entendre que stocker le numéro de téléphone de la personne qui entre en liaison avec le serveur de son fournisseur d'accès internet, en plus de l'identité de l'appelant, poserait problème. Or, si les services de recherche ne disposent pas de cet élément, ils se trouvent dans une position très faible. L'intervenant prend l'exemple d'un cas qui s'est plaidé la semaine passée devant le tribunal correctionnel de Bruxelles.

À un certain moment, l'intervenant constate, sur son propre PC, alors qu'il est occupé à faire une recherche sur l'internet, que quelqu'un essaie d'utiliser un « cheval de Troie » sur son PC. Ce n'était que le détecteur. L'intervenant dresse donc procès-verbal. Le magistrat du parquet fait demander les données à Planet internet, qui s'exécute. L'adresse internet en question a été utilisée à ce moment-là par cet abonné.

En plus, le numéro de téléphone à partir duquel on avait téléphoné au fournisseur d'accès était stocké également. Une perquisition a eu lieu au domicile de l'abonné en question. Il est ainsi apparu qu'il s'agissait d'une personne qui avait été piratée, donc victime d'un « hacking », par quelqu'un qui lui avait envoyé un programme contenant un « cheval de Troie ». Celui-ci s'installe sur son PC. C'est un programme qui permet aux personnes se trouvant de l'autre côté sur l'internet de pénétrer dans votre PC, de lire ce qui s'y trouve, d'effacer des fichiers, etc., ce que la personne en question avait fait.

Si les services de recherche n'avaient pas obtenu le numéro de téléphone à partir duquel la liaison avait été établie avec le fournisseur d'accès, ils n'auraient pas pu déterminer qu'il s'agissait d'un *hacker* utilisant abusivement les données de l'abonné qu'il s'était procurées au moment où il avait « hacké » sa victime. Sans ces données, les *login* ne sont pas toujours utilisables.

Au contraire, il arrive souvent dans les cas de *hacking*, que l'identité de l'appelant soit déterminante pour établir qui est l'auteur ou à quel endroit il se situait au moment de son méfait. Il peut s'agir aussi bien du numéro de téléphone que du numéro de série du modem utilisé, dans le cas des sociétés de distribution.

Il s'agit d'un élément qui va évoluer à mesure que l'on va progresser du point de vue technique. Il doit bien être possible de transmettre une identification

de mentaliteit moet veranderen. Dit dient op internationaal niveau te gebeuren. Het voorliggende ontwerp zal, indien het wordt aangenomen, de vertegenwoordigers van de Belgische regering misschien de kans geven om aan de Raad van Europa te zeggen dat wij inderdaad stappen hebben ondernomen, maar dat zij het ons onmogelijk maken om de wet toe te passen.

De heer Beirens komt nog even terug op de gegevens die moeten worden opgeslagen. ISPA doet het voorkomen alsof het opslaan van het telefoonnummer van de persoon die de verbinding legt met de server van zijn internetprovider, naast het *caller-ID*, een probleem zou zijn. Als de opsporingsdiensten dit element niet hebben, dan staan zij zeer zwak. Spreker geeft het voorbeeld van een geval dat vorige week voorgekomen is voor de correctionele rechtbank in Brussel.

Op een bepaald ogenblik stelt spreker vast op zijn eigen PC, terwijl hij bezig is met een opsporing op internet, dat iemand probeert een Trojaans paard te misbruiken op zijn PC. Het was enkel de detector. Spreker maakt aldus een proces-verbaal op. De parket-magistraat geeft een vordering af om de gegevens op te vragen bij Planet Internet, die de gegevens doorgeeft: dat internetadres is gebruikt op dat ogenblik door die abonnee.

Bijkomend was het telefoonnummer van waaruit gebeld was naar de service provider ook opgeslagen. Bij de abonnee in kwestie vond een huiszoeking plaats. Aldus bleek dat het ging om een persoon die gepirateerd was geweest, dus gehacked, door iemand die hem een programma had opgezonden met een Trojaans paard. Het Trojaans paard installeert zich op zijn PC. Dat is een programma dat toelaat aan personen die aan de andere kant op internet zitten, om op uw PC binnen te dringen, te gaan lezen wat er op uw PC staat, bestanden te wissen enz., wat de persoon in kwestie had gedaan.

Als de opsporingsdiensten het telefoonnummer waarmee de verbinding werd gelegd met de service provider, niet gekregen hadden, dan hadden zij dus niet kunnen uitmaken dat het ging over een *hacker* die misbruik maakte van de abonneegegevens die hij had gekregen op het moment dat hij zijn slachtoffer had gehackt. Zonder die gegevens zijn de logins niet altijd bruikbaar.

Integendeel, bij *hackings* komt het vaak voor dat de *caller-ID* bepalend is om uit te maken wie de dader is of waar de dader zich situeerde op het moment dat hij zijn misdrijf pleegde. Dat kan zowel het telefoonnummer zijn als voor de kabelmaatschappijen het serienummer van de modem die gebruikt wordt.

Dat is een element dat mee zal evolueren met de techniek. Men moet ergens een materiële identificatie kunnen meegeven, hetzij het telefoonnummer, hetzij

matérielle, qu'il s'agisse du numéro de téléphone ou du câblo-modem qui est utilisé pour établir la liaison.

Un sénateur fait remarquer qu'en ce qui concerne cette identification de l'appelant, certaines personnes ont un numéro privé qui n'apparaît pas. Deuxièmement, d'aucuns peuvent éventuellement débrancher ce système d'identification de l'appelant. Est-ce exact?

M. Beirens répond que la plupart des personnes n'ont pas de numéro privé, ce qui fait que 90% des lignes d'appel peuvent être enregistrées dans les *logins*. Lorsqu'il n'y a pas d'identification de l'appelant parce que celui-ci appelle d'un numéro privé, on peut introduire une demande complémentaire à la société qui gère la ligne téléphonique qui a servi à établir la communication. Si l'utilisateur est abonné à Skynet, il est possible qu'il soit passé par Belgacom pour établir sa liaison avec Skynet. On trouvera donc chez Skynet l'information selon laquelle M. X a commencé une session à tel moment et l'a interrompue à tel autre moment. On trouvera, chez Belgacom, une information selon laquelle peu avant le début de la session internet chez Skynet, la personne a établi la liaison avec le point d'accès chez Skynet à partir de tel numéro de téléphone.

Le problème que l'on rencontre en effectuant une telle enquête est lié au nombre considérable susceptible d'avoir établi une liaison au même moment, ce qui rend particulièrement difficile l'identification de la personne en question. Il s'en suit aussi que le délai devient plus long puisqu'il faut prendre contact avec Skynet. On constate que les données qui sont fournies sont insuffisantes et il faut de surcroît se rendre chez Belgacom et commencer le filtrage. Les personnes que l'on cherche figurent précisément parmi toutes celles qui ont cherché à joindre le point d'accès vers la même heure. De tels cas sont monnaie courante.

M. Van Cutsem cite deux exemples: quand Redattack a attaqué Skynet, cela a pris vingt minutes pour l'identifier, via son GSM. Pour identifier l'auteur du virus *I love you,* il a fallu trois jours.

M. Beirens note qu'il faut tout replacer dans son contexte. Les cas ne sont pas toujours des Redattack, au sujet desquels les médias diffusent tout ce qui s'est passé. Il n'y a pas que le virus *I love you*, où la terre s'arrête de tourner parce qu'on est entré dans un système par effraction.

M. Van Cutsem explique comment fonctionne l'identification. On reçoit une demande, voilà telle adresse IP (une série de numéros) a été utilisée à telle heure tel jour. On peut voir dans les bases de données quel client de Skynet à utilisé cette adresse IP à telle heure, tel jour et c'est ainsi qu'on peut identifier le client.

de kabelmodem die gebruikt wordt voor het leggen van de verbinding.

Een senator merkt op, wat die caller identification betreft, dat bepaalde mensen een privé-nummer hebben dat niet wordt weergegeven. Ten tweede, kunnen mensen eventueel die caller identification uitzetten. Klopt dat?

De heer Beirens antwoordt dat de meeste mensen geen privé-nummer hebben, waardoor 90% van de caller ID kan geregistreerd worden in de *logins*. Wanneer er geen caller ID is omdat men een privénummer heeft, kan men een bijkomende vordering doen bij de maatschappij die de verbinding gelegd heeft met de telefoonlijn. Heeft de gebruiker een Skynet-abonnement, dan kan hij Belgacom gebruikt hebben om zijn verbinding naar Skynet te leggen. Men zal dus bij Skynet vinden dat de heer X met een internetsessie gestart is op dit ogenblik en gestopt is op een ander ogenblik. Bij Belgacom gaat men vinden dat vlak voor de internetsessie gestart is bij Skynet, de persoon de verbinding gelegd heeft vanaf dat telefoonnummer naar het inbelpunt van Skynet.

Het probleem bij zulk onderzoek is dat vele mensen zich op dat moment kunnen verbinden en dan is het heel moeilijk om te identificeren over wie we hier nu eigenlijk spreken. Bijkomend wordt de termijn natuurlijk langer want men moet bij Skynet gaan. Men stelt vast dat de gegevens die toegeleverd worden onvoldoende zijn en men moet bijkomend nog eens naar Belgacom gaan en dan beginnen met de filtering. Wie van al de mensen die rond dat uur ingebeld hebben zijn juist de personen die men zoekt? Dat zijn zaken die alle dagen voorkomen.

De heer Van Cutsem geeft twee voorbeelden: toen Redattack Skynet aanviel, heeft het twintig minuten geduurd voor men hem via zijn GSM heeft geïdentificeerd. Voor de auteur van het *I love you*-virus heeft men drie dagen nodig gehad.

De heer Beirens stipt aan dat alles in de juiste context moet worden geplaatst. Het gaat niet altijd over Redattack, waarbij de media alles uitzendt wat er gebeurd is. Niet alles gaat over het *I Love you*-virus, waarbij de hele wereld stil staat omdat er in een systeem ingebroken wordt.

De heer Van Cutsem legt uit hoe de identificatie verloopt. Er komt een vraag binnen, waarbij men weet dat een bepaald IP-adres (samengesteld uit een reeks cijfers) op een bepaald uur en een bepaalde dag gebruikt is. In de gegevensbestanden kan men nagaan welke klant van Skynet dat IP-adres op dat bepaalde moment gebruikt heeft. Zo wordt de klant geïdentificeerd.

M. Olivier van Cutsem confirme qu'on peut identifier le client. Mais il circule sur internet des password et des login de Skynet qui sont disponibles dans des listes sur des sites pirates et des pirates peuvent utiliser le *login* et le password d'un des clients tout en se connectant à partir d'un numéro de téléphone qui n'est pas celui de ce client. Effectivement, si le numéro de téléphone qui est utilisé pour cette connexion ne figure pas dans les informations communiquées, on peut très bien aller perquisitionner chez quelqu'un qui n'a absolument rien a voir parce que simplement son login et son password de Skynet lui ont été dérobés à son insu.

En matière de relations contractuelles entre Skynet et son client, c'est ce dernier qui est responsable vis-à-vis de Skynet de l'utilisation de son login et de son password. On a clairement prévu que si ce login et ce password avaient été dérobés et que l'utilisateur en avait connaissance, celui-ci devait informer l'ISPA ou prendre directement les mesures nécessaires.

On a signalé qu'il existe à Libramont une cellule de Belgacom spécialisée dans les demandes des autorités judiciaires; celle-ci fournit assez rapidement le *feedback*. En cas de plaintes de clients, il suffit de comparer les listings fournis par Skynet et ceux fournis par Belgacom. S'ils ne correspondent pas, c'est qu'il y a un problème.

M. Verbeeren se rallie au point de vue de ses collègues tout en ajoutant qu'avec tous ces abonnements gratuits à internet, il est devenu quasiment impossible aux fournisseurs d'accès à internet de contrôler qui se trouve à l'autre bout de la ligne. On peut prendre un abonnement sous une identité quelconque sans que le moindre contrôle soit possible.

Un sénateur constate que les services de police souhaitent manifestement que l'on ne se limite pas à l'adresse FA, au moment où la connexion avec le point d'accès est établie ou au moment où elle cesse, bref, que l'on puisse aussi conserver des informations à propos de l'identification de l'appelant. Le projet de loi à l'examen emploie des termes très vagues — comme l'a aussi constaté le Conseil d'État — et donne le pouvoir au Roi ou au gouvernement de définir ou de formuler les données d'appel et les données d'identification comme le gouvernement l'entend. L'intervenant se demande si outre la question de l'identification de l'appelant, on pourra aller aussi loin en ce qui concerne, par exemple, l'obligation de noter quelles adresses électroniques ont été visitées ou vers lesquelles des messages ont été envoyés. Plusieurs fournisseurs d'accès internet pourraient tenir un registre des messages et l'on pourrait alors, par exemple, admettre que le gouvernement prévoie dans un arrêté d'exécution que soient aussi conservé les données des courriers, leur contenu, et éventuelle-

De heer Olivier van Cutsem bevestigt dat men de klant kan identificeren. Op het internet worden echter paswoorden en *logins* van Skynet via lijsten verspreid op hackersites, zodat de hackers de login en het paswoord van een klant kunnen gebruiken terwijl ze een verbinding tot stand brengen vanaf een telefoonnummer dat niet overeenstemt met het nummer van de klant. Indien het telefoonnummer waarmee de verbinding tot stand is gekomen niet voorkomt in de opgeslagen gegevens, kan het dus gebeuren dat men een huiszoeking gaat doen bij iemand die niets met de zaak te maken heeft, alleen omdat zijn login en zijn Skynet-paswoord hem buiten zijn medeweten ontfutseld zijn.

Wat de contractuele betrekkingen tussen Skynet en de klant betreft, is deze laatste verantwoordelijk voor het gebruik dat van zijn login en paswoord wordt gemaakt. Er is duidelijk bepaald dat wanneer de gebruiker ontdekt dat zijn login en zijn paswoord gestolen zijn, hij de ISPA op de hoogte dient te brengen of onmiddellijk de nodige maatregelen moet nemen.

Er is opgemerkt dat er in Libramont een cel van Belgacom is die gespecialiseerd is in vragen van het gerecht. Hier wordt vrij snel gereageerd. Wanneer een klant een klacht heeft, volstaat het de lijsten van Skynet te vergelijken met de lijsten van Belgacom. Indien ze niet overeenstemmen, is er een probleem.

De heer Verbeeren sluit zich aan bij de mening van zijn collega's maar wil eraan toevoegen dat met al die gratis internetabonnementen er quasi geen controle meer mogelijk is van de internetprovider over wie aan de andere kant van de lijn zit. Men kan een abonnement nemen op gelijk welke naam zonder dat er enige controle mogelijk is.

Een senator stelt vast dat de politiediensten blijkbaar verder willen gaan dan het zich beperken tot IP, inbelmoment, uitbelmoment, dus dat er ook iets moet bewaard worden in verband met calleridentification. Het voorliggende wetsontwerp — dat was ook opgemerkt door de Raad van State — gebruikt zeer vage woorden en stelt de Koning of de regering in staat om oproepgegevens en identificatiegegevens te definiëren of te formuleren zoals dat de regering schikt. Spreker vraagt zich af of men ook buiten de vraag van de caller identificatie, zo ver kan gaan naar bijvoorbeeld de verplichting om te noteren welke e-mailadressen zijn bezocht of naar welke e-mailadressen berichten zijn verstuurd. Verschillende internetproviders kunnen die e-mails bewaren en dan zou men bijvoorbeeld kunnen veronderstellen dat de regering in het uitvoeringsbesluit vastlegt dat ook e-mailgegevens, inhoud, eventueel verzending, e-mailadressen kunnen worden bijgehouden. Spreker zou dat beschouwen als een inbreuk op de privacy. In die zin acht hij het noodzakelijk om de begrippen op-

ment leur envoi ou des adresses électroniques. L'intervenant considérerait cela comme une infraction à la législation en matière de respect de la vie privée. Il estime dès lors nécessaire de définir plus précisément dans la loi les notions de données d'appel et de données d'identification.

Le ministre est ouvert à des modifications du texte. Dans le texte initial, déposé par le gouvernement, il était inscrit que les données d'appel devaient rester limitées sur avis du ministère de la Justice. Une des solutions serait peut-être que non seulement le délai soit limité sur avis de la Commission de la vie privée, mais aussi les données d'appel.

Une commissaire pose la question de savoir si d'autres pays pourraient reprocher la Belgique de ne pas avoir de législation pour ne pas accepter le principe de la double incrimination exigé pour pouvoir cooperer et échanger des données. Est-ce que l'activité d'une cellule bien représentée en Belgique est limitée au niveau international parce que nous n'avons pas de législation de base et que, de ce fait, les pays tiers bloquent l'entraide et la coopération judiciaire au niveau du principe de double incrimination ?

Le ministre répond, qu'en ce qui concerne l'entraide, il est vrai qu'on pourrait éventuellement compter sur l'imagination des magistrats, puisqu'on parle simplement d'une double incrimination *in abstracto* dans le domaine de l'entraide sauf que l'on revient malgré tout à la double incrimination *in concreto*, lorsqu'on parle de perquisition. Il est vrai que si nous n'avons pas ces mécanismes de prévention, nous ne serons pas à même de résoudre les problèmes qui se poseront. C'est un peu une entraide à double vitesse mais elle se justifie par le fait que l'on parle effectivement d'entraide aboutissant à des perquisitions. La restriction du droit pénal est d'application dans ce cas et il faut donc une mesure bien précise.

M. Coenraets note qu'en ce qui concerne la condition de double incrimination, le projet prévoit que si un État adresse une requête à un autre État en vue de la conservation de données, il faut y donner suite sans hésiter dans un délai minimum de quarante jours sans que la condition de double incrimination doive être remplie. Cette condition ne commence à jouer qu'à partir du moment où on a introduit une requête effective de publication ou de transmission réelle des données.

E. Suite de la discussion (après les auditions)

Une commissaire rappelle que la plate-forme des associations a manifesté une vive inquiétude sur la question du délai.

roepgegevens en identificatiegegevens nauwlettender te formuleren in de wet.

De minister staat open voor wijzigingen in de tekst. In de oorspronkelijke tekst, ingediend door de regering, stond dat de oproepgegevens moeten beperkt blijven op advies van het ministerie van Justitie. Een van de oplossingen is misschien dat niet alleen de termijn beperkt is na advies van de commissie persoonlijke levenssfeer maar tevens de oproepgegevens.

Een commissielid vraagt of andere landen België kunnen verwijten dat hier geen wetgeving bestaat, zodat zij kunnen weigeren om samen te werken en gegevens uit te wisselen op basis van het principe van de dubbele strafbaarstelling. Is de activiteit van een in België goed vertegenwoordigde cel beperkt tot het internationaal niveau omdat wij geen basiswetgeving hebben en worden de internationale rechtshulp en de gerechtelijke samenwerking door andere landen geblokkeerd vanwege het principe van de dubbele strafbaarstelling ?

De minister antwoordt dat men, wat de internationale rechtshulp betreft, misschien kan rekenen op de verbeelding van de magistraten, aangezien er op het vlak van die rechtshulp alleen sprake is van een dubbele strafbaarstelling *in abstracto*. Bij een huiszoeking komt men echter al gauw weer bij de dubbele strafbaarstelling *in concreto* terecht. Zonder preventieve maatregelen zijn wij niet in staat het hoofd te bieden aan alle problemen die kunnen rijzen. Het gaat dus om internationale rechtshulp met twee snelheden, die echter gerechtvaardigd wordt door het feit dat er inderdaad sprake is van rechtshulp die kan leiden tot een huiszoeking. De beperking in het strafrecht is in dit geval van toepassing en er is dus wel een precieze maatregel nodig.

De heer Coenraets stipt aan dat, in verband met de voorwaarde van de dubbele strafbaarstelling, het ontwerp stelt dat als een Staat een verzoek richt tot een andere Staat tot bewaring van gegevens, er onmiddellijk op ingegaan moet worden met een minimumtermijn van veertig dagen zonder dat er moet voldaan zijn aan de dubbele strafbaarstelling. Die voorwaarde begint pas te spelen vanaf het moment dat er een effectief verzoek is tot bekendmaking van de gegevens of tot het effectief overdragen ervan.

E. Vervolg van de bespreking (na de hoorzittingen)

Een commissielid herinnert eraan dat de verenigingen ongerust zijn over de termijn.

Il faut trouver un délai raisonnable, qui permette à la gendarmerie et à la police judiciaire de faire leur travail.

Il est vrai que le stockage des informations peut avoir un coût, mais cet argument ne paraît pas décisif.

Les éléments de droit comparé apportés par les auditions sont intéressants.

L'intervenante se demande, à ce sujet, si le délai de trois mois qui a été évoqué est inscrit dans les textes législatifs, ou s'il s'agit d'un délai que les opérateurs utilisent dans leur pratique.

Mme Nyssens renvoie à l'amendement qu'elle a déposé, et qui propose de fixer un délai maximum, plutôt qu'un délai minimum (amendement nº 1, doc. Sénat, nº 2-392/2 — *cf. infra*, discussion des articles).

À la Chambre, on avait opté pour une délégation au Roi, en ce qui concerne la fixation du délai, sans doute pour tenir compte de l'évolution des technologies, qui devrait permettre aux parquets de travailler de plus en plus rapidement.

Une concertation avec le secteur est nécessaire, de même que l'avis de la Commission pour la protection de la vie privée.

L'intervenante a noté, avec un certain étonnement que, selon les personnes entendues, le libellé actuel des incriminations leur permettrait de faire leur travail, contrairement à la critique exprimée dans un récent article paru dans *le Vif-l'Express,* selon lequel ces incriminations étaient formulées de façon trop vague et trop large.

Le ministre précise que, vérification faite auprès du service des frais de justice, la gendarmerie a, voici deux ans, attiré l'attention des magistrats et du département de la Justice sur le montant des facturations de Belgacom pour les recherches effectuées.

On avait demandé à Belgacom d'identifier deux numéros de téléphone.

La première identification, réalisée six mois environ après les faits, a donné lieu à une facture de l'ordre de 40 000 francs. La seconde identification, demandant une recherche beaucoup plus large, pour un plus grand nombre de numéros, et pour des faits beaucoup plus anciens, a donné lieu à une facture de 10 000 francs. Cela démontre un certain arbitraire dans la taxation des frais.

Par le biais de l'arrêté royal en préparation, les choses devraient être fixées.

Une concertation doit permettre de définir le montant que les opérateurs pourront réclamer et qui couvrira tous les frais exposés.

Il est clair qu'à terme, chaque fois qu'un magistrat demandera un renseignement, le ministère de la Justice paiera les frais.

Er moet een redelijke termijn worden gevonden die de rijkswacht en de gerechtelijke politie toestaat om hun werk te doen.

Het bewaren van de gegevens brengt uiteraard kosten mee maar dat lijkt geen doorslaggevend probleem te zijn.

Tijdens de hoorzittingen zijn interessante elementen van rechtsvergelijking naar voren gebracht.

Spreker vraagt zich af of de genoemde termijn van drie maanden in wetteksten wordt vermeld of daarentegen door de operatoren in de praktijk wordt gebruikt.

Mevrouw Nyssens verwijst naar haar amendement dat een maximum- veeleer dan een minimumtermijn wil vaststellen (amendement nr. 1, Stuk Senaat, nr. 2-392/2 — zie *infra* , bespreking van de artikelen).

De Kamer heeft het vaststellen van de termijn aan de Koning overgelaten wellicht om rekening te kunnen houden met de nieuwe technologieën waardoor de parketten sneller zullen kunnen werken.

Overleg met de sector is nodig, alsook het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Spreekster heeft met een zekere verbazing opgemerkt dat de gehoorde personen vinden dat de huidige formulering van de strafbaarstellingen hun werk mogelijk maakt, in tegenstelling tot de in een recent artikel in *le Vif-l'Express* geuite kritiek dat de strafbaarstellingen te vaag en te ruim geformuleerd waren.

De minister verklaart dat de rijkswacht twee jaar geleden haar licht heeft opgestoken bij de dienst gerechtskosten, en vervolgens de magistraten en het departement Justitie heeft gewezen op de bedragen die Belgacom vraagt voor haar opsporingen.

Men had Belgacom gevraagd twee telefoonnummers te identificeren.

De eerste identificatie is verricht zes maanden na de feiten en koste ongeveer 40 000 frank. De tweede, waarvoor meer onderzoek nodig was met betrekking tot een groter aantal nummers en veel oudere feiten, koste 10 000 frank. Dat bewijst dat de kosten op willekeurige manier worden geschat.

Het koninklijk besluit dat momenteel wordt voorbereid, zal orde op zaken moeten stellen.

Via overleg moet het bedrag worden vastgesteld dat de operatoren mogen vragen en dat alle kosten moet dekken.

Op termijn zal het ministerie van Justitie steeds de kosten betalen als een magistraat een inlichting vraagt.

Une commissaire déclare que la conservation des données la préoccupe surtout sous l'angle de la protection de la vie privée. Il ne convient pas que cette conservation puisse etre effectuée sans limite dans le temps.

L'intervenante se réfère à la toute récente affaire des fichiers d'élèves exigés par un juge d'instruction en Communauté française.

En outre, le délai doit faire l'objet d'une harmonisation au niveau européen, puisqu'on se trouve dans le cadre d'une libéralisation des opérateurs.

On connaîtra prochainement l'avis de la Commission européenne sur les dispositions du projet.

L'intervenante pourrait éventuellement se rallier à l'amendement déposé par Mme Nyssens, si le délai maximum de douze mois qu'il propose est dans la norme européenne.

En effet, la solution reprise dans le projet initial et consistant en une délégation pure et simple au Roi, lui paraît dangereuse au regard de la protection de la vie privée.

L'intervenante espère aussi que, dans le cadre de la nouvelle police, on n'aura pas plusieurs services compétents en la matière, et que la cellule CCU disposera d'un cadre suffisant.

Cette cellule semble chargée de plusieurs tâches, à savoir, d'une part, aider les magistrats, lors des enquêtes, à décoder les informations, par exemple lorsqu'on saisit un disque dur, et, d'autre part, surveiller le réseau, notamment en matière de pornographie enfantine.

À cet égard, il faudrait trouver une méthode policière mais aussi citoyenne d'autoréguler le contenu du réseau.

Enfin, si cette cellule est amenée à travailler sur les nouvelles incriminations, cela lui demandera beaucoup plus de travail, et des spécialistes seront nécessaires. Dispose-t-on de suffisamment de moyens en la matière ?

La collaboration des opérateurs doit être encouragée et poursuivie. Il ne faudrait pas que la loi nouvelle ait un effet négatif sur ce point.

En ce qui concerne les incriminations reprises dans le projet, l'intervenante trouve qu'elles sont décrites de façon extrêmement détaillée.

Les auditions ont permis de mieux comprendre la nature et le motif de certaines de ces incriminations.

Cependant, il n'est pas évident que chaque disposition réponde au souci de poursuivre la criminalité informatique dans ce qu'elle a de spécifique.

Il serait souhaitable que l'application de la loi fasse l'objet d'une évaluation, par exemple dans un an,

Een commissielid verklaart dat het bewaren van gegevens haar vooral zorgen baart met betrekking tot de bescherming van de persoonlijke levenssfeer. In elk geval moet de bewaring beperkt zijn in de tijd.

Spreekster verwijst naar de recente zaak van de leerlingenbestanden die een onderzoeksrechter in de Franse Gemeenschap had opgevraagd.

De termijn moet bovendien op Europees niveau worden geharmoniseerd aangezien de liberalisering van de sector van de operatoren volop aan de gang is.

De Europese Commissie zal eerlang een advies geven over de ontworpen bepalingen.

Spreekster kan het eventueel eens zijn met het amendement van mevrouw Nyssens als de maximumtermijn van twaalf maanden die zij voorstelt, overeenstemt met de Europese norm.

De oplossing van het oorspronkelijke ontwerp die de vaststelling van de termijn overlaat aan de Koning, lijkt haar gevaren in te houden voor de bescherming van de persoonlijke levenssfeer.

Spreekster hoopt dat met de nieuwe structuur van de politiediensten niet meerdere diensten bevoegd zullen zijn voor deze materie en dat de CCU-cel voldoende middelen zal krijgen.

Deze cel moet immers verschillende taken uitvoeren, namelijk enerzijds de magistraten helpen om gegevens te decoderen wanneer zij bijvoorbeeld een harde schijf in beslag nemen en anderzijds controle uitoefenen op het net, met name inzake kinderporno.

Op dat vlak zouden de politiediensten maar ook de burgers een methode moeten vinden om de inhoud van het net controleren.

Als deze cel met nieuwe strafbaarstellingen moet werken, zal dat meer werk meebrengen en moeten er specialisten worden ingeschakeld. Beschikt men over de nodige middelen ?

De medewerking van de operatoren moet aangemoedigd en nagestreefd worden. De nieuwe wet mag op dit vlak geen negatieve gevolgen hebben.

Spreekster vindt dat de strafbaarstellingen uit het ontwerp zeer gedetailleerd zijn beschreven.

Dankzij de hoorzittingen zijn de aard en het motief van bepaalde strafbaarstellingen duidelijker geworden.

Toch is het niet zeker dat alle bepalingen bijdragen tot de vervolging van de informaticacriminaliteit in haar specifieke vormen.

De toepassing van de wet moet geëvalueerd worden, bijvoorbeeld over een jaar. Daarbij moet met

notamment quant à son efficacité, et par rapport à ce qui se fait dans d'autres pays.

Un commissaire renvoie, en ce qui concerne la protection de la vie privée, à l'article 7, § 4, qui prévoit que le procureur du Roi utilise tous les moyens techniques appropriés pour garantir l'intégrité et la confidentialité des données.

À propos de l'article 6, § 2, 3º, l'intervenant estime que la sanction prévue est excessive lorsque le dommage a été causé de façon non intentionnelle.

Un sénateur se rallie aux observations des précédents intervenants au sujet des auditions. Il estime qu'il incombe au législateur de fixer un délai maximum de conservation des données en vue de protéger la vie privée.

La délégation au Roi, d'ailleurs critiquée par le Conseil d'État, ne lui paraît pas être une bonne solution. L'amendement de Mme Nyssens va dans la bonne direction.

Le délai doit être fixé de façon réaliste, en tenant compte des problèmes de terrain et de la situation dans les autres pays.

L'intervenant se dit également frappé par les conditions dans lesquelles les services compétents doivent travailler: cadre insuffisant, impossibilité d'obtenir une carte Visa (parce qu'un montant de 600 ou 700 francs est difficile à comptabiliser, et parce qu'il faut s'adresser aux autorités hiérarchiques les plus élevées, qui ont d'autres priorités).

Il serait donc utile d'attirer l'attention des ministres de la Justice et de l'Intérieur sur l'importance de rechercher les infractions sur internet.

En ce qui concerne l'audition de l'ISPA, l'intervenant estime que la plupart des observations formulées peuvent être rencontrées, au moins partiellement.

Pour le surplus, l'intervenant attend l'avis de la Commission européenne, qui appréciera la conformité du projet avec les règles du marché intérieur. Cet avis est attendu pour le 11 juillet. Jusqu'à cette date, le vote du projet doit être suspendu. Il n'est donc pas exclu que ce vote ne puisse intervenir qu'après les vacances.

Quant aux nouvelles incriminations prévues, il en est une qui a particulièrement retenu l'attention de l'intervenant, à savoir le «hacking» (article 6 — nouvel article 550*bis*).

Il s'est informé auprès de certaines organisations et sociétés qui s'occupent de la sécurité sur internet, et notamment Ubizen.

Dans un rapport annuel, celle-ci publie un index reprenant une série de termes, où l'on trouve la définition suivante des notions «hacker» et «cracker».

Hacker: *the accepted meaning of the term hacker is a person who has expertise in the area of computer*

name gelet worden op haar efficiëntie en vergelijkingen worden gemaakt met andere landen.

Een commissielid verwijst voor de bescherming van de persoonlijke levenssfeer naar artikel 7, § 4, dat bepaalt dat de procureur des Konings alle passende technische middelen aanwendt om de integriteit en de vertrouwelijkheid van gegevens te waarborgen.

Spreekster vindt de straf waarin artikel 6, § 2, 3º, voorziet te streng wanneer de schade onopzettelijk is veroorzaakt.

Een senator sluit zich aan bij de opmerkingen van de vorige sprekers over de hoorzittingen. Hij vindt dat de wetgever de maximumtermijn moet vaststellen voor de bewaring van de gegevens teneinde de persoonlijke levenssfeer te beschermen.

De bevoegdheidsoverdracht aan de Koning, die de Raad van State trouwens bekritiseert, lijkt hem geen goede oplossing. Het amendement van mevrouw Nyssens gaat in de goede richting.

Er moet een realistische termijn worden vastgesteld waarbij rekening wordt gehouden met de praktische problemen en de situatie in andere landen.

Spreker is ook getroffen door de omstandigheden waarin de bevoegde diensten moeten werken: onvoldoende personeel, geen mogelijkheid om een Visakaart te krijgen (omdat een bedrag van 600 of 700 frank moeilijk in de boekhouding te verwerken is en omdat de hoogste instanties, die hun toestemming moeten geven, andere prioriteiten hebben).

Daarom moeten de ministers van Justitie en Binnenlandse Zaken gewezen worden op het belang van het opsporen van misdrijven op het internet.

Wat de hoorzitting van de ISPA betreft, meent spreker dat met de meeste opmerkingen althans gedeeltelijk rekening kan worden gehouden.

Voor het overige wacht spreker op het advies van de Europese Commissie die zal nagaan of het ontwerp overeenstemt met de regels van de interne markt. Dit advies wordt verwacht tegen 11 juli. Tot die datum kan niet over het wetsontwerp worden gestemd. Het is dus niet uitgesloten dat het pas na het reces zal gebeuren.

Bij de nieuwe strafbaarstellingen is het vooral de «hacking» (artikel 6 — nieuw artikel 550*bis*) die de aandacht van de spreker heeft getrokken.

Hij heeft zijn licht opgestoken bij een aantal organisaties en bedrijven die zich met de veiligheid op het internet bezighouden en met name bij Ubizen.

Ubizen publiceert in een jaarverslag een index van een aantal termen waaronder de volgende definitie van «hacker» en «cracker».

Hacker: *the accepted meaning of the term hacker is a person who has expertise in the area of computer*

operating systems and/ or networking. Hackers enjoy digging into the subtleties of how the operating system and the network software interact, frequently developing methods of expanding the capabilities of the system. Often hackers can help system administrators by finding security loopholes and alerting them. A hacker becomes a cracker when they cross a fine ethical line and use their talents in an illegal or unprofessional manner.

Cracker: *in the internet community a cracker is a person who maliciously attempts to break into other peoples computer systems. Once a cracker breaks into a system they waste valuable resource dollars, especially if the user who's account they break into pays for connection time. Once in, a cracker typically arranges back doors and other loopholes in the system. Even worse, crackers can alter or erase files, cancel programs or even crash the system*.

Il en résulte que le terme *hacker* a une connotation positive : il s'agit de celui qui, à la demande ou avec l'accord d'une entreprise, recherche les lacunes dans un système, les signale au *webmaster*, et propose éventuellement une solution.

Il n'y a donc aucune intention frauduleuse dans le chef du *hacker*, selon cette acceptation du terme.

Or, il est frappant de constater que, pour toutes les incriminations prevues par le projet, à l'exception du *hacking*, on exige l'intention frauduleuse, le but de nuire ou l'enrichissement personnel.

Pour le hacking, l'intention frauduleuse n'est qu'une circonstance aggravante (article 550, § 1er, alinéa 2).

L'intervenant se demande, au regard des définitions reprises ci-dessus, si le projet ne va pas trop loin sur ce point.

À titre d'exemple, Distrigaz dispose d'un website (www.distrigas.be), développé en son temps sur base du programme Frontpage de Microsoft, permettant notamment à des amateurs de développer de façon autonome leur propre website. Cela suppose que l'on donne un code de sécurité à celui-ci. Distrigaz a oublié d'introduire un tel code. Des tiers ont découvert cela de façon fortuite, après avoir pénétré dans le site de Distrigaz, et l'ont immédiatement signalé au *webmaster*, qui a réparé cette erreur.

Selon le § 1er, alinéa 2, de l'article 550*bis* en projet, ces tiers sont punissables, et ont tout intérêt à ne rien dire. Cette disposition est donc contreproductive.

Il faut punir ceux qui utilisent l'instrument informatique de façon abusive, et non ceux qui l'utilisent dans une intention positive. C'est pourquoi l'intervenant prépare un amendement à l'article 6 du projet.

operating systems and/ or networking. Hackers enjoy digging into the subtleties of how the operating system and the network software interact, frequently developing methods of expanding the capabilities of the system. Often hackers can help system administrators by finding security loopholes and alerting them. A hacker becomes a cracker when they cross a fine ethical line and use their talents in an illegal or unprofessional manner.

Cracker: *in the internet community a cracker is a person who maliciously attempts to break into other peoples computer systems. Once a cracker breaks into a system they waste valuable resource dollars, especially if the user who's account they break into pays for connection time. Once in, a cracker typically arranges back doors and other loopholes in the system. Even worse, crackers can alter or erase files, cancel programs or even crash the system*.

Hieruit volgt dat het woord *hacker* een positieve connotatie heeft : het gaat om iemand die op verzoek of met instemming van het bedrijf de leemten in een systeem opspoort, ze aan de *webmaster* meedeelt en eventueel een oplossing voorstelt.

In die betekenis van het woord is er bij een *hacker* dus geen sprake van bedrieglijk opzet.

Opmerkelijk is dat voor alle strafbaarstellingen waarin het ontwerp voorziet, bedrieglijk opzet, de bedoeling om te schaden of persoonlijke verrijking vereist is, behalve voor *hacking*.

Voor *hacking* is bedrieglijk opzet slechts een verzwarende omstandigheid (artikel 550, § 1, tweede lid).

Spreker vraagt zich af of, in het licht van de hierboven vermelde definities, het ontwerp niet te ver gaat op dit punt.

Distrigas heeft bijvoorbeeld een website (www.distrigas.be) die indertijd op basis van het Frontpage-programma van Microsoft ontwikkeld werd, een programma dat amateurs de mogelijkheid geeft om op autonome wijze een eigen website te ontwerpen. Dit veronderstelt dat er ook een veiligheidscode aan die website gegeven wordt. Dat heeft Distrigas vergeten. Derden hebben dit toevallig ontdekt nadat ze waren binnengedrongen op de Distrigas-site en hebben onmiddellijk de *webmaster* op de hoogte gebracht, die de vergissing heeft rechtgezet.

Volgens § 1, tweede lid, van artikel 550*bis* van het ontwerp zijn die derden strafbaar en hebben ze er alle belang bij niets te zeggen. Die bepaling is dus contraproductief.

Degenen die met verkeerde bedoelingen een systeem binnendringen, moeten worden gestraft en niet degenen die het met positieve bedoeling gebruiken. Daarom bereidt spreker een amendement voor op artikel 6 van het ontwerp.

Une commissaire déclare, au sujet des auditions, que deux points de vue s'en dégageaient effectivement, mais que l'ISPA ne l'a pas convaincue du bienfondé de sa position.

L'intervenante estime qu'il ne faut pas se focaliser sur tel ou tel délai, mais utiliser comme seul critère le juste équilibre entre les nécessités de l'enquête et la protection de la vie privée.

Les services judiciaires qui ont été entendus sont ceux qui seront amenés à appliquer la loi. Il faut donc tenir compte de leur point de vue, selon lequel un délai minimum de six mois n'est pas praticable.

Le projet prévoit que le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, les modalités et les moyens utilisés pour garantir l'intégrité et la confidentialité des données.

L'intervenante demande si la loi sur la protection de la vie privée ne s'applique pas automatiquement à la conservation de données de nature personnelle, et si cela ne doit pas être mentionné explicitement à titre de garantie.

La lutte contre la criminalité informatique doit très certainement faire l'objet d'une harmonisation au niveau européen. Mais cette considération ne doit pas empêcher la Belgique d'adopter le plus vite possible une législation nationale en la matière.

Une autre commissaire se rallie à l'opinion des précédents intervenants, en ce qui concerne les frais dont les fournisseurs d'accès font état.

Par contre, il faut avoir égard, d'une part, à la situation des pays qui nous entourent, et, d'autre part, à la protection de la vie privée.

L'intervenante est favorable à la fixation d'un délai maximum comme proposé par l'amendement de Mme Nyssens, solution qui est compatible avec l'avis rendu à la Chambre par le président de la Commission de la protection de la vie privée (doc. Chambre, nº 50-213, pp. 29 et suivantes).

L'intervenante est sensible à l'argument de l'ISPA, selon lequel l'obligation de conserver les données sur le territoire est fort lourde dans le cadre d'un marché unique évoluant vers une libéralisation, notamment, des télécommunications.

Cela démontre combien il est important que la coopération en matière pénale s'accroisse au sein de l'Union européenne.

À cette obligation de conservation sur le territoire, l'ISPA oppose son engagement à créer une antenne

Een commissielid verklaart over de hoorzittingen dat er zich duidelijk twee standpunten hebben afgetekend, maar dat de ISPA haar niet heeft kunnen overtuigen van de gegrondheid van haar standpunt.

Spreekster meent dat men zich niet blind mag staren op een termijn maar dat het juiste evenwicht tussen de vereisten van het onderzoek en de bescherming van de persoonlijke levenssfeer het enige te hanteren criterium moet zijn.

De gerechtelijke diensten die gehoord zijn, zijn de diensten die de wet zullen moeten toepassen. Men moet dus rekening houden met hun standpunt, namelijk dat de minimumtermijn van zes maanden in de praktijk niet haalbaar is.

Het ontwerp bepaalt dat de Koning, nadat hij het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer heeft ingewonnen, de nadere middelen bepaalt die gebruikt worden om de integriteit en de vertrouwelijkheid van de gegevens te waarborgen.

Spreekster vraagt zich af of de wet op de bescherming van de persoonlijke levenssfeer niet automatisch van toepassing is op de bewaring van gegevens van persoonlijke aard en of zulks niet uitdrukkelijk moet worden vermeld bij wijze van waarborg.

De strijd tegen de cybercriminaliteit moet op Europees niveau geharmoniseerd worden. Doch die overweging mag België niet verhinderen zo snel mogelijk een eigen wet goed te keuren.

Een ander commissielid is het eens met de vorige sprekers wat betreft de kosten waarop de internetproviders gewezen hebben.

Men moet, enerzijds, oog hebben voor de toestand in de landen die ons omringen en, anderzijds, voor de bescherming van de persoonlijke levenssfeer.

Spreekster pleit voor het vastleggen van een maximumtermijn zoals voorgesteld in het amendement van mevrouw Nyssens. Die oplossing is in overeenstemming met het advies dat door de voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer aan de Kamer is uitgebracht (Stuk Kamer, nr. 50-213, blz. 29 en volgende).

Spreekster heeft begrip voor het argument van de ISPA volgens hetwelk de verplichting om de gegevens op het grondgebied te bewaren zeer zwaar is in een eengemaakte markt die verder geliberaliseerd wordt, in het bijzonder wat de telecommunicatiesector betreft.

Dit toont aan hoe belangrijk een betere samenwerking in strafzaken binnen de Europese Unie wel is.

De ISPA plaatst tegenover de verplichting om de gegevens op het grondgebied te bewaren, een toezeg-

sur place, et à répondre à toute demande des autorités judiciaires.

D'autre part, les services judiciaires compétents soulignent la lourdeur et la longueur des procédures de commission rogatoire.

Comment concilier tout cela et le traduire en termes législatifs ?

Un membre exprime son inquiétude par rapport au piratage effectué par des jeunes pour un usage éducatif privé. Ne pourrait-on, pour ce type d'actes, prévoir des peines moins sévères ?

Un commissaire se réfère à l'article 9, insérant un article 88*quater*, dont le § 1er permet à un juge d'instruction de réquisitionner une personne en vue de fournir des informations sur un système informatique, ou d'y accéder, sur base d'une simple présomption que cette personne connaît le système en question.

Quant au § 3 du même article, il prévoit une sanction pénale pour la personne qui, réquisitionnée de la sorte, refuserait sa collaboration.

L'intervenant s'interroge sur l'opportunité d'une telle sanction, car il ne voit pas comment distinguer, en pratique, celui qui fait preuve de mauvaise volonté de celui qui n'a réellement pas les connaissances nécessaires.

De plus, les personnes réquisitionnées ne sont pas assermentées, ni liées par un quelconque contrat avec les autorités judiciaires. On peut dès lors s'interroger, dans ces conditions, sur la fiabilité du tri d'informations qu'elles effectuent.

Le ministre déclare que, lorsque le projet de loi a été déposé à la Chambre, le gouvernement n'avait pas de réponse préétablie en ce qui concerne l'accessibilité des données.

Un amendement a été déposé à la Chambre et a été adopté.

Mme Nyssens dépose aujourd'hui un autre amendement, auquel le gouvernement pourrait se rallier, puisqu'il faut trouver un équilibre en la matière. Un délai maximum de 12 mois paraît praticable, et devrait permettre à chacun d'assumer ses responsabilités.

Il a été dit que, dans certains États, le délai était de 3 mois. Une précision s'impose à ce sujet. Lorsqu'on parle d'un délai de 3 mois dans ce contexte, c'est en relation avec la protection de la vie privée, car tout organisme privé ne peut pas conserver des données au-delà d'un certain délai, ni être gestionnaire d'un fichier qu'il pourrait utiliser à d'autres fins.

Dans le projet, on parle de conservation de données, dans l'éventualité d'une utilisation à des fins judiciaires.

ging om ter plaatse een steunpunt op te richten en elk verzoek van de gerechtelijke autoriteiten te beantwoorden.

De bevoegde gerechtelijke diensten wijzen er anderzijds op dat de rogatoire commissie een bijzonder omslachtige procedure is, die veel tijd vergt.

Hoe kan men met al die uiteenlopende overwegingen in één wet rekening houden ?

Een lid verklaart ongerust te zijn over het kraken van computers door jongeren voor educatieve privédoeleinden. Zou men voor dit soort handelingen geen minder strenge straffen kunnen bepalen ?

Een commissielid verwijst naar artikel 9 dat een artikel 88*quater* invoegt, waarvan § 1 de onderzoeksrechter machtigt bepaalde personen te bevelen inlichtingen te verlenen over een computersysteem of over de wijze om er toegang toe te verkrijgen wanneer hij vermoedt dat die personen het betrokken systeem kennen.

Paragraaf 3 van hetzelfde artikel voorziet in een straf voor de persoon die weigert de aldus gevorderde medewerking te verlenen.

Spreker heeft vragen over de wenselijkheid van een dergelijke straf want hij ziet niet goed in hoe men in de praktijk degene die blijk geeft van slechte wil, moet onderscheiden van degene die werkelijk niet de vereiste kennis heeft.

Daarenboven zijn de gevorderde personen niet beëdigd, noch door enige overeenkomst met de gerechtelijke autoriteiten gebonden. In die omstandigheden kan men zich dus afvragen hoe betrouwbaar de inlichtingen zijn die zij meedelen.

De minister verklaart dat, bij de indiening van het wetsontwerp in de Kamer, de regering geen vooraf vastgesteld antwoord had op de vraag in verband met de toegankelijkheid van de gegevens.

Er is in de Kamer een amendement ingediend dat is aangenomen.

Mevrouw Nyssens dient vandaag een ander amendement in waarmee de regering het eens kan zijn aangezien terzake naar een evenwicht moet worden gezocht. Een maximumtermijn van 12 maanden lijkt werkbaar en zou iedereen in staat moeten stellen zijn verantwoordelijkheid te nemen.

Er is gezegd dat de bewaartermijn in sommige landen drie maanden bedraagt. Dit behoeft enige verduidelijking. De termijn van drie maanden moet in verband gebracht worden met de bescherming van de persoonlijke levenssfeer want een privé-instelling mag de gegevens niet bewaren nadat een bepaalde termijn verstreken is, noch een bestand beheren dat zij voor andere doeleinden zou kunnen gebruiken.

In het ontwerp heeft men het over gegevensbewaring voor eventueel gebruik door het gerecht.

Ainsi, en Allemagne, il existe pour les opérateurs un délai de conservation de 3 mois à des fins privées. Mais il semble qu'en pratique, le délai de 90 jours soit largement dépassé, et que les opérateurs tiennent ces données à disposition des autorités policières ou judiciaires pendant un délai plus long, non autrement précisé.

La situation est analogue aux Pays-Bas. Au Danemark, le délai de 3 mois existe dans le cadre de la protection de la vie privée, mais on envisage de le porter à un an.

En ce qui concerne l'article 7, et le pouvoir du procureur du Roi à l'égard de certains fichiers, il faut être attentif à la notion de « fichier ».

Il y a des bases de données reconnues et agréées par la Commission pour la protection de la vie privée. La loi sur la protection de la vie privée s'y applique, avec les obligations et garanties que cela suppose. Ce n'est pas là que des problèmes pourraient surgir.

Par contre, il pourrait se faire que, par l'usage d'internet, des personnes créent des fichiers qui ne rencontrent pas tous les éléments prévus par la loi sur la protection de la vie privée.

Dans ces cas, le procureur du Roi et le juge d'instruction doivent pouvoir saisir ces fichiers litigieux, susceptibles de contenir la preuve d'infractions.

Certains s'étonnent des précautions que doivent prendre les officiers de police judiciaire ou les magistrats lorsqu'ils saisissent ce type de données. Or, cette saisie devra se faire sur disquette. La question avait déjà été posée à la Chambre de savoir si ces disquettes seraient conservées, de la même façon que tous les autres objets saisis, dans les greffes correctionnels. Il incombe effectivement aux autorités judiciaires de prendre les mesures nécessaires pour que la conservation de ces données informatiques puisse se faire dans des conditions optimales, qui ne perturbent ni les droits de l'auteur ou du préjudicié, auquel on restituera le matériel, ni le déroulement de l'action publique.

Une autre question concernait la nécessité de la création d'un organe central au niveau de la police fédérale.

L'ISPA voulait appuyer l'idée de faire de la NCCU l'organe central en question. Mais le ministre de la Justice n'est pas maître de la réforme des polices.

La NCCU et le service du BCR de la gendarmerie se retrouveront dans la police fédérale, qui comportera une direction de la criminalité informatique. Mais aussi longtemps que la réforme des polices n'est pas

In Duitsland is er voor de operatoren bijvoorbeeld een bewaringstermijn van 3 maanden voor privédoeleinden. In de praktijk wordt de termijn van 90 dagen echter ruim overschreden en stellen de operatoren deze gegevens ter beschikking van de politie of het gerecht gedurende een langere, niet nader bepaalde termijn.

In Nederland is de situatie dezelfde. In Denemarken bestaat er een bewaringstermijn van 3 maanden in het kader van de bescherming van de persoonlijke levenssfeer, maar overweegt men die termijn te verlengen tot een jaar.

Wat artikel 7 betreft en de bevoegdheden van de procureur des Koning inzake bepaalde gegevensbestanden, moet men voorzichtig zijn met het begrip « gegevensbestand ».

Er zijn gegevensbestanden die erkend en goedgekeurd zijn door de Commissie voor de bescherming van de persoonlijke levenssfeer. De wet tot bescherming van de persoonlijke levenssfeer is hierop van toepassing, met alle verplichtingen en garanties die dat inhoudt. Hier kunnen dus geen problemen ontstaan.

Door internet te gebruiken kan men echter gegevensbestanden creëren die niet beantwoorden aan alle elementen waar de wet tot bescherming van de persoonlijke levenssfeer gewag van maakt.

In dat geval moeten de procureur des Konings en de onderzoeksrechter deze gegevensbestanden, die als bewijs van misdrijven kunnen dienen, in beslag kunnen nemen.

Men verbaast zich soms over de voorzorgen die de officieren van gerechtelijke politie of de magistraten moeten nemen wanneer zij dergelijke gegevens in beslag nemen. Die gegevens staan op een diskette. In de Kamer is reeds de vraag gesteld of deze diskettes, zoals andere voorwerpen die in beslag zijn genomen, bewaard worden op de griffies van de correctionele rechtbank. Het gerecht dient natuurlijk de nodige maatregelen te nemen opdat die computergegevens in de beste omstandigheden worden bewaard. Daarbij mogen noch de auteursrechten noch de rechten van de benadeelde — aan wie het materiaal zal worden terugbezorgd — in het gedrang komen en mag de strafvordering niet gehinderd worden.

Ook is er een vraag over de noodzaak om bij de federale politie een centraal orgaan op te richten.

De ISPA wilde van de NCCU het centrale orgaan maken. De minister van Justitie is echter niet de baas van de politiehervorming.

De NCCU en het CBO van de rijkswacht zullen deel uitmaken van de federale politie die een directie informaticacriminaliteit zal hebben. Zolang de politiehervorming niet in de praktijk is gebracht, kan men

devenue effective, on ne peut anticiper sur celle-ci, ni procéder à une augmentation des personnes affectées à cette tâche, ce qui bouleverserait l'équilibre négocié dans le cadre de cette réforme.

En ce qui concerne la NCCU, il faut souligner le fait qu'elle se trouve au commissariat général de la police judiciaire. Ses membres ne sont pas véritablement des OPJ opérationnels. Ceux qui traitent les dossiers sont ceux qui se trouvent dans les CCU locaux.

La NCCU a un rôle d'assistance technique, et également de point central. Elle recueille l'information, prévient le magistrat national ou le magistrat territorialement compétent, et les collègues des brigades locales.

Surveiller tout le réseau est une tâche impossible.

Les États-Unis voudraient créer une police informatique mondiale, qui serait principalement américaine, et accessoirement européenne, mais ce projet a peu de chances d'aboutir.

Cependant, il est important pour les autorités d'avoir une vue sur le contenu, car la liberté d'expression a ses limites. Au regard des valeurs inscrites dans la Constitution et les lois belges, on ne peut admettre, par exemple, les propos racistes.

Ceci s'applique également sur internet.

En Belgique, territorialement, on considérera donc que certains sites internet contiennent des éléments ou des messages qui rendent leurs auteurs passibles de l'application de la loi pénale belge.

Dans d'autres pays comme les États-Unis, la liberté d'expression a une valeur tellement absolue, que le fait d'écrire un propos raciste n'est pas répréhensible. Cependant, les valeurs américaines ne sont pas nécessairement les nôtres, et l'on peut tendre à une harmonisation des valeurs au niveau européen.

Un membre observe qu'en ce qui concerne la répression du racisme, il n'y a guère de contestation. Mais il y a des cas plus tangents, comme celui de l'Église de Scientologie. Aux États-Unis, elle est autorisée. Chez nous, elle est considérée comme une secte.

Un sénateur réplique que l'on ne peut agir que pour autant que l'on ait un élément de rattachement avec la Belgique (par exemple : si le serveur ou le propriétaire de l'entreprise est belge).

Le ministre répond qu'il y a toujours un élément de rattachement avec la Belgique, dès l'instant où quelqu'un se rend sur internet en Belgique.

Le problème se situe plutôt au niveau de l'exécution de la décision (*cf.* la décision de l'autorité française interdisant qu'un site soit accessible sur son territoire, alors que le serveur est américain).

er echter niet op vooruitlopen en ook niet meer mensen vrijmaken voor deze taak, want dat zou het bereikte evenwicht over de hervorming opnieuw op de helling zetten.

Men mag niet uit het oog verliezen dat de NCCU zich op het commissariaat-generaal van de gerechtelijke politie bevindt. De leden zijn geen echte operationele officieren van gerechtelijke politie. De dossiers worden behandeld door de plaatselijke CCU.

De NCCU biedt technische hulp en fungeert als middelpunt. Zij verzamelt informatie en brengt de federale magistraat of de territoriaal bevoegde magistraat en de collega's van de plaatselijke brigades op de hoogte.

Het is niet mogelijk om het hele net te surveilleren.

De Verenigde Staten willen een wereldwijde computerpolitie oprichten, die voornamelijk een Amerikaanse aangelegenheid zal zijn waaraan de Europeanen mogen meewerken. De kans dat dit project zal slagen, is klein.

Toch moet de overheid zich een beeld kunnen vormen van de inhoud van webpagina's, omdat de vrijheid van meningsuiting grenzen heeft. De waarden die de Grondwet en de Belgische wetten bekrachtigen, staan bijvoorbeeld geen racistische uitlatingen toe.

Dat geldt ook voor het internet.

In België gaat men er dus van uit dat internetsites elementen of boodschappen kunnen bevatten waardoor de makers zich aan strafrechtelijke vervolgingen blootstellen.

In andere landen, zoals in de Verenigde Staten, hecht men zoveel belang aan de vrijheid van meningsuiting dat bijvoorbeeld racistische uitlatingen niet worden gestraft. Wij hoeven ons niet te richten naar de Amerikaanse opvattingen en kunnen streven naar een harmonisering op Europees vlak.

Een lid wijst erop dat er weinig betwisting bestaat over de beteugeling van racisme. Er zijn echter delicatere gevallen, zoals de Scientology Church, die in de Verenigde Staten is toegestaan maar bij ons als een sekte wordt beschouwd.

Een senator antwoordt dat men slechts kan optreden in zover men een aanknopingspunt met België heeft (bijvoorbeeld indien de server of de eigenaar van de onderneming Belgisch is).

De minister antwoordt dat er altijd een aanknopingspunt met België is zodra iemand zich in België op het internet begeeft.

Het probleem doet zich vooral voor bij de uitvoering van de beslissing (*cf.* de beslissing van de Franse overheid om de toegang tot een site op het eigen grondgebied te verbieden, terwijl de server Amerikaans is).

Il faut veiller à ce que les valeurs sanctionnées par les décisions judiciaires nationales continuent à pouvoir trouver leur pleine exécution.

L'argument consistant à dire qu'internet n'est plus un monde géographique, mais virtuel, n'est pas valable. Il reste toujours un lien avec la réalité quotidienne : la loi nationale s'applique entre celui qui se connecte et celui qui répond, même si la situation revêt une certaine ambiguïté.

Revenant à l'Église de Scientologie, une commissaire observe qu'il n'y a aucune raison de sanctionner les informations qu'elle diffuse par voie informatique, alors que l'on ne sanctionne pas ce qu'elle diffuse par la voie écrite ordinaire, même si l'on peut attirer l'attention sur le caractère sectaire de cette organisation, et sur le danger qu'elle représente.

Il faut certes protéger le citoyen, mais il faut aussi le responsabiliser.

Il n'est pas simple de trouver un équilibre entre la protection de certaines valeurs fondamentales et celle de la liberté d'expression.

Le ministre aborde ensuite la question des incriminations, et notamment celles prévues a l'article 6, à savoir l'accès à un système informatique, et la prise de connaissance de données.

À cet égard, le projet de loi prévoit une gradation importante des infractions, qui va de pair avec une gradation des peines imposées.

Accéder à un système informatique peut se faire de différentes manières.

Il peut très bien s'agir d'une simple erreur. Mais il y a aussi des gens pour qui accéder à un système informatique alors qu'il n'en ont pas le droit constitue une sorte de sport. Ils peuvent ne rien faire d'autre que franchir la barrière d'accès au site, sans causer de dommage, puis s'en aller. Ils commettent effectivement une infraction, et sont passibles d'une sanction. Ils peuvent aussi accéder au site et décider de ne rien faire d'autre, mais, par le simple fait de leur présence inappropriée, perturber le système. C'est ce que visent les termes « causer un dommage, même non intentionnel ».

Une commissaire estime qu'il ne s'agit pas là d'une véritable criminalité informatique. Comme le faisait remarquer un précédent intervenant, on pourrait poursuivre sur cette base l'étudiant qui ne fait que « s'amuser un peu ».

Les entreprises qui veulent se protéger n'ont qu'à faire appel à des sociétés spécialisées en matière de sécurisation des systèmes.

Men moet ervoor zorgen dat het mogelijk blijft volledig uitvoering te geven aan de waarden die door de nationale rechterlijke beslissingen bekrachtigd worden.

Het argument dat het internet geen geografische wereld meer is maar een virtuele wereld, gaat niet op. Er blijft altijd een band met de dagelijkse realiteit : de nationale wet is van toepassing tussen degene die op het net is en degene die daarop antwoordt, zelfs al is de toestand enigszins dubbelzinnig.

Terugkomende op de Scientology Church maakt een commissielid de opmerking dat er geen enkele reden is om de informatie die ze op elektronische wijze verspreidt, te bestraffen terwijl niet opgetreden wordt tegen de informatie die via gewone geschreven kanalen verspreid wordt, ook al kan men de aandacht vestigen op het sektarische karakter van die organisatie en op het gevaar dat eraan verbonden is.

Men moet de burger weliswaar beschermen maar men moet hem ook verantwoordelijkheid geven.

Het is niet eenvoudig een evenwicht te vinden tussen de bescherming van een aantal fundamentele waarden en de bescherming van de vrije meningsuiting.

De minister behandelt vervolgens het vraagstuk van de strafbaarstellingen, en met name de strafbaarstellingen bepaald in artikel 6, de toegang tot een informaticasysteem en de kennisname van gegevens.

In dit verband voorziet het wetsontwerp in een duidelijke gradatie van misdrijven, samen met een gradatie in de opgelegde straffen.

Men kan op verschillende manieren toegang verkrijgen tot een informaticasysteem.

Het is zeer goed mogelijk dat het om een gewone vergissing gaat. Maar er zijn ook mensen die het als een sport beschouwen zich toegang te verschaffen tot een informaticasysteem terwijl ze daartoe het recht niet hebben. Het is mogelijk dat ze niets anders doen dan de toegangspoort tot de site binnendringen, zonder schade te berokkenen, en dan weggaan. Ze plegen daadwerkelijk een misdrijf en zijn strafbaar. Ze kunnen zich ook toegang tot de site verschaffen en beslissen niets anders te doen, maar gewoon door hun ongepaste aanwezigheid kunnen ze het systeem verstoren. Dat wordt bedoeld met de termen « schade, zelfs onopzettelijk, veroorzaken ».

Volgens een commissielid gaat het hier niet echt om computercriminaliteit. Zoals een vorige spreker opmerkte, zou men op die basis een student kunnen vervolgen die niet anders doet dan « zich een beetje amuseren ».

De ondernemingen die zich willen beschermen, moeten maar een beroep doen op firma's die gespecialiseerd zijn in de beveiliging van systemen.

Un sénateur souligne qu'aux Pays-Bas, le fait de pénétrer dans un système n'est punissable que si l'on viole un système de sécurité avec l'intention de nuire.

Le § 1er, alinéa 1er, de l'article 6 du projet ne prévoit aucune de ces deux conditions.

Ainsi, si une société oublie de prévoir un code d'accès à certaines informations, et qu'une personne prend connaissance de celles-ci sans aucune intention de nuire, cette personne sera punissable.

Cela ne paraît pas justifié. L'intervenant estime que l'intention frauduleuse doit également être requise dans le cadre du § 1er, alinéa 1er, de l'article 6 du projet.

Un membre se rallie à l'opinion du précédent intervenant. Il est clair que l'on peut arriver sur un site par erreur, ou même par jeu. Ce qui compte, c'est de déterminer s'il y a eu intention de nuire, ou si un dommage a été causé. Cette dernière hypothèse est déjà visée dans le texte. C'est donc le début de l'article 6 qui devrait être revu.

Le ministre répond que l'article 550*bis* doit être replacé dans son contexte, à savoir celui d'un titre IX*bis* nouveau, intitulé «Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ce système».

Il faut faire une distinction entre les sites ouverts, qui permettent à ceux qui le souhaitent de satisfaire leur curiosité, et les autres, qui sont protégés et pour lesquels on n'entend pas permettre l'accès à toute personne.

Il en va ainsi, par exemple, du système de la Défense nationale, où un code est nécessaire, même pour avoir accès à des informations qui ne sont pas nécessairement classifiées.

Si l'on rentre dans ce système sans avoir le code, on ne peut prétendre qu'il s'agit d'un accès légitime.

Autre chose est, bien entendu, de la personne qui accède à des données par suite de la négligence d'un utilisateur, qui laisse en son absence son poste ouvert et accessible.

Il est vrai que l'accès à un système protégé peut se produire par erreur: si tel est le cas, et que la personne reparte aussitôt sans poser aucun autre acte, il n'y a pas d'infraction punissable.

Par contre, celui qui, constatant qu'il a accédé par erreur, va plus loin ou se maintient volontairement dans le système, commet une infraction.

Quant à la distinction entre *hacking* et *cracking,* elle est discutable.

Een senator merkt op dat het binnendringen in een systeem in Nederland alleen maar strafbaar is indien men een veiligheidssysteem kraakt met de bedoeling schade te veroorzaken.

Paragraaf 1, eerste lid, van het ontworpen artikel 6 stelt geen van deze twee voorwaarden.

Zo zal een persoon strafbaar zijn indien een bedrijf voor bepaalde gegevens een toegangscode vergeet aan te brengen en indien deze persoon van de gegevens kennis neemt.

Dat is niet te rechtvaardigen. Spreker meent dat het bedrieglijk opzet ook vereist moet zijn in het kader van § 1, eerste lid, van het ontworpen artikel 6.

Een spreker betuigt zijn instemming met de vorige spreker. Het is duidelijk dat men per vergissing, of zelfs door spel op een bepaalde site kan belanden. Het is belangrijk uit te maken of er een oogmerk is om te schaden en of er schade veroorzaakt is. Deze laatste hypothese wordt reeds in de tekst vermeld. De aanhef van artikel 6 moet dus gewijzigd worden.

De minister antwoordt dat artikel 550*bis* in zijn context geplaatst moet worden, namelijk de context van titel IX*bis* die luidt als volgt: «Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen».

Men moet een onderscheid maken tussen open sites, waar mensen die dat wensen hun nieuwsgierigheid kunnen bevredigen, en de andere die beschermd zijn en waar het niet de bedoeling is aan om het even wie toegang te verlenen.

Dat geldt bijvoorbeeld voor de site van Landsverdediging, waar een code noodzakelijk is, zelfs om toegang te verkrijgen tot informatie die niet noodzakelijk geheim is.

Als men zonder de code in zo'n systeem binnendringt, kan men niet aanvoeren dat het om een rechtmatige toegang gaat.

Het is natuurlijk iets anders wanneer iemand toegang tot gegevens krijgt door de nalatigheid van een gebruiker die zijn werkpost open laat staan.

Het is waar dat men per vergissing toegang kan verkrijgen tot een beschermd systeem: indien dat het geval is en de persoon onmiddellijk vertrekt zonder een andere daad te stellen, gaat het niet om een strafbaar feit.

Degene die daarentegen vaststelt dat hij per vergissing toegang heeft verkregen en daarna verder gaat of bewust in het systeem blijft, pleegt een misdrijf.

Het onderscheid tussen *hacking* en *cracking* is betwistbaar.

Celui qui reçoit un mandat pour contrôler que le système est fiable le fait dans un contexte bien précis. Il peut très bien, ensuite, abuser de sa position privilégiée pour s'approprier des données.

La notion de *hacking* n'est pas reprise dans le projet. Le *hacker* de bonne foi ne tombera pas sous le coup de celui-ci, car il n'y aura pas de plainte.

Un membre répète qu'à son estime, le propriétaire doit protéger son système. Rentrer dans un système non protégé ou mal protégé ne doit pas être punissable. Seule l'utilisation doit l'être.

Un sénateur déclare qu'effectivement, le *hacker* de bonne foi ne fera, dans la plupart des cas, l'objet d'aucune plainte.

Cependant, si une plainte était déposée, le juge ne disposerait d'aucun pouvoir d'appréciation, et ne pourrait que constater que l'infraction est définie de façon très large, sans distinction entre la bonne foi et l'intention de nuire.

L'intervenant annonce dès lors le dépôt d'un amendement tendant à introduire à l'article 6, § 1er, alinéa 1er, l'intention frauduleuse et le but de nuire, et à supprimer l'alinéa 2.

Le § 2 qui, à la différence du § 1er, concerne les *insiders* et mentionne l'intention frauduleuse ou le but de nuire, serait maintenu.

En ce qui concerne le § 3, l'intervenant peut se rallier au 3o, mais les 1o et le 2o lui paraissent manquer de clarté. Qu'est-ce par exemple que «prendre connaissance» de données?

Quant au § 4, il punit la tentative, ce qui étend jusqu'à l'absurde le champ d'application du projet. De plus, la tentative est punie des mêmes peines que les infractions elles-mêmes.

Une commissaire estime que des infractions manquent encore en ce qui concerne le volet «criminalité organisée».

Il faut certes protéger le citoyen ordinaire comme le fait le projet de loi, mais il faut aussi prévoir les outils nécessaires pour poursuivre la criminalité organisée, qui utilise elle aussi l'outil informatique.

Le ministre poursuit en indiquant qu'il s'accorde avec un intervenant, qui avait souligné qu'un équilibre devait être recherché en ce qui concerne la problématique du délai.

Il confirme par ailleurs que la loi sur la protection de la vie privée s'applique.

Degene die belast wordt met de controle van de betrouwbaarheid van een systeem, werkt in een welbepaalde context. Het is zeer goed mogelijk dat hij daarna misbruik maakt van zijn bevoorrechte positie om zich gegevens toe te eigenen.

Het begrip *hacking* is niet in het ontwerp opgenomen. De *hacker* die te goeder trouw is, zal niet onder de wet vallen want tegen hem wordt geen klacht ingediend.

Een lid herhaalt dat de eigenaar volgens hem zijn systeem moet beschermen. In een niet of slecht beschermd systeem binnendringen moet niet strafbaar zijn. Alleen het gebruik moet strafbaar zijn.

Een senator verklaart dat in de meeste gevallen inderdaad geen klacht wordt ingediend tegen de *hacker* die te goeder trouw is.

Indien een klacht zou worden ingediend, zou de rechter echter geen enkele beoordelingsbevoegdheid hebben en zou hij alleen maar kunnen vaststellen dat het misdrijf zeer ruim gedefinieerd is, zonder onderscheid tussen de goede trouw en het oogmerk om te schaden.

Spreker kondigt dan ook aan dat hij een amendement zal indienen om in artikel 6, § 1, eerste lid, de begrippen «bedrieglijk opzet» en «oogmerk om te schaden» in te voegen en om het tweede lid te schrappen.

Paragraaf 2 heeft, in tegenstelling tot § 1, betrekking op de *insiders* en de vermelding van het bedrieglijk opzet of het oogmerk om te schaden zou behouden blijven.

Wat paragraaf 3 betreft, kan spreker zich vinden in het 3o, maar het 1o en het 2o zijn volgens hem niet duidelijk. Wat betekent «kennis nemen van gegevens»?

Paragraaf 4 bestraft de poging, wat de werkingssfeer van dit ontwerp tot in het absurde uitbreidt. Bovendien wordt de poging op dezelfde manier gestraft als de misdrijven zelf.

Een commissielid vindt dat er nog misdrijven ontbreken die ondergebracht kunnen worden bij de georganiseerde criminaliteit.

Uiteraard moet de gewone burger worden beschermd, maar het moet ook mogelijk zijn om de georganiseerde criminaliteit te vervolgen, die immers ook gebruik maakt van computers.

De minister is het eens met de spreker die benadrukte dat inzake de termijn naar een evenwicht moet worden gezocht.

Hij bevestigt dat de wet tot bescherming van de persoonlijke levenssfeer van toepassing is.

Quant à l'avis de la Commission européenne, qui a été demandé par le ministre Daems, il concerne surtout l'article 14 du projet, et est attendu pour le 11 juillet.

On ne dispose d'aucun élément sur cet avis à l'heure actuelle.

L'un des problèmes pourrait être que les fournisseurs d'accès sont, en vertu du projet, tenus de conserver les données sur le territoire belge, ce qui pourrait être jugé contraire aux exigences du marché unique.

En ce qui concerne le «piratage à usage éducatif», si l'on prend sur internet des informations accessibles, il s'agit d'un téléchargement, qui n'est pas constitutif d'infraction.

Le piratage suppose que l'on utilise des moyens informatiques pour se livrer à une activité commerciale. Il faut aussi savoir que, pour briser des codes, on a souvent recours à des logiciels que l'on peut acquérir ou fabriquer. Faut-il dépasser cet interdit? On retombe ici dans la problématique de l'article 550*bis*, § 1er, dont la formulation pourrait, il est vrai, sans doute être revue.

Enfin, il faut avoir à l'esprit que certaines entreprises comme Belgacom fournissent un service au public, aux hôpitaux, etc. Le dommage causé par une intrusion dans leur système peut donc être très important pour les usagers.

En ce qui concerne l'article 9, §§ 1er et 3, la présomption dont il est question n'est pas irréfragable. Si la personne requise objecte qu'elle ne dispose pas des connaissances nécessaires, on n'ira pas plus loin. La preuve incombera toujours au ministère public, car la présomption n'a pas pour but de renverser la charge de la preuve. Le § 3 s'applique non seulement aux personnes visées au § 1er, mais aussi à celles visées au § 2, qui connaissent le système en question.

Quant à la lutte contre la criminalité organisée, elle est possible sur la base du projet.

Pour les organisations criminelles, ce n'est évidemment pas l'article 550, § 1er, du projet qui sera utile. Par contre, mettre la tentative sur le même pied que l'infraction consommée peut s'avérer important dans la lutte contre de telles organisations, pour autant, bien entendu, que l'on reste dans la logique selon laquelle les personnes bien intentionnées ne sont pas visées.

Un sénateur souligne, à propos de l'article 9, qu'aux Pays-Bas une proposition de loi laisse le choix à la personne qui collabore au décryptage d'un message, de communiquer ou non la clé de cryptage à la police.

Qu'en est-il ici? Ce choix existe-t-il en vertu du projet?

Aux Pays-Bas, on utilise également les termes «*beschikbare kennis*» au lieu de «*bijzondere kennis ...*»

Het advies van de Europese Commissie dat door minister Daems is gevraagd, betreft vooral artikel 14 van het ontwerp en wordt verwacht tegen 11 juli.

Momenteel weten we nog niets over dit advies.

Een probleem kan zijn dat de providers krachtens het ontwerp de gegevens op het Belgisch grondgebied moeten bewaren, wat misschien strijdig wordt geacht met de eengemaakte markt.

Wat het «kraken voor educatieve doeleinden» betreft, als men toegankelijke informatie van het internet haalt, dan heet dat gewoon downloaden en dat is geen misdrijf.

Computerkraak veronderstelt dat men informatica gebruikt met het oog op een commerciële activiteit. Om een code te kraken, maakt men vaak gebruik van aangekochte of zelfgemaakte software. Moet het verbod worden uitgebreid? Hier zijn we terug bij het probleem van de formulering van artikel 550*bis*, § 1, die wellicht opnieuw moet worden bekeken.

Men mag niet vergeten dat bepaalde ondernemingen zoals Belgacom een dienst leveren aan een breed publiek, aan ziekenhuizen, enz. Binnendringen in hun systeem kan voor de gebruikers enorme schade meebrengen.

Het vermoeden uit artikel 9, §§ 1 en 3, is niet onweerlegbaar. Als de betrokken persoon opwerpt dat hij niet de nodige kennis heeft, houdt het op. Het openbaar ministerie moet het bewijs van de kennis leveren, aangezien het vermoeden niet tot doel heeft de bewijslast om te keren. Paragraaf 3 is niet alleen van toepassing op de personen bedoeld in § 1, maar ook op de personen bedoeld in § 2, die het systeem in kwestie kennen.

Het ontwerp staat bestrijding van de georganiseerde criminaliteit wel degelijk toe.

Uiteraard is niet artikel 550, § 1, van het ontwerp nuttig in de strijd tegen de criminele organisaties. Het gelijkstellen van de poging met het gepleegde misdrijf kan wel belangrijk zijn in die strijd zolang maar duidelijk is dat goedmenende personen niet geviseerd worden.

Met betrekking tot artikel 9 benadrukt een senator dat in een Nederlands wetsvoorstel de persoon die meewerkt aan het ontcijferen van een boodschap, de keuze wordt gelaten om de code al dan niet aan de politie mee te delen.

Bestaat die keuze ook in dit ontwerp?

In Nederland gebruikt men ook de term «beschikbare kennis» in plaats van «bijzondere kennis ...» om

pour souligner que celui dont la collaboration est requise ne peut être contraint, pour donner suite à cette demande, d'acquérir des connaissances ou de développer ou d'acquérir des instruments complémentaires. Qu'en est-il dans le cadre du présent projet ?

Le ministre répond que le projet ne règle pas le problème du décryptage, qui est un problème spécifique, à résoudre en tenant compte des règles existant en la matière au sein de l'Union européenne. À l'heure actuelle, le codage est totalement libre. La communication obligatoire des codes aux services de police paraîtrait en tout cas assez dangereuse.

Pour le surplus, le projet vise à permettre au juge d'instruction de mettre en œuvre tous les moyens nécessaires pour pouvoir pénétrer dans un système. Le texte du projet paraît adéquat à cet égard.

En ce qui concerne le second point, on ne peut évidemment pas demander à la personne visée au § 1er de l'article 9 des efforts supplémentaires pour pouvoir apporter la collaboration demandée. Sans doute la réponse doit-elle être plus nuancée dans le cadre du § 2 de cet article, mais il ne faut pas aller trop loin.

Une commissaire souhaite poser trois questions complémentaires à propos de l'article 6, § 3, 1o :

1) Quelle est la portée des mots « soit prend connaissance des données ... » ? Quand on accède à un site, on prend inévitablement connaissance d'un certain nombre de données.

Ne faudrait-il pas, dès lors, viser uniquement l'utilisation des données ?

2) Que visent exactement les mots « soit fait un usage quelconque d'un système informatique » ?

3) Compte tenu de la logique évoquée ci-dessus, selon laquelle il faut une intention de nuire, faut-il maintenir les mots « même non intentionnellement » ?

Le ministre répond à la troisième question, sous réserve d'une délimitation correcte du cadre du § 1er, que le simple fait de se trouver dans un système informatique peut perturber celui-ci et causer un dommage (par exemple le blocage du système, ou un problème d'accès par un autre utilisateur).

Bien évidemment, le dommage sera aggravé si l'on détruit les données.

Quant aux termes « soit fait un usage quelconque d'un système informatique », ils visent l'usage du système informatique d'autrui.

Ainsi, voici quelques mois, certains moteurs de recherche américains ont été perturbés par la réception d'un ensemble de messages de provenances diverses. Une recherche d'identité aboutissait à diverses

te benadrukken dat degene wiens medewerking wordt geëist, niet gedwongen kan worden om bijkomende kennis of instrumenten te ontwikkelen of te verwerven. Hoe zit dat in dit ontwerp ?

De minister antwoordt dat dit ontwerp het probleem van het ontcijferen niet regelt, omdat dat een specifiek probleem is dat moet worden opgelost in overeenstemming met de bestaande Europese regelgeving. Momenteel is het coderen volledig vrij. De verplichte mededeling van de code aan de politiediensten lijkt in elk geval nogal gevaarlijk.

Voor het overige wil het ontwerp de onderzoeksrechter toestaan om alle nodige middelen te gebruiken om in het systeem binnen te dringen. In dat opzicht lijkt de tekst van het ontwerp afdoende.

Wat het tweede punt betreft, men kan uiteraard van de in § 1 van artikel 9 bedoelde persoon niet eisen dat hij bijkomende inspanningen levert om de gevraagde medewerking te kunnen verlenen. Met betrekking tot § 2 van dit artikel is het antwoord wellicht wel meer genuanceerd, maar men mag toch niet te ver gaan.

Een commissielid heeft drie bijkomende vragen over artikel 6, § 3, 1o :

1) Wat betekenen de woorden « hetzij kennis neemt van gegevens ... » ? Wanneer men een site binnengaat, neemt men onvermijdelijk kennis van een aantal gegevens.

Is het niet beter enkel te spreken van het gebruik van gegevens ?

2) Wat betekenen de woorden « hetzij enig gebruik maakt van een informaticasysteem » precies ?

3) Moeten de woorden « zelfs onopzettelijk » niet worden geschrapt aangezien, zoals hiervoor is uiteengezet, het opzet om te schaden aanwezig moet zijn ?

De minister antwoordt op de derde vraag — onder voorbehoud van een juiste afbakening van de werkingssfeer van § 1 —, dat aanwezigheid op zich in een informaticasysteem kan leiden tot storingen en schade (bijvoorbeeld omdat het systeem blokkeert of een andere gebruiker problemen heeft om binnen te raken).

Uiteraard is de schade veel erger als men gegevens vernietigt.

De woorden « hetzij enig gebruik maakt van een informaticasysteem » slaan op het gebruik van een informaticasysteem van iemand anders.

Enkele maanden geleden werden bepaalde Amerikaanse zoekprogramma's verstoord door de ontvangst van een aantal boodschappen van uiteenlopende herkomst. Een onderzoek naar de identiteit

universités, qui n'étaient cependant pas à l'origine des messages en question.

Il s'est avéré qu'il s'agissait en fait d'une personne qui avait réussi à pénétrer sur le site de ces universités, et à les faire fonctionner à son profit.

Enfin, en ce qui concerne la première question, l'accès à un site ouvre une première porte qui donne sur un « salon d'accueil » où, en principe, on ne trouve pas d'informations significatives, mais qui sert seulement à orienter l'arrivant.

Un sénateur estime néanmoins que la formulation du texte est trop vague.

Un membre réitère sa remarque selon laquelle prendre connaissance de données sans intention de nuire ne devrait pas être punissable.

Le précédent intervenant fait observer qu'en matière pénale, le législateur fait œuvre éthique. Il faut donc être très attentif à ce que l'on rend punissable.

Or, il est vraisemblable que, pour la plupart des gens, la prise de connaissance de données par simple curiosité et sans but de nuire n'est pas éthiquement condamnable.

IV. DISCUSSION DES ARTICLES

Les articles 1er à 5 ne donnent lieu à aucune observation.

Article 6

A. Discussion

M. Vandenberghe et Mme Nyssens déposent un amendement nº 5 (doc. Sénat, nº 2-392/2) visant à introduire l'intention frauduleuse ou le but de nuire dans l'incrimination prévue à l'article 550*bis*, § 1er, alinéa premier, en projet.

Un des auteurs explique que l'amendement fait suite à la remarque formulée par le Conseil d'État dans son avis du 31 mai 1999 (doc. Chambre, nº 50-213/1, 99/00, p. 52). Aucune raison objective ne permet de justifier le traitement différencié entre l'incrimination prévue à l'article 550*bis*, § 1er, alinéa 1er, selon lequel le simple accès non autorisé à un système informatique est pénalement répréhensible, peu importe l'intention de l'auteur, et celle prévue au § 2 du même article, selon lequel une personne autorisée à accéder à un système informatique mais qui abuserait de son pouvoir ne serait punissable que lorsque l'intention frauduleuse ou le but de nuire est établi. L'amendement entend lever cette discrimination.

leidde naar verschillende universiteiten, vanwaar de boodschappen echter niet verstuurd bleken te zijn.

Uiteindelijk bleek dat een persoon erin geslaagd was op de sites van deze universiteiten binnen te dringen en er gebruik van te maken in zijn eigen voordeel.

Wat de eerste vraag betreft, als men een site binnentreedt, komt men eerst in een soort « ontvangstruimte » van waaruit men verder wordt verwezen, maar waar nog geen belangrijke informatie te vinden is.

Een senator vindt de formulering van de tekst toch te vaag.

Een lid herhaalt zijn opmerking dat kennisnemen van gegevens zonder opzet om te schaden niet strafbaar mag zijn.

De vorige spreker wijst erop dat wanneer het om strafrechtelijke materies gaat, de wetgever eigenlijk het domein van de ethiek betreedt. Men moet dus heel voorzichtig zijn met wat men precies strafbaar maakt.

De meeste mensen zullen het kennisnemen van gegevens uit nieuwsgierigheid en zonder opzet om te schaden, moreel wellicht niet verkeerd vinden.

IV. ARTIKELSGEWIJZE BESPREKING

De artikelen 1 tot 5 geven geen aanleiding tot opmerkingen.

Artikel 6

A. Bespreking

De heer Vandenberghe en mevrouw Nyssens dienen amendement nr. 5 in (Stuk Senaat, nr. 2-392/2) dat ertoe strekt in het voorgestelde artikel 550*bis*, § 1, eerste lid, de woorden « met bedrieglijk opzet of met het oogmerk om te schaden » in te voegen.

Een van de indieners legt uit dat het amendement voortvloeit uit de opmerking van de Raad van State in zijn advies van 31 mei 1999 (Stuk Kamer, nr. 50-213/1, 99/00, blz. 52). Er zijn geen objectieve redenen voorhanden om een verschil in behandeling te wettigen van de handeling bedoeld in artikel 550*bis*, § 1, eerste lid, volgens hetwelk het louter ongeoorloofd binnendringen in een computersysteem reeds een strafbaar feit oplevert ongeacht de bedoeling van de dader, en de handeling bedoeld in § 2 van hetzelfde artikel volgens welke een persoon met recht op toegang tot het informaticasysteem, die van dat recht misbruik maakt, slechts strafbaar zou zijn wanneer er sprake is van bedrieglijk opzet of wanneer hij het oogmerk heeft te schaden. Het amendement wil die discriminatie opheffen.

L'intervenant estime que la rédaction de l'incrimination prévue au § 1er, alinéa 1er, en projet, est trop large. Cela revient à créer un délit par imprudence. Il constate par ailleurs que la solution proposée a pour effet pervers de ne pas inciter les gestionnaires informatiques à sécuriser leurs systèmes dès lors qu'ils savent que chaque accès non autorisé est punissable pénalement.

Pour le ministre, la critique du Conseil d'État n'est pas fondée puisque les §§ 1er et 2 de la disposition en discussion visent deux hypothèses distinctes.

Le § 1er vise les personnes externes à une organisation qui s'introduisent dans un système informatique (*hackers*). Cette pratique met en péril la sécurité du système mais également l'intégrité de tout le réseau étant donné l'interconnexion des systèmes informatiques. Il s'agit d'un délit de mise en danger punissable en tant que tel, où seulement le dol général est requis. L'intention frauduleuse constitue une circonstance aggravante qui alourdit la peine.

En ce qui concerne l'hypothèse envisagée dans le paragraphe 2, le gouvernement considère que l'abus par une personne de son pouvoir d'accès à un système informatique (*insiders*) est en premier lieu un problème interne à l'organisation concernée. Des sanctions disciplinaires, de droit du travail ou civiles sont plus indiquées dans de telles situations. Seuls les cas les plus graves, lorsqu'il y a intention de nuire, sont à réprimer pénalement.

Une commissaire constate que le projet s'inscrit dans le cadre de recommandations internationales invitant les États à prévoir des incriminations minimales en matière de criminalité informatique. Où se situe le projet par rapport aux législations des autres pays européens ?

Le ministre confirme que le projet s'inspire notamment de la recommandation nº R(89)9 du Conseil de l'Europe du 13 septembre 1989 en matière de criminalité informatique. Vu l'évolution rapide dans le secteur des technologies de l'information, ce texte est partiellement dépassé. Des négociations sont en cours en vue d'élaborer une convention internationale en la matière mais celles-ci n'ont pas abouti à ce jour.

Au niveau international, la tendance est d'incriminer pénalement le simple accès non autorisé à un système informatique. Les États sont cependant libres d'imposer, pour cette incrimination, des éléments constitutifs complémentaires tels que l'intention frauduleuse ou le but de nuire. Ce n'est pas l'option retenue dans le projet à l'examen.

Mme Nyssens dépose un sous-amendement à l'amendement nº 5 (doc. Sénat, nº 2-392/2, amendement nº 16), visant à remplacer les mots « sachant qu'il n'y est pas autorisé » par les mots « avec une intention frauduleuse ou dans le but de nuire ». Ces

Spreker meent dat de strafbaarstelling in § 1, eerste lid, te ruim geformuleerd is. Dit komt neer op het creëren van een « onvoorzichtigheidsmisdrijf ». Hij stelt vast dat de voorgestelde oplossing er ongewild toe leidt dat de systeembeheerders niet veel moeite zullen doen om hun computersysteem te beveiligen daar zij toch weten dat elke ongeoorloofde toegang strafbaar is.

Voor de minister is de kritiek van de Raad van State niet gegrond omdat § 1 en § 2 van de besproken bepaling twee aparte gevallen beogen.

Paragraaf 1 beoogt de personen die binnendringen in een computersysteem van een organisatie waarmee ze niets te maken hebben (*hackers*). Die praktijk brengt de veiligheid van het systeem in gevaar maar ook de integriteit van het hele netwerk omdat de informaticasystemen met elkaar verbonden zijn. Het in gevaar brengen op zich is strafbaar en alleen algemeen opzet is vereist. Bedrieglijk opzet vormt een verzwarende omstandigheid die leidt tot een strengere straf.

In het in § 2 beoogde geval gaat de regering ervan uit dat wanneer een persoon die recht van toegang tot een computersysteem heeft (*insiders*), van zijn recht misbruik maakt, dit in eerste instantie een intern probleem van de betrokken organisatie is. In dergelijke gevallen zijn tuchtstraffen, arbeidsrechtelijke of burgerrechtelijke sancties meer op hun plaats. Alleen de zwaarste gevallen, wanneer er een oogmerk om te schaden is, worden strafrechtelijk vervolgd.

Een commissielid stelt vast dat het ontwerp past in het kader van internationale aanbevelingen die de Staten verzoeken minimumstraffen te stellen op cybercriminaliteit. Is het ontwerp te vergelijken met de wetgeving in de andere Europese landen ?

De minister bevestigt dat het ontwerp onder meer gebaseerd is op aanbeveling nr. R(89)9 van de Raad van Europa van 13 september 1989 inzake computergerelateerde criminaliteit. Door de snelle ontwikkelingen in de sector van de informatietechnologieën is die tekst ten dele verouderd. Er lopen thans onderhandelingen om ter zake een internationaal verdrag te sluiten, maar die zijn nog niet afgerond.

Op internationaal niveau is er een tendens om het louter ongeoorloofd binnendringen in een computersysteem strafbaar te stellen. Het staat de Staten evenwel vrij te bepalen welke aanvullende handelingen een strafbaar feit uitmaken, zoals bedrieglijk opzet of het oogmerk te schaden. Dat is niet de keuze die in het voorliggende ontwerp gemaakt wordt.

Mevrouw Nyssens dient een amendement in op amendement nr. 5 (Stuk Senaat, nr. 2-392/2, amendement nr. 16), dat ertoe strekt de woorden « terwijl hij weet dat hij daartoe niet gerechtigd is » te vervangen door de woorden « met bedrieglijk opzet of met het

mots rendent punissable l'accès en toute connaissance de cause au système sans y avoir droit.

M. Van Quickenborne fait remarquer que son amendement nº 3 (doc. Sénat, nº 2-392/2) sous-tend le même objectif que l'amendement nº 5 développé ci-avant. Il constate que l'infraction d'accès non autorisé à un système informatique est la seule infraction du projet à l'examen pour laquelle l'élément intentionnel n'est pas requis. Il ne voit pas quelle raison objective justifie cette différence.

Un commissaire soutient cet amendement. Il veut en effet éviter qu'une personne, accédant par inadvertance dans un réseau informatique sans y être autorisée, soit passible de sanctions pénales.

Le ministre fait remarquer qu'un tel acte n'est pas visé par le projet puisque l'article 550*bis*, § 1er, exige que l'auteur agisse en «sachant qu'il n'est pas autorisé» à accéder au système informatique.

M. Van Quickenborne dépose les amendements nos 9, 10 et 11 (doc. Sénat, nº 2-392/2) qui visent à préciser les circonstances aggravantes mentionnées à l'article 550*bis*, § 3. Selon l'intervenant, le texte proposé aux 1º, 2º et 3º est imprécis, ce qui a pour conséquence que tout auteur d'une infraction définie aux §§ 1er et 2 tombera automatiquement sous le coup des circonstances aggravantes du § 3, ce qui ne saurait être le but.

L'amendement nº 9 vise à limiter la circonstance aggravante du 1º à la reprise de données d'un système informatique. Le texte proposé est trop général puisque la seule prise de connaissance des données constitue une circonstance aggravante.

Le ministre marque son accord sur cet amendement, parce qu'il clarifie la volonté du gouvernement.

L'amendement nº 10 a pour objet de préciser que la circonstance aggravante du 2º suppose l'emploi d'un système informatique d'un tiers.

Le ministre marque son accord sur cet amendement, parce qu'il clarifie la volonté du gouvernement.

L'amendement nº 11 vise à remplacer l'article indéfini «un» par l'article défini «le» de telle sorte que la circonstance aggravante implique que l'auteur cause un dommage au système informatique dans lequel il s'est introduit.

Le ministre partage la préoccupation de l'auteur de l'amendement mais constate que la rédaction du texte ne vise pas le dommage causé au système informatique qui servirait de passerelle pour s'introduire dans

oogmerk om te schaden». Die woorden maken de bewuste wederrechtelijke toegang tot het systeem strafbaar.

De heer Van Quickenborne merkt op dat zijn amendement nr. 3 (Stuk Senaat, nr. 2-392/2) hetzelfde doel heeft als het bovenvermelde amendement nr. 5. Hij stelt vast dat de ongeoorloofde toegang tot een computersysteem het enige misdrijf in het voorliggende ontwerp is waarvoor geen opzet is vereist. Hij ziet niet in welke objectieve reden dit verschil kan verantwoorden.

Een commissielid steunt dit amendement. Hij wil immers voorkomen dat iemand die uit onoplettendheid in een computernetwerk binnendringt zonder daartoe gerechtigd te zijn, strafrechtelijk vervolgd kan worden.

De minister merkt op dat een dergelijke handeling niet door het ontwerp beoogd wordt aangezien artikel 550*bis*, § 1, vereist dat de dader zich toegang verschaft tot een informaticasysteem «terwijl hij weet dat hij daartoe niet gerechtigd is».

De heer Van Quickenborne dient de amendementen nrs. 9, 10 en 11 in (Stuk Senaat, nr. 2-392/2) die ertoe strekken de verzwarende omstandigheden vermeld in artikel 550*bis*, § 3, te preciseren. Volgens spreker is de tekst voorgesteld onder het 1º, 2º en 3º onduidelijk, wat ertoe leidt dat de verzwarende omstandigheden van § 3 automatisch van toepassing zullen zijn op een dader van een misdrijf gedefinieerd in de §§ 1 en 2. Dat kan de bedoeling niet zijn.

Amendement nr. 9 strekt ertoe de verzwarende omstandigheid van het 1º te beperken tot het overnemen van gegevens van een computersysteem. De voorgestelde tekst is te algemeen aangezien de loutere kennisneming van de gegevens reeds een verzwarende omstandigheid is.

De minister is het eens met dit amendement omdat het de wil van de regering verduidelijkt.

Amendement nr. 10 heeft tot doel te verduidelijken dat de verzwarende omstandigheid van het 2º het gebruik maken van een informaticasysteem van een derde veronderstelt.

De minister is het eens met dit amendement omdat het de wil van de regering verduidelijkt.

Amendement nr. 11 strekt ertoe het onbepaald lidwoord «een» te vervangen door het bepaald lidwoord «het» zodat de verzwarende omstandigheid impliceert dat de dader schade veroorzaakt aan het informaticasysteem waarin hij is binnengedrongen.

De minister deelt de bezorgdheid van de indiener van het amendement maar stelt vast dat de tekst, zoals hij geredigeerd is, niet de schade beoogt die veroorzaakt is aan het informaticasysteem dat gebruikt

un autre système, ni le dommage en cascade, alors que l'amendement nº 10 prévoit cette possibilité.

M. Van Quickenborne dépose un sous-amendement nº 15 (doc. Sénat, nº 2-392/2) visant à inclure ce dommage «indirect» dans les circonstances aggravantes.

Mme de T'Serclaes dépose un amendement nº 13 (doc. Sénat, nº 2-392/2) visant à supprimer des mots «même non intentionnellement» à l'article 550*bis*, § 3, 3º. Selon l'auteur de l'amendement, l'adoption d'un amendement ajoutant l'élément intentionnel comme condition constitutive de l'infraction au § 1er a pour conséquence que le dommage visé au 3º ne sait plus être causé non intentionnellement.

Le ministre fait remarquer que même si le dol spécial est introduit comme condition de l'infraction à l'article 550*bis*, § 1er, alinéa 1er — ce que ne souhaite pas le gouvernement —, les mots «même non intentionnellement» devraient malgré tout être maintenus au § 3, 3º, du même article. En effet, il faut opérer une distinction selon que l'élément moral requis porte sur les conditions de l'infraction ou sur la réalisation du dommage.

L'adoption de l'amendement nº 13 assouplirait le régime des circonstances aggravantes puisque l'auteur devrait à la fois avoir l'intention d'accéder à un système informatique sans y être autorisé mais également l'intention de causer un dommage. Or, la volonté du gouvernement est de sanctionner plus lourdement l'auteur qui a occasionné un dommage, même non intentionnellement. Le ministre plaide dès lors pour le rejet de cet amendement.

B. Votes

L'amendement nº 5 de M. Vandenberghe et Mme Nyssens est adopté à l'unanimité des 10 membres présents.

Les amendements nos 9 et 10 de M. Van Quickenborne sont adoptés à l'unanimité des 10 membres présents.

Les amendementes nos 3 et 11 de M. Van Quickenborne, et le sous-amendement nº 16 de Mme Nyssens, sont retirés.

Le sous-amendement nº 15 de M. Van Quickenborne est adopté par 8 voix et 2 abstentions.

L'amendement nº 13 de Mme de T' Serclaes est retiré.

wordt als «brug» om in een ander systeem binnen te dringen, noch de trapsgewijs veroorzaakte schade terwijl amendement nr. 10 wel in die mogelijkheid voorziet.

De heer Van Quickenborne dient subamendement nr. 15 in (Stuk Senaat, nr. 2-392/2) dat ertoe strekt die indirecte schade eveneens als een verzwarende omstandigheid te beschouwen.

Mevrouw de T'Serclaes dient amendement nr. 13 in (Stuk Senaat, nr. 2-392/2) dat ertoe strekt in § 3, 3º, van het voorgestelde artikel 550*bis* de woorden «zelfs onopzettelijk» te doen vervallen. Volgens de indiener heeft de goedkeuring van een amendement dat «opzet» toevoegt als voorwaarde voor het misdrijf in § 1, tot gevolg dat de schade bedoeld in het 3º niet meer onopzettelijk kan zijn veroorzaakt.

De minister merkt op dat zelfs indien bijzonder opzet wordt ingevoegd als voorwaarde voor het misdrijf in artikel 550*bis*, § 1, eerste lid — wat de regering niet wenst — de woorden «zelfs onopzettelijk» ondanks alles behouden moeten blijven in § 3, 3º, van hetzelfde artikel. Er moet immers een onderscheid gemaakt worden naargelang het vereiste morele element slaat op de voorwaarden voor het misdrijf of op het veroorzaken van de schade.

Wordt amendement nr. 13 aangenomen, dan wordt de regeling van de verzwarende omstandigheden versoepeld aangezien de dader zowel de bedoeling moet hebben om in een informaticasysteem binnen te dringen zonder daartoe gerechtigd te zijn maar ook nog voornemens moet zijn schade te veroorzaken. De regering wil juist de dader die schade heeft veroorzaakt, zelfs onopzettelijk, zwaarder straffen. De minister pleit derhalve voor de verwerping van dit amendement.

B. Stemmingen

Het amendement nr. 5 van de heer Vandenberghe en mevrouw Nyssens wordt eenparig aangenomen door de 10 aanwezige leden.

De amendementen nrs. 9 en 10 van de heer Van Quickenborne worden eenparig aangenomen door de 10 aanwezige leden.

De amendementen nrs. 3 en 11 van de heer Van Quickenborne, en het subamendement nr. 16 van mevrouw Nyssens, worden ingetrokken.

Het subamendement nr. 15 van de heer Van Quickenborne wordt aangenomen met 8 stemmen bij 2 onthoudingen.

Het amendement nr. 13 van mevrouw de T' Serclaes wordt ingetrokken.

Article 7

A. Discussion

Le gouvernement dépose un amendement nº 4 (doc. Sénat, nº 2-392/3) qui vise à améliorer la structure de l'article et en préciser le contenu.

Une commissaire se demande ce que l'on entend par l'expression «moyens techniques appropriés» à mettre en œuvre par le procureur du Roi.

Le ministre fait remarquer que cette expression figurait dans le projet initial. Étant donné le caractère volatile des données informatiques, il semble souhaitable d'imposer au procureur de Roi de prendre des mesures spécifiques quant à la conservation, l'accès aux données ... sans que l'on puisse techniquement décrire ces mesures. La formulation générale permet de faire évoluer ces moyens appropriés en fonction de l'évolution de la technologie.

Un membre constate que l'amendement nº 4 du gouvernement introduit une modification radicale par rapport au compromis qui avait été atteint lors des discussions en commission à la Chambre. L'article 39*bis*, § 4, du projet initial permettait au procureur du Roi de rendre les données du système informatique inaccessibles ou même de les retirer. M. Erdman avait fait remarquer que «la destruction et la confiscation sont des décisions qui relèvent de la compétence du juge du fond et la compétence du procureur du Roi doit dès lors être en tout cas limitée à interdire le maintien de l'accès aux données dans l'attente d'une décision du juge du fond» (doc. Chambre, 1999-2000, nº 213/4, p. 56).

Le texte adopté par la Chambre donnait au procureur du Roi la possibilité d'utiliser tous les moyens pour empêcher toute personne de continuer à utiliser les données, sans que celui-ci puisse décider de détruire lesdites données.

Selon l'intervenant, l'amendement nº 4 revient à la solution proposée dans le projet initial. En effet, l'article 39*bis*, § 3, alinéa 2 proposé, prévoit que les données sont retirées du système informatique. L'intervenant estime que le procureur du Roi détient ainsi le pouvoir de décider de détruire les données, ce qui avait justement voulu être évité par la Chambre.

Pour le ministre, la contradiction entre la solution préconisée dans l'amendement nº 4 et le texte approuvé par la Chambre n'est qu'apparente. En effet, la philosophie de l'amendement nº 4 est de permettre au procureur du Roi d'utiliser tous les moyens pour empêcher l'accès aux données dans le système informatique. Lorsque ces données sont contraires à l'ordre public ou aux bonnes mœurs, il faut que les données soient retirées du système après avoir été copiées. On comprendrait mal, en effet,

Artikel 7

A. Bespreking

De regering dient amendement nr. 4 in (Stuk Senaat, nr. 2-392/3) dat ertoe strekt de structuur van het artikel te verbeteren en de inhoud ervan te preciseren.

Een commissielid vraagt zich af wat men verstaat onder de «passende technische middelen» die de procureur des Konings moet aanwenden.

De minister wijst erop dat deze uitdrukking in het oorspronkelijk ontwerp stond. Gezien het vluchtige karakter van informaticagegevens lijkt het wenselijk gewoon te vermelden dat de procureur des Konings de specifieke maatregelen neemt met betrekking tot de bewaring, de toegang tot de gegevens ... zonder deze maatregelen technisch te beschrijven. De algemene formulering maakt het mogelijk dat de «passende middelen» de ontwikkeling van de technologie volgen.

Een lid stelt vast dat amendement nr. 4 van de regering een radicale wijziging inhoudt in vergelijking met het compromis dat tijdens de besprekingen in de Kamercommissie was bereikt. Artikel 39*bis*, § 4, van het oorspronkelijke ontwerp stond de procureur des Konings toe om gegevens uit een informaticasysteem ontoegankelijk te maken of zelfs te verwijderen. De heer Erdman verklaarde: «Vernietiging en verbeurdverklaring zijn beslissingen die aan de rechter ten gronde toebehoren en daarom moet in ieder geval de bevoegdheid van de procureur des Konings worden beperkt tot het verbieden van verdere toegang, in afwachting van een beslissing van de rechter ten gronde» (Stuk Kamer, 1999-2000, nr. 213/4, blz. 56).

De door de Kamer aangenomen tekst stond de procureur des Konings toe met alle middelen te verhinderen dat deze gegevens verder werden gebruikt, maar hij mocht niet beslissen om de gegevens te vernietigen.

Volgens spreker keert amendement nr. 4 terug naar de oplossing van het oorspronkelijke ontwerp. Het voorgestelde artikel 39*bis*, § 3, tweede lid, bepaalt inderdaad dat de gegevens uit het informaticasysteem worden verwijderd. Volgens spreker krijgt de procureur des Konings zo de bevoegdheid om de gegevens te vernietigen, precies wat de Kamer wou voorkomen.

Volgens de minister bestaat tussen de oplossing van amendement nr. 4 en de door de Kamer aangenomen tekst slechts een schijnbare tegenstrijdigheid. De bedoeling van amendement nr. 4 is de procureur des Konings toe te staan om alle middelen aan te wenden om de toegang tot de gegevens van een informaticasysteem te verhinderen. Wanneer deze gegevens strijdig zijn met de openbare orde of de goede zeden, moeten ze uit het systeem worden verwijderd nadat ze gekopieerd zijn. Het zou toch onbegrijpelijk zijn dat

qu'après avoir constaté qu'un système informatique contient un dangereux virus, celui-ci n'en soit pas retiré.

Dans la mesure où il y a obligation de faire une copie des données retirées, il n'y a pas réellement de destruction puisqu'en matière informatique, la copie est parfaitement conforme à l'original.

Un membre estime que l'amendement nº 4 ne remet pas en cause la philosophie du texte adopté par la Chambre. Il ne fait que préciser techniquement les règles en matière de saisie de données informatiques. Elle cite à cet égard l'intervention du ministre qui déclarait à propos de l'amendement de M. Erdman qu'il ne « voit aucune objection à ce que l'on inverse la logique de l'article, mais (...) maintient que le procureur du Roi doit pouvoir effacer des données telles que les offres de pornographie enfantine. Le procureur du Roi devrait évidemment faire réaliser une copie qui servira de pièce à conviction » (doc. Chambre, 1999-2000, nº 213/4, p. 59).

M. Van Quickenborne dépose un sous-amendement nº 17 (doc. Sénat, nº 2-392/2) visant à remplacer, à l'article 39*bis*, § 3, alinéa 2 en projet, la notion de retrait des données du système informatique par celle d'inaccessibilité des données. Cette notion est définie comme « la prise de mesures visant à éviter que le gestionnaire du système informatique ou des tiers ne prennent connaissance ou ne fassent usage de ces données ainsi que la prise de mesures visant à éviter la diffusion desdites données. « Rendre des données inaccessibles » englobe l'élimination (effacement) des fichiers concernés avec conservation d'une copie pour la justice. »

Le ministre marque son accord de principe sur cet amendement.

B. Votes

L'amendement nº 4 du gouvernement, sous-amendé par l'amendement nº 17 de M. Van Quickenborne, est adopté à l'unanimité des 10 membres présents.

Article 8

A. Discussion

Mme de T' Serclaes dépose un amendement nº 18 (doc. Sénat, nº 2-392/2) en vue de supprimer les mots « soit autrement » dans l'article 88*ter*, § 1er, en projet. L'intervenante ne voit pas quel acte d'instruction autre que la perquisition est visé par le texte en projet.

bijvoorbeeld een gevaarlijk virus na ontdekking ervan niet uit een informaticasysteem wordt verwijderd.

Aangezien de verwijderde gegevens gekopieerd moeten zijn, is er niet echt sprake van vernietiging. Als het om informatica gaat, stemt een kopie perfect overeen met het origineel.

Een lid meent dat amendement nr. 4 de basisgedachte van de door de Kamer aangenomen tekst niet aantast. Het amendement is technisch gezien bedoeld om de regels inzake inbeslagneming van computergegevens te verduidelijken. Zij vermeldt in dit verband de verklaring van de minister in verband met het amendement van de heer Erdman, namelijk dat hij « er geen bezwaar tegen (heeft) dat de logica van het artikel omgekeerd zou worden, maar hij blijft er echter bij dat de procureur in de mogelijkheid moet zijn om gegevens te wissen, zo bijvoorbeeld aanbiedingen voor kinderporno. De procureur zal daar natuurlijk een kopie van laten maken die dan als bewijsmateriaal zal worden gebruikt » (Stuk Kamer, 1999-2000, nr. 213/4, blz. 59).

De heer Van Quickenborne dient subamendement nr. 17 in (Stuk Senaat, nr. 2-392/2) dat ertoe strekt in het ontworpen artikel 39*bis*, § 3, tweede lid, het begrip « verwijderen van gegevens uit het informaticasysteem » te vervangen door het begrip « ontoegankelijkheid van de gegevens ». Dit begrip wordt gedefinieerd als « het treffen van maatregelen ter voorkoming dat de beheerder van dat geautomatiseerd netwerk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen (wissen) van de betrokken bestanden, met behoud van een kopie voor justitie ».

De minister gaat in principe akkoord met dit amendement.

B. Stemmingen

Het amendement nr. 4 van de regering, gesubamendeerd door het amendement nr. 17 van de heer Van Quickenborne, wordt eenparig aangenomen door de 10 aanwezige leden.

Artikel 8

A. Bespreking

Mevrouw de T' Serclaes dient amendement nr. 18 (Stuk Senaat, nr. 2-392/2) in om de woorden « hetzij anderszins » in het ontworpen artikel 88*ter*, § 1, te schrappen. Spreekster ziet niet in welke andere onderzoeksdaad dan de huiszoeking in het wetsontwerp beoogd wordt.

Un membre met en garde contre les abus que pourrait engendrer le texte en projet. Une recherche dans un système informatique, dans le cadre d'une perquisition, est soumise à des conditions strictes. Le caractère volatile des données informatiques ne justifie pas que l'on abandonne toutes ces garanties en rendant possibles des «quasi-perquisitions».

L'intervenant met par ailleurs en garde contre le risque non théorique de voir se développer des perquisitions paravents ayant pour but véritable, par la technique de l'extension des recherches, de rassembler des informations dans un autre dossier, ce qui serait totalement inadmissible.

Le ministre explique que le texte ne vise pas seulement des ordinateurs se trouvant par exemple dans un bâtiment, mais aussi des ordinateurs portables ou des téléphones mobiles. Il considère en outre que le texte en projet offre des garanties en prévoyant les conditions dans lesquelles l'extension de recherche est possible.

Un commissaire fait remarquer que la première condition qui prévoit que l'extension doit être nécessaire pour la manifestation de la vérité est une lapalissade. L'intervenant conçoit mal que des actes d'instruction n'aient pas pour but de rechercher la vérité.

En ce qui concerne les autres conditions d'extension des recherches vers un système informatique se trouvant dans un autre lieu (article 88*ter*, § 1er, *in fine*), M. Vandenberghe et Mme Nyssens déposent un amendement nº 6 (doc. Sénat, nº 2-392/2) visant à les rendre cumulatives.

Une commissaire partage ce point de vue et cite un extrait de l'avis nº 33 du 13 décembre 1999 de la Commission de la protection de la vie privée (doc. Chambre, nº 213-4, 99/00, p. 90) selon laquelle «l'extension de la perquisition à d'autres systèmes informatiques ne devrait pouvoir être effectuée que si les trois conditions énoncées dans la disposition sont présentes de façon cumulative».

Le ministre ne peut marquer son accord sur l'amendement proposé: l'extension de la recherche vers des systèmes situés ailleurs doit être possible soit lorsqu'il y a un risque de perdre des éléments de preuve, soit parce que d'autres mesures telles que la délivrance de plusieurs mandats de perquisition seraient disproportionnées. Il s'agit donc de cas de figure différents.

M. Vandenberghe et Mme Nyssens déposent un amendement nº 7 (doc. Sénat, nº 2-392/2) visant à supprimer l'article 88*ter*, § 3 proposé.

Un des auteurs, faisant référence à l'avis du Conseil d'État (doc. Chambre, nº 213/1, 99/00, pp. 45 et

Een lid waarschuwt tegen de misbruiken die de ontworpen tekst zou kunnen meebrengen. Een zoeking in een informaticasysteem, in het kader van een huiszoeking, is aan strikte voorwaarden gebonden. Het vluchtige karakter van de computergegevens rechtvaardigt niet dat men al deze waarborgen opgeeft en «quasi-huiszoekingen» mogelijk maakt.

Spreker waarschuwt voor het overige voor het niet zo theoretische gevaar dat er huiszoekingen worden uitgevoerd die, door de techniek van de uitbreiding van het onderzoek, in werkelijkheid als dekmantel gebruikt worden voor het vergaren van informatie in een ander dossier, hetgeen totaal onaanvaardbaar is.

De minister verklaart dat de tekst niet alleen betrekking heeft op computers die bijvoorbeeld in een gebouw staan maar ook op draagbare computers en telefoons. Hij meent bovendien dat het ontwerp waarborgen biedt door te bepalen onder welke voorwaarden de uitbreiding van het onderzoek mogelijk is.

Een commissielid merkt op dat de eerste voorwaarde, namelijk dat de uitbreiding noodzakelijk is om de waarheid aan het licht te brengen, een gemeenplaats is. Spreker ziet niet goed in hoe onderzoeksdaden niet tot doel zouden hebben de waarheid aan het licht te brengen.

Met betrekking tot de andere voorwaarden om het onderzoek uit te breiden tot een informaticasysteem dat zich op een andere plaats bevindt (artikel 88*ter*, § 1, *in fine*) dienen de heer Vandenberghe en mevrouw Nyssens amendement nr. 6 in dat deze voorwaarden cumulatief wil maken (Stuk Senaat, nr. 2-392/2).

Een commissielid deelt die mening en citeert de bewoordingen van advies nr. 33 van 13 december 1999 van de Commissie voor de bescherming van de persoonlijke levenssfeer (Stuk Kamer, nr. 213/4, 99/00, blz. 90), namelijk dat «de uitbreiding van de huiszoeking naar andere informaticasystemen slechts zou mogen plaatsvinden indien de drie in de voorgestelde bepaling genoemde voorwaarden cumulatief aanwezig zijn».

De minister kan niet akkoord gaan met het voorgestelde amendement: de uitbreiding van het onderzoek naar systemen die zich elders bevinden, moet mogelijk zijn, hetzij wanneer er gevaar bestaat dat bewijselementen verloren gaan, hetzij omdat andere maatregelen als het uitvaardigen van verschillende huiszoekingsbevelen disproportioneel zouden zijn. Het gaat dus om twee verschillende gevallen.

De heer Vandenberghe en mevrouw Nyssens dienen amendement nr. 7 in (Stuk Senaat, nr. 2-392/2) dat de opheffing van het voorgestelde artikel 88*ter*, § 3, beoogt.

Een van de indieners verwijst naar het advies van de Raad van State (Stuk Kamer, nr. 213/1, 99/00, blz. 45

suivantes), estime que la disposition proposée enfreint le principe de territorialité en ce qu'elle permet au juge d'instruction d'investiguer sur des données situées à l'étranger. L'intervenant se pose des questions sur la praticabilité de la procédure envisagée: quel est en effet l'intérêt de charger le ministère de la Justice d'informer l'État étranger alors qu'il n'est pas certain que le comportement incriminé est punissable dans cet État. Il plaide dès lors pour la suppression de cette disposition.

Le ministre fait remarquer que la criminalité informatique ne s'arrête pas aux frontières. Étant donné l'interconnexion des systèmes informatiques, un élément d'extranéité apparaîtra très vite dans le cadre d'une enquête (données stockées à l'étranger, certains éléments constitutifs de l'infraction situés dans plusieurs États différents ...). Comme, par ailleurs, il n'existe pas de conventions internationales fixant les critères de rattachement territoriaux, il n'est pas aisé d'appliquer les principes de territorialité et de souveraineté à la criminalité informatique.

Selon l'intervenant, la solution proposée ne touche pas au principe de territorialité en ce qui concerne la détermination du lieu de l'infraction. En effet, pour déterminer la compétence juridictionnelle du juge belge, il ne faut pas que tous les éléments constitutifs de l'infraction soient localisés en Belgique; il suffit qu'un des éléments le soit.

En ce qui concerne le principe de souveraineté, la procédure envisagée pour étendre les recherches se limite à prévoir une obligation d'information des autorités étrangères lorsque les enquêteurs belges constatent que les résultats de leurs investigations portent sur des données situées à l'étranger. Il appartient à cet État souverain de déterminer les suites qu'il entend réserver à cette information.

Un membre ne partage pas ce point de vue: l'article 88*ter*, § 3, alinéa 2, vise clairement l'hypothèse de données dont on sait qu'elles sont situées à l'étranger. Le libellé est beaucoup plus large que la simple obtention fortuite de données ne se trouvant pas sur le territoire du Royaume.

Un sénateur se rallie à l'intervention de l'orateur précédent: le texte en projet va trop loin par rapport au principe de territorialité en ce qu'il permet d'effectuer sciemment des investigations sur des données localisées à l'étranger.

Le ministre fait remarquer que le texte de l'article 88*ter*, § 3, alinéa 2, prévoit que la procédure s'applique (lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume). Si l'élément d'extranéité est établi *a priori*, les conventions d'entraide judiciaire internationale en matière pénale s'appliquent.

en volgende). Hij is van mening dat de voorgestelde bepaling het territorialiteitsbeginsel schendt omdat de onderzoeksrechter de mogelijkheid wordt verleend om onderzoek te verrichten naar gegevens die zich in het buitenland bevinden. Spreker stelt zich vragen bij de uitvoerbaarheid van de voorgestelde procedure: waartoe dient het immers om het ministerie van Justitie op te dragen de buitenlandse Staat op de hoogte te stellen terwijl het niet zeker is dat het ten laste gelegde gedrag in die Staat strafbaar is? Hij pleit er dan ook voor deze bepaling te schrappen.

De minister merkt op dat computercriminaliteit niet aan de grenzen stopt. Gelet op de onderlinge verbindingen tussen de informaticasystemen, zullen in het onderzoek vrij vlug elementen van buitenlandse oorsprong naar boven komen (gegevens die in het buitenland opgeslagen zijn, een aantal bestanddelen van het misdrijf die zich in verschillende Staten voordoen, ...). Aangezien er voor het overige geen internationale verdragen bestaan die de criteria voor de territoriale aanknoping bepalen, is het niet gemakkelijk de beginselen van territorialiteit en soevereiniteit op de computercriminaliteit toe te passen.

Volgens spreker schendt de voorgestelde oplossing het territorialiteitsbeginsel niet wat de vaststelling van de plaats van het misdrijf betreft. Om de rechtsmacht van de Belgische rechter te bepalen, hoeven immers niet alle bestanddelen van het misdrijf zich in België te bevinden: het is voldoende dat een van de bestanddelen zich in België voordoet.

Wat het soevereiniteitsbeginsel betreft, beperkt de voorgestelde procedure om het onderzoek uit te breiden zich tot een kennisgevingsplicht ten aanzien van de buitenlandse overheden wanneer de Belgische speurders vaststellen dat de resultaten van hun speurwerk betrekking hebben op gegevens die zich in het buitenland bevinden. Deze soevereine Staat moet dan bepalen welk gevolg hij aan deze kennisgeving zal geven.

Een lid deelt deze mening niet: in artikel 88*ter*, § 3, tweede lid, gaat het duidelijk om gegevens waarvan men weet dat ze zich in het buitenland bevinden. De formulering is veel ruimer dan gewoon het toevallig verkrijgen van gegevens die zich niet op het grondgebied van het Rijk bevinden.

Een senator sluit zich aan bij de verklaring van de vorige spreker: de ontworpen tekst gaat veel te ver ten opzichte van het territorialiteitsbeginsel omdat het mogelijk wordt bewust onderzoek te verrichten naar gegevens die zich in het buitenland bevinden.

De minister merkt op dat de tekst van artikel 88*ter*, § 3, tweede lid, bepaalt dat de procedure van toepassing is «wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden». Indien het element van vreemde oorsprong *a priori* bewezen is, zijn de verdragen inzake internationale rechtsbijstand in strafzaken van toepassing.

B. Votes

L'amendement nº 6 de M. Vandenberghe et Mme Nyssens est rejeté par 7 voix contre 2 et 1 abstention.

L'amendement nº 18 de Mme de T'Serclaes est adopté à l'unanimité des 10 membres présents.

L'amendement nº 7 de M. Vandenberghe et Mme Nyssens est rejeté par 7 voix contre 3.

Les articles 9 à 13 ne donnent lieu à aucune observation.

Article 14 — Conservation des données

Pour la discussion de la problématique du délai de conservation, on se réfèrera également à la discussion générale au cours de laquelle cette problématique a été largement évoquée.

A. Discussion

Mme Nyssens dépose un amendement nº 1 (doc. Sénat, nº 2-392/2) visant à introduire à l'article 14, 1º, un délai maximum de 12 mois pour la conservation des données d'appel et d'identification des utilisateurs des services de télécommunications.

Sur le même point, M. Van Quickenborne dépose un amendement nº 12 visant à ramener le délai de conservation des données à 6 mois. Selon l'intervenant, les délais imposés dans les pays voisins sont de trois mois. Il serait injuste d'imposer des délais de conservation plus longs — et dès lors un surcoût non négligeable — aux opérateurs belges. Le délai de six mois est par ailleurs amplement suffisant lorsque l'on constate la rapidité avec laquelle les auteurs d'infractions informatiques peuvent être retrouvés.

Le ministre fait remarquer que la tendance actuelle est de rallonger les délais de conservation des données. Certains pays limitrophes qui imposent des délais de trois mois auxquels l'orateur précédent faisait référence ont tous entamé des procédures de révision à la hausse des délais de conservations des données.

Mme Kaçar propose quant à elle, dans un souci de sécurité juridique, de fixer dans la loi le délai de conservation à 12 mois. C'est le but de son amendement nº 14 (doc. Sénat, nº 2-392/2).

Le ministre se déclare favorable à l'amendement nº 1 de Mme Nyssens. Pour l'intervenant, le délai de 12 mois maximum est un compromis honorable entre le point de vue des opérateurs qui plaident pour le délai le plus court possible et celui des autorités judi-

B. Stemmingen

Het amendement nr. 6 van de heer Vandenberghe en mevrouw Nyssens wordt verworpen met 7 tegen 2 stemmen bij 1 onthouding.

Het amendement nr. 18 van mevrouw de T'Serclaes wordt eenparig aangenomen door de 10 aanwezige leden.

Het amendement nr. 7 van de heer Vandenberghe en mevrouw Nyssens wordt verworpen met 7 tegen 3 stemmen.

Over de artikelen 9 tot 13 zijn geen opmerkingen gemaakt.

Artikel 14 — Bewaring van de gegevens

Voor de bespreking van de problematiek van de bewaringstermijn kan ook worden verwezen naar de algemene bespreking, waar deze problematiek ruimschoots aan bod kwam.

A. Bespreking

Mevrouw Nyssens dient amendement nr. 1 in (Stuk Senaat, nr. 2-392/2) dat ertoe strekt in artikel 14, 1º, een maximumtermijn van 12 maanden in te voeren voor de bewaring van de oproepgegevens en de identificatiegegevens van gebruikers van telecommunicatiediensten.

De heer Van Quickenborne dient amendement nr. 12 in dat ertoe strekt de bewaartermijn tot zes maanden terug te brengen. Volgens spreker gelden in de buurlanden bewaartermijnen van drie maanden. Het is onbillijk om de Belgische operatoren langere bewaartermijnen op te leggen met alle extra-kosten vandien. De termijn van zes maanden volstaat ruimschoots als men ziet hoe snel de daders van informaticamisdrijven kunnen worden opgespoord.

De minister wijst erop dat de bewaartermijnen momenteel overal worden verlengd. Bepaalde buurlanden die termijnen van drie maanden hanteren, hebben allemaal herzieningsprocedures gestart om de bewaartermijnen van de gegevens te verlengen.

Mevrouw Kaçar stelt voor om, met het oog op de rechtszekerheid, in de wet een bewaartermijn van 12 maanden vast te stellen. Daartoe strekt haar amendement nr. 14 (Stuk Senaat, nr. 2-392/2).

De minister sluit zich aan bij amendement nr. 1 van mevrouw Nyssens. Volgens hem is een maximumtermijn van 12 maanden een eervol compromis tussen het standpunt van de operatoren die een zo kort mogelijke termijn willen en dat van de gerechtelijke

ciaires qui souhaitent un délai de 3 ans. Par ailleurs, la solution proposée est la plus souple car elle permet au Roi de fixer un délai plus court en fonction des consultations qui auront lieu avec tous les acteurs concernés.

M. Van Quickenborne dépose un amendement nº 2 (doc. Sénat, nº 2-392/2) visant à imposer au Roi de consulter la Commission de la protection de la vie privée lors de l'élaboration des arrêtés d'exécution définissant les données qui doivent être conservées par les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications. Il s'agit en effet de données sensibles et il est important que les arrêtés d'exécution tiennent compte du respect de la vie privée.

Le ministre confirme que le gouvernement a l'intention de consulter la Commission de la protection de la vie privée ainsi que les acteurs du secteur des télécommunications lors de l'élaboration des arrêtés d'exécution. L'intervenant confirme son accord quant à l'amendement nº 2.

Mme Taelman retire son amendement nº 8 (doc. Sénat, nº 2-392/2) et le remplace par l'amendement nº 19 (doc. Sénat, nº 2-392/2) dont le but est de supprimer l'exigence, pour les opérateurs et fournisseurs de services de télécommunications, de conserver les données à l'intérieur des limites du territoire du Royaume. Le lieu de conservation des données serait dès lors sans importance.

Le gouvernement soutient cet amendement puisqu'il permet d'éviter toute discussion quant à la limitation par la Belgique des règles de concurrence européennes en matière de libre prestation de services. Le texte du projet, en imposant aux opérateurs et fournisseurs de services de télécommunication de conserver leurs données sur le territoire du Royaume, n'était pas à l'abri de critiques.

Plusieurs commissaires se demandent quels seront les moyens de pression dont la justice disposera pour forcer les fournisseurs de services informatiques à collaborer à une enquête à partir du moment où, comme le prévoit l'amendement nº 19, on admet que les données peuvent être stockées partout dans le monde.

Une commissaire estime qu'il ressort des auditions qu'il n'y a pas de problèmes au niveau de la collaboration entre les fournisseurs de services ou les opérateurs et les autorités judiciaires. Un accord de coopération a été conclu sur base volontaire concernant la communication d'informations.

Un sénateur ne partage pas ce point de vue. La police judiciaire a en effet signalé que certains fournisseurs de services américains refusaient systématiquement de collaborer avec les autorités judiciaires.

instanties die een termijn van 3 jaar willen. Dit is ook de meest soepele oplossing omdat de Koning een kortere termijn kan vaststellen na overleg met de betrokkenen.

De heer Van Quickenborne dient amendement nr. 2 in (Stuk Senaat, nr. 2-392/2) dat ertoe strekt de Koning te verplichten om de Commissie voor de bescherming van de persoonlijke levenssfeer te raadplegen bij de redactie van de uitvoeringsbesluiten waarin wordt bepaald welke gegevens de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten moeten bewaren. Het gaat immers om delicate gegevens en in de uitvoeringsbesluiten moet worden gelet op de eerbiediging van de persoonlijke levenssfeer.

De minister bevestigt dat de regering bij de redactie van de uitvoeringsbesluiten de Commissie voor de bescherming van de persoonlijke levenssfeer zal raadplegen en ook mensen uit de telecommunicatiesector. Hij is het dus eens met amendement nr. 2.

Mevrouw Taelman trekt haar amendement nr. 8 in (Stuk Senaat, nr. 2-392/2) en vervangt het door amendement nr. 19 (Stuk Senaat, nr. 2-392/2) dat tot doel heeft het vereiste af te schaffen dat de operatoren en verstrekkers van telecommunicatiediensten gegevens bewaren binnen de grenzen van het Rijk. De plaats waar de gegevens worden bewaard heeft geen belang.

De regering steunt dit amendement omdat daardoor alle discussie wordt voorkomen over eventuele beperkingen die België zou invoeren op de Europese concurrentieregels inzake vrije dienstverlening. Doordat de operatoren en de verstrekkers van telecommunicatiediensten verplicht waren om de gegevens op het Belgisch grondgebied te bewaren, stond de tekst van het ontwerp bloot aan kritiek.

Een aantal commissieleden vraagt zich af over welke middelen het gerecht nog beschikt om de verstrekkers van informaticadiensten te dwingen mee te werken aan een onderzoek als men hen, zoals in amendement nr. 19, toestaat om de gegevens overal ter wereld te bewaren.

Een commissielid is van mening dat uit de hoorzittingen blijkt dat er geen problemen zijn op het niveau van de samenwerking tussen de verstrekkers van informaticadiensten of de operatoren en de gerechtelijke autoriteiten. Er is op vrijwillige basis een samenwerkingsakkoord gesloten over de mededeling van informatie.

Een senator deelt dit standpunt niet. De gerechtelijk politie heeft er immers op gewezen dat bepaalde Amerikaanse verstrekkers van informaticadiensten systematisch weigerden samen te werken met de gerechtelijke autoriteiten.

Pour un autre commissaire, deux options sont possibles : soit la conservation des données sur le territoire du Royaume est contraire au droit européen et il faut alors suivre la solution proposée dans l'amendement nº 8 (conservation sur le territoire de l'Union européenne), soit la conservation des données sur le territoire du Royaume est admise par la Commission européenne et le texte en projet peut rester inchangé.

Le délai de réponse de la Commission européenne à la notification qui lui a été adressée concernant la conformité de l'article 14, 1º, du projet au droit européen venant à échéance le 11 juillet 2000, Mme Taelman décide de retirer son amendement nº 19.

La commission décide dès lors de maintenir le texte du projet dans l'attente d'informations complémentaires.

Un sénateur s'interroge sur la manière dont les responsabilités seront départagées, par exemple entre l'étudiant qui cause un dommage par la dispersion d'un virus, et l'université à laquelle il appartient.

Le même intervenant se réfère à la définition donnée aux Pays-Bas aux notions de « données » et de « système informatique ».

Qu'en est-il dans le cadre de la présente loi ?

Enfin, de quels instruments dispose-t-on lorsque des infractions se commettent dans le cadre de l'envoi d'e-mails ? Il arrive en effet que des e-mails soient envoyés en nombre tel que cela a pour conséquence de bloquer le système de celui qui les reçoit, en l'empêchant de communiquer avec des tiers.

Le ministre renvoie, en ce qui concerne le premier point, à la loi sur la responsabilité pénale des personnes morales. Il est également fait référence aux principes généraux en matière de responsabilité pénale et de participation.

En ce qui concerne la définition de certains concepts, il paraît préférable de ne pas l'intégrer dans le texte de la loi, car elle risquerait d'être rapidement dépassée par l'évolution technologique.

Enfin, en ce qui concerne l'envoi d'e-mails en masse, aboutissant à bloquer le système du destinataire, il y a lieu de se référer, s'il s'agit d'un contexte commercial, à la loi du 14 juillet 1991 sur les pratiques du commerce.

En outre, le présent projet vise, en son article 550*ter*, § 3, ce cas de sabotage informatique.

Si l'envoi massif d'e-mails a les conséquences décrites ci-avant, il empêche le fonctionnement correct d'un système informatique — dont l'une des fonc-

Voor een ander commissielid zijn er twee keuzes mogelijk : ofwel is de bewaring van de gegevens op het grondgebied van het Rijk strijdig met het Europees recht en moet gekozen worden voor de oplossing die wordt voorgesteld in amendement nr. 8 (bewaring op het grondgebied van de Europese Unie) ofwel wordt de bewaring van de gegevens op het grondgebied van het Rijk door de Europese Commissie toegestaan en kan de ontwerptekst ongewijzigd blijven.

Daar de termijn waarbinnen de Europese Commissie moet antwoorden op de vraag die haar gesteld werd over de overeenstemming van artikel 14, 1º, van het ontwerp met het Europees recht, verstrijkt op 11 juli 2000, besluit mevrouw Taelman haar amendement nr. 19 in te trekken.

De commissie besluit derhalve de tekst van het ontwerp te behouden in afwachting van aanvullende informatie.

Een senator stelt zich vragen over de manier waarop de verantwoordelijkheid zal worden gedeeld, bijvoorbeeld tussen de student die schade veroorzaakt door de verspreiding van een virus en de universiteit waartoe hij behoort.

Dezelfde spreker verwijst naar de definitie die in Nederland gegeven wordt aan de begrippen « gegevens » en « informaticasysteem ».

Kan dat ook in dit ontwerp ?

Over welke instrumenten beschikt men tenslotte wanneer misdrijven gepleegd worden bij het versturen van e-mails ? Het gebeurt immers dat het massaal versturen van e-mails de blokkering tot gevolg heeft van het systeem van degene die ze ontvangt, waardoor elke communicatie met derden verhinderd wordt.

De minister verwijst, wat het eerste punt betreft, naar de wet op de strafrechtelijke verantwoordelijkheid van rechtspersonen. Er wordt eveneens verwezen naar de algemene regels inzake strafrechtelijke verantwoordelijkheid en deelneming.

Wat de definitie van bepaalde begrippen betreft, lijkt het verkieslijk in de wettekst geen definities op te nemen want ze zouden wel eens snel verouderd kunnen zijn ingevolge de technologische ontwikkelingen.

Wat het massaal versturen van e-mails betreft die het systeem van de geadresseerde blokkeren, moet verwezen worden, indien het gaat om een commerciële context, naar de wet van 14 juli 1991 op de handelspraktijken.

Deze wet beoogt daarenboven in artikel 550*ter*, § 3, het geval van de computersabotage.

Heeft het massale versturen van e-mails de hierboven beschreven gevolgen, dan wordt daardoor de correcte werking van een computersysteem — waar-

tionnalités est la communication avec les tiers — et tombe dès lors sous le coup de l'article en question.

Votes

Les amendements nos 8 et 19 de Mme Taelman sont retirés.

L'amendement no 1 de Mme Nyssens est adopté par 9 voix et 1 abstention.

L'amendement no 2 de M. Van Quickenborne est rejeté à l'unanimité des 10 membres présents.

L'amendement no 14 de Mme Kaçar est rejeté par 9 voix contre 1.

V. VOTE FINAL

L'ensemble du projet de loi amendé a été adopté à l'unanimité des 10 membres présents.

Confiance a été faite aux rapporteurs pour la rédaction de ce rapport.

Les rapporteurs, *Le président,*
Jean-François ISTASSE. Josy DUBIÉ.
Meryem KAÇAR.

van de communicatie met derden een belangrijke functie is — verhinderd en is het bovenvermelde artikel van toepassing.

Stemmingen

De amendementen nrs. 8 en 19 van mevrouw Taelman worden ingetrokken.

Amendement nr. 1 van mevrouw Nyssens wordt aangenomen met 9 stemmen bij 1 onthouding.

Amendement nr. 2 van de heer Van Quickenborne wordt door de 10 aanwezige leden eenparig verworpen.

Amendement nr. 14 van mevrouw Kaçar wordt met 9 stemmen tegen 1 stem verworpen.

V. EINDSTEMMING

Het geamendeerde wetsontwerp in zijn geheel is eenparig aangenomen door de 10 aanwezige leden.

Vertrouwen werd geschonken aan de rapporteurs voor het uitbrengen van dit verslag.

De rapporteurs, *De voorzitter,*
Jean-François ISTASSE. Josy DUBIÉ.
Meryem KAÇAR.

57.629 — E. Guyot, s. a., Bruxelles