DOC 50 **0213/004**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

24 maart 2000

# WETSONTWERP

**inzake informaticacriminaliteit (I)**

# WETSONTWERP

**inzake informaticacriminaliteit (II)**

---

## VERSLAG

NAMENS DE COMMISSIE
VOOR DE JUSTITIE
UITGEBRACHT DOOR
DE HEER **Servais VERHERSTRAETEN**

---

INHOUDSOPGAVE



Voorgaande documenten :

DOC 50 **213 (1999-2000) :**
01 : Wetsontwerp.
02 en 03 : Amendementen.

*Zie ook :*
05 : Tekst aangenomen door de commissie.

DOC 50 **214 (1999-2000) :**
01 : Wetsontwerp.
02 tot 06 : Amendementen.

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

24 mars 2000

# PROJET DE LOI

**relatif à la criminalité informatique (I)**

# PROJET DE LOI

**relatif à la criminalité informatique (II)**

---

## RAPPORT

FAIT AU NOM DE LA COMMISSION
DE LA JUSTICE
PAR
M. **Servais VERHERSTRAETEN**

---

SOMMAIRE



Documents précédents :

DOC 50 **213 (1999-2000) :**
01 : Projet de loi.
02 et 03 : Amendements.

*Voir aussi :*
05 : Texte adopté par la commission.

DOC 50 **214 (1999-2000) :**
01 : Projet de loi.
02 à 06 : Amendements.

**Samenstelling van de commissie op datum van indiening van het verslag /**
**Composition de la commission à la date du dépôt du rapport :**
Voorzitter / Président : Fred Erdman.

| | A. — **Vaste leden / Titulaires** | B. — **Plaatsvervangers / Suppléants** |
|---|---|---|
| VLD | Hugo Coveliers, Guy Hove, Bart Somers. | Stef Goris, Fientje Moerman, Geert Versnick, Kathleen van der Hooft. |
| CVP | Jo Vandeurzen, Tony Van Parys, Servais Verherstraeten. | Simonne Creyf, Yves Leterme, Trees Pieters, Joke Schauvliege. |
| Agalev/Ecolo | Vincent Decroly, Fauzaya Talhaoui. | Anne-Mie Descheemaeker, Mirella Minne, Géraldine Pelzer-Salandra. |
| PS | André Frédéric, Thierry Giet. | Maurice Dehu, Claude Eerdekens, Patrick Moriau. |
| PRL FDF MCC | Jacqueline Herzet, Charles Michel. | Pierrette Cahay-André, Claude Desmedt, Olivier Maingain. |
| Vlaams Blok | Bart Laeremans, Bert Schoofs. | Gerolf Annemans, Alexandra Colen, Filip De Man. |
| SP | Frederik Erdman. | Erik Derycke, Peter Vanvelthoven. |
| PSC | Joëlle Milquet. | Jean-Pierre Grafé, Jean-Jacques Viseur. |
| VU&ID | Geert Bourgeois. | Danny Pieters, Karel Van Hoorebeke. |

| | | |
|---|---|---|
| *AGALEV-ECOLO* | *:* | *Anders Gaan Leven / Écologistes Confédérés pour l'Organisation de luttes originales* |
| *CVP* | *:* | *Christelijke Volkspartij* |
| *FN* | *:* | *Front national* |
| *PRL FDF MCC* | *:* | *Parti Réformateur libéral - Front démocratique francophone-Mouvement des Citoyens pour le Changement* |
| *PS* | *:* | *Parti socialiste* |
| *PSC* | *:* | *Parti social-chrétien* |
| *SP* | *:* | *Socialistische Partij* |
| *VLAAMS BLOK* | *:* | *Vlaams Blok* |
| *VLD* | *:* | *Vlaamse Liberalen en Democraten* |
| *VU&ID* | *:* | *Volksunie&ID21* |

*Afkortingen bij de nummering van de publicaties :*

| | | |
|---|---|---|
| *DOC 50 0000/000* | *:* | *Parlementair document van de 50e zittingsperiode + het nummer en het volgnummer* |
| *QRVA* | *:* | *Schriftelijke Vragen en Antwoorden* |
| *HA* | *:* | *Handelingen (Integraal Verslag)* |
| *BV* | *:* | *Beknopt Verslag* |
| *PLEN* | *:* | *Plenum* |
| *COM* | *:* | *Commissievergadering* |

*Abréviations dans la numérotation des publications :*

| | | |
|---|---|---|
| *DOC 50 0000/000* | *:* | *Document parlementaire de la 50e législature, suivi du n° et du n° consécutif* |
| *QRVA* | *:* | *Questions et Réponses écrites* |
| *HA* | *:* | *Annales (Compte Rendu Intégral)* |
| *CRA* | *:* | *Compte Rendu Analytique* |
| *PLEN* | *:* | *Séance plénière* |
| *COM* | *:* | *Réunion de commission* |

*Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers*
*Bestellingen :*
*Natieplein 2*
*1008 Brussel*
*Tel. : 02/ 549 81 60*
*Fax : 02/549 82 74*
*www.deKamer.be*
*e-mail : alg.zaken@deKamer.be*

*Publications officielles éditées par la Chambre des représentants*
*Commandes :*
*Place de la Nation 2*
*1008 Bruxelles*
*Tél. : 02/ 549 81 60*
*Fax : 02/549 82 74*
*www.laChambre.be*
*e-mail : aff.generales@laChambre.be*

DAMES EN HEREN,

Uw commissie heeft deze wetsontwerpen besproken tijdens haar vergaderingen van 24 en 30 november 1999, 1 december 1999, 15 en 29 februari en 21 maart 2000.



MESDAMES, MESSIEURS,

Votre commission a examiné ces projets de loi au cours de ses réunions des 24 et 30 novembre, 1er décembre 1999, 15 et 29 février et 21 mars 2000.

## I. — INLEIDING VAN DE HEER MARC VERWILGHEN, MINISTER VAN JUSTITIE

Dit wetsontwerp heeft al een lange voorgeschiedenis achter de rug en vormt er deels een logisch verlengstuk van. Het vraagstuk van de computercriminaliteit is immers niet nieuw. Zo had de vorige regering al een voorontwerp van wet voor advies aan de Raad van State voorgelegd. Daarnaast vormt het ter bespreking voorliggende wetsontwerp eveneens een logisch en concreet vervolg op de werkzaamheden die terzake zijn verricht binnen de OESO en de Raad van Europa.

Uit het oogpunt van zowel de overheid, de bedrijfswereld als de particuliere burger, is de strafrechtelijke bescherming van computernetwerken een noodzaak. De informaticatechnologie vormt niet alleen een middel om criminele feiten te plegen, ze is zelf ook het doelwit van criminele activiteiten.

Teneinde de diverse gerechtelijke instanties de nodige middelen te verschaffen om tegen die vorm van criminaliteit op te treden, voorziet het wetsontwerp in twee benaderingswijzen. Enerzijds wordt zoveel mogelijk getracht gebruik te maken van het Strafwetboek en het Wetboek van strafvordering, zonder dat zulks evenwel diepgaande structurele hervormingen vereist. Anderzijds worden ook nieuwe misdrijven in de wet opgenomen, waarbij het vooral de bedoeling is om, inzake de strafbaarstelling van bepaalde vormen van misbruik van informaticatechnologie, te voorkomen dat overdreven veel feiten strafbaar worden gesteld.

Vier categorieën van misdrijven worden aldus ingevoerd : valsheid in informatica, informaticabedrog, ongeoorloofde toegang tot informaticasystemen (informaticapiraterij zowel van binnenuit als van buitenaf) en data- en informaticasabotage.

Voor het overige worden in het Wetboek van strafvordering een aantal nieuwigheden ingevoegd met betrekking tot de daden die, in zaken van computercriminaliteit, worden verricht in het raam van het opsporingsonderzoek en het gerechtelijk onderzoek. Het betreft vooral bepalingen met betrekking tot de inbeslagname van gegevens, onderzoekswerk op netwerken, bijzondere medewerkingsverplichtingen in een informaticaomgeving, alsook aanpassingen op het vlak van de opsporingstechnieken en het afluisteren van telefoongesprekken.

Tot slot wordt ook de telecommunicatiewetgeving aangepast, zodat de Koning de verplichtingen inzake identificatie en bewaring nader kan preciseren.

Vervolgens geeft de minister de inhoud van een verklarende nota weer, met daarin de voornaamste beginselen die aan dit wetsontwerp ten grondslag liggen.

## I. — EXPOSÉ INTRODUCTIF DE M. MARC VERWILGHEN, MINISTRE DE LA JUSTICE

Le présent projet de loi a déjà connu une longue histoire qui s'inscrit pour partie dans la continuité. Les problèmes relatifs à la criminalité informatique ne sont en effet pas neufs. Le précédent gouvernement avait quant à lui, déjà soumis un avant-projet de loi au Conseil d'État. La continuité se rencontre aussi au niveau de la traduction que réalise le présent projet de loi des travaux menés au sein de l'OCDE et du Conseil de l'Europe.

La nécessité de protéger pénalement les réseaux informatiques se situe aux niveaux de l'autorité publique, des entreprises et des particuliers. L'informatique ne constitue pas uniquement un moyen pour commettre un délit, mais est devenue en elle-même un objectif de criminalité.

Afin de donner aux acteurs de la Justice les instruments pour lutter contre cette forme de criminalité, le projet de loi a retenu deux approches. D'une part, il essaie de se raccrocher tant au Code pénal qu'au Code d'instruction criminelle sans apporter de profondes réformes structurelles. D'autre part, en ce qui concerne l'introduction de nouveaux délits, il s'est penché sur l'incrimination de certains abus en matière de technologie de l'information afin d'éviter une criminalisation excessive.

Quatre nouvelles incriminations sont créées, à savoir le faux en informatique, la fraude informatique, l'accès non autorisé (piratage informatique de l'intérieur comme de l'extérieur) et le sabotage tant de données que de systèmes.

Par ailleurs, 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 de dépistage et d'interception de télécommunications.

Enfin, la législation sur les télécommunications est également adaptée afin de permettre au Roi de préciser les obligations d'identification et de conservation.

Le ministre donne ensuite connaissance d'une note explicative reprenant les principaux principes retenus par le présent projet.

« *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 (x 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. **Valsheid in informatica**

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

— Het 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.

— Het gebruik van valse gegevens.

— Poging tot valsheid in informatica wordt eveneens strafbaar gesteld

2. **Informaticabedrog**

Hieronder wordt verstaan de gerealiseerde computerfraude. Voorbeelden van de gevallen die geviseerd worden zijn : het gebruik van een gestolen kredietkaart om geld uit een automatische biljettenverdeler te halen, het onrechtmatig overschrijden van het krediet van zijn eigen kredietkaart, het invoeren van programma-instructies waardoor bepaalde verrichtingen een ander resultaat opleveren met het oog op het bekomen van een onrechtmatig financieel voordeel, het met winstbejag verduisteren van bestanden of programma's die men enkel voor een welbepaald doel toevertrouwd heeft gekregen.

Poging tot informaticabedrog wordt eveneens strafbaar gesteld.

Deze bepaling 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.

3. **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.

« *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 (x 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. **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 crédits, 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.

2. **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.

3. **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.

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

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, nl. 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 :

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

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

— 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.

Daarnaast worden eveneens een aantal voorbereidingshandelingen tot het *hacken* strafbaar gesteld, meer bepaald : het handelen in *hackertools* en toegangscodezwendel.

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 crimi-

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.

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 avec 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 accordée doit se faire dans un but délibéré de nuire, notamment dans un but lucratif illicite ou avec des intentions malveillantes.

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 punisables sous la forme de circonstances aggravantes de l'infraction de base, sous ses deux variantes, notamment :

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

— 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 »;

— 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* ». Etant donné que, traditionnellement, le recel ne concerne que des biens matériels, cette disposition est surtout importante dans le contexte de l'espionnage industriel.

En outre, un certain nombre d'actes préparatoires au « *hacking* » sont également punissables, en particulier le commerce de « *hackertools* » et le trafic des codes d'accès.

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

nelen dergelijke personen inschakelen om hun plannen uit te voeren.

Gezien de ernst van de gedragingen wordt wat de poging betreft, dezelfde strafmaat voorzien als het voltooide misdrijf. Nemen we hierbij als voorbeeld het geautomatiseerd uitproberen van paswoorden, waarbij de dader eerder geïnteresseerd is in het bekomen van de toegangscode op zich dan in het effectief binnenbreken in de computer.

4. **Data- en informaticasabotage**

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.

Zowel de poging tot sabotage (bijvoorbeeld het inbrengen van virussen), de voltooide datasabotage (bijvoorbeeld vernietigde bestanden), voltooide systeemsabotage (bijvoorbeeld het onbruikbaar maken van harddisks, ontregeling van besturingssystemen) als zekere voorbereidingshandelingen (bijvoorbeeld het ontwerpen en verspreiden van enig middel om computersabotage te plegen) worden strafbaar gesteld.

*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 speci-

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

4. **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.

Tant la tentative de sabotage (par exemple l'introduction de virus), le sabotage de données même (par exemple, la destruction de fichiers), le sabotage du système (par exemple, rendre les disques durs inutilisable, dérégler le système d'exploitation), que certains actes préparatoires (par exemple, développer et distribuer tout moyen permettant le sabotage informatique) sont punissables.

*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

fieke 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. 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.

Nieuw is ook de bepaling die betrekking heeft op de :

### 1. **Netwerkzoeking**

Wanneer een onderzoeksrechter een zoeking verricht in een informaticasysteem, kan hij deze zoeking uitbreiden naar een informaticasysteem dat zich op een

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);

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.

Une nouvelle disposition porte également sur ce qui suit :

### 1. **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

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 zoverre dit noodzakelijk is in het kader van de concrete strafzaak waarmee de onderzoeksrechter belast 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.

Bovendien moet de technische verbinding via de netwerken een element van permanentie en stabiliteit inhouden en mag niet louter occasioneel zijn.

Het is evenmin toegelaten dat de overheidsdiensten via onder meer eigen informaticasystemen binnen zouden dringen in andere systemen die niet openstaan voor het publiek en die ervan verdacht worden aangewend te worden voor criminele doeleinden.

« *Hacking* » door de overheid als nieuwe, geheime bewakingsmaatregel, is verboden.

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.

Uiteraard kan de onderzoeksrechter, zoals voorzien inzake huiszoekingen, zijn bevoegdheid inzake « netwerkzoeking » delegeren aan een officier van gerechtelijke politie, hulpofficier van de procureur des Konings.

2. **Medewerkingsverplichtingen**

Een verdere ingrijpende wijziging is het voorzien van een aantal bijzondere medewerkingsverplichtingen in een geïnformatiseerde omgeving.

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

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, le risque de perdre des éléments de preuve sans cette extension doit être présent ou le juge d'instruction doit estimer que d'autres mesures (par exemple, plusieurs mandats d'arrêt) sont disproportionnées.

Il appartient au juge d'instruction d'apprécier en toute équité ce qui précède.

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

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

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

Les services publics ne sont pas habilités, par le biais de leurs propres systèmes informatiques, à accéder dans d'autres systèmes qui ne sont pas publics et dont on suspecte qu'ils sont utilisés à des fins criminelles.

Il est strictement interdit aux pouvoirs publics d'utiliser le « *hacking* » comme un nouveau système de surveillance secret.

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.

Bien entendu, comme prévu en matière de perquisitions, le juge d'instruction peut déléguer ses compétences de « recherches sur réseaux » à un officier de police judiciaire, auxiliaire du procureur du Roi.

2. **Obligations de coopération**

Un changement plus radical consiste à prévoir un certain nombre d'obligations de coopération particulières dans un environnement informatisé.

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 des personnes qui connaissent le système informatique à examiner, ou qui possèdent une certaine expertise dans certains de ses aspects (par exemple en

encryptie) te kunnen verplichten de gerechtelijke overheid bij te staan.

Hiertoe wordt in twee soorten verplichtingen 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 ».

3. **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.

4. **Verantwoordelijkheid voor de toegebrachte schade**

De burgers die in het kader van deze bepaling verplicht worden mee te werken aan een strafrechtelijk onderzoek, kunnen hierbij schade veroorzaken aan informaticasystemen of data.

Het zou onredelijk zijn dat deze personen hiervoor burgerlijk aansprakelijk zouden worden gesteld, 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 vertrouwelijk-

matière de protection ou de cryptage), soient obligées d'assister les autorités judiciaires.

Ces obligations sont de deux ordres :

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 pour exécuter 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.

3. **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 l'entrave d'une instruction relative à un système informatique seront sanctionnés pénalement.

4. **Responsabilité du dommage causé**

Les citoyens qui, dans le cadre de cette disposition, sont obligés de participer à une enquête criminelle, 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 soit responsable du dommage non intentionnel causé dans le cadre du respect de l'obligation de collaborer.

Le projet de loi vise également une adaptation du régime des écoutes de télécommunications par les services judiciaires. Trois modifications sont apportées :

1. La liste d'infractions autorisant une mesure de mise sur écoute est élargie aux infractions existantes dans le domaine de l'écoute de 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

heid 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 worden gedacht 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 telecommunicatie 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 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.

Het komt ook de Koning toe de periode van bewaring van deze gegevens te bepalen, rekening houdend met de technische en praktische haalbaarheidsfactoren voor de dienstverleners.

Naast deze strafrechtelijk gesanctioneerde verplichting voor de verstrekkers van telecommunicatiedien-

l'intégrité de matériels d'écoute (qui sera de plus en plus souvent numérique), 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 de la loi.

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

Si dans ce cadre il a été opté pour le mot « 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 promulguer 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.

Le Roi déterminera la durée de conservation de ces données, en tenant compte d'aspects de faisabilité techniques et pratiques dans le chef des fournisseurs.

Outre cette obligation imposée aux fournisseurs de télécommunications, dont le non-respect est sanction-

sten wordt tevens voorzien dat de gegevens die zij zullen moeten bewaren, technisch afdoende worden beveiligd vanuit het oogpunt van confidentialiteit en integriteit. »

né 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. »

**Valsheid in informatica**

**Faux en informatique**

| | DELICTOMSCHRIJVING. — *DÉFINITION DE L'INFRACTION* | STRAFMAAT — *PEINE* |
|---|---|---|
| VALSHEID IN INFORMATICA. — *FAUX EN INFORMATIQUE.*<br>(via datamanipulatie vervalsen van juridisch relevante computergegevens). — *(falsification de données informatiques pertinentes sur le plan juridique par manipulation de données).*<br><br>Bv. : vervalsen/namaken van kredietkaarten, valsheid inzake « digitale contracten ». — *Ex. : falsification/ contrefaçon de cartes de crédit, faux en matière de « contrats digitaux ».* | Hij die valsheid pleegt, door gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, in te voeren in een informaticasysteem, te wijzigen, te wissen of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, waardoor de juridische draagwijdte van dergelijke gegevens verandert. — *Celui qui commet un faux, en introduisant dans un système informatique, modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données.* | — gevangenisstraf van 6 maanden tot 5 jaar of — *emprisonnement de 6 mois à 5 ans ou*<br>— geldboete van 26 frank tot 100 000 frank (x 200 door toepassing van de opdecimes). — *amende de 26 francs à 100 000 francs (x 200 par application des décimes additionnels).* |
| GEBRUIK VAN VALSE GEGEVENS. — *USAGE DE FAUSSES DONNÉES.* | Hij die, terwijl hij weet dat aldus bekomen gegevens vals zijn, hiervan gebruik maakt, wordt gestraft alsof hij de dader van de valsheid was zelfde straf. — *Celui qui fait usage des données ainsi obtenues, tout en sachant que celles-ci sont fausses, est puni comme s'il était l'auteur du faux.* | zelfde straf. — *peine identique.* |
| POGING. — *TENTATIVE.* | Poging tot het plegen van het misdrijf, bedoeld in § 1. — *Tentative de commettre l'infraction prévue au § 1er.* | — gevangenisstraf van 6 maanden tot 3 jaar of. — *emprisonnement de 6 mois à 3 ans ou*<br>— geldboete van 26 frank tot 50 000 frank. — *amende de 26 francs à 50 000 francs.* |
| BIJZONDER REGIME VAN HERHALING. — *RÉGIME PARTICULIER EN MATIÈRE DE RÉCIDIVE.* | De straffen gesteld in de §§ 1 tot 3 worden verdubbeld indien een overtreding van één van die bepalingen wordt begaan binnen 5 jaar na de uitspraak van een vonnis of arrest houdende veroordeling wegens één van die strafbare feiten of wegens één van de strafbare feiten bedoeld in de artikelen 259*bis*, 314*bis*, 504*quater* of in Titel IX*bis* van dit Wetboek. — *Les peines portées par les §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent un jugement ou un arrêt de condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 259*bis*, 314*bis*, 504*quater *ou au titre IX*bis *du Code pénal.* | verdubbeling van de voorziene strafmaat. — *doublement de la peine prévue.* |

**Informaticabedrog** | **Fraude informatique**

| | DELICTOMSCHRIJVING. — *DÉFINITION DE L'INFRACTION* | STRAFMAAT — *PEINE* |
|---|---|---|
| POGING TOT INFORMATICABEDROG. — *TENTATIVE DE FRAUDE INFORMATIQUE.*<br>(bedrieglijke gegevensmanipulatie om zich te verrijken). — *(manipulation frauduleuse de données aux fins de s'enrichir).* | Hij die, met het oogmerk voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel te verwerven, gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, in een informaticasysteem invoert, wijzigt, wist of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem verandert. — *Celui qui, en vue de se procurer pour soi-même ou pour autrui un avantage patrimonial frauduleux, introduit dans un système informatique, modifie ou efface des données qui sont stockées, traitées ou transmises par un système informatique, ou modifie par tout moyen technologique l'utilisation possible des données dans un système informatique.* | — gevangenisstraf van 6 maanden tot 3 jaar of — *emprisonnement de 6 mois à 3 ans ou*<br>— geldboete van 26 frank tot 50 000 frank. — *amende de 26 francs à 50 000 francs.* |
| INFORMATICABEDROG. — *FRAUDE INFORMATIQUE.*<br>(de gerealiseerde computerfraude). — *(fraude informatique accomplie).* | Hij die, door het misdrijf bedoeld in § 1 te plegen, voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwerft. — *Celui qui, par la commission de l'infraction visée au § 1er, obtient pour soi-même ou pour autrui un avantage patrimonial frauduleux.* | — gevangenisstraf van 6 maanden tot 5 jaar of. — *emprisonnement de 6 mois à 5 ans ou*<br>— geldboete van 26 frank tot 100 000 frank. — *amende de 26 francs à 100 000 francs.* |
| BIJZONDER REGIME VAN HERHALING. — *RÉGIME PARTICULIER EN MATIÈRE DE RÉCIDIVE.* | De straffen gesteld in §§ 1 en 2 worden verdubbeld indien een overtreding van één van die bepalingen wordt begaan binnen 5 jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens één van die strafbare feiten of wegens één van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis* of in Titel IX*bis* van dit Wetboek. — *Les peines portées par les §§ 1er et 2 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans qui suivent un jugement ou un arrêt de condamnation pour une de ces infractions ou pour une des infractions prévues aux articles 210*bis*, 259*bis*, 314*bis *ou au titre IX*bis *du Code pénal.* | verdubbeling van de strafmaat. — *doublement de la peine.* |

| **Ongeoorloofde toegang tot een informaticasysteem** | **Accès non autorisé** |
|---|---|

| | DELICTOMSCHRIJVING. — *DÉFINITION DE L'INFRACTION* | STRAFMAAT — *PEINE* |
|---|---|---|
| ONGEOORLOOFDE TOEGANG (OUTSIDERS). — *ACCÈS NON AUTORISÉ.*<br>(*hacking* door mensen van buiten de organisatie). — *(piratage informatique de l'extérieur).*<br><br>Bv. : via de openbare telecominfrastructuur de beveiliging van een gesloten netwerk omzeilen en zich aldus toegang verschaffen tot het systeem. — *Ex. : contourner via l'infrastructure de télécommunication publique les défenses d'un réseau fermé et ainsi accéder au système.* | Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft. — *Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient.*<br><br>Het voormelde misdrijf wordt gepleegd met een bedrieglijk opzet. — *Si l'infraction visée au premier alinéa, est commise avec une intention frauduleuse.* | — gevangenisstraf van 3 maanden tot 1 jaar of — *emprisonnement de 3 mois à 1 an ou*<br>— geldboete van 26 frank tot 25 000 frank. — *amende de 26 francs à 25 000 francs.*<br><br>— gevangenisstraf van 6 maanden tot 2 jaar of — *emprisonnement de 6 mois à 2 ans ou*<br>— dezelfde geldboete. — la *même amende.* |
| ONGEOORLOOFDE TOEGANG (INSIDERS). — *ACCÈS NON AUTORISÉ.*<br><br>(*hacking* door mensen die principieel toegang hebben tot een deel van het netwerk). — *(piratage informatique de l'intérieur).*<br><br>Bv. : in delen van een intern bedrijfsnetwerk binnendringen waartoe men niet bevoegd is teneinde schade te berokkenen of bepaalde data voor eigen rekening te commercialiseren. — *Ex. : pénétrer dans des parties du réseau d'entreprise interne auxquelles on n'est pas autorisé à accéder en vue de causer des dommages ou de commercialiser certaines données pour son propre compte.* | Hij die, met bedrieglijk opzet of met het oogmerk te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt. — *Celui qui, avec intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique.* | — gevangenisstraf van 6 maanden tot 2 jaar of — *emprisonnement de 6 mois à 2 ans ou*<br>— geldboete van 26 frank tot 25 000 frank. — *amende de 26 francs à 25 000 francs.* |
| POGING. — *TENTATIVE.* | Poging tot het plegen van één van de misdrijven, bedoeld in §§ 1 en 2, wordt gestraft met de straffen gesteld op het misdrijf zelf. — *La tentative de commettre une des infractions prévues aux §§ 1er et 2 est punie.* | Zelfde straf als op het voltooide misdrijf. — *Même peine que pour l'infraction accomplie.* |
| VERZWARENDE OMSTANDIGHEDEN. — *CIRCONSTANCES AGGRAVANTES.*<br>1° « ontvreemden » van gegevens n.a.v. de *hacking*; bv. in het kader van bedrijfsspionage. — *1° « vol » de données; espionnage.*<br>2° misbruiken van de capaciteit van de computer waar de persoon is binnengedrongen; « tijdsdiefstal ». — *2° usage abusif des capacités de l'ordinateur; « vol de temps ».*<br>3° al dan niet gewild schade toebrengen na de *hacking*. — *3° dommages.* | Hij die zich in één van de gevallen van § 1er en 2 bevindt, en, naar aanleiding daarvan : — *Celui qui se trouve dans une des situations prévues par les §§ 1er et 2 et qui, à cette occasion :*<br>1° hetzij kennisneemt van gegevens die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem of deze op enige manier overneemt. — 1° *soit prend connaissance de données qui sont stockées, traitées ou transmises par un système informatique ou prend de telles données de quelque manière que ce soit.*<br>2° hetzij enig gebruik maakt van een informaticasysteem. — *2° soit fait tout usage d'un système informatique.*<br>3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan een informaticasysteem of aan gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. — *3° soit cause tout dommage, même non intentionnellement, à un système informatique ou à des données qui sont stockées, traitées ou transmises par un tel système.* | — gevangenisstraf van 1 jaar tot 3 jaar of — *emprisonnement de 1 à 3 ans ou*<br>— geldboete van 26 frank tot 50 000 frank. — *amende de 26 francs à 50 000 francs.* |

| **Ongeoorloofde toegang tot een informaticasysteem (*vervolg*)** | **Accès non autorisé (*suite*)** |
|---|---|

| | DELICTOMSCHRIJVING. — *DÉFINITION DE L'INFRACTION* | STRAFMAAT — *PEINE* |
|---|---|---|
| VOORBEREIDINGSHANDELINGEN. — *ACTES PRÉPARATOIRES.*<br><br>Bv. : paswoordenzwendel, *hackertools*. — *Ex. : trafic de mots de passe;* hackertools. | Hij die, met bedrieglijk opzet of met het oogmerk te schaden, gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem en waarmee de misdrijven, bedoeld in §§ 1 tot 4, gepleegd kunnen worden, opspoort, verzamelt, ter beschikking stelt, verspreidt of verhandelt. — *Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1er à 4 peuvent être commises.* | — gevangenisstraf van 6 maanden tot 3 jaar of — *emprisonnement de 6 mois à 3 ans ou*<br>— geldboete van 26 frank tot 100 000 frank. — *amende de 26 francs à 100 000 francs.* |
| OPDRACHTGEVEN TOT *HACKING*. — HACKING *SUR COMMANDE.*<br><br>Bv. : criminele organisaties die een beroep doen op jeugdige hackers om toegangscodes te kraken. — *Ex. : organisations criminelles qui font appel à de jeunes pirates informatiques pour craquer des codes d'accès.* | Hij die opdracht geeft of aanzet tot het plegen van één van de misdrijven, bedoeld in §§ 1 tot 5. — *Celui qui ordonne la commission d'une des infractions prévues aux §§ 1er à 5 ou qui y incite.* | — gevangenisstraf van 6 maanden tot 5 jaar of — *emprisonnement de 6 mois à 5 ans ou*<br>— geldboete van 100 frank tot 200 000 frank. — *amende de 100 francs à 200 000 francs.* |
| HELING VAN VIA HACKING BEKOMEN DATA. — *RECEL DE DONNÉES OBTENUES PAR PIRATAGE INFORMATIQUE*.<br>(misbruiken van via hacking bekomen data). — *(usage abusif de données obtenues par piratage informatique).* | Hij die terwijl hij weet dat gegevens bekomen zijn door het plegen van één van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt. — *Celui qui, sachant que des données ont été obtenues par la commission d'une des infractions prévues aux §§ 1er à 3, les détient, les révèle à une autre personne ou les divulgue, ou en fait un usage quelconque.* | — gevangenisstraf van 6 maanden tot 3 jaar of — *emprisonnement de 6 mois à 3 ans ou*<br>— geldboete van 26 frank tot 100 000 frank. — *amende de 26 francs à 100 000 francs.* |
| BIJZONDER REGIME VAN HERHALING. — *RÉGIME PARTICULIER EN MATIÈRE DE RÉCIDIVE.* | § 8. De straffen gesteld in de §§ 1 tot 7 worden verdubbeld enz. — *Les peines portées par les §§ 1er à 7 sont doublées, etc.* | verdubbeling van de straf-maat. — *doublement de la peine.* |

**Data- en informaticasabotage** | **Sabotage informatique et de données**

| | DELICTOMSCHRIJVING. — *DÉFINITION DE L'INFRACTION* | STRAFMAAT — *PEINE* |
|---|---|---|
| POGING TOT SABOTAGE. — *TENTATIVE DE SABOTAGE.*<br><br>(kwaadwillige manipulaties van data). — *(manipulations malveillantes de données).*<br><br>Bv. : Inbrengen van virussen, *worms. — Ex. : Introduction de virus, de* worms. | Hij die, met het oogmerk te schaden, rechtstreeks of onrechtstreeks, gegevens in een informaticasysteem invoert, wijzigt, wist, of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem verandert. — *Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout autre moyen technologique l'utilisation possible de données dans un système informatique.* | — gevangenisstraf van 6 maanden tot 3 jaar of — *emprisonnement de 6 mois à 3 ans ou*<br>— geldboete van 26 frank tot 25 000 frank. — *amende de 26 francs à 25 000 francs.* |
| VOLTOOIDE DATASABOTAGE. — *SABOTAGE DE DONNÉES.*<br>(kwaadwillige manipulaties die in effectieve schade aan data resulteren). — *(manipulations malveillantes causant des dommages effectifs à des données).*<br><br>Bv. : vernietigde files. — *Ex. : destruction de fichiers.* | Hij die, tengevolge van het plegen van het misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem. — *Celui qui, suite à la commission d'une infraction prévue au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique.* | — gevangenisstraf van 6 maanden tot 5 jaar of — *emprisonnement de 6 mois à 5 ans ou*<br>— geldboete van 26 frank tot 75 000 frank. — *amende de 26 francs à 75 000 francs.* |
| VOLTOOIDE SYSTEEMSABOTAGE. — *SABOTAGE DE SYSTEME.*<br>(kwaadwillige manipulaties die in effectieve schade aan computers resulteren). — *(manipulations malveillantes causant des dommages effectifs à des ordinateurs).*<br><br>Bv. : onbruikbare harddisk, ontregeling van de bestuurssystemen van een netwerk. — *Ex. : disque dur inutilisable.* | Hij die, tengevolge van het plegen van het misdrijf bedoeld in § 1, de correcte werking van dit of enig ander informaticasysteem geheel of gedeeltelijk belemmert. — *Celui qui, suite à la commission d'une infraction prévue au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique.* | — gevangenisstraf van 1 jaar tot 5 jaar of — *emprisonnement de 1 à 5 ans ou*<br>— geldboete van 26 frank tot 100 000 frank. — *amende de 26 francs à 100 000 francs.* |
| VOORBEREIDINGSHANDELINGEN. — *ACTES PRÉPARATOIRES.*<br>(ontwerpen en verspreiden van virussen en andere middelen om computersabotage te plegen). — *(conception et diffusion de virus et autres moyens en vue de commettre un sabotage informatique).*<br><br>Bv. : virusgenerator. — *Ex. : générateur de virus.* | Hij die, met bedrieglijk opzet of met het oogmerk te schaden, gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, ontwerpt, ter beschikking stelt, verspreidt of verhandelt, terwijl hij weet dat deze gegevens aangewend kunnen worden om schade te berokkenen aan gegevens of, geheel of gedeeltelijk, de correcte werking van een informaticasysteem te belemmeren. — *Celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des données stockées, traitées ou transmises par un système informatique, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique.* | — gevangenisstraf van 6 maanden tot 3 jaar of — *emprisonnement de 6 mois à 3 ans ou*<br>— geldboete van 26 frank tot 100 000 frank. — *amende de 26 francs à 100 000 francs.* |
| BIJZONDER REGIME VAN HERHALING. — *RÉGIME PARTICULIER EN MATIÈRE DE RÉCIDIVE.* | De straffen gesteld in de §§ 1 tot 4 worden verdubbeld enz. — *Les peines portées par les §§ 1er à 4 sont doublées, etc.* | verdubbeling van de strafmaat. — *doublement de la peine.* |

Tot besluit wijst de minister erop dat het ter bespreking voorliggende wetsontwerp, dat overduidelijk een leemte aanvult, een raamwerk vormt dat nog andere wetgevende initiatieven vereist, met name inzake telecommunicatie.

## II. — **ALGEMENE BESPREKING**

### A. **VRAGEN EN OPMERKINGEN VAN DE LEDEN**

*De heer Erik Derycke (SP)* onderstreept het belang van het ter bespreking voorliggende wetsontwerp en formuleert een aantal bedenkingen :

#### 1. **Algemene opmerkingen**

a) Het wetsontwerp brengt oude begrippen uit het Strafwetboek opnieuw bij de tijd, door er een moderne inhoud aan te gegeven zodat zij kunnen worden aangewend in de strijd tegen een nieuw maatschappelijk verschijnsel. Die werkwijze is niet alledaags, want ze komt erop neer dat afstand wordt genomen van de oorspronkelijke juridische grondbetekenis van die begrippen, om ze vervolgens op een nieuwe manier te kunnen toepassen. Volgens het lid is die werkwijze niet zonder gevaar.

b) Het is de spreker opgevallen dat de in uitzicht gestelde straffen zeer zwaar zijn in vergelijking met die voor vergelijkbare delicten, alsook ten opzichte van de in andere Europese landen terzake gehanteerde strafmaat. Hij vraagt dat over dit aspect zou worden nagedacht. We evolueren meer en meer naar een samenleving waarin het verantwoordelijkheidsbesef van de burgers afneemt en alle problemen strafrechtelijk worden opgelost. Een teleurstellende evolutie, zo vindt de spreker.

c) Het advies van de Raad van State maakt brandhout van nagenoeg de volledige oorspronkelijke tekst van het voorontwerp van wet. In de memorie van toelichting wordt echter niet nader ingegaan op de door de Raad geformuleerde aanmerkingen in verband met de schending van de internationale rechtsregels. Nochtans ware het aangewezen in informatica-aangelegenheden uiterst omzichtig te werk te gaan. Als men wil dat het wetsontwerp door de rechtbanken kan worden toegepast, behoort men zich naar de internationale rechtsregels te schikken.

d) In zijn advies (DOC 50 0213/001 en 0214/001, blz. 49 en volgende) wijst de Raad van State eveneens op het gevaar van vorderingen tot nietigverklaring voor het Arbitragehof, wegens de discriminatie waartoe het wetsontwerp aanleiding dreigt te geven. De wetgever hoeft weliswaar niet altijd alle opmerkingen van de Raad van State te volgen, maar het ware wenselijk dat

En guise de conclusion, le ministre attire l'attention sur le fait que le présent projet de loi, qui remplit un vide manifeste, constitue un projet cadre qui nécessitera la prise d'autres initiatives sur le plan législatif, en particulier dans le domaine des télécommunications.

## II. — **DISCUSSION GÉNÉRALE**

### A. **QUESTIONS ET OBSERVATIONS DES MEMBRES**

*M. Erik Derycke (SP)* souligne l'importance du présent projet de loi et formule plusieurs observations :

#### 1. **Observations générales**

a) Le projet de loi actualise d'anciennes notions du Code pénal. Il les traduit de façon moderne pour pouvoir lutter contre un nouveau phénomène de société. Cette technique est étrange car elle écarte le fondement juridique originaire de ces notions pour pouvoir les appliquer différemment. Selon le membre, cette méthode n'est pas sans danger.

b) L'orateur constate la grande sévérité des peines prévues par rapport à des délits comparables ainsi que par rapport à celles prévues dans les États européens en cette matière. Il demande qu'une réflexion soit menée à cet égard. Actuellement, on se dirige vers une société où la responsabilité du citoyen s'estompe et où tout problème se trouve solutionné par une sanction pénale. L'orateur se déclare déçu devant une telle évolution.

c) L'avis du Conseil d'État laisse peu subsister du texte originaire de l'avant-projet de loi. Aucune solution n'est apportée dans l'exposé des motifs aux observations formulées quant à la violation du droit international. En matière informatique, il y a lieu d'être particulièrement prudent. Si l'on veut que le projet de loi puisse être appliqué par les tribunaux, il échet de se conformer au droit international.

d) L'avis du Conseil d'État soulève également le danger d'un recours devant la Cour d'Arbitrage en raison des discriminations qu'il crée (DOC 50 0213/001 et 0214/001 pp. 49 et suivantes). Même si le législateur ne doit pas toujours répondre à l'ensemble des observations émises par le Conseil d'État, il est toutefois souhaitable qu'une réponse soit à tout le moins appor-

er in het raam van de parlementaire voorbereiding op zijn minst op wordt gezinspeeld, zodat de rechtspraak en de rechtsleer eveneens een aanwijzing krijgen over welke richting een en ander uit moet.

### 2. **Wijzigingen in het Strafwetboek**

Met dit wetsontwerp worden bijzondere misdrijven in het leven geroepen. In de ogen van het lid veronderstelt het gebruik van begrippen als « valsheid » en « bedrog » dat ook de thans voor die begrippen bestaande omschrijving kan worden gehanteerd. Zo kan « valsheid in informatica » worden ondergebracht in de afdeling « Valsheid in authentieke en openbare geschriften, in handels- of bankgeschriften en in private geschriften », die deel uitmaakt van het hoofdstuk « Valsheid in geschriften en in telegrammen ».

De heer Derycke gaat na of de door de rechtspraak in aanmerking genomen wezenlijke bestanddelen van « valsheid » ook in het nieuwe artikel 210*bis* terug te vinden zijn.

In dat verband stipt hij aan dat het Hof van Cassatie in 1984 al oordeelde dat het bedrieglijk opzet dat nodig is om valsheid in geschriften te kunnen bewijzen, de vorm moet aannemen van de bedoeling zichzelf een onwettig gewin of voordeel te verschaffen. Volgens een arrest uit 1982 moeten de openbare en private geschriften bovendien rechtsgevolgen hebben, dat wil zeggen : door het gebruik dat ermee wordt beoogd, kunnen die geschriften derden nadeel toebrengen, alsook gevolgen voor hen hebben.

In de memorie van toelichting staat evenwel niets te lezen over de voorwaarden die moeten vervuld zijn om te kunnen spreken van « valsheid » als bedoeld in artikel 210*bis*. Dat van enig bijzonder opzet geen melding wordt gemaakt, is volgens de regering verantwoord omdat het bedrieglijk opzet inzake informaticafraude is opgenomen in artikel 504*quater*, terwijl het voor informatica- en datasabotage vereiste oogmerk om schade te berokkenen, terug te vinden is in artikel 550*ter* (DOC 50 0213/001 en 0214/001, blz. 14).

Die werkwijze is juridisch onnauwkeurig. Het had de voorkeur verdiend de grondvoorwaarde in artikel 210*bis* op te nemen, te weten : het oogmerk om iemand een onwettig gewin of voordeel te verschaffen.

De beschrijving van het informaticabedrog is daarentegen correct.

De drie bestanddelen van het bedrog zijn opgenomen in artikel 504*quater* (het morele bestanddeel, de middelen om het misdrijf te plegen, het resultaat (de oplichting bedoeld in artikel 496)).

In verband met artikel 550*bis*, dat betrekking heeft op de ongeoorloofde toegang tot een informaticasysteem, vraagt de spreker dat een nauwkeuriger omschrijving wordt gegeven van de bewoordingen « Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is ».

tée dans le cadre des travaux parlementaires afin de pouvoir donner quelques indications à la jurisprudence et à la doctrine.

### 2. **Modifications apportées au Code pénal**

Le présent projet de loi crée des infractions particulières. Pour le membre, le recours à des notions comme celles de faux ou de fraude implique que l'on puisse se référer aux qualifications qui y sont actuellement données. Ainsi, le faux en informatique peut être classé dans la section relative aux faux en écritures authentiques et publiques, en écritures de commerce ou de banque et en écritures privées, section qui forme une partie du chapitre consacré aux faux commis en écritures et dans les dépêches télégraphiques.

M. Derycke examine si les éléments essentiels du faux retenus par la jurisprudence se retrouvent dans le nouvel article 210*bis*.

Il cite à ce propos un extrait d'un arrêt de la Cour de cassation de 1984 selon lequel « l'intention frauduleuse requise pour l'existence du faux en écriture est l'intention de procurer à soi-même un profit, un avantage illicite. Selon un autre arrêt de 1982, « il faut que les écritures publiques ou privées soient de nature à produire des effets judiciaires, c'est-à-dire qu'ils puissent par l'usage en vue duquel ils ont été rédigés porter préjudice aux tiers et entraîner des conséquences à leur égard. »

L'exposé des motifs ne s'attarde pas quant à lui aux conditions requises pour l'existence du faux en écriture en ce qui concerne l'article 210*bis*. Le gouvernement justifie l'absence d'intention particulière par le fait que l'intention frauduleuse est visée en matière de fraude informatique (article 504*quater*) et que l'intention de nuire est requise en matière de sabotage informatique et de sabotage de données (article 550*ter*) (DOC 50 0213/001 et 0214/001, p. 14).

Ce procédé n'est pas correct sur le plan juridique. Il eût été préférable de reprendre à l'article 210*bis* la condition essentielle à savoir celle de procurer à autrui un profit ou un avantage illicite.

Par contre, la description donnée à la fraude informatique est correcte.

Les trois éléments constitutifs de la fraude sont repris à l'article 504*quater* (l'élément moral, les moyens de commettre le délit, le résultat (escroquerie visée à l'article 496)).

En ce qui concerne l'article 550*bis* qui porte sur l'accès illicite à un système informatique, l'orateur demande qu'une description plus précise soit apportée aux termes « celui qui, sachant qu'il n'y est pas autorisé ».

3. **Wijzigingen in het Wetboek van strafvordering**

Wat de procedure betreft, zou het wetsontwerp moeten worden verbeterd op het stuk van de bestaanbaarheid ervan met het internationaal recht. Het feit dat een onderzoeksrechter gegevens verzamelt die zich niet op het Belgisch grondgebied bevinden en die gegevens vervolgens ter kennis te brengt van de bevoegde buitenlandse autoriteiten is immers in strijd met het internationaal recht.

*
* *

*Voorzitter Fred Erdman (SP)* is terughoudend op het stuk van de bevoegdheidsverdeling tussen de Kamer en de Senaat (artikelen 77 en 78 van de Grondwet). De opmerkingen van de Raad van State terzake berusten op zijn eigen rechtspraak, die de wetgever niet altijd heeft gevolgd. Hij vraagt dan ook dat die bevoegdheidsverdeling grondig wordt onderzocht.

In verband met de opmerking van de vorige spreker over de heel strenge straffen waarin het onderhavige ontwerp voorziet, is hij van oordeel dat een vergelijking kan worden gemaakt met de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, waarin men dezelfde strengheid vindt, behalve inzake gevangenisstraf, waar de wetgever van 1992 minder repressief is geweest.

Wat ten slotte het internationaal recht betreft, doet niet alleen de bestaanbaarheid met de internationale verplichtingen problemen rijzen, maar ook de plaats waar het misdrijf wordt gepleegd.

*
* *

*De heer Jean-Pol Poncelet (PSC)* zegt dat hij, persoonlijk en namens zijn fractie, verheugd is over de indiening van het voorliggende wetsontwerp. Het komt te gelegener tijd of zelfs misschien een beetje te laat. De samenleving heeft inderdaad lang gewacht alvorens te reageren op de juridische vraagstukken die de nieuwe technologieën doen rijzen en heeft dus weinig verweer tegen een aantal misdrijven.

1. **Algemene opmerkingen**

a) Het onderhavige wetsontwerp is slechts een onderdeel van een geheel dat zal moeten worden aangevuld, enerzijds wat het Burgerlijk Wetboek betreft op het stuk van de verplichtingen inzake bewijslevering (elek-

3. **Modifications au Code d'instruction criminelle**

En matière de procédure, le projet de loi devrait être amélioré en ce qui concerne sa compatibilité avec le droit international. Le fait pour un juge d'instruction de rassembler des données qui ne se trouvent pas sur le territoire belge et d'ensuite aviser les autorités étrangères compétentes, est en effet contraire au droit international.

*
* *

*Le président, M. Fred Erdman (SP)* émet des réserves quant à la répartition des compétences entre la Chambre et le Sénat (articles 77 et 78 de la Constitution). Les observations émises par le Conseil d'État à ce propos se basent sur la jurisprudence du Conseil d'État qui n'a pas toujours été suivie par le législateur. Il demande dès lors que cette répartition fasse l'objet d'un examen approfondi.

En ce qui concerne la remarque de l'orateur précédent relative à la grande sévérité des peines retenues par le présent projet , il considère qu'une comparaison peut être faite avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. La même sévérité s'y retrouve si ce n'est en matière d'emprisonnement où le législateur de 1992 a été moins répressif.

Enfin, en matière de droit international, ce n'est pas seulement l'articulation avec les obligations internationales qui pose problème, c'est aussi la localisation de l'infraction qui suscite des difficultés.

*
* *

*M. Jean-Pol Poncelet (PSC)* se réjouit, à titre personnel et au nom de son groupe, devant le dépôt de ce projet de loi. Il vient à son heure, peut-être même un peu tardivement. La société a en effet tardé à réagir face aux problèmes de droit posés par les nouvelles technologies et se trouve dès lors démunie par rapport à un certain nombre de délits.

1. **Remarques générales**

a) Le présent projet de loi ne constitue qu'un seul élément d'un ensemble qu'il y aura lieu de compléter, d'une part, en ce qui concerne le Code civil en matière de preuve des obligations (signature électronique) et

tronische handtekening) en anderzijds op het stuk van de waarmerking van de elektronische handtekeningen.

Het lid informeert welke projecten de regering in dat verband op stapel heeft staan.

b) De heer Poncelet vraagt ook of de regering het advies heeft ingewonnen van de Commissie voor de bescherming van de persoonlijke levenssfeer. Dat advies zou immers van grote waarde zijn.

2. **Meer bijzondere opmerkingen**

a) Er is een verschil tussen de Franse en de Nederlandse tekst van artikel 9 (DOC 50 0214/001). Naar luid van de Franse tekst gelden de verplichtingen alleen voor de verstrekkers van telecommunicatiediensten terwijl de Nederlandse tekst die verplichtingen oplegt aan de operatoren van telecommunicatienetwerken en aan de verstrekkers van telecommunicatiediensten. Welke versie dient in aanmerking te worden genomen ?

b) Het probleem van de medewerking van technici in de ruime zin komt te berde in artikel 4, § 3 en in artikel 7, § 4 (DOC 50 0214/001). Is er een onderscheid tussen dat begrip en het begrip « technische steun » ?

3. **Advies van de Raad van State**

a) De Raad van State maakt een belangrijke opmerking over de schending van de soevereiniteit van de Staten, meer bepaald in verband met artikel 88*ter*. Dat begrip verliest in die aangelegenheid weliswaar een deel van zijn betekenis omdat de netwerken per definitie de landsgrenzen overschrijden. Het lid is bijgevolg van mening dat men de Raad van State op dat punt niet hoeft te volgen. Ook wat de internationale wederzijdse rechtshulp betreft, zijn de bestaande middelen niet aangepast aan de virtuele realiteit.

b) Het wetsontwerp blijkt bepaalde feiten die in een informaticaomgeving worden gepleegd strenger te straffen en kan dus aanleiding geven tot discriminaties. Met andere woorden, het Strafwetboek zou strenger zijn naargelang het misdrijf al dan niet in een informaticaomgeving wordt gepleegd. De heer Poncelet wenst dat het principe wordt toegepast van het parallellisme tussen de bestaande strafbaarstellingen en wat daarmee overeenstemt in de virtuele werkelijkheid.

Om af te ronden wijst het lid op het belang van dat wetsontwerp, dat, wanneer het met andere wetgevende initiatieven zal zijn aangevuld, België de juridische middelen zal geven om het hoofd te bieden aan een aantal misbruiken.

*De minister* deelt in verband met artikel 9 mee dat de Nederlandse tekst in aanmerking moet worden genomen.

*
* *

d'autre part, en ce qui concerne la certification des signatures électroniques.

Le membre demande si le gouvernement a des projets en ces matières.

b) M. Poncelet demande également si le gouvernement a sollicité l'avis de la Commission de protection de la vie privée. Une telle consultation serait en effet précieuse.

2. **Remarques plus particulières**

a) À l'article 9 (DOC 50 0214/001), il existe une divergence entre les textes français et néerlandais. Le texte français limite les obligations aux fournisseurs de service tandis que le texte néerlandais retient les opérateurs et les fournisseurs. Quelle version faut-il retenir ?

b) Les articles 4, §§ 3 et 7, § 4 (DOC 50 0214/001) envisagent le problème de la collaboration de techniciens au sens large. Cette notion est-elle différente de celle de « concours technique »?

3. **Avis du Conseil d'État**

a) Le Conseil d'État soulève une importante observation en ce qui concerne le non-respect de la souveraineté des États, notamment à l'article 88*ter*. Dans la présente matière, ce concept perd cependant une partie de sa signification puisque par définition, les réseaux dépassent les limites territoriales. Le membre est dès lors d'avis qu'il n'y a pas lieu de suivre le Conseil d'État sur ce point. De même, en ce qui concerne l'entraide judiciaire internationale, les instruments existants sont inadaptés à la réalité virtuelle.

b) Le projet de loi semble sanctionner plus fortement certains faits commis dans un environnement informatique et peut dès lors conduire à des discriminations. En d'autres termes, le Code pénal serait plus sévère selon que le délit est commis dans un environnement informatique ou non. M. Poncelet souhaite, quant à lui, appliquer le principe du parallélisme entre les incriminations existantes et leur correspondance dans la réalité virtuelle.

Le membre conclut en soulignant l'importance de ce projet de loi qui donnera à la Belgique, lorsqu'il sera complété par d'autres initiatives législatives, les moyens juridiques pour faire face à un certain nombre de dérives.

*Le ministre* communique qu'en ce qui concerne l'article 9 évoqué, le texte néerlandais doit être retenu.

*
* *

*Voorzitter Fred Erdman* wijst erop dat het begrip « medewerking » van derden reeds aan bod is gekomen tijdens de bespreking van de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie (artikel 90*quater*, paragraaf 2, tweede lid, van het Wetboek van strafvordering).

*
* *

*De heer Servais Verherstraeten (CVP)* vestigt de aandacht op het feit dat dit wetsontwerp in nagenoeg dezelfde termen door de vorige regering werd goedgekeurd. Zijn fractie steunt dit ontwerp dan ook en wenst dat het spoedig wordt goedgekeurd.

Hij formuleert evenwel een aantal bedenkingen en opmerkingen.

1. Goedkeuring van een wet houdt in dat men ook over de nodige middelen beschikt om ze uit te voeren. Men mag bij de mensen uit het veld immers geen verwachtingen wekken die men nadien onmogelijk kan inlossen. Zo impliceert dit ontwerp *in casu* een knowhow en een infrastructuur waarover Justitie niet beschikt.

2. Net als de vorige sprekers vraagt het lid zich af of terzake het internationaal recht werd nageleefd. Een aantal rechtsregels zijn ongetwijfeld achterhaald, maar zulks neemt niet weg dat een aantal in het strafrecht geldende regels, zoals het beginsel *« nulla poena sine lege »,* geëerbiedigd moeten blijven. Is het dan ook niet ongepast dat het wetsontwerp geen rekening houdt met de opmerkingen die de Raad van State terzake heeft geformuleerd ? Moet men op z'n minst niet bepalen dat de buitenlandse wetgeving moet worden nageleefd ? Dezelfde moeilijkheid rijst op het vlak van de interne werking wanneer gegevens in andere rechterlijke arrondissementen worden ingezameld.

3. De heer Verherstraeten heeft de indruk dat dit wetsontwerp door technici werd geredigeerd. Zo voert het ontwerp een aantal zeer ruime bevoegdheden in, wat niet te rijmen valt met de nauwgezetheid die het strafrecht in acht pleegt te nemen. Zo kunnen de procureur des Konings en de onderzoeksrechter alle « *passende middelen »* aanwenden. Het lid wenst die concepten dan ook graag nader gepreciseerd te zien.

4. Hij heeft de indruk dat de poging weliswaar wordt bestraft, maar dat zulks voor computerfraude niet het geval is.

5. Het lid heeft tevens een aantal vragen rond de zware strafmaat. Moet iemand die een computersysteem beschadigt, daarvoor strafrechtelijk worden bestraft ? Wordt in dat geval niet bij voorkeur artikel 1382 van het Burgerlijk Wetboek toegepast ? De laatste vraag ligt in de lijn van de gedachtegang van een van de

*Le président, M. Fred Erdman* rappelle que la notion de « collaboration » de tiers a déjà été abordée lors de l'examen de la loi du 10 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées (article 90*quater*, paragraphe 2, alinéa 2 du Code d'instruction criminelle).

*
* *

*M. Servais Verherstraeten (CVP)* attire l'attention sur le fait que ce projet de loi avait été approuvé en des termes presque identiques par le précédent gouvernement. Son groupe soutient dès lors ce projet et souhaite que son adoption se fasse rapidement.

Il émet cependant plusieurs questions et observations.

1. L'adoption d'une loi implique que l'on dispose des moyens nécessaires pour l'appliquer. Il ne faut en effet pas créer sur le terrain des attentes qui ne peuvent se réaliser. En l'espèce, ce projet implique un savoir-faire et une logistique que la Justice ne dispose pas.

2. Comme les orateurs précédents, le membre s'interroge sur le respect du droit international. Si plusieurs règles de droit sont sans doute vétustes, il n'empêche qu'en droit pénal, certaines règles comme celle « *nulla poena sine lege* » doivent être respectées. N'est-ce dès lors pas à tort que le projet de loi ne suit pas les observations du Conseil d'État à ce propos ? Ne faudrait-il pas au moins prévoir que la législation étrangère doit être respectée ? La même difficulté se rencontre dans l'ordre interne lorsque des données sont recueillies dans d'autres arrondissements judiciaires.

3. M. Verherstraeten a l'impression que ce projet de loi a été rédigé par des techniciens. Certaines compétences très larges sont ainsi introduites, ce qui ne correspond pas à la précision attendue en droit pénal. Le procureur du Roi et le juge d'instruction peuvent ainsi recourir à « *tous les moyens appropriés* ». Le membre émet dès lors le souhait que ces notions soient précisées.

4. Il lui paraît que si la tentative est sanctionnée, elle ne l'est pas en matière de fraude informatique.

5. Le membre se pose également des questions en ce qui concerne la lourdeur des peines. Quelqu'un qui cause un dommage à un système informatique doit-il être pénalement sanctionné ? Ne serait-il pas préférable que le droit commun de l'article 1382 du Code civil trouve à s'appliquer ? Cette dernière question s'inscrit

vorige sprekers, die ervoor pleitte in onze samenleving een aantal handelingen uit de criminele sfeer te lichten.

6. De spreker legt dit wetsontwerp naast de tekst die de vorige regering in overweging heeft genomen. Hij stelt daarbij vast dat dit ontwerp een verbetering inhoudt doordat het een verplichte samenwerking tussen de terzake bevoegde personen inbouwt. Sterker voorbehoud maakt hij daarentegen bij de aangebrachte wijziging waardoor de mogelijkheid wordt geboden uit het computernetwerk gegevens te verwijderen die strijdig zijn met de openbare orde of de goede zeden. Ook al is de wetgever de hoeder van de openbare orde en de goede zeden, toch vraagt de spreker zich af of het wetsontwerp terzake niet al te ver gaat door niet langer te eisen dat soortgelijke gegevens aan een overtreding gelinkt moeten zijn. Voor magistraten en politiediensten wordt het bijgevolg mogelijk buiten het strafrechtelijk raam op te treden. Volgens de spreker bevat het strafrecht voldoende verwijzingen naar seksuele misdrijven om dat optreden wettelijk te onderbouwen.

Tot besluit vraagt de spreker zich af of men inzake de strafmaat niet meer vindingrijkheid aan de dag moet leggen. Die strafbare feiten worden ook in de economische sfeer begaan. Ware het dan niet wenselijk erin te voorzien de daders — net zoals zulks voor bedrieglijk bankroet het geval is — een verbod op te leggen om hun activiteit gedurende een bepaalde tijd uit te oefenen ?

*
* *

*De heer Peter Vanhoutte (Agalev-Ecolo)* valt de door de heer Derycke gemaakte opmerkingen bij; hij wenst er alleen een aantal opmerkingen aan toe te voegen die specifiek betrekking hebben op de informatica.

1. De strafmaat waarin het wetsontwerp voorziet, is zeer zwaar, als men alle daders over dezelfde kam scheert. Dat is evenwel niet het geval. De daders vertonen namelijk een verschillend profiel : het kunnen mensen uit de economische wereld zijn, maar het kan ook om jongeren gaan, die zeer beslagen zijn in de informatica. De samenleving gaat al te ver wanneer ze die jongeren zo hard aanpakt. Het ware verkieslijk voor hen in alternatieve straffen te voorzien, zodat ze niet langer tégen maar ten bate van de samenleving handelen.

2. In tegenstelling tot de vorige de spreker, heeft hij niet de indruk dat dit wetsontwerp door technici is geredigeerd. Zo komt het hem voor dat de tekst de enorme complexiteit van de computernetwerken onderschat. Die complexiteit vereist bovendien dat zo snel mogelijk een internationaal samenwerkingsverband wordt opgezet.

3. De spreker wijst er tevens op hoe zwaar de straffen zijn waarin voor krakers van elektronische bestanden wordt voorzien. Momenteel vind je in de handel

dans la réflexion d'un des précédents orateurs de vouloir décriminaliser la société.

6. Examinant le présent projet de loi par rapport au texte retenu par le précédent gouvernement, l'orateur considère qu'une amélioration a été apportée en prévoyant la collaboration forcée des personnes compétentes en la matière. Par contre, il formule plus de réserves quant à la modification apportée qui octroie la possibilité de retirer du système informatique des données qui sont contraires à l'ordre public ou aux bonnes mœurs. Même si le législateur est le gardien de l'ordre public et des bonnes mœurs, il se demande si le projet de loi ne va pas trop loin en n'exigeant plus que de telles données soient liées à une infraction. Les magistrats et les services de police reçoivent dès lors la possibilité d'agir en dehors du droit pénal. Il lui semble que le droit pénal contient assez de références aux délits sexuels pour pouvoir encadrer leur action.

En guise de conclusion, l'orateur se demande s'il ne faudrait pas être plus inventif en matière de sanction. Étant donné que ces infractions se produisent également dans le domaine économique, ne serait-il pas opportun de prévoir que les auteurs soient interdits de l'exercice de leur activité pendant une période déterminée, comme en matière de faillite frauduleuse ?

*
* *

Tout en rejoignant les observations émises par M. Derycke, *M. Peter Vanhoutte (Agalev-Ecolo)* tient à les compléter par des remarques se situant plus sur le plan informatique.

1. Les sanctions prévues par le projet de loi sont d'autant plus lourdes qu'il y a lieu de faire une distinction selon les auteurs. Si ceux-ci peuvent appartenir au monde économique, il peut également s'agir de jeunes, très doués en la matière. La société va trop loin en sanctionnant ces jeunes de façon aussi sévère. Il serait préférable de prévoir pour eux des peines alternatives afin qu'ils n'agissent plus contre mais en faveur de la société.

2. Contrairement à ce qu'a affirmé le précédent orateur, il ne lui semble pas que ce projet de loi a été rédigé par des techniciens. Il a ainsi l'impression que le texte sous-estime l'extrême complexité des réseaux informatiques. Cette complexité exige en outre qu'un cadre international soit au plus tôt mis en place.

3. L'orateur relève également la sévérité des sanctions prévues en matière de piratage informatique. Actuellement, on trouve facilement dans le commerce des

probleemloos zogenaamde *« hackertools »*, waarmee toegangscodes kunnen worden gekraakt. Die instrumenten kunnen uiteraard voor een andere dan de oorspronkelijke doelstelling worden aangewend, maar dat belet niet dat ze ontegenzeglijk nuttig zijn. Die software moet dan ook vanuit een meer objectieve invalshoek worden benaderd.

4. Er bestaan versleutelingssystemen die niet kunnen worden gekraakt. Deze moeilijkheid zou eveneens ter sprake moeten komen. Voorts ware het, met het oog op een effectieve toepassing van dit wetsontwerp, aangewezen een beroep te doen op specialisten.

5. Er werd gewezen op de bescherming van de goede zeden en de openbare orde. Voorts is het lid ook van oordeel dat niet mag worden geraakt aan de persvrijheid. Terzake moet een parallellisme in acht worden genomen zowel wat de schrijvende en gesproken pers als wat het Internet betreft. De persvrijheid moet, ongeacht het gebruikte informatiemedium, worden gewaarborgd.

*
* *

*De heer Bert Schoofs (Vlaams Blok)* uit zijn tevredenheid over de volgende drie punten :

1. Het wetsontwerp is gebaseerd op bestaande strafbepalingen. Het gaat niet om een bijzondere wetgeving. Het wetsontwerp poogt de samenhang in het strafrecht te bewaren via een invoeging in het Strafwetboek, wat de coherentie ten goede komt van het strafrecht.

2. Het wetsontwerp bepaalt dat het voortaan verboden is informaticamateriaal te « bewerken », ook wanneer het in beslag wordt genomen tijdens een opsporings- of gerechtelijk onderzoek.

3. Gelet op de belangrijkheid van de te beschermen sectoren is het verantwoord in zware straffen te voorzien. Het ware aangewezen alternatieve straffen achterwege te laten, aangezien die steeds kunnen worden opgelegd door de rechter overeenkomstig het gemeen strafrecht.

Niettemin betreurt zijn fractie dat het wetsontwerp geen rekening houdt met de opmerking van de Raad van State, die stelt dat de bevoegdheidsoverdracht die de Koning inzake het registreren en bewaren van de gegevens wordt gegeven, niet verenigbaar is met de grondwettelijke vereiste om te voorzien in wettelijke beperkingen inzake het recht op eerbiediging van het privé-leven. In de memorie van toelichting wordt het argument van de Raad van State verworpen. Als reden wordt de techniciteit van het onderwerp opgegeven, hetgeen een argument is dat niet volstaat.

Voor het overige stelt het lid zich vragen over het verzoek van de Raad van State om de gebruikte termen beter te preciseren. De term « computervredebreuk » is

« *hackertools* » permettant de casser les codes d'accès. Même si ceux-ci peuvent être détournés de leur utilité première, ils ont une utilité incontestable. Ces instruments devraient dès lors être placés dans un contexte plus objectif.

4. Il existe des systèmes de verrouillage qu'il n'est pas possible de casser. Cette difficulté devrait également être abordée. Par ailleurs, il y aura lieu de recourir à des personnes très spécialisées si on veut donner une application effective à ce projet.

5. Le souci de sauvegarder les bonnes mœurs et l'ordre public a été évoqué. Le membre se déclare quant à lui également très soucieux de la liberté de la presse. À ce propos, un parallélisme doit être respecté tant en ce qui concerne la presse écrite et orale qu'en ce qui concerne le réseau Internet. La liberté de la presse doit être garantie peu importe son moyen d'expression.

*
* *

*M. Bert Schoofs (Vlaams Blok)* communique sa satisfaction sur trois points :

1. Le projet de loi s'appuie sur des dispositions pénales existantes. Il ne s'agit pas d'une législation particulière. Le projet essaie de maintenir la cohérence du droit pénal en insérant des dispositions dans le Code pénal, ce qui contribue à renforcer la cohérence du droit pénal.

2. Le projet de loi interdit dorénavant « la manipulation » de matériel informatique, même si ce matériel est saisi au cours d'une information ou d'une instruction judiciaire.

3. Devant l'importance des secteurs à protéger, il est justifié de prévoir de lourdes peines. Il n'y a pas lieu d'inscrire dans le projet des peines alternatives, étant donné que celles-ci peuvent toujours être prononcées par le juge conformément au droit pénal commun.

Son groupe déplore néanmoins le fait que le projet ne répond pas à l'observation formulée par le Conseil d'État selon laquelle la délégation de compétence donnée au Roi en matière d'enregistrement et de conservation des données est incompatible avec l'exigence constitutionnelle de prévoir des restrictions légales en matière de droit au respect de la vie privée. L'exposé des motifs rejette l'argument du Conseil d'État en invoquant la technicité de la matière, ce qui n'est pas un argument suffisant.

Pour le reste, le membre se pose des questions concernant la demande du Conseil d'État de mieux préciser les termes retenus. Au fond, l'expression « vio-

bij nader toezien echter niet zo vreemd of ongepast, omdat deze wet in feite zoals bij huisvredebreuk de virtuele « woning », met name de PC, in de virtuele wereld of « *cyberspace* » beoogt te beschermen.

*
* *

*De heer Jean-Pol Poncelet (PSC)* komt terug op het internationale karakter van het huidige knelpunt, dat aantoont dat het territorialiteitsbeginsel volkomen onaanvaardbaar is. Voorts is de rechterlijke macht, ook al zou ze over de middelen beschikken die de regering bereid is haar te geven, technisch niet in staat om de criminaliteits- en veiligheidsproblemen in de netwerken op te lossen. Het feit zelf dat er een netwerk bestaat, betekent dat het kan worden gekraakt. Er zou een tussenstructuur moeten komen. Die zou het gerecht en in meer algemene zin de overheid helpen de veiligheid te garanderen. De spreker verwijst in dat verband naar de « netwerkrijkswachter » die inzake telecommunicatie werd aangesteld. Het lid wijst op de noodzakelijke veiligheid van de eigen netwerken van de regering. Momenteel is hun vertrouwelijkheid niet gewaarborgd. Daarover wordt in de regeringsverklaring met geen woord gerept.

## B. **ANTWOORDEN VAN DE MINISTER VAN JUSTITIE**

### 1. **Opsplitsing van de wetsontwerpen (artikelen 77 en 78 van de Grondwet)**

De minister deelt mee dat hij zich neer zal leggen bij de beslissing van de commissie. Het wetsontwerp volgt niet helemaal de interpretatie van de Raad van State. Hij stipt aan dat vroeger noch de Kamer van volksvertegenwoordigers, noch de parlementaire overlegcommissie die interpretatie van de Raad van State hebben gevolgd.

### 2. **Internationaal aspect**

Er moet bijzondere aandacht worden besteed aan de te volgen procedure wanneer een onderzoek betrekking heeft op gegevens die zich in het buitenland bevinden. Die procedure moet *a priori*, en niet *a posteriori* worden gevolgd. De minister verklaart zich bereid alle mogelijkheden op het terrein te bestuderen. Aangezien er geen ander wettelijk instrument voorhanden is in het raam van de internationale rechtshulp, moet de rechterlijke overheid de betrokken Staat op de hoogte brengen van het voornemen om gegevens te verzamelen. Net zoals de internationale rogatoire commissies kunnen

lation d'ordinateur » n'est cependant pas si insolite ou inappropriée, puisque la loi en projet vise en fait, comme dans le cas de la violation de domicile, à protéger la « demeure » virtuelle, en l'occurrence le PC dans le monde virtuel ou « *cyberspace* ».

*
* *

*M. Jean-Pol Poncelet (PSC)* revient au caractère international de la présente problématique qui démontre que le principe de territorialité est tout à fait inacceptable. Par ailleurs, le pouvoir judiciaire, même dôté des moyens budgétaires que le gouvernement est prêt à lui donner n'est pas en mesure de faire face techniquement aux problèmes de criminalité et de sécurité dans les réseaux. Le fait même de l'existence d'un réseau constitue en soi une ouverture à du piratage. Une structure intermédiaire devrait être mise en place. Elle serait un auxiliaire de la Justice et de façon plus générale des pouvoirs publics pour assumer la sécurité. Un « gendarme » du réseau a ainsi été mis en place en matière de télécommunication. Le membre attire l'attention sur la nécessaire sécurité des propres réseaux d'information du gouvernement. Actuellement, leur confidentialité n'est pas garantie. La déclaration gouvernementale est muette à ce propos.

## B. **RÉPONSES DU MINISTRE DE LA JUSTICE**

### 1. **Scission des projets (articles 77 et 78 de la Constitution)**

Le ministre annonce qu'il respectera la décision de la commission. Le projet de loi n'a pas entièrement suivi l'interprétation donnée par le Conseil d'État. Il fait remarquer qu'antérieurement, cette interprétation du Conseil d'État n'a été suivie ni par la Chambre des représentants ni par la commission parlementaire de concertation.

### 2. **Aspect international**

Une attention particulière doit être accordée à la procédure à suivre lorsque les investigations portent sur des données situées à l'étranger. Cette procédure doit être suivie *a priori* et non *a posteriori*. Le ministre se déclare prêt à examiner sur le terrain toutes les possibilités. Étant donné qu'il n'existe pas d'autre instrument légal dans le cadre de l'entraide judiciaire internationale en matière pénale, il est prévu que les autorités judiciaires informent l'État concerné qu'elles ont l'intention de recueillir des données. Tout comme en matière de commissions rogatoires internationales, les enquêteurs

de onderzoekers pas in actie schieten nadat de betrokken Staat zijn fiat heeft gegeven. Bijgevolg is het absoluut noodzakelijk terzake te voorzien in een bijzonder soepele rechtshulpprocedure.

Een van de leden heeft gewezen op de noodzakelijkheid over een « rijkswachter » van het netwerk te beschikken. Momenteel wordt een dergelijke regulerende factor niet overwogen omdat het technische en politieke ingrepen vergt die nog niet werden verwezenlijkt.

Een ander lid heeft eraan herinnerd dat het knelpunt betreffende het internationaal recht ook terug te vinden is op intern vlak in geval speurders gegevens zoeken buiten de territoriale bevoegdheden van de rechterlijke arrondissementen. De minister stipt aan dat artikel 62*bis* van het Wetboek van strafvordering bepaalt dat de onderzoeksrechter handelend binnen zijn bevoegdheid kan optreden op het hele grondgebied.

De medewerker van de minister formuleert vervolgens de volgende overwegingen in verband met de opmerking van de Raad van State betreffende het ietwat te lichtzinnig gebruik van de *hot pursuit*. In werkelijkheid is die verwijzing naar het internationale zeerecht bijzonder interessant omdat ze eveneens kan worden toegepast in het kader van de computercriminaliteit. Net zoals in volle zee bestaan er geen grenzen op het vlak van de computercriminaliteit; de grenzen zijn fictief. Volgens het internationale zeerecht moet toestemming worden gevraagd aan de Staat tot welke de territoriale wateren behoren waarnaar het onderzoek leidt. Het wetsontwerp gaat diezelfde richting uit. Het knelpunt inzake computercriminaliteit is evenwel ingewikkelder, in die zin dat het internationale aspect nooit op voorhand kan worden bepaald.

Die moeilijkheid rechtvaardigt de in het wetsontwerp opgenomen verschillen. De medewerker van de minister deelt mee dat in de Raad van Europa momenteel de laatste hand wordt gelegd aan een ontwerpverdrag met betrekking tot het internationaalrechtelijk aspect van de aangelegenheid. Het valt niet mee om oplossingen te vinden die aanvaardbaar zijn voor alle lidstaten, want die zijn niet altijd te vinden voor een nieuwe fase die voor hen afstand van soevereiniteit betekent. Wil men *überhaupt* nog soevereiniteit hebben dan moet die gedeeld worden, aldus de medewerker van de minister.

### 3. **Parallellisme met de sancties waarin wordt voorzien inzake de bescherming van de persoonlijke levenssfeer**

Wegens het wezenlijk verschil tussen beide aangelegenheden bestaat er geen volledig parallellisme tussen de straffen waarin het wetsontwerp voorziet en die welke van toepassing zijn inzake de bescherming van de persoonlijke levenssfeer. Iemands persoonlijke levenssfeer aantasten betekent zonder de instemming van de betrokkene wederrechtelijk in het bezit proberen

sont dépendants du bon vouloir de l'État concerné. Il est dès lors indispensable de prévoir en cette matière une procédure d'entraide judiciaire très souple.

Un membre a évoqué la nécessité d'avoir un « gendarme » du réseau. Un tel élément régulateur n'est pas envisagé actuellement vu qu'il nécessite des interventions techniques et politiques qui n'ont pas encore été réalisées.

Un autre membre a rappelé que la problématique du droit international se rencontrait également en droit interne en cas de recherche de données en dehors des compétences territoriales des arrondissements judiciaires. Le ministre attire l'attention sur le fait que l'article 62*bis* du Code d'instruction criminelle prévoit que le juge d'instruction, agissant dans les limites de ses compétences, peut intervenir sur tout le territoire.

Le collaborateur du ministre émet ensuite les considérations suivantes en ce qui concerne la remarque du Conseil d'État relative à l'usage un peu léger du « *hot pursuit* ». En réalité, cette référence au droit maritime international est très intéressante car elle peut également s'appliquer dans le cadre de la criminalité informatique. Tout comme en haute mer, les frontières dans le domaine de la criminalité informatique n'existent pas et constituent un fiction. En droit maritime international, il y a lieu de demander l'accord de l'État dont dépend les eaux territoriales dans lesquelles la poursuite se continue. Le projet de loi s'engage dans cette voie. Le problème en matière de criminalité informatique se complique en ce sens que l'aspect international ne peut jamais être déterminé à l'avance.

Cette difficulté justifie les différences qui ont été insérées dans le projet de loi. Le collaborateur du ministre communique qu'au sein du Conseil de l'Europe, un projet de convention portant sur l'aspect international est en train d'être finalisé. Il est difficile de trouver des solutions qui soient acceptables par tous les États car ceux-ci ne sont pas toujours prêts à admettre une étape nouvelle qui constitue un abandon de souveraineté. Selon le collaborateur du ministre, il y a lieu de partager la souveraineté si on veut encore en avoir une.

### 3. **Parallélisme avec les sanctions prévues en matière de protection de la vie privée**

Il n'existe pas un parallélisme complet entre les sanctions retenues par le présent projet de loi et celles applicables en matière de protection de la vie privée étant donné qu'il règne une différence essentielle. L'atteinte à la vie privée signifie que de façon injustifiée et sans l'accord de l'intéressé, on essaie d'obtenir des données qui ont une influence sur sa vie privée. Ceci ne

te komen van gegevens die een invloed hebben op diens privé-leven. Welnu, dat is niet noodzakelijk een oogmerk van de computercriminaliteit die zeer vaak een financieel doel heeft. Hoewel dus een zeker parallellisme kan worden vastgesteld, mag men de economische aspecten van de computercriminaliteit niet uit het oog verliezen.

4. **Laattijdigheid van het wetsontwerp**

Hoewel de heer Poncelet zich verheugt over de indiening van dit wetsontwerp, meent hij toch te moeten wijzen op de laattijdigheid ervan. Men moet er rekening mee houden dat het niet mag worden benaderd als een geïsoleerd ontwerp. Er moeten er immers nog andere volgen, met name inzake de elektronische handtekening en inzake de bewijslevering.

5. **Raadpleging van de Commissie voor de bescherming van de persoonlijke levenssfeer**

De minister heeft die commissie niet geraadpleegd, maar hij heeft er geen bezwaar tegen dat ze door de commissie voor de Justitie wordt geraadpleegd.

6. **Toepassing van het wetsontwerp**

Sommigen hebben de vrees uitgesproken dat de voor de toepassing van de wet vereiste investering achterwege zal blijven. Het is natuurlijk wel zo dat bij de opsporingsdiensten slechts weinigen met die aangelegenheid vertrouwd zijn. Men zal er dan ook voor moeten zorgen dat voor dat werk voldoende personeel wordt ingezet. De minister vestigt er niettemin de aandacht op dat het wetsontwerp in de mogelijkheid voorziet om de nodige bijstand te vragen en een externe deskundige in de arm te nemen. Eigenlijk zou moeten worden gedacht aan een multidisciplinaire benadering waarvoor men niet alleen juristen maar ook informaticaspecialisten bij de parketten in dienst zal moeten nemen.

7. **Begrip « passende middelen »**

Op de vraag naar een betere definitie van dat begrip antwoordt de minister dat het Wetboek van strafvordering tal van onderzoeksmaatregelen bevat die al evenmin nader worden omschreven.

8. **Problematiek van de straffen**

Een lid merkt op dat personen die zich te goeder trouw tot een systeem toegang verschaffen, strafrechconstitue pas nécessairement un objectif de la criminalité informatique. Très souvent, un objectif financier est poursuivi. Si dès lors un parallélisme peut être établi, il ne faut pas oublier les aspects économiques de la criminalité informatique.

4. **Aspect tardif du projet de loi**

M. Poncelet, tout en se réjouissant du dépôt du présent projet, a souligné qu'il avait un aspect tardif. Il ne faut pas négliger le fait que ce projet ne peut être abordé comme étant isolé. D'autres projets de loi doivent suivre notamment en matière de signature électronique et de preuve.

5. **Consultation de la commission de protection de la vie privée**

Cette commission n'a pas été consultée par le gouvernement. Le ministre ne formule néanmoins aucune objection à sa consultation par la commission de la Justice.

6. **Application du projet de loi**

Des craintes ont été émises que l'investissement nécessaire à l'application du projet de loi ne suivrait pas. Certes, au sein des services d'enquête, peu sont ceux qui sont familiarisés avec cette matière. Il faudra dès lors veiller à ce qu'un personnel suffisant soit affecté à ce travail. Le ministre attire cependant l'attention sur le fait que le projet de loi prévoit la possibilité de requérir l'assistance nécessaire. Il peut également être fait appel à un expert extérieur. En définitive, il y aura lieu de réfléchir à une approche multidisciplinaire qui implique non seulement le recrutement de juristes mais également de spécialistes en informatique au sein des parquets.

7. **Notion de « moyens appropriés »**

Devant la demande faite de mieux définir cette notion, le ministre répond qu'il existe dans le Code d'instruction criminelle, de nombreuses mesures d'instruction qui ne sont également pas plus précisées.

8. **Problématique des peines**

Un membre a fait remarquer que des personnes qui de bonne foi, s'introduisent dans un système, vont se

telijke straffen boven het hoofd hangen, hoewel hun zaak in voorkomend geval civielrechtelijk haar beslag zou kunnen krijgen.

De minister weerlegt die opmerking met erop te wijzen dat de regering bij de vaststelling van de diverse omschrijvingen van de strafbaarstellingen erg omzichtig te werk is gegaan. Tot de vereisten behoorden altijd het bijzonder opzet en de gelijktijdige aanwezigheid van de morele en de materiële factor.

Dit betekent echter niet dat men de civielrechtelijke weg noodzakelijkerwijze links moet laten liggen.

De in het wetsontwerp gestelde straffen sluiten overigens de mogelijkheid van alternatieve straffen niet uit. Rest nog de vraag of andere straffen moeten worden uitgesproken, zoals een beroepsverbod. De minister merkt ook op dat de « *hackers* » niet altijd beroepsmensen zijn. De genuanceerde beoordeling door de rechter op grond van het dossier biedt dan ook meer waarborgen.

Ter afronding geeft de medewerker van de minister aan dat men inzake de sabotage van computergegevens niet de aanzienlijke schade mag vergeten die ze kan aanrichten. De straffen moeten in verhouding staan tot de mogelijke schade.

9. **Verwijdering van gegevens die strijdig zijn met de openbare orde of de goede zeden**

De minister meent dat de onderzoeksrechter of de procureur des Konings die mogelijkheid moeten krijgen.

10. **Recht op eerbied voor de persoonlijke levenssfeer**

De Raad van State adviseert dat alleen de wet sommige beperkingen kan opleggen aan het recht op een persoonlijke levenssfeer. Volgens de minister blijkt uit de analyse van dat advies dat de Raad van State ook opportuniteitskwesties heeft aangesneden. Hij vraagt zich dan ook af of die kwesties niet buiten de bevoegdheid van de Raad van State vallen.

11. **« *Hackertools* »**

Het is de minister bekend dat « *hackertools* » vrij in de handel te koop zijn. Het wetsontwerp strekt er alleen toe bestraffend op te treden tegen personen die deze « *hackertools* » gebruiken met het voornemen schade te berokkenen; er worden uiteraard geen straffen in uitzicht gesteld voor wie die techniek aanwendt als er zich moeilijkheden voordoen om toegang te krijgen tot het eigen netwerk.

trouver sanctionnées pénalement alors que cette situation pourrait être régie par le droit civil.

Le ministre réfute cette remarque en faisant valoir que le gouvernement a été très prudent dans les qualifications qui ont été retenues pour les diverses incriminations. Une intention spéciale a toujours été requise. Tant l'élément moral que l'élément matériel doivent coexister.

Ceci ne signifie cependant pas que la piste du droit civil doit *ipso facto* être abandonnée.

Par ailleurs, les peines prévues dans le projet de loi n'excluent nullement que des peines alternatives soient prononcées. Il reste la question de savoir si d'autres peines ne doivent pas être prononcées comme des interdictions professionnelles. Le ministre fait pour sa part, remarquer que les « *hackers* » n'appartiennent pas toujours au monde professionnel. L'appréciation nuancée faite par le juge sur base du dossier offre plus de garanties.

Enfin, le collaborateur du ministre précise qu'en ce qui concerne le sabotage des données informatiques, il ne faut pas oublier le préjudice non négligeable qui peut être causé. Les sanctions doivent être proportionnées au dommage qui peut être causé.

9. **Retrait de données contraires à l'ordre public et aux bonnes mœurs**

Le ministre est d'avis que cette possibilité doit être accordée au juge d'instruction et au procureur du Roi.

10. **Droit au respect de la vie privée**

Selon le Conseil d'État, seule la loi peut apporter certaines restrictions au droit à la vie privée. Pour le ministre, l'analyse de cet avis révèle que le Conseil d'État a également abordé des questions d'opportunité. Il se pose dès lors la question de savoir si ces questions ne sont pas étrangères à la compétence du Conseil d'État.

11. **« *Hackertools* »**

Le ministre est conscient que ceux-ci sont librement en vente dans le commerce. Le projet de loi tend uniquement à sanctionner ceux qui utilisent ces « *hackertools* » avec la volonté de nuire et non dans le but d'avoir accès à leur propre réseau en cas de difficulté.

12. **Inachtneming van de persvrijheid**

De minister is geenszins gekant tegen het argument dat wordt ingeroepen om in dit verband de inachtneming van de persvrijheid te garanderen. Er zullen voorzorgen moeten worden genomen om te voorkomen dat noch de openbare orde en de goede zeden, noch de persvrijheid worden aangetast.

13. **Poging tot computerfraude**

In artikel 504*quater* in ontwerp komt het begrip « poging » niet voor.

Voorts wordt alleen in § 2 gewag gemaakt van het verwerven van een bedrieglijk vermogensvoordeel, hoewel dat begrip in § 1 zou moeten worden opgenomen.

De minister kondigt aan dat in dit verband een amendement zal worden ingediend.

C. **REPLIEKEN**

*De heer Derycke* suggereert dat in artikel 210*bis* zou worden vermeld dat de valsheid (waardoor de juridische draagwijdte van de gegevens verandert), schade toebrengt aan derden. Rechtspraak en rechtsleer vereisen het element van « schade » indien een bijzonder opzet dient te worden vastgesteld.

*De voorzitter* stelt voor om dit op te lossen door middel van een wijziging van het opschrift van deze bepalingen. Concreet stelt hij voor om in artikel 193 van het Strafwetboek de woorden « geschriften of in telegrammen » te vervangen door de woorden « geschriften, in informatica of in telegrammen ».

De voorzitter stelt tevens vast dat er een discrepantie is tussen de bevoegdheden van de procureur des Konings en van de onderzoeksrechter. De procureur des Konings kan zaken wissen, die bevoegdheid is niet aan de onderzoeksrechter toegekend. Vandaar de vraag of er een verhaal is tegen de beslissing van de procureur om een bestand te wissen.

12. **Respect de la liberté de la presse**

Le ministre n'est nullement insensible à l'argument invoqué demandant la garantie du respect de la liberté de la presse dans ce domaine. Des précautions devront être prises pour que tant l'ordre public et les bonnes moeurs que la liberté de la presse soient respectés.

13. **Tentative de fraude en informatique**

L'examen de l'article 504*quater* en projet montre que le terme « tentative » n'y figure pas.

Par ailleurs, l'obtention d'un avantage patrimonial frauduleux est seulement invoqué au paragraphe deux alors qu'il devrait figurer au paragraphe premier.

Le ministre annonce le dépôt d'un amendement à ce propos.

C. **RÉPLIQUES**

*M. Derycke* suggère qu'il soit précisé à l'article 210*bis* que le faux (qui modifie la portée juridique des données) porte préjudice à des tiers. La jurisprudence et la doctrine requièrent en effet qu'il y ait un « préjudice » s'il y a lieu de constater l'existence d'une intention particulière.

*Le président* propose de résoudre ce problème en modifiant l'intitulé de ces dispositions. Concrètement, il propose de remplacer, dans l'article 193 du Code pénal, les mots « en écritures ou dans des dépêches télégraphiques » par les mots « en écritures, en informatique ou dans des dépêches télégraphiques ».

Le président constate également qu'il y a discordance entre les compétences du procureur du Roi et celles du juge d'instruction. Le procureur du Roi pourra effacer des données, alors que le juge d'instruction n'aura pas cette possibilité. Aussi peut-on se demander s'il y aura une possibilité de recours contre la décision du procureur d'effacer un fichier.

## III. — **HOORZITTINGEN**

### A. HOORZITTING MET DE HEER THOMAS, VOORZITTER VAN DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER, EN MET MEVROUW BOULANGER, SECRETARIS VAN DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

#### 1. **Uiteenzetting**

De heer Thomas wijst er meteen op dat hij zijn uiteenzetting binnen een zeer kort tijdsbestek heeft moeten voorbereiden.

Hij herinnert eraan dat de commissie een college is dat is samengesteld uit 17 leden, van wie er 16 niet vast zijn (professoren, ambtenaren-generaal, advocaten, magistraten enz.). Alleen de voorzitter is vast.

Hij voegt eraan toe dat hij bij de voorbereiding van zijn uiteenzetting is bijgestaan door de secretaris van de commissie — mevrouw Boulanger — die zelf een ploeg van zes juristen en een informaticus vertegenwoordigt. Dat betekent dat wat zal volgen niet alleen zijn bescheiden mening is, maar ook de vrucht van een voorbereiding door juristen verbonden aan het secretariaat van de commissie; het is geenszins de uitdrukking van het collegiaal advies van de 16 andere leden van de commissie. Daar ligt het hele verschil tussen de Commissie voor de bescherming van de persoonlijke levenssfeer en de Raad van State. Adviesverstrekking binnen 3 dagen is bij deze laatste instelling mogelijk; met uitzondering van de assessoren, is de Raad van State ook grotendeels samengesteld uit vaste leden die bovendien niet collegiaal moeten beslissen, maar zijn onderverdeeld in min of meer gespecialiseerde kamers.

Aangezien er met betrekking tot de bescherming van de persoonlijke levenssfeer heel wat op het spel staat, werd een bijzondere inspanning geleverd. De heer Thomas zal zich ook niet beperken tot een uiteenzetting op deze hoorzitting. Hij verbindt er zich toe in de loop van de maand december op eigen initiatief een advies in te dienen dat de vrucht zal zijn van collegiale arbeid en dat de twee ingediende ontwerpen artikelsgewijs zal onderzoeken. Vandaag zal hij zich beperken tot ontwerp nr 214/1; na contact met de professoren De Schutter van de VUB en Poullet van de Rechtsfaculteit van Namen, heeft hij immers moeten vaststellen dat de meningen inzake ontwerp nr 213/1 uiteenlopen, zodat een collegiale bespreking nodig is.

De door beide wetsontwerpen beoogde gegevens behoren tot de beschermingssfeer van de privacywet en haar specifieke beginselen voorzover die gegevens

## III. — **AUDITIONS**

### A. AUDITION DE M. THOMAS, PRÉSIDENT DE LA COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE ET DE MME BOULANGER, SECRÉTAIRE DE LA COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE

#### 1. **Exposé**

D'emblée, *M. Thomas* tient à préciser qu'il n'a disposé que d'un délai fort court pour préparer son exposé.

Il rappelle que la commission est un collège composé de 17 membres dont 16 sont non permanents (professeurs d'université, fonctionnaires généraux, avocats, magistrats, etc.). Seul le président est permanent.

Il ajoute qu'il a été assisté, dans la préparation de son exposé, par la secrétaire de la commission — Mme Boulanger — qui représente elle-même une équipe composée de six juristes et d'un informaticien. Cela signifie que les propos qui vont suivre sont non seulement son modeste avis mais le fruit d'une préparation de juristes attachés au secrétariat de la commission; ils ne sont en rien l'expression de l'avis collégial des 16 autres membres de la commission. C'est là toute la différence entre la commission pour la protection de la vie privée et le Conseil d'État; en effet, ce dernier peut être consulté dans les 3 jours et est composé en très grande partie, hormis les assesseurs, de membres permanents qui, de plus, ne doivent pas délibérer en collège mais sont subdivisés en chambres plus ou moins spécialisées.

Les enjeux étant importants en termes de protection de la vie privée, un effort tout spécial a été fourni. Aussi, l'exposé de M. Thomas ne s'arrêtera pas à la présente audition. Il s'engage à remettre, dans le courant du mois de décembre, un avis d'initiative qui sera le fruit d'un travail collégial et étudiera les deux projets soumis, article par article. Aujourd'hui, il se bornera à évoquer le projet n° 214/1. En effet, après avoir contacté les professeurs De Schutter de la VUB et Poullet de la Faculté de droit de Namur, il a dû constater des opinions divergentes en ce qui concerne le projet n° 213/1, d'où la nécessité d'un débat au sein de l'organe collégial.

Dans la mesure où les données envisagées par ces deux projets de loi portent sur des personnes physiques identifiées ou identifiables, elles tombent dans le

betrekking hebben op een natuurlijke persoon die is of kan worden geïdentificeerd.

Wat haar beginselen betreft, moet aan ten minste twee ervan worden herinnerd. Het eerste, waarnaar de Raad van State in zijn uiteenzetting overigens verwijst, betreft de vereiste rechtsgrond — voorgeschreven bij artikel 22 van de Grondwet — om van schending te kunnen spreken van het recht dat ieder heeft op eerbiediging van zijn privé- en gezinsleven. Zo moeten de maatregelen waarbij de politie-, gerechtelijke en veiligheidsdiensten zich met het privé-leven inlaten, een rechtsgrond krijgen, maar ook noodzakelijk worden geacht in het kader van een democratische samenleving : zij moeten niet alleen een wettelijke, maar ook een wettige finaliteit hebben.

Een tweede beschermingsbeginsel is dat van de evenredigheid. De commissie brengt dit beginsel in elk van haar adviezen in herinnering, zoals bijvoorbeeld in het advies van 1997 betreffende het opsporen van nummers en titularissen van communicatie- en telecommunicatietoestellen of nog, begin dit jaar, in het advies over een ontwerp inzake de noodzakelijke medewerking van netwerkoperatoren en dienstenverstrekkers. De commissie heeft in dat geval niet nagelaten het evenredigheidsbeginsel te benadrukken. Dit betekent dat maatregelen om zich met het privé-leven te kunnen inlaten, uitzonderlijk moeten blijven en maar wettig zijn indien strikt noodzakelijk voor het lopende onderzoek.

Wat de teksten van de wetsontwerpen zelf betreft, mag men niet vergeten dat de algemene beginselen voor de bescherming van het privé-leven als maatstaf moeten dienen om elk artikel te toetsen aan de vereisten van de wetgeving inzake de bescherming van de persoonlijke levenssfeer.

De heer Thomas neemt het laatste artikel van wetsontwerp nr 214/1 onder de loep : artikel 9, dat tot doel heeft artikel 109*ter*, e) van de wet van 21 maart 1991 te wijzigen. Het zou toelaten de dienstenverstrekkers te verplichten oproep- en identificatiegegevens van door de Koning te bepalen gebruikers te registreren en te bewaren — wat inhoudt dat ze afzonderlijk worden verwerkt — binnen een door de Koning te bepalen termijn. De Koning zou dit regelgevend werk moeten verrichten na beraadslaging in de Ministerraad. De Raad van State heeft niet nagelaten op te merken dat dit regelgevend werk volstrekt niet de vereiste rechtsgrond vormt. De indiener van het ontwerp beroept zich op de techniciteit van de zaak en de technologische evolutie, die soepelheid vergen om zich aan die evolutie te kunnen aanpassen.

Het is de spreker niet duidelijk in welke mate de technologische evolutie van invloed kan zijn op het bepalen van de bewaringstermijn van de gegevens die aldus op een afzonderlijke manier worden verwerkt. Die

champ protecteur de la loi sur la protection de la vie privée et de ses principes spécifiques.

Quant à ces principes, il y a lieu d'en rappeler au moins deux. Un premier — qui a d'ailleurs fait l'objet d'un exposé de la part du Conseil d'État — concerne l'exigence de bases légales — prescrit de l'article 22 de la Constitution — pour permettre d'enfreindre le droit de chacun au respect de sa vie privée et familiale. Ainsi, les mesures d'ingérence dans la vie privée par les services judiciaires, de police ou de sûreté doivent faire l'objet d'une base légale mais doivent aussi être jugées nécessaires dans le cadre d'une société démocratique; elles doivent avoir une finalité non seulement légale mais aussi légitime.

Un deuxième principe protecteur, c'est le principe de proportionnalité. La commission rappelle ce principe dans chacun de ses avis comme, par exemple, l'avis rendu en 1997 concernant le repérage des numéros et titulaires de postes de communications et de télécommunications ou encore, au début de cette année, l'avis concernant un projet touchant à la collaboration nécessaire des opérateurs de réseaux et fournisseurs de services. En l'occurrence, la Commission n'a pas manqué d'expliciter ce principe de proportionnalité. Cela signifie que les mesures d'ingérence dans la vie privée doivent rester l'exception et ne sont légitimes que dans la seule mesure du strict nécessaire à l'instruction en cours.

Pour aborder plus exactement les textes des projets de loi, il faut se rappeler que les principes généraux de la protection de la vie privée doivent servir d'aune pour apprécier chaque article au regard des exigences de la législation sur la vie privée.

M. Thomas prend en considération le dernier article du projet de loi n° 214/1, l'article 9 qui a pour vocation de modifier l'article 109*ter*, e) de la loi du 21 mars 1991. Il permettrait d'obliger les fournisseurs de services d'enregistrer et de conserver — c'est-à-dire créer un traitement distinct —, dans un délai à déterminer par le Roi, les données d'appel et d'identification des utilisateurs à déterminer par le Roi. Le Roi devrait accomplir ce travail réglementaire après en avoir délibéré en Conseil des ministres. Le Conseil d'État n'a pas manqué d'observer que le travail réglementaire royal n'était pas du tout la base légale requise. L'auteur du projet a invoqué la technicité de la question et l'évolution des techniques qui demandent une souplesse permettant de s'adapter à cette évolution.

Plus particulièrement en ce qui concerne la détermination de la durée de conservation des données ainsi traitées d'une manière distincte — cette détermination de la durée de conservation étant d'une importance

bepaling is overigens van het grootste belang voor de bescherming van die gegevens.

Hij herhaalt dat er talrijke verschillen bestaan tussen de Commissie voor de bescherming van de persoonlijke levenssfeer en de Raad van State. De Raad van State is samengesteld uit eminente theoretici, terwijl de commissie, ook al hebben daarin een aantal universiteitsprofessoren zitting, is samengesteld uit personen die praktijkervaring hebben opgebouwd. Het gemengde karakter van de commissie laat hem toe te stellen dat er wellicht technischer gegevens zijn, zoals de minimale capaciteitsgrens, die meer soepelheid zouden kunnen vergen. Eventueel kan worden overwogen dergelijk flexibel werk van aanpassing aan de technologische evolutie over te laten aan de Koning, maar dan dient men de logica te volgen van het ontwerp in paragraaf 4 van hetzelfde artikel 109*ter*, e). Overeenkomstig die paragraaf is het de Koning die ervoor zorgt dat maatregelen worden getroffen om de vertrouwelijkheid en de integriteit van de oproep- en identificatiegegevens te waarborgen, en krijgt de Commissie voor de bescherming van de persoonlijke levenssfeer adviserende bevoegdheid.

In de mate dat de parlementsleden van oordeel zijn dat de door de minister aanbevolen soepelheid noodzakelijk is, zou dezelfde commissie ook voor paragraaf 2 adviserende bevoegdheid kunnen krijgen.

Het is eveneens interessant een en ander te toetsen aan het evenredigheidsbeginsel. Volgens dit artikel kunnen de gegevens in kwestie op om het even wie betrekking hebben, ongeacht of men al dan niet onder verdenking staat. Nadere preciseringen ontbreken volkomen. Aldus neemt dat onderzoek de vorm aan van een proactieve recherche, waarvan bij wijze van spreken de hele bevolking het voorwerp zou kunnen uitmaken — of op zijn minst alle klanten van telecommunicatiebedrijven. Iedereen loopt aldus het risico dat zijn of haar gegevens onder de loep worden genomen. Een en ander komt neer op een algemeen onderzoek dat verder gaat dan wat strikt noodzakelijk is in het raam van een lopend gerechtelijk onderzoek. Het verschil is evenwel dat de proactieve recherche bij wet is vastgelegd en georganiseerd; bovendien bestaat terzake een raamwerk, aangezien de procureur des Konings, de procureur-generaal, het college van procureurs-generaal of de nationaal magistraten, als vertegenwoordigers van de rechterlijke macht, hun verantwoordelijkheid op zich kunnen nemen en op voorhand een vorm van proactieve recherche kunnen aanvaarden, rekening houdend met bepaalde voorwaarden, beperkingen

capitale pour la protection desdites données — l'orateur ne voit pas bien en quoi cette détermination serait liée à l'évolution des techniques.

Il répète que plusieurs différences existent entre la Commission pour la protection de la vie privée et le Conseil d'État. Le Conseil d'État est composé de grands théoriciens alors que la commission, certes si elle comporte quelques professeurs d'université, est composée de personnes qui ont acquis sur le terrain une expérience pratique. Cette mixité de la commission lui permet de dire qu'il y a sans doute des données plus techniques comme, par exemple, le seuil minimum de capacité qui pourraient demander plus de souplesse. On pourrait peut-être envisager que le Roi effectue ce travail de souplesse et d'adaptation au gré des évolutions de la technique mais alors il faudrait conserver la logique dont le projet a fait état dans le paragraphe 4 du même article 109*ter*, e). Ce paragraphe qui laisse au Roi le soin de prévoir les mesures qui garantissent la confidentialité et l'intégrité des données d'appel et d'identification, et ne manque pas de prévoir l'avis de la Commission pour la protection de la vie privée.

Dans la mesure où les parlementaires estimeraient que la souplesse recommandée par le ministre s'impose, le paragraphe 2 pourrait aussi faire l'objet d'un avis de la même commission.

On peut poursuivre l'exercice en abordant la question du principe de proportionnalité. À lire cet article, les données visées peuvent concerner quiconque, personne soupçonnée ou non. Rien n'est précisé. C'est ainsi que cette recherche prend les allures d'une recherche pro-active qui pourrait viser, à la limite, la population entière ou, en tout cas, l'ensemble des utilisateurs des services de télécommunications. Tout le monde risque de voir ses données traitées. On se trouve alors dans une recherche générale qui s'éloigne du strictement nécessaire à une instruction judiciaire en cours. La différence, c'est que la recherche pro-active est prévue et organisée; de plus, un encadrement est mis en place en ce sens que le pouvoir judiciaire, incarné tantôt par le procureur du Roi, le procureur général, le collège des procureurs généraux ou les magistrats nationaux, prend sa responsabilité pour accepter à l'avance telle recherche pro-active selon telles modalités, dans telles limites et à telle finalité. C'est un grand progrès réalisé récemment. Cependant, en l'occurrence, on se trouve devant une pratique qui semble se détacher de ce contexte bien organisé qu'est la recherche pro-active tout en en ayant les caractéristiques mais sans l'enca-

en doelstellingen. Het betreft hier een recente evolutie die een grote stap vooruit betekent. Niettemin wijkt die praktijk af van de in een goed georganiseerde context ingebedde proactieve recherche : alleen de kenmerken ervan werden overgenomen, maar niet het raamwerk. Het kan niet anders dan dat de commissie voor de bescherming van de persoonlijke levenssfeer bij die evolutie voorbehoud zal maken.

Tevens brengt de heer Thomas in herinnering dat de voor de bescherming van de persoonsgegevens bevoegde Europees commissarissen in een gemeenschappelijke vergadering op basis van artikel 29 van een Europese richtlijn van 1995 hebben verwezen naar de rechtspraak van het Europees Hof voor de rechten van de mens, dat elk grootschalig gebruik van telecommunicatiegegevens voor algemene doeleinden of voor onderzoeksdoeleinden verbiedt.

Samenvattend kan dus worden gesteld dat de gegevens waarover het in artikel 109*ter*, e), moet gaan, niet nader zijn omschreven; dat is evenmin het geval voor de in aanmerking genomen misdrijven, personen of categorieën van personen. Tot slot is nergens sprake van een bewaringstermijn, terwijl die bijvoorbeeld in Duitsland drie maanden bedraagt.

Zo'n bewaringstermijn moet er hoe dan ook komen. De parlementsleden hebben de taak en de verantwoordelijkheid daarvoor te zorgen, in naam van de bescherming van de persoonlijke levenssfeer en overeenkomstig artikel 22 van de Grondwet.

Het zou niet door de beugel kunnen dat men verschillende afzonderlijke en bijkomende gegevensbanken creëert, gewoon « omdat die wel eens van pas zouden kunnen komen ».

In dat verband zij erop gewezen dat de dienstverleners nieuwe systemen voor gegevensbeheer of gegevensbanken moeten uitwerken, al zouden zij dat normaal gezien niet hebben gedaan of in elk geval met een ander oogmerk, bijvoorbeeld voor factureringsdoeleinden. Het beleid terzake moet hoe dan ook nog worden uitgestippeld, maar die explosieve toename van het aantal nieuwe gegevensbanken doet een nieuwe bedreiging voor de persoonlijke levenssfeer ontstaan. Derhalve is waakzaamheid geboden, met name bij de advies- en controle-instanties.

Voorts is gepoogd de in de ontworpen tekst opgenomen misdrijven en de bij de wet op de bescherming van de persoonlijke levenssfeer bepaalde en bestrafte overtredingen meer op elkaar af te stemmen. Er doen zich op dat vlak overlappingen voor.

Zo wordt een nieuw misdrijf in het leven geroepen, valsheid in informatica genaamd, dat zou worden omschreven in artikel 210*bis* van het Strafwetboek. Dat misdrijf zou kunnen worden ingepast in het begrip « gegevensverwerking », aangezien het verband houdt met onjuiste gegevens zoals bepaald en bestraft bij artikel 39, 1°, van de wet tot bescherming van de persoondrement; ceci ne peut qu'alarmer la commission pour la protection de la vie privée.

M. Thomas rappelle aussi que l'ensemble des commissaires européens à la protection des données, regroupés en vertu de l'article 29 d'une directive européenne de 1995, ont rappelé la jurisprudence de la Cour européenne des droits de l'homme qui proscrit toute surveillance exploratoire ou générale des télécommunications à grande échelle.

En résumé, les données dont il doit s'agir dans cet article 109*ter*, e), ne sont pas circonscrites; les délits visés ne le sont pas non plus de même que les personnes ou catégories de personnes. Enfin, le délai de conservation n'est pas défini alors qu'en Allemagne, par exemple, un délai de 3 mois est prévu.

Il faut déterminer un délai de conservation; c'est la tâche des parlementaires et leur responsabilité au nom même de cette protection de la vie privée et de l'article 22 de la Constitution.

Il ne faudrait pas en arriver à créer diverses banques de données distinctes et supplémentaires en application du fantasme qui veut que « cela peut toujours servir un jour ».

À cet égard, on relève que les fournisseurs de services sont tenus de créer de nouveaux traitements ou banques de données alors que normalement ils ne l'auraient pas fait ou l'auraient fait pour une autre finalité comme, par exemple, une finalité de facturation. C'est une politique à déterminer mais cette prolifération de nouvelles banques de données engendre des risques nouveaux pour la vie privée. La vigilance s'impose et, en particulier, dans le chef d'instances d'avis et de contrôle.

Un autre exercice a été livré, à savoir rapprocher les délits prévus par le texte en projet et les infractions prévues et sanctionnées par la loi sur la protection de la vie privée. On constate des chevauchements en la matière.

Tout d'abord, une nouvelle infraction serait le faux informatique tel qu'il serait défini à l'article 210*bis* du Code pénal. Ce faux pourrait se rapprocher du traitement dans la mesure où il porte sur des données personnelles inexactes prévues et sanctionnées à l'article 39, 1°, de la loi sur la protection de la vie privée ou encore de la communication de renseignements

lijke levenssfeer. Voorts zou men valsheid in informatica ook kunnen gelijkstellen met de verstrekking van onjuiste gegevens wanneer de betrokkene zijn inzagerecht uitoefent (zie artikel 5 van dezelfde wet).

Vervolgens zou het in artikel 504*quater* van het ontwerp omschreven informaticabedrog of nog de *hacking* bedoeld in artikel 550*bis* van het ontwerp, kunnen overeenstemmen met inbraak in een gegevensbank, met ongeoorloofde verwerking, of zelfs met doelafwending, drie strafbare handelingen die de wet op de bescherming van de persoonlijke levenssfeer ook als zodanig bestraft.

Dat parallellisme is een zaak. Een andere is de vaststelling dat de in de bestudeerde teksten voorgestelde strafmaat zwaarder is dan die waarin de wet op de bescherming van de persoonlijke levenssfeer voorziet : voormelde teksten voorzien immers ook in gevangenisstraffen, terwijl de wet op de bescherming van de persoonlijke levenssfeer terzake — op de geldboetes na — gematigder is. Daarbij komt nog dat de teksten voorzien in een gevangenisstraf van 6 maanden, terwijl de wet op de bescherming van de persoonlijke levenssfeer alleen bij recidive een gevangenisstraf van 3 maanden toepast. De vraag rijst dan ook of de wetgever overweegt verschillende kwalificaties onderling te cumuleren : moet of kan het parket de diverse misdrijven samenvoegen die in het wetsontwerp én in de vigerende de wet op de bescherming van de persoonlijke levenssfeer omschreven zijn ? Zal die optelling van misdrijven dan ook leiden tot een gecumuleerde strafmaat of is de wetgever voornemens de ene wetgeving op de andere te laten prevaleren ? Zo ja, welke wetgeving zal prioritair van toepassing zijn ? De elementaire rechtszekerheid vraagt dat terzake klaarheid wordt geschapen.

Vooraleer te besluiten, wenst de spreker te preciseren dat de leden van de commissie voor de Justitie — in weerwil van de in de wet op de bescherming van de persoonlijke levenssfeer ingebouwde termijn van 2 maanden — van oordeel zijn dat terzake urgentie geboden is. Als dat zo is, dan moet de samenstelling van de Commissie voor de bescherming van de persoonlijke levenssfeer opnieuw worden bekeken (bijvoorbeeld minder losse commissarissen maar, naast de vaste voorzitter, een of twee vaste commissarissen) en moet ook worden nagegaan hoe de personele middelen van de commissie (aantal deskundigen-juristen en informatici) kunnen worden verhoogd.

In vergelijking met de commissies van de ons omringende landen in de Europese Unie, beschikt België over een bestaffing die tussen een derde en een tiende van die van onze buurlanden draait.

inexacts lorsque l'intéressé exerce son droit d'accès (cf. article 5 de la même loi).

Ensuite, la fraude informatique prévue à l'article 504*quater* en projet ou encore le *hacking* prévu à l'article 550*bis* en projet pourraient correspondre à une intrusion dans un fichier, à un traitement illicite, voire à un détournement de finalité, trois agissements coupables et sanctionnés comme tels dans la loi sur la protection de la vie privée.

Ce parallèle étant fait, l'observation s'impose que les peines imaginées dans les textes étudiés sont plus lourdes que celles prévues par la loi sur la protection de la vie privée en ceci qu'elles comportent des emprisonnements alors que la loi sur la protection de la vie privée est plus modérée, sauf en ce qui concerne les amendes; il faut ajouter qu'un emprisonnement de l'ordre de 6 mois est prévu alors que la loi sur la protection de la vie privée n'appliquait une peine de 3 mois qu'en cas de récidive. La question se pose de savoir si le législateur envisage le cumul des qualifications; pour un même fait, le parquet peut-il ou doit-il reprendre l'accumulation de ces différentes infractions définies, tantôt dans la loi en projet, tantôt dans la loi existante sur la protection de la vie privée ? Ce cumul entraînera-t-il le cumul des peines ou, au contraire, le législateur envisage-t-il une priorité d'une législation par rapport à l'autre ? Si oui, laquelle ? La sécurité juridique élémentaire exige une clarté en la matière.

Avant de conclure, l'orateur souhaite préciser que, si l'urgence est aux yeux des membres de la commission de la Justice un impératif, malgré le délai de 2 mois prévu par la loi sur la protection de la vie privée, il faudra revoir la composition de la Commission pour la protection de la vie privée (par exemple, moins de commissaires non permanents mais un ou deux commissaires permanents à côté du président permanent) et/ou revoir l'extension des moyens de la commission en nombre d'experts juristes et informaticiens.

Si l'on fait la comparaison avec l'ensemble des commissions des pays voisins au sein de l'Union européenne, la Belgique dispose d'un effectif se situant entre le tiers et le dixième de celui de ses voisins.

2. **Bespreking**

*De voorzitter* merkt op dat hij, bij de eerste lezing van het ontwerp, een aantal technische problemen had opgemerkt, en tevens op het verschil had gewezen tussen de in dit ontwerp ingebouwde strafmaten en die waarin de wet op de bescherming van de persoonlijke levenssfeer voorziet. Bovendien kan een bespreking aan de valsheid in geschriften worden gewijd : het Strafwetboek voorziet daarvoor namelijk in criminele straffen waarbij dan telkens moet worden gepreciseerd dat de behandeling voor de correctionele rechtbank moet geschieden, terwijl het ter bespreking voorliggende ontwerp die correctionele behandeling impliciet inbouwt.

*
* *

*De heer Geert Bourgeois (VU&ID)* maakt de volgende opmerkingen :

Ten eerste, in verband met de voorgestelde wijziging van artikel109*ter*, e) van de wet op de bescherming van de persoonlijke levenssfeer, wijst hij erop dat de heer Thomas een reeks bedenkingen heeft geformuleerd die gedeeltelijk overeenstemmen met de stelling van de Raad van State, namelijk, verwijzend naar artikel 22 van de Grondwet : « Het (staat) aan de wetgever te bepalen welke gegevens moeten worden geregistreerd en bewaard en in welk geval zulke maatregelen moeten worden genomen. Ten slotte mag ook alleen de wetgever bepalen met welke middelen voor een toereikende technische bescherming van die gegevens kan worden gezorgd. » (advies van de Raad van State, blz. 56).

De spreker zegt dat de heer Thomas bij die bepaling onder meer heeft verwezen naar paragraaf 4, waarin is gesteld dat het advies van de commissie moet worden verleend, terwijl het volgens de voorgestelde aanvulling van artikel 2 niet moet gebeuren. Persoonlijk kan hij deze suggestie onderschrijven.

De heer Thomas meende ook dat er eventueel een onderscheid kan worden gemaakt, namelijk dat de Koning bepaalde bevoegdheden heeft om zelf te legifereren omtrent sommige gegevens van meer technische aard, terwijl het voor andere niet zo is.

De spreker vraagt of de heer Thomas aan de commissie ook een advies kan geven aangaande de bepalingen die in de wet zouden kunnen worden opgenomen. Hiermee bedoelt hij de aard van de gegevens, die niet altijd technisch zijn, zoals de oproepgegevens en de identificatie van de betrokkene. Hij is van oordeel dat deze aangelegenheden fundamenteel zijn. Hij voegt eraan toe dat sommige zaken wellicht in een koninklijk besluit kunnen worden opgenomen.

2. **Discussion**

*Le président* remarque que, lors de sa première lecture des projets, il avait relevé des problèmes techniques, tout comme la différence entre les peines prévues et celles figurant dans la loi sur la protection de la vie privée. De plus, une discussion peut avoir lieu au sujet des faux dans la mesure où le Code pénal prévoit des peines criminelles qu'il faut, à chaque fois, correctionnaliser alors que dans le projet à l'étude il y a une correctionnalisation implicite.

*
* *

*M. Geert Bourgeois (VU&ID)* formule les observations suivantes :

En ce qui concerne, tout d'abord, la modification proposée à l'article 109*ter*, e), de la loi relative à la protection de la vie privée, il fait observer que M. Thomas a formulé un certain nombre d'observations qui recoupent en partie l'avis du Conseil d'État, en renvoyant à l'article 22 de la Constitution : « Il appartient au législateur d'identifier les données qui devront être enregistrées et conservées ainsi que les cas dans lesquels de telles mesures seront prises. Enfin, il doit également revenir au législateur de déterminer les moyens permettant une protection technique suffisante de ces données. » (avis du Conseil d'État, p. 56).

L'intervenant précise qu'en ce qui concerne cette disposition, M. Thomas a notamment fait allusion au § 4 qui prévoit que la commission doit donner son avis, alors que tel n'est pas le cas en vertu de l'ajout proposé à l'article 2. Personnellement, l'intervenant peut souscrire à cette observation.

M. Thomas estimait également qu'une distinction pouvait être faite, étant donné que le Roi a le pouvoir de légiférer lui-même pour certaines données à caractère technique, alors qu'Il n'a pas le pouvoir pour d'autres données.

L'intervenant demande si M. Thomas peut formuler un avis à l'intention de la commission au sujet des dispositions qui pourraient être reprises dans la loi. Il vise en fait la nature des données, qui ne présentent pas toujours un caractère technique, telles que les données d'appel et l'identification de l'utilisateur concerné. Il estime qu'il s'agit là de questions fondamentales et ajoute que certains aspects peuvent sans doute être réglés par voie d'arrêté royal.

Hij vraagt of de heer Thomas in zijn advies op dit punt een onderscheid zou kunnen maken, zodanig dat de wetgever er rekening kan mee houden.

De heer Thomas heeft in zijn uiteenzetting vermeld dat de categorie van de personen waaromtrent een bewaring moet gebeuren helemaal niet is omschreven. Zo zou een proactieve recherche die de hele bevolking potentieel kan treffen een zeer verregaande ingreep kunnen zijn in ieders persoonlijke levenssfeer.

Hij vraagt of daaromtrent eventueel een advies kan worden gegeven dat zou aanduiden in welke welomschreven gevallen eventueel een bewaring gedurende een bepaalde termijn nuttig kan zijn.

Inzake de termijn is de spreker van oordeel dat het nuttig zou zijn dat de wetgever zelf die termijn van bewaring bepaalt al biedt een koninklijk besluit meer flexibiliteit. Bovendien moet een termijn worden bepaald binnen welke het nuttig en wenselijk is mededeling van de gegevens te krijgen en hij ziet niet in waarom de wetgever die termijn niet zou kunnen bepalen.

De heer Bourgeois verwacht dat deze aangelegenheden in het advies worden opgenomen.

Meer algemeen sprak de heer Thomas over bepalingen die nu reeds in de wet op de bescherming van de persoonlijke levenssfeer zijn opgenomen en die eventueel een overlapping kunnen zijn.

De spreker vraagt of hij daaruit mag afleiden — terzake is geopteerd voor een integratie in het Strafwetboek en in het Wetboek van strafvordering — dat de heer Thomas eventueel opteert voor een inschrijving van die artikelen in de wet op de bescherming van de persoonlijke levenssfeer.

Dit probleem moet worden uitgewerkt om latere discussies over de kwalificatie te vermijden.

*
* *

Volgens *mevrouw Boulanger*, die eveneens in eigen naam spreekt, vormt de vraag naar de omvang van de bij koninklijk besluit te nemen uitvoeringsmaatregelen de kern van het debat. Die vraag moet zorgvuldig worden onderzocht. Regels die *a priori* van technische aard blijken te zijn, leiden er in de praktijk soms toe dat de bescherming van de persoonlijke levenssfeer in het gedrang komt.

Wat de termijnen betreft, beperken de internationale teksten (waaronder een algemene richtlijn, een specifieke richtlijn betreffende de telecommunicatietechnieken, de rechtspraak van het Europees Hof voor de rechten van de mens en de teksten van de voormelde groep van Europese commissarissen) de bewaringstermijn doorgaans tot de termijn waarbinnen de factuur

Il demande si M. Thomas peut faire une distinction à ce propos dans son avis, afin que le législateur puisse en tenir compte.

Dans son exposé, M. Thomas a fait observer que la loi ne contient aucune définition de la catégorie de personnes pour lesquelles une conservation s'impose. C'est ainsi qu'une recherche proactive pouvant porter sur l'ensemble de la population pourrait constituer une atteinte importante à la vie privée de chaque citoyen.

L'intervenant demande si l'orateur pourrait, à cet égard, donner un avis indiquant dans quels cas précis la conservation des données pendant un certain laps de temps pourrait s'avérer utile.

À ce propos, l'intervenant estime qu'il serait utile que le législateur fixe lui-même la durée de cette période de conservation même si la fixation de celle-ci par voie d'arrêté royal permet une plus grande flexibilité. Il faudrait en outre fixer un délai pendant lequel il est utile et souhaitable d'obtenir communication des données et l'intervenant estime que rien ne s'oppose à ce que ce soit le législateur qui le fixe.

M. Bourgeois souhaite que ces éléments figurent dans l'avis.

D'une manière plus générale, M. Thomas a évoqué des dispositions qui figurent déjà dans la loi relative à la protection de la vie privée et qui pourraient faire double emploi avec celles de la loi en projet.

L'intervenant demande s'il peut en inférer — il a été opté, à cet égard, pour l'insertion de ces dispositions dans le Code pénal et dans le Code d'instruction criminelle — que M. Thomas préférerait que ces articles soient insérés dans la loi relative à la protection de la vie privée.

Cette question doit être tranchée afin d'éviter ultérieurement toute discussion quant à la qualification de la loi.

*
* *

*Madame Boulanger*, qui s'exprime également à titre personnel, est d'avis que, quand on pose la question de l'étendue des mesures d'exécution par arrêté royal, on touche le cœur du débat. Cette question doit être examinée avec soin. Ces mesures ne constituent pas des garanties fondamentales; en effet, des mesures qui, *a priori*, peuvent sembler avoir un caractère technique conduisent parfois, en pratique, à empiéter sur la protection de la vie privée.

Au niveau du délai, les textes internationaux (dont une directive générale, une directive spécifique aux techniques de télécommunications, la jurisprudence de la Cour européenne des droits de l'homme et les textes du groupe de l'article 29) conduisent à limiter, en général, le délai de conservation à la durée de contestation de la facture. En Belgique, ces matières sont souvent

kan worden betwist. In België wordt die aangelegenheid veelal geregeld door de algemene voorwaarden van de operatoren van telecommunicatienetwerken of van de verstrekkers van telecommunicatiediensten. De ontworpen tekst is enigszins verschillend doordat hij bepaalt dat zelfs indien de gegevens niet worden bewaard, de verplichting kan worden opgelegd ze te registreren. Momenteel achten de verstrekkers van telecommunicatiediensten bepaalde gegevens niet dienstig zodat zij ze bijgevolg niet registreren. De ontworpen tekst biedt echter de mogelijkheid « nieuwe verwerkingen » te gaan creëren die dergelijke gegevens bevatten. In de internationale teksten wordt die hypothese doorgaans niet als dusdanig begrepen want wat men voor ogen heeft, is het hergebruik van de bestaande gegevens, met een begrenzing die dikwijls overeenkomt met de termijn waarbinnen de factuur kan worden betwist.

Nog andere opmerkingen zouden kunnen worden gemaakt over het type van gegevens waartoe men toegang zou kunnen krijgen, onder meer — sluit ze daarbij *a priori* uit — bijvoorbeeld de lokalisatiegegevens. Ook daaromtrent bestaat een zekere ambiguïteit in zover men erkent dat die gegevens wellicht niet hoeven te worden geregistreerd want ze kunnen *de facto* al beschikbaar zijn bij de operatoren en dienstenverstrekkers.

Kunnen die gegevens worden meegedeeld zonder dat nieuwe verplichtingen in het leven worden geroepen ?

In verband met de aangestipte overlapping met de wet op de bescherming van de persoonlijke levenssfeer, zij beklemtoond dat die wet onverkort van toepassing blijft. Het is niet de bedoeling wetten in elkaar te laten opgaan, maar wel in te spelen op de in de wet op de bescherming van de persoonlijke levenssfeer bedoelde voorwaarden inzake proportionaliteit en andere. Maar vooral de samenhang tussen de beide teksten is van belang, met name wat de straffen betreft.

*De heer Fred Erdman, voorzitter,* pikt in op het probleem, aangehaald door mevrouw Boulanger.

Hij wijst erop dat die aanbevelingen in feite de grondslag vormen van de voorgestelde wetswijziging. Ze verplichten de wetgever binnen het jaar de strafwet aan te passen aan de bepalingen van de aanbevelingen. Het advies kan dus worden opgesteld aan de hand van « drie kolommen » :

1. Wat was er bepaald in de wet inzake de bescherming van de privacy en welke was de interpretatie ervan ? Was de interpretatie ervan « valsheid » of « inbreuk *sui generis* » ? Dit is trouwens niet opgenomen in het Strafwetboek, maar blijft behouden in de wet op de privacy.

2. De aanbevelingen die de verplichting inhouden om het Strafwetboek aan te passen.

réglées par les conditions générales des opérateurs ou des fournisseurs de services de télécommunications. Le texte en projet est un peu différent puisqu'il prévoit que, même dans le cas où il n'y a pas conservation, on peut imposer l'obligation d'enregistrer les données. À l'heure actuelle, les fournisseurs de services de télécommunications estiment que certaines données ne sont pas utiles et donc ne les enregistrent pas. Or, le texte en projet ouvrira la possibilité de créer « des nouveaux traitements » comprenant de telles données. Dans les textes internationaux, cette hypothèse n'est généralement pas appréhendée en tant que telle car ce que l'on vise, c'est la réutilisation des données existantes avec une limite qui est souvent la durée de contestation de la facture.

D'autres remarques pourraient être faites sur les types de données auxquelles on pourrait éventuellement accéder dont notamment — et l'exposé des motifs en parle en les excluant *a priori* — par exemple les données relatives à la localisation. Là aussi il existe une certaine ambiguïté dans la mesure où l'on reconnaît qu'il ne faudrait peut-être pas enregistrer ces données alors qu'elles peuvent être disponibles *de facto* auprès des opérateurs et des fournisseurs de services.

Sans créer de nouvelles obligations, ces données seraient-elles susceptibles d'être communiquées ?

Pour ce qui concerne le chevauchement avec la loi sur la protection de la vie privée dont il a été question, il faut souligner que la loi sur la protection de la vie privée reste applicable. Il ne s'agit pas d'intégrer les législations; il s'agit plutôt de répondre aux conditions de proportionnalité et autres prévues dans la loi sur la protection de la vie privée. Mais ce qu'il faut surtout, c'est une cohérence entre les deux textes, notamment au niveau des sanctions pénales.

*M. Fred Erdman, président,* se penche sur le problème évoqué par Mme Boulanger.

Il fait observer que ces recommandations constituent en fait le fondement de la modification qu'il est proposé d'apporter à la loi. Celles-ci visent en effet à contraindre le législateur à adapter dans l'année la loi pénale en fonction des dispositions qu'elles contiennent. L'avis peut donc être établi sur la base de « trois colonnes » :

1. Que prévoyait la loi sur la protection de la vie privée et comment était-elle interprétée ? S'agissait-il d'un « faux » ou d'une « infraction *sui generis* » ? Si elles ne figurent d'ailleurs pas dans le Code pénal, ces notions sont maintenues dans la loi sur la protection de la vie privée.

2. Les recommandations qui prévoient l'obligation d'adapter le Code pénal.

Het is juist dat er zich, behoudens het kennisnemen of het eventueel wissen en wijzigen, andere situaties kunnen voordoen. Het kennisnemen hoort misschien eerder in de wet op de privacy, terwijl wissen en wijzigen eerder in de sfeer van het strafrecht thuishoort.

3. Moet de wet op de bescherming van de persoonlijke levenssfeer niet worden aangepast en/of moeten eventueel bepaalde begrippen die nu strafrechtelijk worden aangehaald, op z'n minst niet als privacy-inbreuken worden gekwalificeerd ?

De voorzitter verwijst naar de door de heer Thomas aangehaalde moeilijkheid in verband met de kwalificatie van één feit. Op het eerste gezicht lijkt hem dat geen probleem te zijn, omdat er nog bepalingen zijn — hetzij in bijzondere wetten, hetzij bepalingen van het Strafwetboek — waarbij een feit kan worden gekwalificeerd onder verscheidene strafbaarstellingen en uiteindelijk maar strafbaar is met de zwaarste straf. Op sommige plaatsen werd dat uitgesloten en op andere niet.

Los van de noodzaak om de strafbepalingen aan te passen ingevolge de aanbevelingen, is men geconfronteerd met een domein dat gestaag uitbreidt.

De voorzitter vestigt er de aandacht van de heer Thomas op dat hij niet heeft geantwoord op sommige opmerkingen van de Raad van State.

De Raad van State maakt een vergelijking inzake de raadpleging van een privé-agenda — die niet toegankelijk is — en de informatica-gegevens — die wel toegankelijk zijn. Wat is de mening van de heer Thomas hierover ?

*De heer Marc Verwilghen, minister van Justitie* dankt de heer Thomas voor het omstandig advies, waarin zijn persoonlijke visie is weergegeven.

De minister is het echter niet volledig eens met de voorstellen van de heer Thomas en waarschuwt ervoor onderhavige wet te koppelen aan of af te stemmen op de wet op de privacy. Hij is van oordeel dat dit een uiterst gevaarlijke oefening voor de beide wetgevingen inhoudt.

Volgens hem is de finaliteit van beide wetgevingen totaal anders : het gaat hem meestal om bescherming van gegevens en ook om bescherming van private belangen. In de voorliggende wet gaat het om een aantal bepalingen van het Strafwetboek, het Wetboek van strafvordering, alsook van de wetten op de economische overheidsbedrijven en de telecommunicatiesector. Het hoofddoel is echter dat de rechtshandhaving op het vlak van de informatica wordt verzekerd. De twee na te streven belangen zijn, enerzijds de bescherming van eigendommen en, anderzijds het openbaar vertrouwen in het functioneren van bepaalde systemen. In feite staat hier het rechtshandhavingssysteem ter discussie.

Il est exact qu'il peut se produire des situations autres que la consultation ou l'effacement et la modification éventuelles. La consultation relève peut-être plutôt de la loi sur la protection de la vie privée, alors que l'effacement et la modification relèvent plutôt du droit pénal.

3. Ne conviendrait-il pas d'adapter la loi sur la protection de la vie privée et/ou au moins de ne pas qualifier d'atteintes à la vie privée certaines notions qui sont utilisées actuellement en droit pénal ?

Le président évoque le problème soulevé par M. Thomas en ce qui concerne la qualification d'un fait. Il estime de prime abord qu'il ne s'agit pas d'un problème, étant donné qu'il existe d'autres dispositions — dans des lois spécifiques ou dans le Code pénal — aux termes desquelles un même fait peut être rangé sous plusieurs incriminations et n'être finalement passible que de la peine la plus lourde. Cette possibilité a été exclue à certains endroits et à d'autres, non.

Indépendamment de la nécessité d'adapter les dispositions pénales à la suite des recommandations, l'on a affaire à un domaine qui ne cesse de gagner en importance.

Le président fait observer à M. Thomas qu'il n'a pas répondu à certaines observations du Conseil d'État.

Le Conseil d'État établit une comparaison entre la consultation d'un agenda privé — qui n'est pas accessible — et celle de données informatiques — qui le sont. Quelle est l'opinion de M. Thomas à ce sujet ?

*M. Marc Verwilghen*, *ministre de la Justice*, remercie M. Thomas pour l'avis circonstancié dans lequel il expose sa vision personnelle.

Le ministre ne peut toutefois souscrire entièrement aux propositions de M. Thomas et met en garde contre toute initiative visant à lier ou à adapter la loi en projet à la loi relative à la protection de la vie privée. Il estime que ce serait très dangereux pour ces deux législations.

Selon lui, les deux législations ont des finalités totalement différentes : il s'agit en général, à ses yeux, de protéger les données ainsi que les intérêts privés. Le projet de loi à l'examen concerne certaines dispositions du Code pénal, du Code d'instruction criminelle et des lois relatives aux entreprises publiques économiques et au secteur des télécommunications. L'objectif principal est toutefois de faire respecter les règles de droit en matière informatique. Les deux intérêts à prendre en compte sont la protection des propriétés, d'une part, et la confiance générale dans le fonctionnement de certains systèmes, d'autre part. En fait, le débat porte sur le système coercitif à mettre en œuvre pour que les règles de droit soient respectées.

Ten tweede, is hij van oordeel dat het inzake terminologie gevaarlijk zou zijn terug te gaan naar de basiswet. Inmiddels is de informatica onderhevig geweest aan een enorme evolutie door de invoering van nieuwe technieken en nieuwe begrippen.

Daar moet nu op worden ingespeeld. Vervolgens meent hij dat de definities van de wet op de privacy aan aanpassing toe zijn, in het licht van de diverse Europese richtlijnen.

De spreker komt terug tot de Raad van State die omtrent de definities een opmerking heeft gemaakt. Indien wordt gewerkt op dezelfde wijze en met dezelfde definities van de wet van 1991, vreest hij dat de strafwethandhaving zich al te zeer op een « eerder administratieve » wet zal toespitsen, terwijl onderhavige wet een andere context heeft.

Vervolgens stelt de minister dat hij de geuite kritieken kan aanvaarden, maar dat er toch rekening mee moet worden gehouden dat de regering uitdrukkelijk heeft gekozen voor continuïteit. Door de wetsontwerpen van verval te ontheffen, werd het reeds door de vorige regering gedane werk dat de toets bij de Raad van State heeft doorstaan, opnieuw op de agenda geplaatst zodat er een snelle reactie van de maatschappij kan zijn op dit type van criminaliteit. Dit neemt echter niet weg dat de continuïteit terzake ook voor bepaalde problemen zorgt.

Daarbij rijst de vraag waarom voordien niet werd gepoogd het advies in te winnen van de Commissie voor de bescherming van de persoonlijke levenssfeer. Hij zegt dat hij in feite die werkwijze had verkozen, omdat het nu in alle haast moet gebeuren.

Thans gaat de minister in chronologische volgorde over tot de kritieken op het wetsontwerp nr 214.

Hij is van oordeel dat de problemen in het artikel 9, waar het gaat over de wijziging van artikel 109*ter*, § 1, kunnen worden opgevangen indien voorafgaand het advies van de commissie wordt gevraagd telkens wanneer een in de Ministerraad overlegd koninklijk besluit wordt voorbereid. Dergelijke aanpassing kan hij volledig onderschrijven.

Betreffende de opmerking over de lijst, waarschuwt de minister ervoor dat indien de aanpassing gebeurt binnen de wet op de privacy, er wordt voorbijgegaan aan de vooropgestelde rechtshandhaving. Zowel de voorgaande als de huidige regering wenste deze materie in het Strafwetboek te regelen.

Inzake de termijn van bewaring is de minister niet ongevoelig voor het argument van de proportionaliteit.

Il estime par ailleurs qu'il serait dangereux, du point de vue terminologique, de se référer à la loi de base, l'informatique ayant connu, depuis lors, une énorme révolution par l'introduction de nouvelles techniques et notions.

Il faut en tenir compte. Il estime en outre que les définitions de la loi relative à la protection de la vie privée doivent être adaptées à la lumière des diverses directives européennes.

L'intervenant revient au Conseil d'État, qui a formulé une observation en ce qui concerne les définitions. Il craint que, si l'on adopte les mêmes procédures et les mêmes définitions que celles prévues par la loi de 1991, les mesures coercitives visant à faire respecter la loi pénale présentent un aspect trop « administratif », alors que la loi en projet s'inscrit dans un autre contexte.

Le ministre déclare ensuite qu'il peut comprendre les critiques qui ont été formulées, mais qu'il faut néanmoins tenir compte du fait que le gouvernement a explicitement opté pour la solution de continuité. Les projets de loi ayant été relevés de caducité, le travail accompli par le précédent gouvernement — travail qui avait passé avec succès l'épreuve du Conseil d'État — a été remis à l'ordre du jour, de manière que la société puisse réagir rapidement à ce type de criminalité. Il n'empêche que la continuité pose aussi certains problèmes en la matière.

C'est ainsi que l'on peut se demander pourquoi le précédent gouvernement n'a pas essayé précédemment de demander l'avis de la Commission de la protection de la vie privée. Le ministre précise qu'il aurait en fait préféré suivre cette procédure, étant donné qu'il faut à présent consulter cette instance dans la précipitation.

Le ministre passe ensuite en revue, par ordre chronologique, les différentes critiques qui ont été formulées à l'encontre du projet de loi n° 214.

Il estime que les problèmes posés par l'article 9, qui tend à modifier l'article 109*ter*, § 1er, pourraient être résolus en prévoyant que l'avis de la commission est demandé préalablement chaque fois qu'un arrêté royal délibéré en Conseil des ministres est en préparation. Il souscrit sans réserve à l'adaptation de l'article en ce sens.

En ce qui concerne la remarque relative à la liste, le ministre fait observer que si la modification est apportée dans le cadre de la loi sur la protection de la vie privée, on ne parviendra pas à rendre effective la sanction que l'on veut instaurer. Tant le précédent que l'actuel gouvernement souhaitaient régler cette matière dans le cadre du Code pénal.

En ce qui concerne la durée de la période de conservation, le ministre n'est pas insensible à l'argument de la proportionnalité.

Indien voor de termijn van bewaring maatregelen moeten worden getroffen, bijvoorbeeld een beperking tot drie maanden — termijn die hier werd geciteerd — dan beschikt men over « *no time* » in de strijd tegen de misdrijven. Bovendien geeft men het wezenlijk bestanddeel, hetzij het morele, hetzij het materiële bestanddeel van het misdrijf, uit handen door in een zeer korte bewaringstermijn te voorzien.

Ook de verjaringstermijnen spelen een rol, zodat toch enige voorzichtigheid in acht moet worden genomen.

De minister bevestigt dat de straffen misschien moeten worden aangepast. Door sommigen worden ze als exorbitant beschreven. Daarom is hij van oordeel dat daarover in de commissie voor de Justitie een debat moet worden gevoerd, teneinde te bepalen in hoeverre men de straffen, zowel de geldboeten als de gevangenisstraffen, op het huidige niveau behoudt. Ze zijn zwaarder dan in de wet op de privacy.

Ten slotte maakt de minister een opmerking ten behoeve van de heer Thomas aangaande de bijkomende werklast voor de Commissie voor de bescherming van de persoonlijke levenssfeer. Hij zegt begrip op te brengen voor het feit dat de commissie zich afvraagt of ze daarvoor wel degelijk is uitgerust, zowel inzake personeel als inzake technische ondersteuning.

De heer Thomas heeft een vergelijking gemaakt met de ons omringende landen. Hij kwam daarbij tot de bevinding dat de ondersteuning in ons land in feite zeer mager uitvalt.

De minister zegt dat daaromtrent een discussie moet worden gevoerd, maar dat ze dient te worden losgekoppeld van het huidige debat. Men moet zich wel degelijk buigen over de reële structurele problemen, want een dergelijke commissie moet bij machte zijn haar opdracht uit te voeren.

*De heer Hugo Coveliers (VLD)* stelt een vraag in verband met de methodologie. Hij zegt dat het interessant is dat er een tekst van de Commissie voor de bescherming van de persoonlijke levenssfeer in het vooruitzicht wordt gesteld. Hij wijst erop dat deze tekst ook een gebruiksaanwijzing is voor de politiediensten die zich met de opsporing van bepaalde misdrijven bezighouden.

Om het verwijt te vermijden dat er aan de politiediensten geen middelen worden gegeven om op te treden, stelt hij voor ook deze diensten te horen, zodat de beide bezwaren met elkaar kunnen worden vergeleken, want ze worden wellicht vanuit een verschillende gezichtshoek bekeken. Uiteindelijk komt het de wetgever toe de waarde en de normen te bepalen.

De spreker wijst op een van de problemen, namelijk dat er nu reeds een aantal interne regels uitsluitend voor de telematica bestaan, zo bijvoorbeeld dat gegevens niet worden uitgeprint. Wanneer later in het kader

Si des mesures doivent être prises en ce qui concerne la durée de la période de conservation (limiter celle-ci à trois mois, par exemple, comme cela a été suggéré), on ne disposera d'aucun délai lorsqu'il s'agira de lutter contre les infractions. En prévoyant une période de conservation très courte, on se dessaisit de l'élément constitutif essentiel de l'infraction, qu'il soit moral ou matériel.

Les délais de prescription ayant également leur importance, une certaine circonspection s'impose tout de même.

Le ministre confirme que les peines devraient sans doute être adaptées. Certains les ont qualifiées d'excessivement sévères. C'est la raison pour laquelle il estime qu'il faut en débattre au sein de la commission de la Justice, afin de déterminer dans quelle mesure il faut maintenir les peines, aussi bien les amendes que les peines d'emprisonnement, à leur niveau actuel. Ces peines sont plus sévères que celles prévues par la loi relative à la protection de la vie privée.

Enfin, le ministre formule, à l'adresse de M. Thomas, une observation concernant le surcroît de travail que la loi en projet pourrait donner à la Commission pour la protection de la vie privée. Il comprend que la commission se demande si elle dispose bien des moyens nécessaires, tant en personnel que sur le plan technique, pour remplir cette mission.

M. Thomas a comparé la situation en Belgique à celle des pays voisins et a constaté que la Belgique faisait réellement figure de parent pauvre pour ce qui est des moyens techniques.

Le ministre déclare que cette question devra être discutée, mais qu'elle ne doit pas l'être dans le cadre de l'actuel débat. Il conviendra toutefois d'examiner les problèmes structurels réels, car une telle commission doit être en mesure de s'acquitter de sa mission.

*M. Hugo Coveliers (VLD)* pose une question à propos de la méthode retenue. Il juge intéressant que la Commission de la protection de la vie privée fournisse un texte, soulignant que ce texte servira également de mode d'emploi aux services de police chargés de rechercher certains délits.

Afin d'éviter que l'on reproche au législateur de ne pas donner aux services de police les moyens d'intervenir, l'intervenant propose d'entendre également ces services, ce qui permettra de comparer les deux objections, car elles sont peut-être considérées sous un angle différent. Il reviendra en définitive au législateur de définir les normes.

L'intervenant attire l'attention sur l'un des problèmes, à savoir qu'il existe déjà un certain nombre de règles internes s'appliquant uniquement à la télématique, de sorte, par exemple, que des données ne sont pas

van een strafprocedure een bepaald feit moet worden aangetoond, blijkt dat de gegevens bij sommige politiediensten slechts gedurende zes maanden worden bewaard.

*De minister van Justitie* brengt begrip op voor het verzoek. Hij stelt dat er momenteel, zowel bij de politiediensten als bij de parketten, geen personen aanwezig zijn die over de nieuwe kwalificaties al studiewerk hebben verricht.

Hij besluit dat, bij gebrek aan kwalificatie, in deze materies geen onderzoek kan worden gedaan.

Wel kunnen, in het kader van andere strafrechtelijke bepalingen, de personen op het terrein belast met de bestrijding van van computercriminaliteit, worden gehoord teneinde vast te stellen welke problemen zich op het terrein voordoen.

*De voorzitter* zegt aan de heer Coveliers dat deze wetgeving de regels betreffende de bewaargeving zou moeten bepalen. Hij zegt dat het zijns inziens niet opgaat dat politiediensten bepaalde gegevens zelf zouden bewaren. Hij wijst erop dat in bepaalde omstandigheden een gelijkaardige regeling als de neerlegging ter griffie, wenselijk is.

*De heer Thomas* toont zich verheugd dat de Kamercommissie voor de Justitie bereid is in te gaan op het verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer in verband met het advies dat die commissie zou kunnen verstrekken over de louter technische aspecten. Hij geeft aan dat er voorbeelden dienen te worden gegeven van louter technische preciseringen die het voorwerp kunnen zijn van het regelgevende optreden van de Koning, dat wordt ondersteund door de collegiale werkzaamheden in de Ministerraad en door het advies van de commissie. Een en ander zal bijgevolg geen betrekking hebben op alle gegevens, noch op de duur van de bewaring ervan, en evenmin op de categorieën van betrokken personen, noch op de categorieën van gegevens waarop die bewaring en die bijzondere verwerking slaan.

Wat de proactiviteit betreft, erkent de spreker dat de minister er geen doekjes heeft omgewonden en heel duidelijk heeft gesteld dat het in feite om proactieve verwerkingen gaat.

Wordt evenwel uitgegaan van proactief werk, hetgeen inderdaad meer algemene onderzoeksdaden mogelijk maakt, dan wijkt men af van alles wat is opgenomen in de ontwerpen betreffende de aanpassing van de strafrechtspleging.

Die aanpassingen hebben betrekking op een lopend onderzoek; terzake zijn de onderzoeksrechter, de procureur des Konings, de hulpofficieren van gerechtelijke politie of nog de hulpofficieren van de procureur des Konings betrokken. Zulks gebeurt in een bepaald verband, maar heeft geen uitstaans met proactiviteit. Er heerst daaromtrent dus enige verwarring. Er dient uitdrukkelijk te worden verwezen naar de lopende onderimprimées. Lorsque, ultérieurement, un fait spécifique doit être démontré dans le cadre d'une procédure pénale, il apparaît que les données ne sont conservées que six mois par certains services de police.

*Le ministre de la Justice* comprend la demande formulée par le membre. Il précise que, jusqu'ici, personne n'a acquis les nouvelles qualifications nécessaires, que ce soit au sein des services de police ou des parquets.

Il en conclut qu'en l'absence de qualifications, aucune enquête ne peut être effectuée dans ces matières.

On peut en revanche, dans le cadre d'autres dispositions pénales, entendre les personnes chargées de la lutte contre la criminalité informatique sur le terrain, afin de déterminer quels sont les problèmes qui se posent à ce niveau.

*Le président* déclare à M. Coveliers que la loi en projet devrait déterminer les règles s'appliquant à la mise en dépôt. Il juge inapproprié que les services de police conservent eux-mêmes certaines données. Il précise qu'il paraît en l'occurrence souhaitable de prévoir, en certaines circonstances, une procédure telle que le dépôt au greffe.

Quant à l'avis que la commission pourrait donner sur les aspects purement techniques, *M. Thomas* se réjouit que la commission de la Justice de la Chambre se montre favorable à la demande exprimée par la Commission pour la protection de la vie privée. Il signale qu'il faudra donner des exemples de précisions purement techniques qui pourraient faire l'objet du travail réglementaire du Roi éclairé par son travail collégial au sein du Conseil des ministres et nanti de l'avis de la commission. Dès lors, cela ne concernera ni l'ensemble des données, ni la durée de conservation, ni les catégories de personnes visées, ni encore les catégories de données qui font l'objet de cette conservation et de ce traitement particulier.

En ce qui concerne la pro-activité, il reconnaît que le ministre a joué cartes sur table en disant bien clairement qu'il s'agissait en fait de traitements pro-actifs.

Or, si l'on se trouve dans une perspective de travail pro-actif, qui permet effectivement des recherches plus générales, on s'éloigne de tout ce que l'on retrouve dans ces projets concernant l'adaptation de la procédure pénale.

Ces adaptations se situent dans le cadre d'une instruction en cours; on parle du juge d'instruction, du procureur du Roi, des officiers auxiliaires de police judiciaire ou encore des auxiliaires du procureur du Roi dûment mandatés par le juge d'instruction. On se trouve dans un cadre bien particulier qui n'est pas celui de la pro-activité. Dès lors, il règne une certaine confusion. Il faudrait se référer explicitement non seulement aux

zoeken én naar de behoeften van de proactiviteit, waaraan moet kunnen worden voldaan overeenkomstig de wettelijke bepalingen terzake.

*De minister* repliceert dat het woord « proactief » niet moet worden geïnterpreteerd alsof het de bedoeling van deze wet is om proactief te werken. Hij ontkent dit en onderstreept dat ze ertoe strekt, in het kader van het Wetboek van strafvordering, aan de onderzoeksrechter of aan de procureur des Konings de middelen te verstrekken om het onderzoek te voeren. Mogelijk zal hij daarbij controles moeten uitvoeren op basis van gegevens en deels zal hij ook recherche moeten doen, die misschien proactief kan zijn.

Hij legt er de nadruk op dat terzake de hele scala van maatregelen, gaande van het proactieve tot het loutere repressieve, met eerbiediging van alle bepalingen van de strafrechtsprocedure, van toepassing is.

*De heer Coveliers* komt terug op de uiteenzetting van professor Thomas. De kwalilificatie die de professor gaf aan het begrip « proactieve recherche » heeft hem verbaasd. Hij zegde dat er hier geen sprake is van proactieve recherche, omdat er sprake is van een onderzoeksrechter en een procureur.

De spreker is echter van oordeel dat beiden, sinds de wet-Franchimont, pro actief kunnen optreden. Het zal overigens precies in de proactieve recherche zijn dat deze tekst nodig is, veeleer dan in de repressieve recherche.

Vandaar zijn verzoek om de betrokken politiediensten te horen. Nu gebeurt het onderzoek meestal zonder het optreden van een parketmagistraat, omdat die terzake geen kwalificaties heeft. Daarom is het interessant na te gaan hoe dat sinds de wet-Franchimont wettelijk verloopt.

*De voorzitter* zegt dat het in de terminologie van de artikelen 39*bis* en 88 van het Wetboek van strafvordering, zoals voorgesteld, een opsporings- of een gerechtelijk onderzoek betreft, onverminderd eventueel wat in de proactieve recherche is voorzien, namelijk de toestemming van de procureur des Konings, soms *a posteriori*, en het optreden van een onderzoeksrechter.

*De heer Poncelet* verwijst naar de hoorzittingen die zouden worden gehouden met leden van politiediensten. Hij stelt voor dat ook aan de veiligheidsdiensten zou worden gevraagd of zij het opportuun achten om hun bevindingen in commissie mee te delen. Deze diensten hebben immers ontegensprekelijk een grote deskundigheid opgebouwd inzake informatica, piraterij en eventueel bedrog; tevens kunnen zij naar ervaringen in het buitenland verwijzen.

instructions en cours mais aussi à des besoins de pro-activité qui doivent se réaliser en conformité avec l'encadrement tel qu'il est prévu légalement.

*Le ministre* réplique que le mot « pro-actif » ne doit pas être interprété comme si l'approche pro-active était l'objectif de la loi en projet. Il souligne que cette dernière tend à donner, dans le cadre du Code d'instruction criminelle, les moyens nécessaires au juge d'instruction ou au procureur du Roi pour mener l'instruction. Le magistrat instructeur devra éventuellement procéder en l'occurrence à des contrôles sur la base de données ainsi qu'à des recherches, qui pourront peut-être être pro-actives.

Il souligne que toute la panoplie de mesures, allant des mesures pro-actives aux mesures purement répressives, s'appliquent à cet égard dans le respect de toutes les dispositions de la procédure pénale.

*M. Coveliers* revient à l'exposé du professeur Thomas. Il est surpris par la qualification que le professeur a donnée à la notion de « recherche pro-active ». Il a fait observer qu'il ne s'agit pas en l'occurrence de recherche pro-active, étant donné qu'il est question d'un juge d'instruction et d'un procureur.

L'intervenant estime néanmoins que depuis la loi Franchimont, ceux-ci peuvent intervenir pro-activement. Le texte à l'examen présentera d'ailleurs un intérêt précisément pour la recherche pro-active, plutôt que pour la recherche répressive.

D'où sa demande d'entendre les services de police concernés. À l'heure actuelle, l'instruction se déroule généralement sans l'intervention d'un magistrat du parquet, étant donné que celui-ci n'a pas de qualifications en la matière. Il serait dès lors intéressant d'examiner comment cela se passe sur le plan légal depuis la loi Franchimont.

*Le président* précise que dans les articles 39*bis* et 88 du Code d'instruction criminelle, tels qu'ils sont proposés, il s'agit d'une information ou d'une instruction, sans préjudice éventuellement de ce qui est prévu dans la recherche pro-active, à savoir l'autorisation du procureur du Roi, quelquefois *a posteriori*, et l'intervention d'un juge d'instruction.

*M. Poncelet* rappelle que la commission devait entendre des membres des services de police et suggère que l'on demande également aux services de sécurité, qui possèdent une expertise incontestable dans le domaine de l'informatique, du piratage et des fraudes éventuelles et qui peuvent faire état des expériences à l'étranger, s'ils jugent opportun de faire part de leurs constatations à la commission.

## B. HOORZITTING MET LEDEN VAN DE GERECHTELIJKE POLITIE EN VAN DE RIJKSWACHT

### 1. **Uiteenzettingen**

*De heer Guy Verbeeren (NCCU-GPP)* deelt mee dat de gerechtelijke politie per hof van beroep over een *computer crime unit* beschikt die bijstand verleent bij de gerechtelijke onderzoeken inzake informaticacriminaliteit.

Deze misdrijven kunnen worden onderverdeeld in twee groepen, met name de « a-specifieke misdrijven », dat zijn misdrijven waarvoor reeds strafbepalingen bestaan (bijvoorbeeld verspreiding van kinderpornografie), waarbij het informaticasysteem als middel wordt gebruikt. Tegen deze categorie van misdrijven kan reeds afdoende worden opgetreden. De « specifieke » computermisdrijven zijn de misdrijven waarbij de computer of het informaticasysteem het doel van het misdrijf is. Op de wet op de kruispuntbank na, die strafbepalingen bevat voor wie zich onrechtmatig toegang tot de gegevens verschaft, zijn er geen bijzondere wettelijke bepalingen die de bestrijding van deze vorm van misdadigheid beogen.

Het voorliggende wetsontwerp is afgestemd op de aanbeveling 89/9 van de Raad van Europa die een minimale optielijst vastlegt met een aantal strafbare gedragingen die door alle lidstaten zouden moeten worden vervolgd.

*De heer Luc Beirens (BOGO-team/CBO)* is dienshoofd van de cel « BOGO » (Bijstand en opsporing in geautomatiseerde omgevingen) van de rijkswacht. Deze cel functioneert op het niveau van het CBO en staat ter beschikking van alle rijkswachteenheden. De cel werd opgericht in 1995. Sedertdien steeg het aantal interventies van 130 naar 260 tot 360 in 1998 en tot 500 in 1999. De dienst moet steeds vaker optreden in verband met fraude op het internet (gepirateerde abonnementen, *hacking*, …).

De zeer snelle technische evolutie van de informatica maakt het steeds moeilijker om de opsporing efficiënt te organiseren. Bovendien kan de overheid slechts optreden op basis van de « Belgacomwet » van 21 maart 1991. Deze wet kan echter alleen worden toegepast op publieke netwerken zoals op het internet. De wet kan echter niet worden gebruikt bij *hacking* binnen een netwerk van een bepaald bedrijf.

Aangezien het onmogelijk is om de werking van alle systemen te kennen, zijn de opsporingsdiensten vaak verplicht om de medewerking te vragen van de systeembeheerder zelf. Die medewerking kan evenwel niet worden opgelegd. Indien de systeembeheerder niet wenst mee te werken, dan moet er een externe deskundige worden ingezet.

## B. AUDITION DE MEMBRES DE LA POLICE JUDICIAIRE ET DE LA GENDARMERIE

### 1. **Exposés**

*M. Guy Verbeeren (NCCU-PJP)* indique que la police judiciaire dispose, dans chaque ressort de cour d'appel, d'une *computer crime unit* qui prête son assistance pour les enquêtes judiciaires en matière de criminalité informatique.

Ces délits peuvent être répartis en deux groupes, à savoir les délits « aspécifiques », c'est-à-dire les délits pour lesquels des dispositions pénales existent déjà (par exemple la diffusion de pornographie enfantine) et pour lesquels le système informatique est utilisé comme support. Il est déjà possible d'intervenir de manière efficace contre les délits de cette catégorie. Les délits informatiques « spécifiques » sont les délits pour lesquels l'ordinateur ou le système informatique est le but du délit. Hormis la loi sur la banque-carrefour, qui prévoit des dispositions pénales à l'encontre de ceux qui accèdent de manière illicite aux données de cette banque, il n'existe pas de dispositions légales particulières visant à lutter contre cette forme de criminalité.

Le projet de loi à l'examen est basé sur la recommandation 89/9 du Conseil de l'Europe, qui établit une liste minimale d'options et définit un certain nombre de comportements punissables qui devraient faire l'objet de poursuites dans tous les États membres.

*M. Luc Beirens (cellule AREA/BCR)* est à la tête de la cellule « AREA » (Assistance et recherche dans des environnements informatisés) de la gendarmerie. Cette cellule fonctionne au niveau du BCR et est à la disposition de toutes les unités de gendarmerie. La cellule a été créée en 1995. Depuis lors, le nombre des interventions est passé de 130 à 260, puis à 360 en 1998 et à 500 en 1999. La cellule intervient de plus en plus fréquemment pour des affaires de fraude sur internet (abonnements piratés, *hacking*, …).

L'évolution technique très rapide que connaît l'informatique a pour conséquence qu'il est de plus en plus difficile d'organiser efficacement la recherche. Les autorités ne peuvent en outre intervenir que sur la base de la « loi Belgacom » du 21 mars 1991. Cette loi ne peut toutefois être appliquée qu'aux réseaux publics tels qu'internet. Elle ne peut donc être utilisée en cas de piratage par l'intérieur d'un réseau d'une entreprise donnée.

Étant donné qu'il est impossible de connaître le fonctionnement de tous les systèmes, les services de recherche sont souvent obligés de demander au gestionnaire du système même de prêter son concours. Ils ne peuvent toutefois pas l'obliger à collaborer. Si celui-ci refuse de collaborer, il faut faire appel à un expert externe.

Volgens de heer Beirens biedt het wetsontwerp een antwoord op een aantal problemen die zich thans stellen. De spreker vraagt echter ook bijzondere aandacht voor de noodzaak tot bewaring door de telecomoperatoren of *providers* van gegevens over de *login*-internetverbindingen die zij voor hun klanten realiseren.

Belgacom bewaart deze gegevens thans gedurende 6 maanden, maar dat gebeurt niet steeds bij alle operatoren en *providers*. Bovendien is die termijn te kort. Het gebeurt immers dat een *hacking* pas geruime tijd na de feiten wordt vastgesteld. Sommige *hackers* (bijvoorbeeld bij spionage) hebben er alle belang bij dat de sporen zo perfect mogelijk worden uitgewist en dat de toegang zo lang mogelijk bruikbaar blijft.

*De heer Olivier Bogaert (CCU-GPP)* vertegenwoordigt de *Computer Crime Unit* van de gerechtelijke politie van Brussel. De dienst bestaat sedert 1995 en functioneert als een bijstandsteam voor alle brigades van de gerechtelijke politie.

*De heer Walter Coenraets (NCCU)* werkt als jurist voor de Nationale *Computer Crime Unit* van de gerechtelijke politie.

Het is zijn taak om de interpretatieproblemen van de bestaande wetgeving op te lossen.

De wetgeving zou er moeten naar streven teksten te maken die duidelijk zijn en toch voldoende ruimte bieden om de snelle technologische evolutie te volgen. Dit is geen gemakkelijk evenwicht.

## 2. **Bespreking**

*Politiesamenwerking*

*De heer Hugo Coveliers (VLD)* wenst te vernemen of er samenwerking is tussen de politiediensten bij de bestrijding van de informaticacriminaliteit.

*De heer Verbeeren* antwoordt bevestigend. De rijkswacht en de gerechtelijke politie volgen samen dezelfde opleidingssessies en ontmoeten mekaar ook op Europees niveau, in een interpolwerkgroep.

*Bewaring*

*De heer Hugo Coveliers (VLD)* wenst te vernemen hoelang de speurders zouden wensen dat de *providers* hun gegevens zouden bewaren.

*De heer Beirens* antwoordt dat de gegevens soms maar drie maanden worden bewaard en dat de opsporing daardoor vaak onmogelijk wordt.

Hij legt uit dat, zodra de verbinding met het internet via de telefoon of via de kabel tot stand komt, aan de

M. Beirens estime que le projet de loi apporte une solution à une série de problèmes qui se posent actuellement. L'intervenant demande toutefois que l'on accorde une attention toute spéciale à la nécessité, pour les opérateurs de services de télécommunications ou les fournisseurs d'accès, de conserver les données concernant les connexions au réseau qu'ils établissent pour leurs clients.

Belgacom conserve ces données pendant six mois. Ceci n'est pas toujours le cas chez les autres opérateurs et fournisseurs d'accès. Ce délai est en outre trop court. Il arrive en effet qu'un piratage ne soit constaté que longtemps après les faits. Certains pirates (par exemple, en cas d'espionnage) ont tout intérêt à ce que les traces soient effacées aussi parfaitement que possible et à ce que l'accès demeure utilisable aussi longtemps que possible.

*M. Olivier Bogaert (CCU-PJP)* représente la *Computer Crime Unit* de la police judiciaire de Bruxelles. Ce service existe depuis 1995 et fait office d'équipe d'assistance pour toutes les brigades de la police judiciaire.

*M. Walter Coenraets (NCCU)* travaille en tant que juriste à la *National Computer Crime Unit* de la police judiciaire.

Son travail consiste à résoudre les problèmes d'interprétation que pose la législation existante.

Le législateur devrait s'efforcer d'élaborer des textes clairs tout en laissant une marge suffisante pour pouvoir tenir compte de l'évolution technologique, qui est très rapide. Il est toutefois difficile d'établir un tel équilibre.

## 2. **Discussion**

*Collaboration policière*

*M. Hugo Coveliers (VLD)* demande si les services de police collaborent dans le cadre de la lutte contre la criminalité informatique.

*M. Verbeeren* répond par l'affirmative. Des membres de la gendarmerie et de la police judiciaire suivent ensemble les mêmes cycles de formation et se rencontrent également au niveau européen au sein d'un groupe de travail interpol.

*Conservation*

*M. Hugo Coveliers (VLD)* demande pendant combien de temps, selon les enquêteurs, les fournisseurs d'accès devraient conserver leurs données.

*M. Beirens* répond que les données ne sont parfois conservées que pendant trois mois et que la recherche est dès lors souvent impossible.

Il explique que dès que la connexion internet est établie par le téléphone ou par le câble, une adresse

gebruiker een internetadres wordt toegekend dat uit een reeks van nummers bestaat. Per dag wordt hetzelfde nummer vaak aan tientallen abonnees toegekend. De *provider* zou moeten opslaan welke abonnee gedurende welke periode een bepaald internetadres heeft gebruikt.

Het internetadres wordt per sessie toegekend. Zodra de verbinding wordt verbroken, kan een andere abonnee dat nummer krijgen. Gelet op de termijnen die er vaak liggen tussen de vaststelling van een misdrijf en het vatten van de dader zouden de politiediensten gedurende een drietal jaren over die gegevens moeten kunnen beschikken.

Thans worden de gegevens opgevraagd op grond van artikel 46*bis* van het Wetboek van strafvordering. Op basis van hetzelfde artikel kan ook de abonnee worden geïdentificeerd. Wil men over de oproepgegevens beschikken dan dient artikel 88*bis* van het Wetboek van strafvordering te worden toegepast.

Wat Belgacom, dat via *Skynet* werkt, aan gegevens kan meedelen is meestal onvoldoende voor een efficiënte opsporing.

De bewaringstermijn van 6 maanden voor de gegevens van communicaties die bijvoorbeeld door Belgacom en het dochterbedrijf Skynet wordt aangehouden, is in vele gevallen onvoldoende voor een efficiënte opsporing.

*Toepasbaarheid van de definities*

*Mevrouw Fauzaya Talhaoui (Agalev-Ecolo)* wenst te vernemen of de teksten die thans voorliggen beter voldoen aan de behoeften van de opsporingsdiensten.

*De heer Coenraets* deelt mee dat de wet ruim genoeg is en het voordeel heeft niet te veel definities te gebruiken en toch een duidelijke terminologie hanteert wat de toepasbaarheid ten goede komt.

*Personeelsbestand en opleiding*

*De heer Servais Verherstraeten (CVP)* vraagt of de politiediensten over voldoende personeel en voldoende middelen beschikken om de informaticacriminaliteit afdoende te bestrijden.

*De heer Beirens* antwoordt dat de computercriminaliteit in stijgende lijn gaat. Zo geeft de recente opkomst van de *e-commerce* aanleiding tot nieuwe misdrijven. Het misbruik van kredietkaartnummers via het internet is een bekend fenomeen. Elke nieuwe technologische evolutie houdt steeds de mogelijkheid van misbruik in. Het personeelsbestand zal dus noodgedwongen worden uitgebreid. Bovendien moeten al de politiemensen die op dit terrein werkzaam zijn ook continu worden opgeleid en bijgeschoold.

internet, consistant en un série de chiffres, est attribuée à l'utilisateur. Le même numéro est souvent attribué à des dizaines d'abonnés au cours de la même journée. Le fournisseur d'accès devrait enregistrer le nom de chaque abonné qui a utilisé une adresse internet déterminée ainsi que la période d'utilisation correspondante.

L'adresse internet est attribuée pour la durée d'une session. Dès que la connexion est interrompue, un autre abonné peut obtenir ce numéro. Vu les délais qui s'écoulent souvent entre la constatation d'une infraction et l'arrestation de l'auteur, les services de police devraient pouvoir disposer de ces données pendant trois ans.

Actuellement, la communication des données peut être demandée sur la base de l'article 46*bis* du Code d'instruction criminelle. L'abonné peut également être identifié en vertu du même article. Si l'on veut disposer des données d'appel, il faut appliquer l'article 88*bis* du Code d'instruction criminelle.

Les données que Belgacom, qui fonctionne via *Skynet*, peut fournir sont généralement insuffisantes pour permettre une recherche efficace.

Le délais de conservation de 6 mois pour les données de communications qui est par exemple respecté par Belgacom et sa filiale Skynet, est dans beaucoup de cas insuffisant pour une recherche efficace.

*Définitions et applicabilité*

*Mme Fauzaya Talhaoui (Agalev-Ecolo)* demande si les textes à l'examen répondent mieux aux besoins des services de recherche.

*M. Coenraets* fait observer que la loi a une portée suffisamment large et offre l'avantage de ne pas contenir trop de définitions tout en utilisant une terminologie précise, ce qui en accroît l'applicabilité.

*Cadre du personnel et formation*

*M. Servais Verherstraeten (CVP)* demande si les services de police disposent de personnel et de moyens suffisants pour combattre efficacement la criminalité informatique.

*M. Beirens* répond que la criminalité informatique est en progression. C'est ainsi que l'apparition récente du commerce électronique est source de nouvelles infractions. L'usage abusif de numéros de carte de crédit par le biais de l'internet est un phénomène connu. Toute nouvelle évolution technologique recèle toujours la possibilité d'abus. Il faudra donc nécessairement étendre le cadre du personnel. En outre, les policiers travaillant dans ce domaine doivent être formés et recyclés en permanence.

*Mevrouw Jacqueline Herzet (PRL FDF MCC)* vraagt of de politiediensten opgewassen zijn tegen de *« hackers »*.

*De heer Beirens* antwoordt dat de opsporing niet noodzakelijk dezelfde kennis vereist als de kennis die nodig is om een frauduleus systeem op te zetten.

De opsporing zelf vereist een eerder algemene systeemkennis en inzicht om te kunnen optreden bij de telecomoperator, de *provider* en bij het *gehackte* bedrijf. De speurders moeten daarnaast een beroep kunnen doen op de bijstand van enkele hooggekwalificeerde medewerkers.

De spreker verwijst naar de structuur die in Nederland werd opgezet waar, naast de lokale bijstands*teams,* op nationaal niveau een beroep kan worden gedaan op de Centrale Recherche- en informatiedienst en op de afdeling Computeronderzoek van het Gerechtelijk Laboratorium dat over een twintigtal personen beschikt die zich uitsluitend bezighouden met computeronderzoek in diverse domeinen : cryptoanalyse, Internet-opsporingen en -interceptie, betaalkaarten, …

De Belgische opsporingsdiensten doen eveneens beroep op deze eenheid. Het zou ideaal zijn indien een dergelijke *background* ook in ons land tot stand zou kunnen worden gebracht.

*De heer Bogaert* onderstreept, in antwoord op een vraag van mevrouw Herzet dat de contacten tussen de politiediensten en de telecomoperatoren goed zijn maar dat ze soms té traag verlopen.

*Beslag*

*De voorzitter* wenst te vernemen in welke gevallen de volledige apparatuur in beslag wordt genomen en in welke gevallen de bestanden worden gekopieerd.

*De heren Beirens en Bogaerts* antwoorden dat het in sommige gevallen (bijvoorbeeld bij een onderzoek in grote bedrijven of banken) onmogelijk is om de ganse apparatuur in beslag te nemen. In dat geval worden de *backups* in beslag genomen of worden er kopies genomen van een selectie van de aanwezige bestanden. Bij kleinere bedrijven, voorzover de bedrijfsactiviteit dit toelaat, wordt de ganse apparatuur in beslag genomen.

Ook in dat geval worden er eerst *back-up's* gemaakt om te vermijden dat achteraf zou worden aangevoerd dat het materiaal tijdens het onderzoek werd gewijzigd.

Bij de inbeslagname van materiaal is het te verkiezen om al het materiaal in beslag te nemen omdat de aansluiting op andere *hardware* de opgeslagen gegevens kan wijzigen.

*Mme Jacqueline Herzet (PRL FDF MCC)* demande si les services de police sont en mesure de faire face aux « *hackers* ».

*M. Beirens* répond que les recherches ne nécessitent pas nécessairement les mêmes connaissances que la mise sur pied d'un système frauduleux.

Les recherches requièrent une connaissance du système et une vision plutôt générales pour pouvoir intervenir auprès de l'opérateur du réseau de télécommunications, du fournisseur d'accès et de l'entreprise piratée. Les enquêteurs doivent par ailleurs pouvoir recourir à l'assistance de quelques collaborateurs hautement qualifiés.

L'intervenant fait allusion à la structure aux Pays-Bas, où, après les unités locales d'expertise digitale, au niveau national on peut faire appel au Service Central de recherche et d'information et au département de recherche digitale qui dispose d'une vingtaine de personnes s'occupant exclusivement de divers domaines de recherche informatique : crypto-analyse, Recherche et Interception sur Internet, cartes de paiement, etc.

Les services de recherche belges font également appel à cette unité. Il serait idéal de pouvoir créer un support similaire dans notre pays.

Répondant à Mme Herzet, *M. Bogaert* souligne que les contacts entre les services de police et les opérateurs de réseaux de télécommunications sont bons, mais quelquefois trop lents.

*Saisie*

*Le président* demande dans quels cas on saisit l'ensemble du matériel et dans quels cas on copie les fichiers.

*MM. Beirens et Bogaerts* répondent que, dans certains cas (par exemple, lorsque l'on enquête dans de grandes entreprises ou de grandes banques), il est impossible de saisir tout le matériel. Dans ce cas, on saisit les copies de sauvegarde ou on prend des copies d'une sélection des fichiers présents. Dans les petites entreprises, pour autant que l'activité de l'entreprise le permette, on saisit tout le matériel.

Dans ce cas, on commence également par faire des copies de sauvegarde, afin d'éviter que l'on prétende ultérieurement que le matériel a été modifié pendant l'enquête.

En cas de saisie de matériel, il est préférable de saisir tout le matériel, parce que toute connexion à un autre matériel peut modifier les données stockées.

*Pro-actieve opsporing*

In antwoord op een vraag van de voorzitter delen *de heren Verbeeren en Beirens* mee dat er geen pro-actief onderzoek op het internet gebeurt.

Daar is onvoldoende personeel voor.

*Opvolging*

*De heren Beirens en Verbeeren* delen mee dat hun diensten optreden als bijstandsteam en dat zij niet op de hoogte worden gehouden van het resultaat van hun werkzaamheden.

Het zou wel nuttig zijn indien het parket, via de terugzending van een standaardformulier, informatie zou geven over het gevolg dat aan de opsporing werd gegeven.

*Wissen*

*De minister* vraagt of de kopies die door de bijstandteams worden gemaakt voldoende bewijs zijn indien de « originele » gegevens, op gezag van de procureur des Konings worden gewist.

*De heer Beirens* antwoordt dat de kopie steeds de volledige harde schijf bevat, van de eerste tot de laatste *bit*.

Indien het onmogelijk is om een volledige kopie te maken, dan rijst er inderdaad een probleem.

Sommige bestanden kunnen besmet zijn door virussen. Het wissen van een onderdeel kan ook tot gevolg hebben dat het systeem wordt gewijzigd.

Soms verkiest men alleen een bepaald bestand ontoegankelijk te maken, om verder onderzoek mogelijk te maken.

*De voorzitter* vraagt of er in dat geval volledige zekerheid is dat de toegang niet wordt gebruikt.

*De heer Verbeeren* antwoordt dat het systeem via encodering ontoegankelijk kan worden gemaakt.

Zolang de code niet gekend is, is de toegang onmogelijk.

Bij bedrijven wordt die oplossing vaak gekozen om te vermijden dat het volledige systeem ontoegankelijk wordt en het bedrijf zijn economische activiteit zou dienen te staken.

*Bewaring van* back-up's

*De deskundigen* zijn het erover eens dat *tapes* zeer gevoelig zijn voor externe invloeden.

*Back-up's* worden best genomen op optische schijven die groter zijn dan CD-rom's.

De garantieperiode voor *tapes* bedraagt 5 jaar, voor optische schijven en CD-rom's 30 jaar.

*Recherche proactive*

Répondant à une question du président, *MM. Verbeeren et Beirens* soulignent qu'aucune recherche proactive n'est effectuée sur internet.

Il n'y a pas suffisamment de personnel pour ce faire.

*Suivi*

*MM. Beirens et Verbeeren* font observer que leurs services opèrent comme équipes auxiliaires et qu'ils ne sont pas tenus au courant du résultat de leurs activités.

Il serait pourtant utile que le parquet fournisse des informations, par exemple en renvoyant un formulaire type, sur la suite qui a été donnée à la recherche.

*Effacement*

*Le ministre* demande si les copies qui sont faites par les équipes d'appui constitueraient des preuves suffisantes en cas d'effacement des données « originales » sous l'autorité du procureur du Roi.

*M. Beirens* répond que la copie contient toujours l'ensemble des données se trouvant sur le disque dur, du premier au dernier octet.

Un problème se pose effectivement s'il est impossible de faire une copie complète.

Certains fichiers peuvent être contaminés par des virus. L'effacement d'une partie des données peut aussi avoir pour conséquence de modifier le système.

On préfère parfois se limiter à rendre un fichier déterminé inaccessible, afin de permettre des recherches ultérieures.

*Le président* demande s'il est, dans ce cas, absolument certain que l'on ne puisse pas accéder au fichier.

*M. Verbeeren* répond que le système peut être rendu inaccessible par le biais d'un encodage.

L'accès est impossible aussi longtemps que le code n'est pas connu.

On choisit souvent cette solution dans les entreprises pour éviter que l'ensemble du système devienne inaccessible et que l'entreprise doive suspendre son activité économique.

*Conservation de* back-up's

*Les experts* s'accordent pour constater que les bandes sont très sensibles aux influences extérieures.

Il est préférable d'enregistrer les *back-up's* sur des disques optiques qui sont plus grands que les CD-rom.

Les bandes sont couvertes par une garantie de 5 ans, tandis que cette période est de 30 ans pour les disques optiques et les CD-rom.

Het is ook van belang dat het materiaal in een aangepaste ruimte wordt opgeslagen. De kelders van de justitiepaleizen, die thans door de griffies als opslagruimte voor bewijsmateriaal worden gebruikt, laten op dat vlak veel te wensen over.

Het zou nuttig zijn om op dit vlak over duidelijke richtlijnen te kunnen beschikken.

*De heer Beirens* meent dat er best meerdere kopies worden gemaakt, de eerste zou dan kunnen worden verzegeld en als bewijsstuk worden bewaard, de tweede zou een werkdocument zijn. In bepaalde landen wordt reeds op die manier tewerk gegaan.

*De minister* wenst te vernemen of het technisch mogelijk is om gegevens langer dan zes maanden te bewaren.

*De heer Verbeeren* meent van wel. Ze kunnen worden opgeslagen op een CD-rom die na de vastgestelde tijd wordt vernietigd.

Die procedure houdt voor het betrokken bedrijf uiteraard een economische kost in.

*De heer Bogaert* merkt op dat het nuttig zou zijn om een minimumtermijn voor bewaring vast te leggen.

De *sites* waarop wordt gediscussieerd, de zogenaamde « *chat lines* » zijn in België vrij populair. De activiteit op deze *site* is zo intens dat de oudere gegevens worden vernietigd door de nieuwe gegevens. Indien een persoon zich bijvoorbeeld onrechtmatig een identiteit toeëigent, dan is het na een tiental dagen reeds onmogelijk om de betrokkene te betrappen.

*De heer Verbeeren* vermeldt ook dat *providers*, die in België hun diensten aanbieden, hun bestanden in een ander land kunnen bewaren.

Zo bewaart *« America on line »* zijn gegevens in de Verenigde Staten.

Opsporingen zijn dan slechts mogelijk na een internationaal rechtshulpverzoek.

## IV. — STANDPUNTEN OVER HET ADVIES 33/1999 VAN DE COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER (CF. BIJLAGE II)

De minister van Justitie onderstreept dat in de context van de problematiek van de informatiesnelwegen en van het internet in het bijzonder, de bescherming van de privacy van de burgers afdoende dient te worden gewaarborgd.

De invoeging van nieuwe strafbaarstellingen in het Strafwetboek, meer bepaald de misdrijven inzake ongeoorloofde toegang en daden van computer- of datasabotage, betekenen op dit vlak een grote vooruitgang.

Ook de nieuwe dwangmaatregelen moeten in dit licht worden bekeken. Zij maken het immers voor de be-

Il est également important que le matériel soit stocké dans des locaux adéquats. Les caves des palais de justice, qui sont actuellement utilisés par les greffes pour stocker les pièces à conviction, laissent beaucoup à désirer dans ce domaine.

Il serait utile de disposer de directives précises à ce sujet.

*M. Beirens* estime qu'il serait préférable de faire plusieurs copies; la première pourrait être mise sous scellés et conservée comme pièce à conviction, tandis que la deuxième serait un document de travail. Dans certains pays, on applique déjà cette procédure.

*Le ministre* demande s'il est techniquement possible de conserver les données pendant plus de six mois.

*M. Verbeeren* pense que oui. Elles peuvent être stockées sur un CD-rom qui est détruit à l'expiration du délai fixé.

Cette procédure implique évidemment un coût économique dans le chef de l'entreprise concernée.

*M. Bogaert* fait observer qu'il serait utile de fixer un délai de conservation minimal.

Les *sites* sur lequel on discute, les *« chat-lines »,* sont très populaires en Belgique. L'activité sur ce type de site est tellement intense que les anciennes données sont effacées par les nouvelles. Si une personne usurpe, par exemple, une identité, il n'est déjà plus possible de la surprendre après une dizaine de jours.

*M. Verbeeren* indique également que certains fournisseurs d'accès qui proposent leurs services en Belgique peuvent conserver leurs fichiers dans un autre pays.

C'est ainsi qu'*« America on line »* conserve ses données aux États-Unis.

Les recherches ne sont dès lors possibles qu'après une demande d'entraide judiciaire internationale.

## IV. — POINTS DE VUE À PROPOS DE L'AVIS 33/1999 DE LA COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE (CF. ANNEXE II)

Le ministre de la Justice souligne que, dans le cadre de la problématique des autoroutes de l'information et de l'Internet en particulier, la protection de la vie privée des citoyens doit être suffisamment garantie.

L'insertion de nouvelles incriminations dans le Code pénal, et, plus précisément celle des infractions en matière d'accès illicite et d'actes de sabotage de systèmes informatiques ou de données, représentent un progrès considérable en la matière.

Les nouvelles mesures coercitives doivent également être considérées sous cet angle. Elles permettent

voegde gerechtelijke diensten mogelijk om de daders van informaticagerelateerde delicten, met inbegrip van deze die een privacyschending uitmaken, op een efficiënte wijze op te sporen en te vervolgen.

Dwangmaatregelen houden per definitie een beperking van grondrechten in en moeten bijgevolg precies worden afgebakend om misbruiken tegen te gaan. De toepasbaarheid van de wet van 8 december 1992 over de bescherming van persoonsgegevens staat in dit verband buiten elke twijfel.

De suggestie die de Commissie voor de bescherming van de persoonlijke levenssfeer doet om geconsulteerd te worden inzake de te nemen uitvoeringsbesluiten die betrekking hebben op de verwerking van persoonsgegevens of die de beveiliging van data betreffen, kan de minister dan ook ten volle onderschrijven. In de voorliggende tekst wordt hier reeds ten dele aan tegemoet gekomen.

Verschillende opmerkingen in het advies lijken het wetsontwerp, niet alleen vanuit het oogpunt van de privacyreglementering, maar ook vanuit een traditioneel strafrechtelijk perspectief te becommentariëren.

De minister verwijst naar de bedenkingen inzake de regels over de samenloop van strafbaarstellingen, het beroepsgeheim, de verplichtingen tot medewerking van personen aan de bewijsgaring in een strafzaak, zelfs de strafrechtelijke verantwoordelijkheid van rechtspersonen … Terzake moet worden opgemerkt dat de gemeenrechtelijke principes van het strafrecht hier onverminderd spelen.

Dit geldt tevens voor het evenredigheidsbeginsel, een principe dat niet enkel relevant is inzake dataprotectie, maar dat geldt voor het hele strafrecht en strafprocesrecht. De discussie terzake spitst zich in de context van het wetsontwerp informaticacriminaliteit vooral toe op de voorgestelde wijziging van artikel 109*ter*E van de telecommunicatiewet, waar het erom gaat operatoren en dienstenverstrekkers algemene, maar tijdelijke registratie- en bewaringsplichten op te leggen inzake bepaalde telecommunicatiegegevens, volgens in uitvoeringsreglementering te preciseren modaliteiten. De minister stelt vast dat de commissie in het advies aanzienlijke aandacht besteedt aan deze problematiek. De commissie laat evenwel na om vanuit haar ervaring concrete suggesties te doen die het zouden mogelijk maken om deze bepaling, conform de principes van dataprotectie, beter wettelijk af te bakenen, zonder dat de effectiviteit van een aantal specifieke dwangmaatregelen uit het Wetboek van strafvordering verloren gaat. Met het oog op deze evenwichtsoefening ware het wellicht aangewezen om de voorzitter van de Commissie ter bescherming van de persoonlijke levenssfeer op dit punt opnieuw te horen.

en effet aux services juridiques compétents de rechercher et de poursuivre de manière efficace les auteurs de délits informatiques, y compris de ceux qui constituent une atteinte à la vie privée.

Les mesures coercitives impliquent par définition une limitation des droits fondamentaux et leur portée doit, par conséquent, être définie avec précision afin de lutter contre les abus. Il ne fait aucun doute que la loi du 8 décembre 1992, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, s'applique en l'espèce.

Le ministre peut dès lors accepter sans réserve la suggestion faite par la Commission de la protection de la vie privée d'être consultée au sujet des arrêtés d'exécution à prendre concernant le traitement des données à caractère personnel ou la sécurisation des données. Le texte à l'examen répond déjà partiellement à cette préoccupation.

Plusieurs observations formulées dans l'avis paraissent analyser le projet de loi non seulement sous l'angle de la réglementation de la protection de la vie privée, mais également sous l'angle du droit pénal traditionnel.

Le ministre fait allusion aux observations relatives aux règles concernant le concours d'incriminations, au secret professionnel, à l'obligation faite à certaines personnes de coopérer à la collecte de preuves dans une affaire pénale, voire à la responsabilité pénale de personnes morales. Il est à noter à ce sujet que les principes de droit commun prévus dans le droit pénal s'appliquent sans réserve.

Il en va de même pour le principe de proportionnalité, qui ne vaut pas uniquement pour la protection des données, mais également pour l'ensemble du droit pénal et de la procédure pénale. Dans le contexte du projet de loi relatif à la criminalité informatique, la discussion à ce sujet porte essentiellement sur la proposition de modification de l'article 109*ter*E de la loi portant réforme de certaines entreprises publiques économiques, qui impose aux opérateurs et aux fournisseurs de services des obligations générales mais provisoires d'enregistrement et de conservation de certaines données de télécommunications, selon des modalités à préciser par voie d'arrêté d'exécution. Le ministre constate que, dans son avis, la commission accorde énormément d'attention à cette problématique. La commission s'abstient cependant de formuler, sur la base de son expérience, des suggestions concrètes qui permettraient de mieux délimiter la portée de cette disposition, conformément aux principes de la protection des données, tout en préservant l'efficacité d'un certain nombre de mesures contraignantes spécifiques prévues par le Code d'instruction criminelle. Afin de tenter de concilier ces deux impératifs, il serait sans doute opportun de réentendre le président de la Commission de la protection de la vie privée sur ce point.

Tot slot herhaalt de minister en hij verwijst daarbij tevens naar de actualiteit (met name naar het recente geval van het tijdelijk blokkeren van één van de belangrijkste zoekmachines op het internet, « Yahoo ») — dat het wetsontwerp informaticacriminaliteit een belangrijke juridische steun zal betekenen voor de beveiliging van de netwerken en aldus mee zal bijdragen aan het vertrouwen van het publiek en de industrie in de verdere uitbouw van de informatiemaatschappij.

*De voorzitter, de heer Fred Erdman (SP)*, stelt voor aan de commissie om schriftelijk aan de Commissie voor de bescherming van de persoonlijke levenssfeer te vragen op welke wijze zij moet worden geraadpleegd voordat de koninklijke besluiten tot uitvoering van de wet worden goedgekeurd. Punt 4 van de conclusies bij advies nr 33/1999 bepaalt niet hoe die raadpleging praktisch moet verlopen. Er zal haar een brief worden gestuurd om daaromtrent nadere details te verkrijgen. In verband met de gewenste verwijzing naar de wet van 1992, betreffende de bescherming van de persoonlijke levenssfeer, stelt de voorzitter voor die verwijzing op te nemen in artikel 2 van elk van de ontwerpen.

Hierop heeft de Commissie voor de bescherming van de persoonlijke levenssfeer bij brief van 24 februari 2000, het volgende medegedeeld :

*« De commissie was van mening dat een systeem van* follow-up *van de voorziene maatregelen ingevoerd zou moeten worden (binnen het kader van de toepassing van de wetgeving op de informaticacriminaliteit). De commissie wenste bij deze* follow-up *te worden betrokken, voor zover elementen van de persoonlijke levensfeer in het geding zijn. De commissie had bijvoorbeeld in het verleden de wens geuit om te worden betrokken bij de* follow-up *van de door de politiediensten verrichte activiteiten van proactief onderzoek, voor zover de bescherming van de persoonlijke levenssfeer betrokken was. Hoewel niet werd ingegaan op deze wens, wenst zij niettemin een identiek verzoek te herhalen voor de haar thans in beslag nemende materie.*

*Hoewel de commissie wellicht niet de* ad hoc *instelling is om met precisie te bepalen hoe deze* follow-up *in de praktijk zou moeten worden, kan ik volgende gedachtesporen voorstellen : een instelling die de materie goed kent (het college van procureurs-generaal, de Dienst voor het Strafrechtelijk Beleid, het Nationaal Instituut voor Criminalistiek en Criminologie) zou in hoofdzaak met deze* follow-up *kunnen worden belast. De commissie zou hierbij betrokken kunnen worden door onder meer deel te nemen aan de uitwerking van criteria voor de* follow-up *die speciaal gericht zijn op de bescherming van de persoonlijke levenssfeer, en door deel te nemen aan de uitwerking van de conclusies van elk verslag. De hoofdidee achter deze samenwerking is dat indien de commissie niet de middelen heeft om de volledige* follow-up *uit te voeren (dat zou overigens misschien ook niet wenselijk zijn, daar de materie haar*

Enfin, renvoyant également à l'actualité (à savoir le récent blocage temporaire de « Yahoo », l'un des principaux moteurs de recherche sur l'Internet), le ministre répète que le projet de loi relatif à la criminalité informatique contribuera largement, d'un point de vue juridique, à la sécurisation des réseaux et accroîtra ainsi la confiance du public et de l'industrie dans le développement futur de la société de l'information.

*M. Fred Erdman (SP), président*, propose à la commission de contacter par écrit la Commission de la protection de la vie privée pour lui demander selon quelles modalités elle devrait être consultée avant l'adoption des arrêtés royaux d'exécution de la loi. Le point 4 des conclusions de l'avis n° 33/1999 ne spécifie rien des modalités pratiques de cette consultation. Un courrier lui sera adressé pour obtenir plus de détails. Quant à la référence souhaitée à la loi de 1992 sur la protection de la vie privée, le président propose que cette référence soit simplement inscrite dans l'article 2 de chacun des projets.

En réponse à la demande qui lui a été adressée, la Commission de la protection de la vie privée a précisé ce qui suit, par lettre du 24 février 2000 :

*« La commission a estimé qu'un système de suivi des mesures envisagées devrait être mis en place (dans le cadre de l'application de la législation sur la criminalité informatique). La commission a souhaité être associée à ce suivi, pour autant que des éléments de la vie privée soient en cause. La commission avait, par exemple, exprimé précédemment le souhait d'être associée au suivi des activités de recherche pro-active, déployées par les services de police, pour autant que la protection de la vie privée soit en cause. Bien qu'il n'ait pas été accédé à ce souhait, la commission tient néanmoins à formuler une demande identique en ce qui concerne la matière actuellement à l'examen.*

*Bien que la commission ne soit sans doute pas l'organe* ad hoc *pour déterminer comment ce suivi devrait être organisé dans la pratique, je peux vous proposer les pistes de réflexion suivantes : une institution connaissant bien la matière (le collège des procureurs généraux, le Service de la Politique criminelle, l'Institut national de Criminalistique et de Criminologie) pourrait être chargé, à titre principal, d'assurer ce suivi. La commission pourrait y être associée en participant, par exemple, à la formulation des critères de suivi ayant spécialement trait à la protection de la vie privée et en étant associée à la rédaction des conclusions de chaque rapport. Cette collaboration procède essentiellement de l'idée que si la commission ne dispose pas des moyens d'assurer l'intégralité du suivi (cela ne serait sans doute pas souhaitable, étant donné que la matière dépasse le cadre de ses compétences), elle pourrait y*

*bevoegdheden te buiten gaat), zij een bijdrage zou kunnen leveren op grond van haar specifieke bevoegdheden. »*

## V. — **ARTIKELSGEWIJZE BESPREKING EN STEMMINGEN**

### A. WETSONTWERP Nr 213

#### Artikel 1

Dit artikel geeft geen aanleiding tot bespreking en wordt eenparig aangenomen.

#### Artikel 1*bis*

*De heren Fred Erdman (SP) en Erik Derycke (SP)* hebben *amendement nr 1* ingediend tot invoeging van een artikel 1*bis* dat betrekking heeft op artikel 193 van het Strafwetboek. Het amendement luidt als volgt :

« Een artikel 1*bis* (*nieuw*) invoegen, luidend als volgt :

« *Artikel 1bis. — In artikel 193 van het Strafwetboek worden de woorden « geschriften of in telegrammen » vervangen door de woorden « geschriften, in informatica of in telegrammen ». ».*

#### VERANTWOORDING

Enerzijds wordt daardoor onderstreept dat de algemene principen vervat in artikel 193 in het licht van een vaststaande rechtsleer en rechtspraak toepasselijk zijn op de beoogde valsheid in informatica. Door de rangorde is dit ook in overeenstemming met de plaats die wordt toegewezen aan artikel 210*bis* zoals voorzien. » (DOC 50 0213/002).

*De heer Erdman* herinnert eraan dat hij dit amendement reeds heeft aangekondigd tijdens de algemene bespreking.

*De minister* oppert een aantal bezwaren.

Allereerst is het zo dat elektronische gegevens ook spraak en beeld kunnen voorstellen, die als zodanig niet onder de bescherming van de bepalingen inzake schriftvervalsing kunnen ressorteren.

Voorts merkt hij op dat de misdrijven die in artikel 193 worden opgesomd in tegenstelling tot de gemeenrechtelijke valsheid in geschrifte gepaard gaan met een bijzonder opzet (het oogmerk te bedriegen of te schaden), terwijl voor valsheid in informatica een algemeen opzet vereist is.

Bijzonder opzet (of het oogmerk van bedrieglijke verrijking) is daarentegen wel vereist voor het misdrijf van

*apporter sa contribution en fonction de ses compétences spécifiques. »*

## V. — **DISCUSSION DES ARTICLES ET VOTES**

### A. PROJET DE LOI N° 213

#### Article 1er

Cet article ne donne lieu à aucune discussion et est adopté à l'unanimité.

#### Article 1er*bis*

*MM. Fred Erdman (SP) et Erik Derycke (SP)* présentent un *amendement (n° 1*) visant à insérer un article 1er*bis* relatif à l'article 193 du Code pénal. Cet amendement est libellé comme suit :

« Insérer un article 1er*bis (nouveau)*, libellé comme suit :

*« Article 1erbis. — Dans l'article 193 du Code pénal, les mots « , en informatique » sont insérés entre les mots « en écritures » et les mots « ou dans les dépêches télégraphiques ». ».*

#### JUSTIFICATION

Il s'agit de souligner que, conformément à une doctrine et à une jurisprudence constantes, les principes généraux de l'article 193 s'appliquent aux faux commis en informatique. L'ordre adopté est également en concordance avec la place qui est attribuée à l'article 210*bis* proposé. » (DOC 50 0213/002).

*M. Erdman* rappelle qu'il a annoncé le dépôt de cet amendement dès la discussion générale.

*Le ministre* formule un certain nombre d'objections.

Tout d'abord, les données électroniques peuvent représenter tant des données vocales que des images, qui ne peuvent relever de la protection des dispositions en matière de faux en écritures.

Il fait par ailleurs observer que, contrairement au faux en écriture de droit commun, les délits énumérés à l'article 193 vont de pair avec un but particulier (le but de tromper ou de nuire), alors qu'un but général est requis pour le faux informatique.

Une intention particulière (ou le but de s'enrichir frauduleusement) est en revanche requise pour l'infraction

informaticabedrog (artikel 504*quater*) en datamanipulatie met het specifieke doel schade te berokkenen die wordt geviseerd door de bepalingen inzake informatica- en datasabotage (artikel 550*ter*).

*De minister* geeft toe dat er een onvolledigheid zit in het huidige artikel 193 omdat het slechts een opsomming geeft van de misdrijven waarvoor het bijzonder opzet vereist is en dat het in te voegen artikel 210*bis* daar wat dit aspect betreft, niet in past. Toch stelt hij voor om naar een betere legistieke oplossing te zoeken.

Ingaand op dit argument merkt *de heer Erdman* op dat het afzonderlijk vermelden van informaticamisdrijven in het inleidend artikel juist duidelijk maakt dat er een onderscheid is tussen de vermelde incriminaties. Uiteraard moet dit onderscheid voldoende tot uiting komen.

Voorts meent de spreker dat het misdrijf bijzonder zwaar wordt bestraft in het geval er geen oogmerk van bedrieglijke verrijking zou zijn.

*De minister* antwoordt dat de rechter die vaststelt dat de verdachte niet de bedoeling had om schade toe te brengen steeds de mogelijkheid heeft om de strafmaat aan te passen. Algemeen opzet heeft ontegensprekelijk het voordeel dat de bewijslast die op het openbaar ministerie rust minder zwaar is.

De minister merkt tevens op dat valsheid in geschrifte in feite een misdaad is die in de meeste gevallen gecorrectionaliseerd wordt. Dat verklaart waarom een bijzonder opzet wordt vereist.

*De heer Bourgeois* merkt op dat het Nederlands Strafwetboek voor valsheid in informatica een bijzondere opzet vereist.

*De voorzitter* vraagt of het niet mogelijk is om in verschillende straffen te voorzien voor het bijzonder opzet enerzijds en het algemeen opzet anderzijds.

*De minister* blijft erbij dat de rechter voldoende ruimte heeft op de strafschaal. Hij maakt de vergelijking met de eenvoudige diefstal (artikel 463 van het Strafwetboek). De straf voor diefstal, dat eveneens slechts een algemeen opzet vereist, ligt in dezelfde lijn.

*De voorzitter* merkt op dat het tweede lid van voormeld artikel 463 nochtans een lichtere straf bepaalt voor « het bedrieglijk wegnemen van andermans goed voor een kortstondig gebruik ». Deze bepaling wordt onder meer toegepast voor « *joy riding* ». Men zou de parallel kunnen maken met de « nieuwsgierige *hacker* ».

De voorzitter maakt tevens de vergelijking met de fiscale fraude (artikel 450 van het Wetboek van inkomstenbelastingen). Artikel 450 schrijft straffen voor van 1 maand tot 5 jaar en geldboetes voor wie fiscale fraude

que constitue la fraude informatique (article 504*quater*) et pour la manipulation de données dans le but spécifique de nuire, manipulation visée par les dispositions relatives au sabotage informatique et au sabotage des données (article 550*ter*).

*Le ministre* reconnaît que l'actuel article 193 présente une lacune, étant donné qu'il ne fait qu'énumérer les infractions pour lesquelles l'intention particulière est requise et que l'article 210*bis* à insérer n'y a pas sa place, en ce qui concerne cet aspect. Il propose néanmoins de chercher une meilleure solution légistique.

À propos de cet argument, *M. Erdman* fait observer qu'en mentionnant séparément les infractions informatiques dans l'article introductif, on fait précisément apparaître clairement qu'il y a une distinction entre les incriminations mentionnées. Cette distinction doit évidemment apparaître clairement.

L'intervenant estime par ailleurs que l'infraction est très sévèrement punie dans le cas où il n'y aurait pas d'intention de s'enrichir frauduleusement.

*Le ministre* fait observer que le juge qui constate que l'inculpé n'avait pas l'intention de nuire peut toujours adapter la sanction. Le fait de n'exiger qu'une intention générale présente l'avantage d'alléger le fardeau de la preuve qui pèse sur le ministère public.

Le ministre souligne en outre que le faux en écriture est en fait un crime qui est, dans la plupart des cas, correctionnalisé, ce qui explique qu'il faille une intention particulière.

*M. Bourgeois* fait observer que, selon le Code pénal néerlandais, il faut une intention particulière pour qu'il y ait faux en informatique.

*Le président* demande s'il ne serait pas possible de prévoir des peines différentes selon que l'intention est particulière ou générale.

*Le ministre* maintient que le juge dispose d'une marge de manœuvre suffisante pour fixer la peine et établit une comparaison avec le vol simple (article 463 du Code pénal). La peine prévue en cas de vol, qui ne suppose aussi qu'une intention générale, se situe dans la même ligne.

*Le président* fait remarquer que l'alinéa 2 de l'article 463 précité prévoit toutefois une sanction plus légère pour « le fait de soustraire frauduleusement la chose d'autrui en vue d'un usage momentané ». Cette disposition s'applique, entre autres, au « *joy riding* ». Un parallèle pourrait être fait avec le « *hacker* agissant par curiosité ».

Le président compare également la fraude informatique à la fraude fiscale (article 450 du Code des impôts sur les revenus). L'article 450 prévoit des peines d'emprisonnement de 1 mois à 5 ans et des amendes pour

pleegt, maar vereist tegelijk een bedrieglijk opzet (artikel 449 van WIB).

*
* *

Amendement nr 1 van de heren Fred Erdman en Erik Derycke wordt eenparig aangenomen.

Art. 2

Dit artikel voegt in het Strafwetboek een artikel 210*bis* in dat het misdrijf valsheid in informatica bestraft.

*De regering* dient *amendement nr 4* in (DOC 50 0213/003) dat in de inleidende zin van artikel 2 de woorden « titel V » vervangt door de woorden « titel III ».

Het amendement beoogt een zuiver technische correctie en geeft geen aanleiding tot bespreking.

*
* *

Amendement nr 4 van de regering en het aldus gewijzigde artikel 2 worden achtereenvolgens en eenparig aangenomen.

Art. 3

Artikel 3 voegt in het Strafwetboek een nieuw artikel 504*quater* in dat betrekking heeft op « informaticabedrog ».

*De regering* dient *amendement nr 5* in, dat de paragrafen 1 en 2 van het ontworpen artikel omwisselt waardoor de verhouding tussen de strafbare manipulaties als zodanig en de gerealiseerde fraude beter tot uiting komt.

Het amendement luidt als volgt :

« In het voorgestelde artikel 504*quater*, de paragrafen 1 en 2 vervangen als volgt :

*« § 1. Hij die voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwerft door gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 26 frank tot 100 000 frank of met een van die straffen alleen.*

*§ 2. Hij die, met het oogmerk voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel te verwerven, gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, in een*

celui qui fraude le fisc, à condition toutefois qu'il y ait dessein de nuire (article 449 du CIR).

*
* *

L'amendement n° 1 de MM. Fred Erdman et Erik Derycke est adopté à l'unanimité.

Art. 2

Cet article insère dans le Code pénal un article 210*bis* qui punit l'infraction de faux en informatique.

*Le gouvernement* présente un *amendement* (*n° 4,* DOC 50 0213/003) tendant à remplacer les mots « titre V » par les mots « titre III » dans la phrase liminaire de l'article 2.

Cet amendement tend à apporter une correction purement technique et ne donne pas lieu à discussion.

*
* *

L'amendement n° 4 du gouvernement et l'article 2, ainsi modifié, sont successivement adoptés à l'unanimité.

Art. 3

L'article 3 insère un nouvel article 504*quater* relatif à la « fraude informatique » dans le Code pénal.

*Le gouvernement* présente un *amendement* (*n° 5*) qui vise à remplacer les §§ 1er et 2 afin de mieux traduire la relation entre les manipulations punissables en tant que telles et la fraude réalisée.

L'amendement est libellé comme suit :

« Dans l'article 504*quater* proposé, remplacer les paragraphes 1er et 2 comme suit :

*« § 1. Celui qui obtient pour soi-même ou pour autrui un avantage patrimonial frauduleux, en introduisant dans un système informatique, modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs à 10 000 francs ou d'une de ces peines seulement.*

*§ 2. Celui qui, en vue de se procurer pour soi-même ou pour autrui un avantage patrimonial frauduleux, introduit dans un système informatique, modifie ou efface des données qui sont stockées, traitées ou transmises*

*informaticasysteem invoert, wijzigt, wist of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem verandert, wordt gestraft met gevangenisstraf van zes maanden tot drie 3 jaar en met geldboete van 26 frank tot 50 000 frank of met een van die straffen alleen. ».*

VERANTWOORDING

Dit amendement strekt ertoe de verhouding tussen de strafbare manipulaties als zodanig en de gerealiseerde fraude beter te articuleren. » (DOC 50 0213/003).

*De heren Fred Erdman (SP) en Erik Derycke (SP)* hebben de *amendementen nrs 2 en 3* ingediend met dezelfde strekking.

Amendement nr 2 :

« In het voorgestelde artikel 504*quater*, § 1 vervangen door wat volgt :

*« § 1. Hij die, voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwerft, door gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, in een informaticasysteem in te voeren, te wijzigen, te wissen of op enige andere technologische wijze de mogelijke aanwending van gegevens in een informaticasysteem te veranderen, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen. ».*

VERANTWOORDING

Het is duidelijk dat, in § 1 in overeenstemming met § 1 van het voorgestelde artikel 210*bis*, het voltrokken misdrijf eerst moet worden omschreven en bestraft. » (DOC 50 0213/002).

Amendement nr 3 :

« In het voorgestelde artikel 504*quater*, § 2 vervangen door wat volgt :

*« § 2. Poging tot het plegen van het misdrijf bedoeld in § 1 wordt gestraft met een gevangenisstraf van 6 maanden tot 3 jaar en met een geldboete van 26 Belgische frank tot 50 000 Belgische frank, of met een van die straffen alleen. ».*

VERANTWOORDING

Hierdoor wordt de correctie volledig doorgevoerd en wordt § 2 volledig in overeenstemming gebracht met de bewoordingen van § 3 van het voorgestelde artikel 210*bis*. » (DOC 50 0213/002).

*par un système informatique, ou modifie par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs à 50 000 francs ou d'une de ces peines seulement. ».*

JUSTIFICATION

Cet amendement vise à mieux articuler la relation entre les manipulations punissables en tant que telles et la fraude réalisée. » (DOC 50 0213/003).

*MM. Fred Erdman (SP) et Erik Derycke (SP)* présentent des *amendements* (*nos 2 et 3*) ayant la même portée.

Amendement n° 2 :

« Dans l'article 504*quater* proposé, remplacer le § 1er par la disposition suivante :

*« § 1er. Celui qui se procure, pour soi-même ou pour autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines seulement. ».*

JUSTIFICATION

Il est évident qu'il faut d'abord que le § 1er de l'article définisse et punisse l'infraction commise, comme le fait le § 1er de l'article 210*bis* proposé. » (DOC 50 0213/002).

Amendement n° 3 :

« Dans l'article 504*quater* proposé, remplacer le § 2 par la disposition suivante :

« *§ 2. La tentative de commettre l'infraction visée au § 1er est punie d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 50 000 francs belges ou d'une de ces peines seulement. ».*

JUSTIFICATION

Cette correction assure la parfaite cohérence de l'article 504*quater* proposé et met son § 2 en concordance avec le § 3 de l'article 210*bis* proposé. » (DOC 50 0213/002).

*De heer Erdman* verduidelijkt dat in de door hem voorgestelde formulering paragraaf 2 volledig in overeenstemming wordt gebracht met de bewoordingen van § 3 van het voorgestelde artikel 210*bis*, wat de concordantie van de teksten ten goede komt.

*De minister* zegt niet volledig te kunnen instemmen met de tekst die door de heer Erdman wordt voorgesteld.

De omschrijving van *de poging* in het regeringsamendement is ruimer dan de klassieke strafrechtelijke poging. Er is reeds strafbaarstelling, zelfs indien de betrokkene zijn daad zonder tussenkomst van een derde stopzet.

De minister acht deze verruiming noodzakelijk omdat men er kan van uitgaan dat zelfs de voorbereidende handelingen bij deze misdrijven een voldoende inbreuk betekenen om te worden strafbaar gesteld.

Hij haalt het voorbeeld aan van een bankbediende die een computersimulatie maakt van een financiële operatie, met rekeningen van cliënten, om zichzelf frauduleus te kunnen verrijken.

Zelfs indien hij zijn poging staakt zonder tussenkomst van een derde, dan nog is het duidelijk dat hij zijn bevoegdheid te buiten is gegaan door het manipuleren van gegevens waartoe hij beroepshalve toegang had.

*De voorzitter* vraagt waar de grens ligt met een intentie of een bedoeling, wat op zich toch niet strafbaar kan worden gesteld. Hij vreest dat een verruiming van het begrip « poging », zoals de minister voorstelt, zal worden overgenomen bij de beoordeling van gemeenrechtelijke misdrijven.

Wie de bedoeling heeft om een diefstal te plegen en zich inbrekersmateriaal aanschaft, maar uiteindelijk beslist om terug naar huis te keren, kan volgens de gemeenrechtelijke bepalingen niet worden gestraft.

De minister opent hier mogelijkheden die tot nu toe niet bestonden.

*De heer Jean-Pol Poncelet (PSC)* treedt het standpunt van de minister bij en vraagt aandacht voor het specifieke karakter van de informaticamisdrijven. Hij verwijst opnieuw naar het voorbeeld van de bankbediende die een simulatie doet met de rekeningen van cliënten. Die poging wordt terecht strafbaar gesteld zelfs indien betrokkene niet op de « enter- »toets drukt om het misdrijf te finaliseren.

*De minister* meent dat de poging op zich in het systeem zal worden geregistreerd en dus toetsbaar en bijgevolg strafbaar is.

*
* *

Amendement nr 5 van de regering wordt ingetrokken.

De amendementen nrs 2 en 3 van de heren Erdman en Derycke en het aldus gewijzigde artikel 3 worden achtereenvolgens en eenparig aangenomen.

*M. Erdman* précise que la formulation du § 2 qu'il propose met ce paragraphe en concordance avec le § 3 de l'article 210*bis* proposé, ce qui améliore la concordance des textes.

*Le ministre* déclare ne pas pouvoir marquer totalement son accord sur le texte proposé par M. Erdman.

*La tentative,* telle qu'elle est définie dans l'amendement du gouvernement, a un sens plus extensif que la tentative criminelle classique. Il y a acte criminel, même si l'intéressé met fin à son acte sans intervention d'un tiers.

Le ministre juge cette extension nécessaire, car on peut partir du principe que même les actes préparatoires de telles infractions constituent une violation qui mérite d'être punie.

Il cite l'exemple d'un employé de banque qui procède à la simulation informatique d'une opération financière au moyen des comptes de clients en vue de s'enrichir frauduleusement.

Même s'il met fin à sa tentative sans intervention d'un tiers, il reste évident qu'il a outrepassé ses droits en manipulant des données auxquelles il avait accès de par sa profession.

*Le président* demande où se situe la limite entre les notions de tentative et d'intention ou dessein, l'intention ou le dessein ne pouvant quand même pas être incriminés en soi. Il craint que la notion de tentative ne soit interprétée dans le sens élargi que propose de lui donner le ministre lorsqu'il s'agira de juger des infractions de droit commun.

En vertu du droit commun, celui qui a l'intention de commettre un vol et acquiert du matériel de cambrioleur, mais décide en fin de compte de rentrer chez lui, ne peut pas être puni.

Le ministre ouvre, en l'espèce, des possibilités qui n'existaient pas jusqu'à présent.

*M. Jean-Pol Poncelet (PSC)* souscrit au point de vue du ministre et demande que l'on soit attentif au caractère spécifique des délits liés à l'informatique. Il renvoie à nouveau à l'exemple d'un employé de banque qui effectue une simulation avec les comptes de clients. Cette tentative est incriminée à juste titre même si l'employé ne presse pas la touche « *enter* » pour finaliser l'infraction.

*Le ministre* estime que cette tentative sera enregistrée comme telle dans le système, sera vérifiable et par conséquent punissable.

*
* *

L'amendement n° 5 du gouvernement est retiré.

Les amendements nos 2 et 3 de MM. Erdman et Derycke et l'article 3, ainsi modifié, sont successivement adoptés à l'unanimité.

Art. 4

Dit artikel voegt een nieuwe titel IX*bis* in het Strafwetboek in, betreffende de misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen verwerkt of overgedragen.

*De heer Jean-Pol Poncelet (PSC)* geeft het voorbeeld van een persoon die beroepshalve de toegangscode van een informaticasysteem kent en deze doorgeeft aan een onbevoegde. Is dit voorbeeld geviseerd door de omschrijvingen van artikel 4 ?

*De minister* antwoordt dat de paragrafen 5 en 6 in dit geval toepasbaar kunnen zijn.

*Sommige leden* stellen de vraag of het hier niet eerder gaat om een nalatigheid, die niet als zodanig strafrechtelijk moet worden bestraft dan wel in het arbeidsrecht of door een interne sanctie van het bedrijf moet worden geviseerd.

*De heer Poncelet* is van oordeel dat het nuttig zou zijn om ook hier in strafbepalingen te voorzien.

Het eenvoudig doorgeven van een toegangscode impliceert immers dat het voor een onbevoegde mogelijk wordt om allerlei daden te stellen in dat informaticasysteem die ontwrichtend kunnen zijn, zelfs zonder dat men dat ooit zal kunnen bewijzen. Hij kan bijvoorbeeld de elektronische post misbruiken en verkeerde berichten doorsturen zonder dat iemand ooit zal kunnen aantonen dat de berichten door een derde werden ingebracht.

Hierin ligt het verschil met de gemeenrechtelijke misdrijven waar bijna steeds sporen kunnen worden gevonden (braak, diefstal, …).

*De heer Servais Verherstraeten (CVP)* blijft erbij dat het schuldig verzuim op zich beter niet wordt gestraft, maar dat in dat geval artikel 1382 van het Burgerlijk Wetboek moet worden toegepast.

Anderzijds stelt het lid de vraag naar het onderscheid dat wordt geviseerd in het eerste en het tweede lid van paragraaf 1. Het eerste lid betreft degene die weet dat hij niet gerechtigd is en zich toegang verschaft en het tweede lid betreft degene die zich bedrieglijk toegang verschaft.

De spreker vraagt of een niet-gerechtigde die zich wetens toegang verschaft niet gelijk moet worden gesteld met degene die zich met bedrieglijk opzet toegang verschaft.

*De voorzitter* voegt hieraan toe dat de formulering in strafzaken meestal « wetens en willens » is. Hij merkt op dat met de formulering die hier wordt gebezigd de rechter spoedig de stap zal zetten van het « weten » naar het « moest weten ».

*
* *

Art. 4

Cet article vise à insérer dans le Code pénal un nouveau titre IX*bis* concernant les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données stockées, traitées ou transmises au moyen de ce système.

*M. Jean-Pol Poncelet (PSC)* cite l'exemple d'une personne qui, de par sa profession, connaît le code d'accès à un système informatique et le communique à une personne non autorisée. Ce cas de figure est-il visé par les définitions figurant à l'article 4 ?

*Le ministre* répond que les §§ 5 et 6 sont d'application dans ce cas.

*Certains membres* demandent s'il ne s'agit pas plutôt d'une négligence ne devant pas, en tant que telle, donner lieu à une sanction pénale, mais devant plutôt relever de l'application du droit du travail ou faire l'objet d'une sanction interne infligée par l'entreprise.

*M. Poncelet* estime qu'il serait utile de prévoir également des sanctions pénales dans ce cas.

La simple communication d'un code d'accès implique en effet que l'on permet à une personne non autorisée d'accomplir, dans ce système informatique, toutes sortes d'actes pouvant le désorganiser sans que l'on puisse même jamais le prouver. C'est ainsi que cette personne peut faire un usage abusif du courrier électronique et transmettre de faux messages sans que personne puisse jamais prouver que ces messages ont été introduits dans le système par un tiers.

C'est là que se situe la différence avec les infractions de droit commun dont on peut quasi toujours trouver des traces (effraction, vol, …).

*M. Servais Verherstraeten (CVP)* maintient qu'il est préférable de ne pas sanctionner l'abstention coupable en tant que telle, mais qu'il convient en l'occurrence d'appliquer l'article 1382 du Code civil.

Le membre s'interroge par ailleurs sur la distinction faite à l'alinéa 1er et à l'alinéa 2 du § 1er. L'alinéa 1er concerne celui qui, sachant qu'il n'y est pas autorisé, accède à un système, alors que l'alinéa 2 vise celui qui accède frauduleusement à un système.

L'intervenant demande s'il ne conviendrait pas d'assimiler la personne non autorisée qui accède sciemment à un système à celui qui y accède avec une intention frauduleuse.

*Le président* ajoute qu'en matière pénale, la formule généralement utilisée est « sciemment et volontairement ». Il fait observer que le libellé proposé permettra au juge de franchir rapidement le pas entre « sachant » et « devant savoir ».

*
* *

Artikel 4 wordt eenparig aangenomen.

*
* *

B. WETSONTWERP Nr 214

Artikel 1

Voor de bespreking van dit artikel wordt verwezen naar C. Kwalificering (zie *infra*).

Art. 2

In het Wetboek van strafvordering worden een aantal vernieuwingen ingevoerd inzake opsporing en onderzoekshandelingen in een geïnformatiseerde context. De eerste hiervan is vervat in het nieuwe artikel 39*bis* van het Wetboek van strafvordering en heeft betrekking op het databeslag.

*De heer Fred Erdman (SP)* heeft een amendement *nr 2* (DOC 50 0214/003) ingediend dat reeds werd aangekondigd tijdens de algemene bespreking. Het beoogt in de eerste plaats de omkering van de redenering die in het voorgesteld artikel 2 wordt gevolgd in die zin dat wordt uitgegaan van het principe, dat in het ontworpen artikel 2 op het einde van de tekst wordt geplaatst. Tevens wordt bepaald dat deze tekst geen afbreuk doet aan de andere door het Wetboek bepaalde bevoegdheden.

Het is legistiek logischer de onder paragraaf 6 voorgestelde bepaling als principe vooraan te plaatsen.

Voor de duidelijkheid worden de paragrafen 2, 1e lid en 3 samengevoegd omdat het hier om parallelle bepalingen gaat.

De spreker heeft ook kritiek bij paragraaf 4 van het voorgestelde artikel 39*bis*.

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. Dat de procureur ook het verdere gebruik van het geheel of een deel van deze gegevens kan toestaan moet niet worden vermeld, hier geldt het algemene principe « *qui peut le plus, peut le moins* ».

Aangezien de procureur alle passende technische middelen (cf. terminologie voorgesteld door de Raad van State) dient aan te wenden om de integriteit en de vertrouwelijkheid van de in beslag genomen gegevens

L'article 4 est adopté à l'unanimité.

*
* *

B. PROJET DE LOI N° 214

Article 1er

Pour la discussion de cet article, il est renvoyé au point C. Qualification (voir *infra*).

Art. 2

Un certain nombre d'innovations, relatives aux actes d'information et d'instruction accomplis dans un contexte informatisé, sont insérées dans le Code d'instruction criminelle. La première d'entre elles est contenue dans l'article 39*bis* (nouveau) du Code d'instruction criminelle et concerne la saisie des données.

*M. Fred Erdman (SP)* présente un amendement *n° 2*, (DOC 50 0214/003), qu'il avait déjà annoncé au cours de la discussion générale. Cet amendement vise avant tout à inverser le raisonnement qui sous-tend l'article 2 du projet, de manière à partir du principe qui est énoncé à la fin du texte de cet article. Le texte de l'amendement dispose également qu'il ne déroge pas aux autres compétences prévues par le Code.

Il est plus logique, d'un point de vue légistique, de commencer par énoncer comme principe la disposition contenue dans le § 6 du texte du projet.

Dans un souci de clarté, les §§ 2, alinéa 1er et 3 sont fusionnés, étant donné qu'ils contiennent des dispositions parallèles.

L'intervenant émet également des critiques concernant le § 4 de l'article 39*bis* proposé.

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. Il ne faut dès lors pas mentionner que le procureur du Roi peut autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, étant donné que s'applique, en l'espèce, le principe général selon lequel « qui peut le plus, peut le moins ».

Étant donné que le procureur du Roi doit utiliser les moyens techniques appropriés (cf. terminologie du Conseil d'État) pour garantir l'intégrité et la confidentialité des données saisies, l'auteur propose

te waarborgen, stelt de indiener voor dat toepassing zou worden gemaakt van artikel 90*septies*, leden 2 tot 4 (regeling met betrekking tot de opname inzake afluisteren).

Het amendement luidt als volgt :

« Het voorgestelde artikel 39*bis* vervangen door de volgende bepaling :

« *Art. 39*bis*. — § 1. Met betrekking tot opgeslagen gegevens in een informaticasysteem zijn de regels van dit Wetboek inzake inbeslagneming van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van deze gegevens.*

*Indien de inbeslagneming van de drager evenwel niet wenselijk is, worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopiëerd op dragers die toebehoren aan de overheid. Indien het gebruik van dergelijke dragers wegens de dringendheid of de techniciteit niet mogelijk is, kan gebruikt worden gemaakt van dragers die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.*

*§ 2. Indien de in § 1 bedoelde gegevens strijdig zijn met de openbare orde of de goede zeden, of een gevaar opleveren voor de integriteit van informaticasystemen of gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wendt de procureur des Konings alle passende technische middelen aan om het verder gebruik van deze gegevens aan eenieder te verhinderen.*

*§ 3. Ingeval de procureur des Konings tot inbeslagneming overgaat, of gegevens heeft laten kopiëren op dragers, of wanneer om technische redenen of omwille van de omvang van de gegevens de in § 1 bedoelde maatregelen niet kunnen worden toegepast, wendt de procureur des Konings alle passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de eventuele kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.*

*§ 4. Onverminderd de bepalingen van artikel 550*bis *van het Strafwetboek wendt de procureur des Konings alle passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.*

*Gepaste technische middelen worden aangewend voor de bewaring ervan op de griffie, met overeenkomstige toepassing van de bepalingen van artikel 90*septies*, lid 2, 3 en 4.*

*§ 5. De procureur des Konings brengt de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking in dit systeem en deelt hem een samenvatting mee van de gegevens die zijn gekopiëerd of ontoegankelijk zijn gemaakt. Iedere belanghebbende, ongeacht of het informaticasysteem dan wel de daarin* que l'on applique l'article 90*septies*, alinéas 2 à 4 (règles concernant l'enregistrement des écoutes).

L'amendement est libellé comme suit :

« Remplacer l'article 39*bis* proposé par la disposition suivante :

*« Art. 39*bis*. — §1er. En ce qui concerne les données stockées dans un système informatique, les règles du présent Code en matière de saisie sont d'application lorsqu'il s'agit de copier, de rendre inaccessibles et de retirer ces données.*

*Si la saisie du support n'est pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. Si l'utilisation de tels supports n'est pas possible en raison de l'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont à la disposition de personnes autorisées à utiliser le système informatique.*

*§ 2. Si les données visées au § 1er sont contraires à l'ordre public ou aux bonnes mœurs, ou si elles présentent un danger pour l'intégrité des systèmes informatiques ou pour des données qui sont stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour empêcher toute personne de continuer à utiliser ces données.*

*§ 3. Si le procureur du Roi procède à la saisie ou s'il a fait copier des données sur des supports, ou si, pour des raisons techniques ou à cause du volume des données, il n'est pas possible d'appliquer les mesures prévues au § 1er, le procureur du Roi utilise tous les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies éventuelles de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, et pour garantir leur intégrité.*

*§ 4. Sans préjudice des dispositions de l'article 550*bis *du Code pénal, le procureur du Roi utilise tous les moyens techniques appropriés pour garantir l'intégrité et la confidentialité de ces données.*

*Des moyens techniques appropriés sont utilisés pour leur conservation au greffe, en appliquant par analogie les dispositions de l'article 90*septies*, alinéas 2, 3 et 4.*

*§ 5. Le procureur du Roi informe le responsable du système informatique de la recherche effectuée dans le système informatique et lui communique un résumé des données qui ont été copiées ou rendues inaccessibles. Toute personne intéressée, qu'elle soit ou non propriétaire du système informatique ou des données qui y sont*

*opgeslagen gegevens zijn eigendom zijn, kan overeenkomstig artikel 28*sexies *het lichten van de maatregelen aan de procureur des Konings vragen. ».*

VERANTWOORDING

1. Door het voorgestelde artikel wordt er natuurlijk geen afbreuk gedaan aan de bevoegdheden van de procureur des Konings, zowel met betrekking tot mogelijke verzegeling of inbeslagneming.

In de gegeven omstandigheden is dan ook nuttig terzake aan te duiden dat deze bepaling geen afbreuk doet aan andere door het Wetboek bepaalde bevoegdheden.

Daarom is het legistiek logischer de onder paragraaf 6 voorgestelde bepaling als principe vooraan te plaatsen.

Het is de specificiteit van de « in een informaticasysteem opgeslagen gegevens » die een bijzondere maatregel vereist, gelet vooral op de technische mogelijkheden of beperkingen.

2. In het advies van de Raad van State wordt verwezen naar de aanbeveling n$^{r}$ R (95)-13, waarbij gebruik gemaakt wordt van de term « *chiffrement* » of « becijfering ».

3. Voor de duidelijkheid is het ook goed om de §§ 2, eerste lid, en 3 samen te voegen, daar hierin dezelfde benadering terug te vinden is.

4. Wat « de gegevens die strijdig zijn met de openbare orde of de goede zeden » betreft kan het natuurlijk niet dat de procureur des Konings zelf de « verwijdering », hetgeen gelijk staat met de vernietiging, zou beslissen zonder mogelijke tegenspraak. Paragraaf 4 van het voorgestelde artikel 39*bis* lost niets op, onverminderd zelfs de opmerkingen hiernavermeld. 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 beperkt worden tot het verbieden van verdere toegang, in afwachting van een beslissing van de rechter ten gronde.

Er is wat de in het voorgestelde artikel 34*bis*, § 2, tweede lid, bedoelde gegevens betreft trouwens een fundamentele onduidelijkheid :

ofwel zijn deze gegevens nuttig voor een onderzoek en kan de « vergrendeling » volstaan, juist zoals met betrekking tot goederen, voorwerpen, geschriften een inbeslagname kan volstaan. Maar indien deze gegevens op zich, los van het gevoerde informatie-onderzoek een inbreuk zouden uitmaken, dan moet men ook een wijziging van artikel 380*quinquies* doorvoeren. Het lijkt de indiener dan ook logisch van de twee pistes te volgen en geen daarvan te zien uitsluiten. Daarom wordt ook een nieuw amendement op ontwerp II (DOC 50 0214/001) voorgesteld. Het is niet voldoende dat de recht-

*stockées, peut, conformément à l'article 28*sexies*, demander la levée des mesures au procureur du Roi. ».*

JUSTIFICATION

1. L'article proposé ne remet évidemment pas en cause les compétences du procureur du Roi, ni en ce qui concerne la mise sous scellé, ni en ce qui concerne la saisie.

Il est dès lors utile de préciser, en l'occurrence, que la disposition en question ne porte pas préjudice aux autres compétences prévues par le Code.

C'est pourquoi il est plus logique, d'un point de vue légistique, de placer la disposition du § 6 au début de l'article et de l'ériger en principe.

C'est la spécificité des « données qui sont stockées dans un système informatique » qui requiet une mesure particulière, compte tenu essentiellement des possibilités ou limitations techniques.

2. L'avis du Conseil d'État fait référence à la recommandation n° R (95)-13, qui utilise le terme « chiffrement ».

3. Pour plus de clarté, il s'indique également de fusionner les §§ 2, alinéa 1$^{er}$, et 3, étant donné leur parallélisme.

4. En ce qui concerne les « données qui sont contraires à l'ordre public ou aux bonnes mœurs », il est évidemment inadmissible que le procureur du Roi puisse lui-même décider le « retrait », c'est-à-dire la destruction de telles données, sans qu'il soit possible de contester sa décision. Le § 4 de l'article 39*bis* proposé ne résout rien, même si l'on ne tient pas compte des observations formulées ci-après. La destruction et la confiscation sont des décisions qui relèvent du juge appelé à se prononcer sur le fond, c'est pourquoi le pouvoir du procureur du Roi doit en tout état de cause être limité à la faculté d'interdire l'accès ultérieur aux données, et ce, dans l'attente d'une décision du juge appelé à se prononcer sur le fond.

L'imprécision règne d'ailleurs en ce qui concerne les données visées à l'article 39*bis*, § 2, alinéa 2, proposé :

ou bien ces données sont utiles dans le cadre d'une information et leur « verrouillage » peut suffire, tout comme une saisie peut suffire dans le cas de biens, d'objets et d'écritures; ou bien les données visées constituent en soi, indépendamment des résultats de l'information menée, une infraction et il conviendra alors de modifier également l'article 380*quinquies* du Code pénal. L'auteur de l'amendement juge par conséquent logique de prévoir les deux possibilités sans en exclure aucune, c'est pourquoi il présente également un nouvel amendement au projet de loi II (DOC 50 0214/001). On

spraak mettertijd de woorden « enigerlei wijze, direct of indirect, » en « enig reclamemiddel » zou interpreteren als zijnde ook omvattende « de opgeslagen gegevens van een informaticasysteem ». Nochtans zal dit amendement het probleem van de « gegevens strijdig met de openbare orde en ... of (gegevens die) een gevaar opleveren voor de integriteit van informaticasystemen » niet oplossen.

5. Met betrekking tot de notificatie door de procureur des Konings heeft de Raad van State gewezen op de terminologie :

« de verantwoordelijke van het informaticasysteem » biedt niet noodzakelijkerwijze een voldoende garantie voor tegenspraak (dit zou nog minder garanties bieden indien effectief, zoals in het voorgestelde artikel, de procureur des Konings eigenmachtig bepaalde gegevens zou mogen wissen !)

Uit de toelichting blijkt ten overvloede dat het in ieder geval de bedoeling is dat artikel 28*sexies*, zoals ingevoegd door de wet Franchimont, als correctief ten overstaan van de maatregelen genomen door de procureur des Konings toegepast wordt. Hier moet toch de aandacht worden gevestigd op het feit dat artikel 28*sexies* spreekt over « éénieder die geschaad wordt door een opsporingshandeling met betrekking tot zijn goederen », waar met betrekking tot het informaticasysteem het niet noodzakelijkerwijze duidelijk is of een belanghebbende zich eigenaar kan noemen van de kwestieuze gegevens.

Daarom is dan ook met betrekking tot de voorgestelde formule, zoals verwoord in de voorgestelde paragraaf 4 een aanpassing nodig met uitdrukkelijke verwijzing naar artikel 28*sexies*.

6. Wanneer anderzijds de procureur des Konings ook de integriteit, de vertrouwelijkheid en het bewaren van de gegevens moet waarborgen, dan zou kunnen worden verwezen naar de regeling die getroffen is in artikel 90*septies* met betrekking tot de opname inzake afluisteren. Het kan toch niet zijn, zoals uit het voorgestelde artikel zou blijken, dat de procureur des Konings zelf de bewaarnemer wordt van de dragers en dus zullen deze ter griffie worden neergelegd : daarom is terzake de aanpassing noodzakelijk, onverminderd bepaalde strafbepalingen die worden voorgesteld onder artikel 550*bis* Strafwetboek (artikel 4 van het ontwerp DOC 50 0213/001). » (DOC 50 0214/003).

*De minister* heeft er geen bezwaar tegen 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. De essentie van dit artikel is dat inbeslagneming mogelijk is, met inbegrip

ne peut se contenter d'attendre qu'au fil du temps, la jurisprudence étende l'application des termes « quel qu'en soit le moyen », « de façon directe ou indirecte » et « un moyen quelconque de publicité » aux « données stockées dans un système informatique ». Cet amendement ne réglera toutefois pas le problème des « données qui sont contraires à l'ordre public ou aux bonnes moeurs ou qui présentent un danger pour l'intégrité des systèmes informatiques ».

5. En ce qui concerne la notification par le procureur du Roi, le Conseil d'État a attiré l'attention sur la terminologie :

le « responsable du système informatique » n'offre pas nécessairement une garantie suffisante de contradiction (il y aurait encore moins de garanties si le procureur du Roi pouvait effectivement effacer certaines données d'initiative, ainsi que le prévoit l'article !).

Il ressort suffisamment de l'exposé des motifs que le but est en tout cas d'adapter l'article 28*sexies*, inséré par la loi Franchimont, afin d'apporter un correctif aux mesures prises par le procureur du Roi. Il convient cependant de souligner à ce propos que l'article 28*sexies* concerne « toute personne lésée par un acte d'information relatif à *ses* biens », alors qu'en matière de système informatique, on ne sait pas nécessairement si un intéressé peut se considérer comme propriétaire des données litigieuses.

C'est pourquoi il faut adapter la formule proposée au § 4, en renvoyant explicitement à l'article 28*sexies*.

6. Si, d'autre part, le procureur du Roi doit également garantir l'intégrité, la confidentialité et la conservation des données, on pourrait renvoyer à la règle prévue à l'article 90*septies* concernant l'enregistrement des écoutes. Il est inconcevable, ainsi qu'il résulterait de l'article proposé, que le procureur du Roi soit lui-même le dépositaire des supports, de sorte que ceux-ci seront déposés au greffe. Il faut donc adapter le dispositif en ce sens, sans préjudice de certaines dispositions pénales proposées à l'article 550*bis* du Code pénal (article 4 du projet DOC 50 0213/001). » (DOC 50 0214/003).

*Le ministre* ne voit aucune objection à ce que l'on inverse la logique de l'article, mais il maintient que le procureur du Roi doit pouvoir effacer des données telles que les offres de pornographie enfantine. Le procureur du Roi devra évidemment faire réaliser une copie des données incriminées, une copie qui servira de pièce à conviction. L'essence de cet article consiste à permettre la saisie tout en l'assortissant des possibili-

van de beroepsmogelijkheden en in het bijzonder artikel 28*sexies*.

Omwille van de rechtszekerheid werd analytisch te werk gegaan en worden de verschillende hypothesen vermeld.

Indien de gegevens zich op een drager bevinden dan kan die drager in beslag worden genomen; maken zij echter deel uit van een groter systeem, bijvoorbeeld de boekhouding van een onderneming dan moet naar andere oplossingen worden gezocht. In dat geval zal er voor worden geopteerd om de gegevens te kopiëren en niet te blokkeren, zodat de onderneming haar werkzaamheden kan voortzetten.

Gaat het evenwel om gegevens die niet mogen worden verspreid, omdat ze schokkend zijn (kinderporno, racistische propaganda) of schadelijk (virussen), dan moet men verder gaan. Indien de gegevens uit een bestand worden gewist nadat ze werden overgebracht op een andere drager dan benadert men nog steeds zeer dicht de situatie van de traditionele inbeslagneming omdat er in informatica geen onderscheid is tussen de kopie en het origineel.

Op de vraag of er geen bijzondere maatregelen dienen te worden genomen inzake bewaring, antwoordde de minister dat het gaat om interceptie van telecommunicatie waarvoor een specifiek regime geldt.

*De heer Servais Verherstraeten (CVP)* dient op amendement nr 2 een subamendement *nr 5* in, luidende :

« In het voorgestelde artikel 39*bis*, § 2, de woorden, « Indien de in § 1 bedoelde gegevens strijdig zijn » vervangen door de woorden *« Indien de gegevens het onderwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de in § 1 bedoelde gegevens strijdig zijn ».*

VERANTWOORDING

Deze toevoeging zorgt ervoor dat de band met het strafrecht behouden blijft. » (DOC 50 0214/004).

*De minister* betwijfelt het nut van subamendement nr 2 van de heer Verherstraeten dat, volgens hem, de tekst nodeloos ingewikkeld maakt.

*
* *

De amendementen nrs 5 (van de heer Servais Verherstraeten) en 2 (van de heer Fred Erdman) worden achtereenvolgens en eenparig aangenomen.

Artikel 2, zoals gewijzigd, wordt eenparig aangenomen.

tés de recours et en particulier de celle d'invoquer l'article 28*sexies*.

Par souci de sécurité juridique, on a procédé de manière analytique et on a mentionné les différents cas de figure.

Si les données se trouvent sur un support, ce support pourra être saisi. En revanche, si les données font partie d'un système plus vaste, par exemple la comptabilité d'une entreprise, il conviendra de chercher d'autres solutions. On choisira en l'occurrence de copier, et non de bloquer les données, de manière à permettre à l'entreprise de poursuivre ses activités.

S'il s'agit toutefois de données qui ne peuvent pas être diffusées en raison de leur caractère choquant (pornographie enfantine, propagande raciste) ou dommageable (virus informatiques), il conviendra de prendre des mesures plus radicales. Lorsque les données seront effacées d'un fichier après avoir été transférées sur un autre support, on se trouvera dans une situation très similaire à celle de la saisie traditionnelle, étant donné qu'en informatique, il n'existe pas de différence entre la copie et son original.

Répondant à la question de savoir s'il ne conviendrait pas de prendre des mesures particulières en matière de conservation, le ministre répond qu'il s'agit d'un acte d'interception de télécommunications auquel s'applique un régime spécifique.

*M. Servais Verherstraeten (CVP)* dépose un sous-amendement, *n° 5* à l'amendement n° 2. Il est rédigé comme suit :

« Dans l'article 39*bis*, § 2, proposé, remplacer les mots « Si les données visées au § 1er sont contraires » par les mots *« Si les données constituent l'objet de l'infraction ou découlent de l'infraction et si les données visées au § 1er sont contraires ».*

JUSTIFICATION

Cet ajout permet de maintenir le lien avec le droit pénal. » (DOC 50 0214/004).

*Le ministre* doute toutefois de l'intérêt du sous-amendement de M. Servais Verherstraeten, qui complique selon lui inutilement la lecture du texte.

*
* *

Les amendements nos 5 (de M. Servais Verherstraeten) et 2 (de M. Fred Erdman) sont successivement adoptés à l'unanimité.

L'article 2, tel qu'il a été modifié, est adopté à l'unanimité.

Art. 3

*Paragraaf 1*

Artikel 3 strekt ertoe in het Wetboek van strafvordering een artikel 88*ter (nieuw)* in te voegen met betrekking tot onderzoeksopdrachten in informaticanetwerken.

*De heer Servais Verherstraeten (CVP)* dient amendement *nr 6* in, dat ertoe strekt de tekst aan te passen aan het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer (bijlage II). Het amendement luidt als volgt :

« In het voorgestelde artikel 88*ter*, § 1, tweede gedachtestreepje, het woord « of » vervangen door het woord *« en ».*

VERANTWOORDING

Dit amendement wil de tekst van het ontwerp aanpassen aan het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

De uitbreiding van de huiszoeking naar de andere informaticasystemen mag volgens de Commissie slechts plaatsvinden als drie voorwaarden cumulatief aanwezig zijn. » (DOC 50 0214/004).

*De heer Jean-Pol Poncelet (PSC)* dient amendement *nr 15* in, luidende :

« In het voorgestelde artikel 88*ter*, § 1, tweede gedachtestreepje, het woord « of » vervangen door het woord *« en ».*

VERANTWOORDING

Dit amendement wil de tekst van het ontwerp aanpassen aan het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. De uitbreiding van de huiszoeking naar de andere informaticasystemen mag volgens de Commissie slechts plaatsvinden als drie voorwaarden cumulatief aanwezig zijn. » (DOC 50 0214/005).

*De minister* vreest dat het bijzonder moeilijk zal worden huiszoekingen te verrichten, mocht dit amendement worden goedgekeurd. Het legt immers al te beperkende voorwaarden op.

Volgens *de heer Hugo Coveliers (VLD*) moet de onderzoeksrechter zich altijd naar het proportionaliteitsbeginsel (derde gedachtestreepje van de ontworpen paragraaf 1) voegen. Het amendement van de heer Verherstraeten is dus overbodig.

Art. 3

*Paragraphe 1er*

L'article 3 insère dans le Code d'instruction criminelle un nouvel article 88*ter* qui concerne les recherches sur les réseaux.

*M. Servais Verherstraeten (CVP)* présente un amendement *n° 6* tendant à adapter le texte en fonction de l'avis de la Commission de la vie privée (annexe II). Il est rédigé ainsi :

« Dans l'article 88*ter*, § 1er, deuxième tiret, proposé, remplacer le mot « ou » par le mot *« et ».*

JUSTIFICATION

Le présent amendement tend à adapter le texte en fonction de l'avis de la Commission de la protection de la vie privée.

Celle-ci estime en effet que la perquisition ne peut être étendue à d'autres systèmes informatiques que si les trois conditions sont remplies de manière cumulative. » (DOC 50 0214/004).

*M. Jean-Pol Poncelet (PSC)* dépose l'amendement *n° 15* suivant :

« À l'article 88*ter*, § 1er, proposé, remplacer au second tiret le mot « ou » par le mot *« et* ».

JUSTIFICATION

Dans l'optique de l'avis rendu par la Commission pour la protection de la vie privée, il apparaît souhaitable, vu le caractère exceptionnel de l'extension de la recherche dans un système informatique, de préciser le caractère cumulatif des conditions retenues. » (DOC 50 0214/005).

*Le ministre* craint qu'en adoptant cet amendement, il devienne particulièrement difficile de procéder à des perquisitions. Les conditions pour ce faire seraient trop restrictives.

*M. Hugo Coveliers (VLD)* estime que le critère de proportionnalité (le troisième tiret du § 1er en projet) est une règle à laquelle le juge d'instruction doit toujours se conformer. L'amendement de M. Servais Verherstraeten est donc superflu.

*De heer Verherstraeten (CVP)* staat erop zijn standpunt te nuanceren. Het proportionaliteitsbeginsel zal volgens hem effect sorteren zodra het risico ontstaat dat voor het onderzoek noodzakelijke elementen verloren gaan. Ofwel komt de handhaving van de in het wetsontwerp gehanteerde formulering neer op een pleonasme, ofwel heeft zij tot gevolg dat het mogelijk is het proportionaliteitsbeginsel naast zich neer te leggen.

*De heer Bert Schoofs (Vlaams Blok)* stelt voor de eerste twee cumulatieve voorwaarden te handhaven en de derde voorwaarde weg te laten. Beide voorwaarden behelzen impliciet het proportionaliteitsbeginsel, waarvan de beoordeling aan de onderzoeksrechter wordt overgelaten.

*De heer Hugo Coveliers (VLD)* vat het proportionaliteitsvraagstuk als volgt samen : in sommige gevallen kan een in een informaticasysteem aangetroffen gegeven meer onderzoekswerk vergen dan het uitbreiden van het onderzoek tot een ander systeem. Zo er in dat geval geen sprake is van een risico op het verlies van gegevens, kan de uitbreiding van het onderzoek tot een ander systeem buiten verhouding staan tot de omvang van de zaak.

*De minister* is het met die zienswijze eens.

*De heer Charles Michel (PRL FDF MCC)* vraagt wat moet worden verstaan onder « dit onderzoek uitbreiden naar een informaticasysteem dat zich op een andere plaats bevindt dan daar waar dit onderzoek plaatsvindt ». Betekent dit dat vanuit dezelfde computers in een ander systeem wordt gezocht, ofwel dat de onderzoekers zich naar een andere plaats kunnen begeven om de computers aldaar aan een onderzoek te onderwerpen ?

*De minister en de voorzitter* bevestigen dat alleen de eerste hypothese in aanmerking komt. Zo de onderzoeksrechter het noodzakelijk acht dat de onderzoekers zich ter plaatse begeven, moet hij een nieuw huiszoekingsbevel uitvaardigen.

Of een en ander in verhouding staat tot de omvang van de zaak, moet worden afgewogen in het licht van de andere maatregelen die de onderzoeksrechter kan treffen. Zo moet die zich bijvoorbeeld afvragen wat de redelijkste werkwijze is : het aantal huiszoekingen uitbreiden of het hele onderzoek één keer en vanuit één computer uitbreiden ?

*De heer Charles Michel (PRL FDF MCC)* vreest dat de ontworpen tekst niet zal beletten dat bewijzen verloren kunnen gaan. Het ware wenselijk enkele correcties aan te brengen, teneinde de leesbaarheid te verbeteren. Voorts zij erop gewezen dat de tekst uitgaat van een huiszoekingsbevel. Het gaat dus niet om een door de onderzoeksrechter zelf uitgevoerd onderzoek. Met de thans voorliggende tekst zullen de onderzoekers om een nieuwe rechterlijke beslissing moeten verzoeken, telkens als zij een uitbreiding van hun onderzoekswerk aangewezen achten. De spreker suggereert om een

*M. Servais Verherstraeten (CVP)* tient à nuancer sa position. Le critère de proportionnalité serait à ses yeux rempli dès qu'il existe un risque de perdre des éléments nécessaires à l'enquête. Garder la formulation du projet reviendrait soit à faire un pléonasme, soit à permettre de ne pas respecter la proportionnalité.

*M. Bert Schoofs (Vlaams Blok)* propose de garder les deux premières conditions cumulatives et de supprimer la troisième. Cela inclut implicitement le principe de proportionnalité, qu'il faut laisser au juge d'instruction le pouvoir d'apprécier.

*M. Hugo Coveliers (VLD)* résume la question de la proportionnalité en exposant que dans certains cas, une donnée peut être trouvée sur un système informatique, mais en demandant plus d'efforts de recherches qu'en étendant la perquisition vers un autre système. Dans ce cas, s'il n'existe pas risque de perte de données, il peut y avoir disproportionnalité à étendre la recherche à un autre système.

*Le ministre* approuve cette interprétation.

*M. Charles Michel (PRL FDF MCC)* demande dans quel sens il faut entendre l'expression « étendre la recherche vers un système informatique qui se trouve dans un autre lieu que celui où la recherche est effectué ». S'agit-il de procéder à une recherche dans un autre système à partir des mêmes ordinateurs, ou bien les enquêteurs peuvent-ils se déplacer pour aller consulter des appareils installés en d'autres lieux ?

*Le ministre et le président* confirment que seule la première hypothèse est visée. Si le juge d'instruction estime qu'un déplacement des enquêteurs est nécessaire, il doit délivrer un nouveau mandat de perquisition.

La proportionnalité doit être évaluée par rapport aux autres mesures mises à la disposition du juge d'instruction. Par exemple, la question qu'il faut se poser est de savoir s'il est plus raisonnable de multiplier les perquisitions ou d'étendre une seule fois la recherche à partir d'un même ordinateur.

*M. Charles Michel (PRL FDF MCC)* craint que le texte projeté ne permette pas de supprimer le risque de déperdition des preuves. Quelques corrections seraient souhaitables pour en éclaircir la lecture. D'autre part, il convient de remarquer que le texte vise le cas d'un mandat de perquisition. Il ne s'agit donc pas d'une perquisition effectuée par le juge d'instruction lui-même. Le texte, tel qu'il est rédigé, va obliger les enquêteurs à demander une nouvelle décision du juge chaque fois qu'une extension de la perquisition leur paraît opportune. L'intervenant suggère de confier une

dergelijke beslissing over te laten aan de onderzoekers of aan het parket. Hij erkent dat zijn voorstel tal van moeilijkheden oplevert in verband met de bescherming van de persoonlijke levenssfeer, maar hij verzoekt de regering dat vraagstuk onder de loep te nemen.

*De voorzitter* antwoordt dat via een eenvoudige tekstcorrectie deels aan de bekommering van de heer Charles Michel kan worden tegemoetgekomen, met name door het woord « verricht » te vervangen door het woord « beveelt ». De commissie is het met die tekstcorrectie eens.

*De heer Hugo Coveliers (VLD)* stipt aan dat het begrip « informaticasysteem » zelf tot moeilijkheden kan leiden. In geval van een informaticasysteem dat verscheidene landen bestrijkt, is het mogelijk dat de Belgische speurders, precies door de uitbreiding van hun onderzoek, in het buitenland strafbare feiten aan het licht brengen. Er rijzen dus problemen met betrekking tot de territoriale toepassingssfeer van het strafrecht, de dubbele tenlastelegging en de internationale bevoegdheid van de Belgische rechtbanken.

*De heer Charles Michel (PRL FDF MCC)* denkt dat die situatie niet onverenigbaar is met het territorialiteitsbeginsel waarop het strafrecht is gebaseerd. Zo het via terminals in België mogelijk is toegang te krijgen tot strafbare informatie (bijvoorbeeld pornografie) op een gegevensbank in het buitenland, moet men ervan uit kunnen gaan dat aan het territorialiteitscriterium werd voldaan. Niettemin ware het wellicht verkieslijk dat de wetgever terzake klare wijn schenkt.

Wat het specifiek door het ontworpen artikel 88*ter* ontstane knelpunt betreft, denkt de spreker dat het doeltreffender ware het huiszoekingsbevel ruimer te omschrijven. Men zou in de mogelijkheid moeten voorzien het onderzoek onder bepaalde voorwaarden uit te breiden.

*De heer Hugo Coveliers (VLD*) is het met de heer Charles Michel eens, maar hij denkt dat er altijd een probleem zal blijven bestaan. Hoe goed men de technische aspecten van de informaticanetwerken ook onder de knie heeft, het zal allesbehalve eenvoudig zijn die begrippen om te zetten in interne en internationale strafrechtelijke bepalingen.

*De voorzitter* besluit om de Commissie voor de bescherming van de persoonlijke levenssfeer bijkomende verduidelijkingen te vragen omtrent de interpretatie van het proportionaliteitsbeginsel in dit artikel.

*
* *

telle décision aux enquêteurs ou au parquet. Il reconnaît que sa proposition pose nombre de problèmes sur le plan de la protection de la vie privée, mais prie le gouvernement de se pencher sur cette question.

*Le président* répond que, pour une part, la préoccupation de M. Charles Michel peut être rencontrée par une simple correction de texte, en remplaçant le mot « procède » par « ordonne ». La commission souscrit à cette correction du texte.

*M. Hugo Coveliers (VLD)* relève qu'un problème vient de la notion même de « système informatique ». Lorsqu'un système informatique s'étend sur plusieurs États différents, il serait possible à des enquêteurs belges de découvrir des faits punissables situés à l'étranger par la simple extension de la perquisition. Se pose alors le problème du champ d'application territoriale du droit pénal et de la double incrimination, ainsi que de la compétence internationale des tribunaux belges.

*M. Charles Michel (PRL FDF MCC)* pense que le principe de territorialité sur lequel est basé le droit pénal peut s'accommoder de cette situation. Si des terminaux situés en Belgique peuvent accéder à des données punissables, comme des images pornographiques, contenues dans une banque de donnée installée à l'étranger, le critère territorial doit pouvoir être considéré comme rempli. Toutefois, il serait sans doute préférable que le législateur effectue un choix clair à ce propos.

Quant au problème précis posé par l'article 88*ter* projeté, l'orateur pense qu'il serait plus adéquat de songer à une définition large des termes du mandat de perquisition. Celui-ci peut prévoir une possibilité d'étendre la recherche dans certaines conditions.

*Hugo Coveliers (VLD)* approuve M. Charles Michel, mais pense qu'un problème subsistera toujours. Même avec une bonne connaissance des aspects techniques des réseaux informatiques, il sera très difficile de transposer ces concepts en droit pénal interne et international.

*Le président* décide de demander des précisions complémentaires à la Commission de la protection de la vie privée quant à l'interprétation du principe de proportionnalité dans le contexte de cet article.

*
* *

*De heer Thomas, voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer,* heeft bij brief van 24 februari 2000 het volgende antwoord verstrekt :

*« U wenst tevens mijn zienswijze te kennen over de wijze waarop het proportionaliteitsbeginsel dient geïnterpreteerd in de context van artikel 3 van het wetsontwerp nr 214. De commissie was in haar advies van mening dat de uitbreiding van een onderzoek tot andere informaticasystemen slechts toegestaan zou mogen worden indien de in artikel 3 van het wetsontwerp nr 214 vermelde voorwaarden cumulatief toegepast zijn. In haar commentaar op het voorgaande artikel (artikel 2 van het wetsontwerp nr 214), had de commissie gewezen op het belang van zich zoveel mogelijk te beperken tot enkel die gegevens betreffende personen die vervolgd worden, zoals de toepassing van het proportionaliteitsbeginsel vereist.*

*Voor zover artikel 3 een uitbreiding beoogt van het onderzoek tot andere systemen (die andere types van gegevens bevatten, en eventueel voor een geheel andere finaliteit werden gecreëerd), loopt men een verhoogd risico om in deze bestanden gegevens terug te vinden die niet relevant zijn omdat ze niet rechtstreeks met de betreffende inbreuk verbonden zijn. Dit dreigt dus de eerbiediging van het proportionaliteitsbeginsel, waarvan de commissie steeds het belang benadrukt heeft, in gevaar te brengen. Om deze reden is zij van mening dat de mogelijkheden tot uitbreiding van het onderzoek door stevige waarborgen dient geschraagd; de met het oog hierop door de commissie aanbevolen wijze bestaat uit het cumulatief toepassen van de drie voorwaarden van artikel 3. ».*

Tot besluit van deze bespreking dient de *regering* amendement *nr 18* in dat de limieten van de zoeking beter vastlegt. *De vertegenwoordiger van de minister* onderstreept dat het niet de bedoeling kan zijn dat voor de uitbreiding van de zoeking naar een tweede systeem steeds een nieuw mandaat van de onderzoeksrechter wordt gevraagd.

Het amendement is als volgt opgesteld :

« In het voorgestelde artikel 88*ter*, § 1 vervangen als volgt :

« *§ 1. Wanneer de onderzoeksrechter een zoeking beveelt in een informaticasysteem of een deel daarvan, hetzij in het kader van een huiszoeking, hetzij anderszins, kan deze zoeking worden uitgebreid naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt dan daar waar deze zoeking plaatsvindt, indien :*

*— deze uitbreiding noodzakelijk is voor de waarheidsvinding ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en*

*— andere maatregelen disproportioneel zouden zijn, of er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan.* ».

*M. Thomas, président de la Commission de la protection de la vie privée,* a fourni la réponse suivante par lettre du 24 février 2000 :

*« Vous souhaitez également connaître mon point de vue sur la manière dont il convient d'interpréter le principe de proportionnalité dans le contexte de l'article 3 du projet de loi n° 214. La commission a estimé, dans son avis, que l'extension d'une perquisition à d'autres systèmes informatiques ne devrait être autorisée que si les conditions énumérées à l'article 3 du projet de loi n° 214 sont appliquées de façon cumulative. Dans son commentaire concernant l'article précédent (article 2 du projet de loi n° 214), la commission a souligné l'importance de limiter autant que possible les mesures prises aux seules données concernant des personnes poursuivies, ainsi que l'exige l'application du principe de proportionnalité.*

*Dans la mesure où l'article 3 vise à étendre la recherche à d'autres systèmes informatiques (qui contiennent d'autres types de données et qui ont éventuellement été créés dans une toute autre finalité), on risque encore davantage de retrouver dans ces fichiers des données qui ne sont pas pertinentes, parce qu'elles ne sont pas directement liées à l'infraction concernée. Cela risque dès lors de compromettre le respect du principe de proportionnalité, dont la commission a toujours souligné l'importance. C'est la raison pour laquelle elle estime que les possibilités d'étendre la recherche doivent être assorties de garanties solides. La commission recommande à cet effet de ne permettre l'extension de la recherche que si les trois conditions énoncées à l'article 3 sont remplies de façon cumulative. ».*

En conclusion de cette discussion, le *gouvernement* présente l'amendement *n° 18* tendant à mieux fixer les limites de la recherche. *Le représentant du ministre* souligne que le but n'est pas de devoir obtenir systématiquement un deuxième mandat du juge d'instruction pour l'extension de la recherche vers le deuxième système.

L'amendement est libellé comme suit :

« À l'article 88*ter* proposé, remplacer le § 1er comme suit :

« *§ 1er. Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, soit dans le cadre d'une perquisition, soit autrement, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, si :*

*— cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et*

*— d'autres mesures seraient disproportionnées, ou il existe un risque que, sans cette extension, des éléments de preuve soient perdus.* ».

VERANTWOORDING

Dit amendement strekt ertoe de draagwijdte van de tekst te verduidelijken :

1° In tegenstelling tot de letter van de bestaande tekst is het niet de bedoeling dat voor de uitbreiding van de zoeking naar het tweede systeem een tweede mandaat van de onderzoeksrechter wordt bekomen; dit zou immers de maatregel van elke effectiviteit beroven.

2° Er zijn twee cumulatieve voorwaarden voor de uitbreiding van de zoeking.

Inzake de tweede voorwaarde worden twee alternatieve hypothesen geviseerd : hetzij een bewijsrisico, hetzij het onevenredig karakter *in concreto* van andere onderzoeksmaatregelen. ».

*Paragraaf 2*

*De heer Jean-Pol Poncelet (PSC)* dient amendement *nr 14* in, dat als volgt luidt :

« In het voorgestelde artikel 88*ter*, § 2, de woorden « toegang hebben » vervangen door de woorden « *specifiek toegang hebben op grond van een bijzondere machtiging* ».

VERANTWOORDING

In het licht van de memorie van toelichting, alsook van het door de Commissie voor de bescherming van de persoonlijke levenssfeer uitgebrachte advies, ware het aangewezen in de tekst van het ontworpen artikel 88*ter* nader te preciseren dat de uitbreiding van het onderzoek alleen betrekking heeft op informaticasystemen waartoe de gerechtigde personen specifiek toegang hebben. » (DOC 50 0214/005).

*De regering* dient vervolgens *amendement nr 21* in dat werd opgesteld ingevolge het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en dat in dezelfde zin gaat als het amendement van de heer Poncelet. Het luidt als volgt :

« In § 2 van het voorgestelde artikel 88*ter* de woorden « *in het bijzonder* » invoegen tussen de woorden « te gebruiken », en het woord « toegang ».

VERANTWOORDING

Dit amendement strekt ertoe de tekst te preciseren. » (DOC 50 0214/006).

JUSTIFICATION

Cet amendement vise à clarifier la portée du texte.

1° Contrairement à la lettre de la version actuelle du texte, le but n'est pas de devoir obtenir un deuxième mandat du juge d'instruction pour l'extension de la recherche vers le deuxième système; en effet, cela dénuerait la mesure de toute effectivité.

2° Il y a deux conditions cumulatives concernant l'extension de la recherche.

Quant à la deuxième condition, deux hypothèses alternatives sont visées : soit, le risque en matière de preuve, soit, le caractère démesuré *in concreto* d'autres mesures d'instruction. ».

*Paragraphe 2*

*M. Jean-Pol Poncelet (PSC)* dépose un amendement *n° 14* ainsi libellé :

« À l'article 88*ter*, § 2, proposé, remplacer le mot « accès » par les mots « *spécifiquement accès en vertu d'une autorisation particulière ».*

JUSTIFICATION

Eu égard à l'exposé des motifs et dans l'optique de l'avis rendu par la Commission pour la protection de la vie privée, il convient de préciser le texte de l'article 88*ter* en projet pour faire ressortir que seule est visée l'extension à des systèmes auxquels les perosnnes autorisées ont spécifiquement accès. » (DOC 50 0214/005).

*Le gouvernement* présente ensuite *l'amendement n° 21*, rédigé à la suite de l'avis de la commission de la protection de la vie privée et ayant la même teneur que l'amendement de M. Poncelet. L'amendement du gouvernement est libellé comme suit :

« À l'article 88*ter*, § 2, proposé, insérer le mot « *spécifiquement* » entre le mot « ont » et le mot « accès ».

JUSTIFICATION

Cet amendement vise à apporter une précision dans le texte. » (DOC 50 0214/006).

*Paragrafen 3 en 4*

*De heer Servais Verherstraeten (CVP)* dient *amendement nr 11* in, luidend als volgt :

« In het voorgestelde artikel 88*ter*, § 3, eerste lid, de laatste zin vervangen door de volgende zin :

« *De onderzoeksrechter brengt de technische verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet kan achterhaald worden, in welk geval de bewaarder ervan dient op de hoogte gebracht.* ».

VERANTWOORDING

De indiener verwijst naar het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

De technische verantwoordelijke informeren of bij ontstentenis daarvan de bewaarder in de zin van artikel 1384 van het Burgerlijk Wetboek, is meer gespecifieerd.

*Noot :* Het huidig amendement kan eventueel als een subamendement op amendement nr 2,(DOC 50 0214/003) van de heer Erdman worden aangewend.

Het lijkt mij toch zinvol om de vermelding in het ontwerp, zijnde « tenzij diens identiteit of woonplaats niet achterhaald kan worden », aan te houden. ». » (DOC 50 0214/005).

In de ogen van *de minister* is het voorgestelde amendement te beperkend. Het zou het risico doen ontstaan dat de « technisch » verantwoordelijke onvindbaar is, wat zou impliceren dat onmogelijk kan worden achterhaald wie juridisch aansprakelijk is. ».

*
* *

Amendement *nr 18* van de regering wordt aangenomen met 12 stemmen en 2 onthoudingen.

Bijgevolg wordt amendement *nr 15* van de heer Jean-Pol Poncelet zonder voorwerp.

Amendement *nr 6* van de heer Verherstraeten wordt verworpen met 11 tegen 1 stem en 1 onthouding.

Amendement *nr 21* van de regering wordt aangenomen met 9 stemmen en 5 onthoudingen.

Amendement *nr 11* van de heer Verherstraeten wordt ingetrokken.

Artikel 3, zoals gewijzigd, wordt aangenomen met 12 stemmen en 2 onthoudingen.

*Paragraphes 3 et 4*

*M. Servais Verherstraeten (CVP)* dépose *l'amendement n° 11* :

« Au § 3, alinéa 1er, de l'article 88*ter* proposé, remplacer la dernière phrase par la phrase suivante :

« *Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, auquel cas le dépositaire des données doit être informé.* ».

JUSTIFICATION

L'auteur renvoie à l'avis de la Commission de la protection de la vie privée.

Il est mieux précisé qu'il faut informer le responsable du système ou, en l'absence de ce dernier, le dépositaire des données au sens de l'article 1384 du Code civil.

*Nota bene* : Le présent amendement peut éventuellement être présenté comme sous-amendement à l'amendement n° 2 de M. Erdman (DOC 50 0214/003).

Il me paraît quand même utile de conserver dans le projet les termes « sauf si son identité ou son adresse ne peuvent être retrouvées ». » (DOC 50 0214/005).

*Le ministre* explique que l'amendement proposé est trop restrictif. On risque de voir apparaître des situations où le responsable « technique » sera introuvable et où il n'y aura dès lors pas moyen de trouver un responsable juridique. ».

*
* *

L'amendement n° 18 du gouvernement est adopté par 12 voix et 2 abstentions.

L'amendement *n° 15* de M. Jean-Pol Poncelet devient dès lors sans objet.

L'amendement *n° 6* de M. Verherstraeten est rejeté par 11 voix contre 1 et une abstention.

L'amendement *n° 21* du gouvernement est adopté par 9 voix et 5 abstentions.

L'amendement *n° 11* de M. Verherstraeten est retiré.

L'article 3, ainsi modifié, est adopté par 12 voix et 2 abstentions.

Art. 4

Dit artikel strekt tot invoeging van een artikel 88*quater (nieuw)* in het Wetboek van strafvordering. Dat artikel voorziet met name in een aantal bijzondere verplichtingen tot samenwerking in een informaticaomgeving.

*De heer Verherstraeten (CVP)* dient amendement *nr 10* in, luidend :

« Het voorgestelde artikel 88*quater*, § 1, aanvullen met de volgende zin :

« *De onderzoeksrechter vermeldt de feitelijke omstandigheden van de zaak die de maatregel wettigen in een met redenen omkleed bevelschrift dat hij meedeelt aan de procureur des Konings. ».*

VERANTWOORDING

De opdracht om inlichtingen te verlenen over de werking van de informaticasystemen en over de wijze om in een verstaanbare vorm toegang te krijgen tot de gegevens moet, eventueel achteraf, schriftelijk worden bevestigd aan de procureur des Konings. Om de snelheid van deze interventie te garanderen, opteert men voor een schriftelijke bevestiging in plaats van een schriftelijke opdracht. Dit naar analogie met de afluisterwet. » (DOC 50 0214/005).

*De minister* heeft geen bezwaar tegen de goedkeuring van dit amendement.

*De heer Hugo Coveliers (VLD)* wijst erop dat die bepaling een internationale draagwijdte heeft. In de wetgeving van sommige landen, en met name in die van de Verenigde Staten, zijn pogingen tot het verkrijgen of verspreiden van geïnformatiseerde toegangscodes strafbaar. Het is dus denkbaar dat een Belgische onderzoeksrechter, via de netwerken en overeenkomstig de Belgische wetgeving, iemand opdraagt de Amerikaanse wet te overtreden door in een Amerikaanse terminal toegangscodes op te sporen.

De *voorzitter* heeft een opmerking van taalkundige aard bij de Franse tekst van § 2. De verwijzing naar « *toute personne pertinente* » is voor hem niet precies genoeg. De Nederlandse tekst, die verwijst naar elke « *relevante* » persoon is duidelijker.

*De regering* dient vervolgens amendement *nr 19* in dat in de Franse tekst, het woord « *pertinente* » vervangt door « *appropriée* » (DOC 50 0214/006).

*
* *

Art. 4

Cette disposition insère un nouvel article 88*quater* dans le Code d'instruction criminelle qui prévoit un certain nombre d'obligations particulières de coopérer dans un environnement informatisé.

*M. Servais Verherstraeten (CVP)* dépose un amendement *n° 10* ainsi libellé :

« Compléter l'article 88*quater*, § 1er, proposé, par la phrase suivante :

*« Le juge d'instruction mentionne les circonstances objectives de l'affaire justifiant la mesure dans une ordonnance motivée qu'il transmet au procureur du Roi. »*.

JUSTIFICATION

L'ordre de fournir des informations sur le fonctionnement des systèmes informatiques et sur la manière d'accéder aux données dans une forme compréhensible doit être confirmé, éventuellement par la suite, par écrit au procureur du Roi. Afin de garantir la rapidité de cette intervention, on opte pour une confirmation écrite plutôt que pour un ordre écrit, et ce, par analogie avec la loi sur les écoutes. » (DOC 50 0214/005).

*Le ministre* ne voit pas d'objection à l'adoption de cet amendement.

*M. Hugo Coveliers (VLD)* attire l'attention sur l'aspect international de la disposition concernée. Certains pays, les États-Unis notamment, ont une législation réprimant le fait de tenter d'obtenir ou de divulguer les codes d'accès informatique. Via les réseaux, on pourrait voir un juge d'instruction belge ordonner, en vertu de la loi belge, à quelqu'un d'enfreindre le droit américain sur un terminal américain en livrant des codes d'accès.

*Le président* formule une observation d'ordre linguistique concernant le texte français du § 2. Il estime que la référence à « toute personne pertinente » n'est pas assez précise. Le texte néerlandais qui renvoie à toute « *relevante persoon* » est plus clair.

*Le gouvernement* présente ensuite un *amendement n° 19* tendant à remplacer, dans le texte français, le mot « pertinente » par le mot « appropriée » (DOC 50 0214/006).

*
* *

De amendementen nrs 10 van de heer Servais Verherstraeten en 19 van de regering en het aldus gewijzigde artikel worden achtereenvolgens en eenparig aangenomen.

Art. 5

Dit artikel geeft geen aanleiding tot opmerking en wordt eenparig aangemomen.

Art. 6

De artikelen 6, 7 en 8 betreffen een aanpassing van de nadere regels voor het gerechtelijk onderscheppen van telecommunicatie.

Allereerst dient de lijst van misdrijven waarvoor een tapmaatregel mogelijk is te worden uitgebreid met de volgende artikelen : 210*bis*, 259*bis*, 314*bis*, 504*quater*, 550*bis* en 550*ter* van het Strafwetboek.

*De regering* dient amendement *nr 17* in dat het voorgestelde artikel 6 technisch verbetert en dat de artikelen 324*bis* en 324*ter* aan de lijst toevoegt.

Het amendement luidt als volgt :

« Dit artikel vervangen door de volgende bepaling :

« *Art. 6. — In artikel 90*ter*, § 2, van hetzelfde Wetboek, ingevoegd bij de wet van 30 juni 1994 en gewijzigd bij de wet van 13 april 1995 en bij de wet van 10 juni 1998, worden de volgende wijzigingen aangebracht :*

*A) het 1°*bis *wordt vervangen door de volgende bepalingen :*

*« 1°*bis*. Artikel 210*bis *van hetzelfde Wetboek;*

*1°*ter*. Artikel 259*bis *van hetzelfde Wetboek;*

*1°*quater*. Artikel 314*bis *van hetzelfde Wetboek;*

*1°*quinquies*. Artikelen 324*bis *en 324*ter *van hetzelfde Wetboek; »*

*B) een 10°*bis*, luidend als volgt wordt ingevoegd :*

*« 10*bis*. Artikel 504*quater *van hetzelfde Wetboek; »;*

*C) een 13°*bis*, luidend als volgt, wordt ingevoegd :*

*« 13°*bis*. Artikelen 550*bis *en 550*ter *van hetzelfde Wetboek. ».* ».

VERANTWOORDING

Dit amendement strekt ertoe een technische verbetering door te voeren, aangezien de wet van 10 januari 1999 reeds een 1*bis* heeft ingevoegd in artikel 90*ter*, § 2. » (DOC 50 0214/006).

*
* *

Les amendements nos 10 de M. Servais Verherstraeten et 19 du gouvernement ainsi que l'article, ainsi modifié, sont successivement adoptés à l'unanimité.

Art. 5

Cet article ne donne lieu à aucune observation. Il est adopté à l'unanimité.

Art. 6

Les articles 6, 7 et 8 concernent une adaptation des modalités du mode d'interception de la télécommunication par les autorités judiciaires.

Premièrement, la liste des infractions pour lesquelles une mesure d'écoute est possible doit être élargie aux infractions visées par les articles 210*bis*, 259*bis*, 314*bis*, 504*quater*, 550*bis* et 550*ter* du Code pénal.

*Le gouvernement* présente un amendement *n° 17* tendant à apporter des corrections d'ordre technique à l'article 6 proposé et à ajouter à la liste les articles 324*bis* et 324*ter* du Code pénal.

L'amendement est libellé comme suit :

« Remplacer cet article par la disposition suivante :

*« Art. 6. — À l'article 90*ter*, § 2, du même Code, inséré par la loi du 30 juin 1994 et modifié par la loi du 13 avril 1995 et par la loi du 10 juin 1998, sont apportées les modifications suivantes :*

*A) le 1°*bis *est remplacé par les dispositions suivantes :*

*« 1°*bis*. à l'article 210*bis *du même Code;*

*1°*ter*. à l'article 259*bis *du même Code;*

*1°*quater*. à l'article 314*bis *du même Code;*

*1°*quinquies *aux articles 324*bis *et 324*ter *du même Code; »;*

*B) il est inséré un 10°*bis*, rédigé comme suit :*

*« 10°*bis*. à l'article 504*quater *du même Code; »;*

*C) il est inséré un 13°*bis*, rédigé comme suit :*

*« 13°*bis*. aux articles 550*bis *et 550*ter *du même Code. ».* ».

JUSTIFICATION

Cet amendement vise à introduire une correction technique, vu le fait que la loi du 10 janvier 1999 a déjà inséré un 1°*bis* à l'article 90*ter*, § 2. » (DOC 50 0214/006).

*
* *

Amendement *nr 17* van de regering, dat het artikel volledig vervangt, wordt eenparig aangenomen.

Art. 7

Dit artikel machtigt de onderzoeksrechter om een bijzondere medewerkingsverplichting op te leggen in het kader van het onderscheppen van telecommunicatie.

*De heren Fred Erdman (SP)* en *Eric Derycke (SP)* dienen amendement *nr 1* in dat artikel 458 van het Strafwetboek van toepassing verklaart op degenen die hun technische medewerking dienen te verlenen in het kader van het gerechtelijk onderzoek.

« Het voorgestelde artikel 90*quater*, § 4, vierde lid, vervangen door het volgende lid :

« *Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of die ertoe wordt geroepen zijn technische medewerking te verlenen, is gebonden door het geheim van het gerechtelijk onderzoek. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. ».* » (DOC 50 0214/002).

*De minister* stemt met deze toevoeging in.

*
* *

Amendement *nr 1* van de heren Fred Erdman en Erik Derycke en het aldus gewijzigde artikel worden achtereenvolgens en eenparig aangenomen.

Art. 8

*De heer Servais Verherstraeten (CVP)* dient amendement *nr 7* in, dat gevolg geeft aan een suggestie van de Commissie voor de bescherming van de persoonlijke levenssfeer (zie bijlage II) en dat luidt als volgt :

« In de voorgestelde tekst, eerste zin, het woord « kunnen » vervangen door het woord *« moeten »*.

VERANTWOORDING

De Commissie voor de bescherming van de persoonlijke levenssfeer oordeelde in zijn advies dat aangezien de persoonsgegevens niet van deze bewaring uitgesloten zijn, men bij voorkeur moet verduidelijken dat de middelen « moeten » en niet « mogen » worden aangewend voor de integriteit en de vertrouwelijkheid. » (DOC 50 0214/004).

L'amendement *no 17* du gouvernement tendant à remplacer cet article par une nouvelle disposition, est adopté à l'unanimité.

Art. 7

Cet article autorise le juge d'instruction à imposer une obligation particulière de collaborer dans le cadre de l'interception de la télécommunication.

*MM. Fred Erdman (SP) et Eric Derycke (SP)* présentent l'amendement *n° 1* tendant à rendre l'article 458 du Code pénal applicable à toute personne qui est appelée à prêter son concours technique dans le cadre de l'instruction.

« Remplacer l'article 90*quater*, § 4, alinéa 4, proposé, par l'alinéa suivant :

« *Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou est appelée à y prêter son concours technique, est liée par le secret de l'instruction. Toute violation du secret sera punie conformément à l'article 458 du Code pénal. ».* » (DOC 50 0214/002).

*Le ministre* marque son accord sur cet ajout.

*
* *

L'amendement *n° 1* de MM. Fred Erdman et Erik Derycke et l'article, ainsi modifié, sont successivement adoptés à l'unanimité.

Art. 8

*M. Servais Verherstraeten (CVP)* présente l'amendement *n° 7* qui reprend la suggestion de la Commission de la protection de la vie privée (voir annexe II) et qui est libellé comme suit :

« Dans le texte proposé, première phrase, remplacer les mots « peuvent être utilisés » par les mots *« doivent être utilisés ».*

JUSTIFICATION

La Commission de la protection de la vie privée fait valoir, dans son avis, qu'il convient de prévoir que les moyens « doivent » et non « peuvent » être utilisés pour garantir l'intégrité et la confidentialité, étant donné que les données à caractère personnel ne sont pas exclues de la conservation en question. » (DOC 50 0214/004).

Volgens *de minister* is de door de heer Servais Verherstraeten voorgestelde formulering te strak. De mogelijkheden en de beperkingen van de techniek kunnen niet over het hoofd worden gezien. Niemand kan worden gedwongen iets te doen wat technisch onmogelijk is.

*De heer Jean-Pol Poncelet (PSC)* dient amendement *nr 13* in, waarmee hij hetzelfde doel nastreeft. Het amendement luidt als volgt :

« In de voorgestelde tekst, het woord « kunnen » vervangen door het woord « *moeten* ».

VERANTWOORDING

Rekening houdend met het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer is terzake de verplichting te verkiezen boven de mogelijkheid. » (DOC 50 0214/005).

*De regering* dient ten slotte amendement *nr 20* in dat de volledige vervanging van het artikel beoogt. De voorgestelde tekst luidt als volgt :

« Dit artikel vervangen door de volgende bepaling :

*« Art. 8. — In artikel 90*septies *van hetzelfde Wetboek wordt tussen het vierde en het vijfde lid het volgende lid ingevoegd :*

*« De passende middelen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen, en voorzover mogelijk, de overschrijving of vertaling hiervan tot stand te brengen. Hetzelfde geldt voor de bewaring op de griffie van de opnamen en de overschrijving of vertaling hiervan en voor de vermeldingen in het bijzonder register. De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, deze middelen en het ogenblik waarop deze middelen de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en het vierde lid, vervangen. ».* ».

VERANTWOORDING

Dit amendement strekt ertoe de beveiliging van de gegevens duidelijk als een verplichting te formuleren, en integreert vanuit dezelfde bekommernis, het voorafgaand advies van de privacycommissie voor de uitvoeringsbesluiten. » (DOC 50 0214/006).

*
* *

De amendementen *nrs 7 en 8* van de heer Servais Verherstraeten worden ingetrokken.

*Le ministre* répond que la formulation proposée par M. Servais Verherstraeten est trop rigide. Il faut tenir compte des possibilités techniques et de leurs limites. On ne peut pas contraindre quelqu'un à faire une chose techniquement impossible.

*M. Jean-Pol Poncelet (PSC)* présente un amendement *n° 13* visant le même but et libellé comme suit :

« Dans le texte proposé, remplacer le mot « peuvent » par le mot *« doivent ».*

JUSTIFICATION

Dans l'optique de l'avis de la Commission de protection de la vie privée, l'obligation est préférable à l'option en la matière. » (DOC 50 0214/005).

Le gouvernement présente enfin l'amendement *n° 20* tendant à remplacer l'ensemble de l'article. Le texte proposé est libellé comme suit :

« Remplacer cet article par la disposition suivante :

*« Art. 8. — À l'article 90*septies *du même Code, insérér l'alinéa suivant entre le quatrième et le cinquième alinéa :*

*« Les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée et, dans la mesure du possible, pour réaliser sa transcription ou sa traduction. La même règle vaut pour la conservation au greffe des enregistrements et de leur transcription ou de leur traduction et pour les mentions dans le registre spécial. Le Roi détermine, après avoir recueilli l'avis de la Commission de la protection de la vie privée, ces moyens et le moment où ces moyens remplacent la conservation sous pli scellé ou le registre spécial prévus aux troisième et quatrième alinéas. ».* ».

JUSTIFICATION

Cet amendement vise à formuler clairement la protection des données comme une obligation, et intègre, dans le même souci, l'avis préalable de la commission de la vie privée pour les arrêtés d'exécution. » (DOC 50 0214/006).

*
* *

Les amendements *nos 7 et 8* de M. Servais Verherstraeten sont retirés.

Amendement *nr 20* van de regering wordt eenparig aangenomen en vervangt artikel 8. Bijgevolg wordt amendement nr 13 van de heer Jean-Pol Poncelet zonder voorwerp.

Art. 9

*De regering* dient amendement *nr 3* in, luidende :

« In het 1°, in de voorgestelde Franse tekst, tussen het woord « pour » en de woorden « les fournisseurs » **de woorden** « *les opérateurs de réseaux de télécommunication et »* invoegen.

VERANTWOORDING

Dit amendement strekt ertoe de Franstalige versie van de tekst in overeenstemming te brengen met de Nederlandstalige. » (DOC 50 0214/003).

*De heer Jean-Pol Poncelet* dient amendement nr 12 in, dat de volgende wijziging beoogt : « In het punt 1° van de voorgestelde tekst, tussen de woorden « besluit » en de woorden « en op voorstel van » de woorden « *na het advies te hebben ingewonnen van de Commissie voor de bescherming van de persoonlijke levenssfeer* » invoegen.

VERANTWOORDING

Rekening houdend met het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer is het beter ook in § 2 te bepalen dat het advies van de Commissie moet worden ingewonnen. » (DOC 50 0214/005).

*De heer Servais Verherstraeten (CVP)* dient amendement *nr 9* in, luidende :

« Het punt 1 van de voorgestelde tekst vervangen door wat volgt :

*« — 1° het eerste lid van § 2 wordt aangevuld als volgt :*

*« , evenals de verplichtingen voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten om de oproepgegevens van telecommunicatiemiddelen en de identificatiegegevens van gebruikers van telecommunicatiediensten te registreren en te bewaren, in de gevallen, te bepalen bij een in Ministerraad overlegd besluit en op voorstel van de minister van Justitie en de minister van Telecommunicatie, Overheidsbedrijven en Participaties en gedurende een bepaalde termijn. Deze termijn wordt bepaald bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de*

L'amendement *n° 20* du gouvernement, remplaçant l'article 8, est adopté à l'unanimité. l'amendement n° 13 de M. Jean-Pol Poncelet devient dès lors sans objet.

Art. 9

*Le gouvernement* présente l'amendement *n° 3* suivant :

« Au 1°, dans le texte proposé, insérer les mots « *les opérateurs de réseaux de télécommunication »* entre le mot « pour » et les mots « les fournisseurs ».

JUSTIFICATION

Cet amendement vise à mettre en conformité la version française du texte avec la version néerlandaise. » (DOC 50 0214/003).

*M. Jean-Pol Poncelet* présente l'amendement n° 12 qui vise à apporter la modification suivante : « Au 1°, dans le texte proposé, insérer les mots *« , après avis de la Commission pour la protection de la vie privée* » entre le mot « ministres » et les mots « et sur proposition ».

JUSTIFICATION

Dans l'optique de l'avis de la Commission pour la protection de la vie privée, il est préférable de prévoir également la consultation de la Commission au § 2. » (DOC 50 0214/005).

*M. Servais Verherstraeten (CVP)* dépose l'amendement *n° 9* suivant :

« Remplacer le 1° du texte proposé par ce qui suit :

*« — 1° L'alinéa 1er du § 2 est complété comme suit :*

*« , ainsi que les obligations pour les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications d'enregistrer et de conserver, pendant un certain délai, dans les cas à déterminer par arrêté royal délibéré en Conseil des ministres et sur proposition du ministre de la Justice et du ministre des Télécommunications et des Entreprises et Participations publiques, les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications. Ce délai est déterminé par arrêté royal délibéré en Conseil des ministres et après avis de la Commission de la*

*persoonlijke levenssfeer en deze mag nooit minder zijn dan 12 maanden.*

*De bovenvermelde bewaringsplicht voor de operatoren van de telecommunicatienetwerken en de verstrekkers van de telecommunicatiediensten moet plaatsvinden binnen de grenzen van het Belgische Rijk. ». ».*

VERANTWOORDING

Momenteel bestaat er geen enkele bepaling die aan de internetproviders een bewaringstermijn oplegt van hun gegevens. Sommige providers houden geen gegevens bij, anderen daarentegen houden hun gegevens bij gedurende zes maanden.

In de praktijk ijvert men ervoor om een wettelijke termijn op te leggen. Deze bewaringstermijn mag nooit minder zijn dan 12 maanden.

Bepaalde internetproviders in België bewaren hun bestanden in andere landen. Dit vergt vaak een moeizame internationale opzoeking en bewaargeving. Daarom stelt men hier voor om de bewaringsplicht te verplichten binnen de landsgrenzen. » (DOC 50 0214/004).

*De heer Jean-Pol Poncelet (PSC)* dient amendement *nr 16* in, luidende :

« In het 1° van de voorgestelde tekst, de woorden « evenals de verplichtingen voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten om de oproepgegevens van telecommunicatiemiddelen en de identificatiegegevens van gebruikers van telecommunicatiediensten te registreren en in de gevallen en gedurende een termijn door de Koning te bepalen, te bewaren » vervangen door de woorden « *evenals de verplichtingen voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten om de oproepgegevens van telecommunicatiemiddelen en de identificatiegegevens van gebruikers van telecommunicatiediensten te registreren en ze, zo de behoeften van de dienst dat vereisen, gedurende een termijn van drie maanden te bewaren* ».

VERANTWOORDING

Dit amendement wil ten eerste, zoals de Nederlandse versie het doet, in de Franse tekst de operatoren van telecommunicatienetwerken opnemen.

Daarnaast wil het, overeenkomstig het standpunt van de Commissie voor de bescherming van de persoonlijke levenssfeer, het toepassingsgebied van het voorgestelde artikel beperken door in de wettekst een termijn te bepalen tijdens welke de gegevens worden

*protection de la vie privée et ne peut jamais être inférieur à 12 mois.*

*La conservation des données imposée aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications doit s'effectuer à l'intérieur des limites du territoire du Royaume. ». ».*

JUSTIFICATION

Il n'existe actuellement aucune disposition qui impose aux fournisseurs d'accès à l'Internet de conserver leurs données pendant un délai déterminé. Certains fournisseurs d'accès ne conservent aucune donnée, d'autres conservent par contre leurs données pendant six mois.

Dans la pratique, on préconise d'imposer un délai légal de conservation. Ce délai ne pourra jamais être inférieur à 12 mois.

Certains fournisseurs d'accès à l'Internet en Belgique conservent leurs fichiers à l'étranger. Cela pose fréquemment des problèmes en matière de recherche et de dépôt au niveau international. C'est la raison pour laquelle nous proposons que la conservation doive impérativement s'effectuer dans les limites du territoire national. » (DOC 50 0214/004).

*M. Jean-Pol Poncelet (PSC)* introduit un amendement *n° 16*, libellé comme suit :

« Au 1°, dans le texte proposé, remplacer les mots « , ainsi que les obligations pour les fournisseurs de services d'enregistrer et de conserver dans les cas et pendant un délai à déterminer par le Roi » par les mots *« , ainsi que les obligations pour les opérateurs de réseaux de télécommunications et les fournisseurs de services d'enregistrer et de conserver, lorsque les nécessités de l'instruction l'exigent, pendant un délai de 3 mois ».*

JUSTIFICATION

Premièrement, cet amendement vise à inclure dans le texte français les opérateurs de réseaux, conformément au texte néerlandais.

En outre, dans l'optique développée par la Commission pour la protection de la vie privée, l'amendement vise à limiter le champ d'application de l'article proposé en précisant dans le texte légal une durée de conservation et en limitant l'obligation d'enregistrer et de conser-

bewaard en door de verplichting om die gegevens te registreren en te bewaren alleen op te leggen als dat ten behoeve van een onderzoek vereist is. » (DOC 50 0214/003).

*De minister* geeft de voorkeur aan de door de heer Servais Verherstraeten voorgestelde termijn van twaalf maanden, boven die van drie maanden, zoals naar voor geschoven door de heer Jean-Pol Poncelet. Hij verwijst in dat verband naar de hoorzittingen met de leden van de gerechtelijke politie en de rijkswacht (zie bijlage II).

*De heer Hugo Coveliers (VLD)* is van oordeel dat de meest verkieslijke termijn ergens tussenin ligt, met name zes maanden. Een bewaringstermijn van twaalf maanden voor niet langer gebruikte gegevens lijkt hem overdreven.

*De heer Bert Schoofs (Vlaams Blok)* vindt de lengte van de termijn minder belangrijk dan de wijze waarop de gegevens worden bewaard. Het is van fundamenteel belang te weten waar de gegevens worden bewaard, wie er toegang toe heeft en wat voor beschermingsmaatregelen erop van toepassing zijn.

Voor *de heer Vanhoutte (Agalev-Ecolo*) is een termijn van zes maanden het aanvaardbare minimum. Maar hoe dan ook moet duidelijkheid worden geschapen over wat men wil beschermen. Tevens moeten ook de nodige maatregelen worden getroffen met het oog op een gedegen bewaring van die gegevens.

Recent heeft men, naar aanleiding van het échelonnetwerk kunnen vaststellen dat het mogelijk is om via een informaticanetwerk informatie te verzamelen waar men geen toegang toe heeft. Bij de bewaring dient dus te worden gegarandeerd dat de toegang voor onbevoegde derden onmogelijk is.

*
* *

Amendement *nr 9* van de heer Verherstraeten wordt eenparig aangenomen.

De amendementen *nrs 12* (van de heer Poncelet), *3* (van de regering) en *16* (van de heer Poncelet) worden bijgevolg zonder voorwerp.

Art. 10 (*nieuw*)

*De heer Fred Erdman (SP)* licht zijn amendement *nr 4* toe dat artikel 380*quinquies* van het Strafwetboek (strafbaarstelling van reclame voor diensten van seksuele aard waar minderjarigen bij betrokken zijn) aanvult in de zin dat het aanbod via een informaticasysteem

ver au cas d'une instuction, lorsque c'est nécessaire. » (DOC 50 0214/003).

*Le ministre* déclare préférer le délai de douze mois proposé par M. Servais Verherstraeten à celui de trois mois proposé par M. Jean-Pol Poncelet. Il renvoie à l'audition de membres de la police judiciaire et de la gendarmerie (voir annexe II).

*M. Hugo Coveliers (VLD)* estime qu'un délai intermédiaire de six mois serait préférable. Imposer un délai de conservation de douze mois pour des données qui ne sont plus utilisées lui semble exagéré.

Pour *M. Bert Schoofs (Vlaams Blok),* il n'est pas aussi important de s'attacher à la longueur du délai qu'à la manière de conserver les données. L'essentiel est de savoir où celles-ci sont conservées, qui y a accès, de quelles mesures de protection elles jouissent.

*M. Vanhoutte (Agalev-Ecolo)* pense qu'un délai de six mois constituerait le minimum acceptable. Mais en toute hypothèse, il faut être clair quant à ce que l'on veut protéger. Il faut aussi prendre les mesures nécessaires à la bonne conservation de ces données.

On a pu constater récemment, à l'occasion de la découverte du réseau Échelon, qu'il était possible, au moyen d'un réseau informatique, de collecter des informations auxquelles on n'a pas légalement accès. Il faut dès lors garantir, dans le cadre de la conservation des données, que celles-ci ne seront pas accessibles à des tiers non qualifiés.

*
* *

L'amendement *n° 9* de M. Verherstraeten est adopté à l'unanimité.

Les amendements *nos 12* de M. Poncelet, *3* du gouvernement et *16* de M. Poncelet deviennent dès lors sans objet.

Art. 10 (*nouveau*)

*M. Fred Erdman (SP)* précise la portée de son amendement *n° 4* tendant à compléter l'article 380*quinquies* du Code pénal (incrimination de la publicité pour des services de nature sexuelle impliquant des mineurs) de manière à incriminer également

eveneens strafbaar wordt gesteld. Het amendement luidt als volgt :

« Een artikel 10 (*nieuw*) invoegen, luidend als volgt :

*« Art. 10. — In artikel 380*quinqies *van het Strafwetboek worden de volgende wijzigingen aangebracht :*

*a) in § 1, eerste lid, tussen de woorden « op enigerlei wijze, direct of indirect » en de woorden « reclame maakt » worden de woorden « of door opgeslagen gegevens in een informaticasysteem » ingevoegd;*

*b) in § 2 , tussen de woorden « op enigerlei wijze, direct of indirect » en de woorden « reclame maakt », worden de woorden « of door opgeslagen gegevens in een informaticasysteem » ingevoegd;*

*c) in § 3, eerste lid, tussen de woorden « door enig reclamemiddel » en de woorden « zelfs indien », worden de woorden « of door opgeslagen gegevens in een informaticasysteem » ingevoegd;*

*d) in § 3, tweede lid, tussen de woorden « door enig reclamemiddel » en het woord « aanzet », de woorden « of door opgeslagen gegevens in een informaticasysteem » invoegen. ».*

VERANTWOORDING

Men moet rekening houden met het feit dat bepaalde gegevens in een informaticasysteem strijdig kunnen zijn met de openbare zeden, of de objectieven bedoeld in artikel 380*quinqies* nastreven. Het is, rekening houdend met de doelstelling van het wetsontwerp DOC 50 0214/001, essentieel dat specifiek hiervoor een aanpassing van artikel 380*quinquies* van het Strafwetboek wordt doorgevoerd. » (DOC 50 0214/003).

*De medewerker van de minister* vindt dit amendement overbodig : op grond van de thans in artikel 380*quinquies* van het Strafwetboek gehanteerde formulering doet het niet terzake welke drager wordt gebruikt. Door in deze bepaling een expliciete verwijzing naar de informaticadrager op te nemen, loopt men het risico op een tegenovergestelde lezing wanneer het om andere misdrijven gaat, bijvoorbeeld om racistische propaganda. Een en ander zou er immers op neerkomen dat, zonder expliciete verwijzing in de tekst, informaticadragers niet in aanmerking komen. Het uitgangspunt moet daarentegen zijn dat alles wat in het algemeen strafbaar is, ook strafbaar moet zijn in het kader van de informaticanetwerken.

*Mevrouw Jacqueline Herzet (PRL FDF MCC)* vraagt hoe kan worden achterhaald wie verantwoordelijk is voor misdrijven in netwerken van het type Internet.

*De medewerker van de minister* geeft toe dat de concrete tenuitvoerlegging van de wet niet van een leien dakje zal lopen. In theorie is het mogelijk de strafbare feiten te omschrijven, maar in een wereldomvattend netwerk is het bijzonder moeilijk dergelijke feiten te identificeren en de daders ervan te vervolgen. Dat zal de

l'offre de ces services au moyen d'un système informatique. L'amendement est libellé comme suit :

« Insérer un article 10 (*nouveau*), libellé comme suit :

*« Art. 10. — À l'article 380*quinquies *du Code pénal sont apportées les modifications suivantes :*

*a) dans le § 1er, alinéa 1er, les mots « ou par des données stockées dans un sytème informatique » sont insérés entre les mots « de façon directe ou indirecte » et les mots « , même en en dissimulant »;*

*b) dans le § 2, les mots « ou par des données stockées dans un système informatique » sont insérés entre les mots « de façon directe ou indirecte » et les mots « même en en dissimulant »;*

*c) dans le § 3, alinéa 1er, les mots « ou par des données stockées dans un système informatique, » sont insérés entre les mots « par un moyen quelconque de publicité » et les mots « même en dissimulant »;*

*d) dans le § 3, alinéa 2, les mots « ou par des données stockées dans un sytème informatique » sont insérés entre les mots « par un moyen quelconque de publicité » et le mot « , incitera ». ».*

JUSTIFICATION

Il faut tenir compte du fait que certaines données stockées dans un sytème informatique peuvent être contraires aux bonnes moeurs ou peuvent poursuivre les objectifs visés à l'article 380*quinquies*. Eu égard à l'objet du projet de loi DOC 50 0214/001, il est essentiel d'adapter l'article 380*quinquies* du Code pénal afin de prendre spécifiquement en compte ces possibilités. » (DOC 50 0214/003).

*Le collaborateur du ministre* estime cet amendement superflu : dans la rédaction actuelle de l'article 380*quinquies* du Code pénal, le type de support utilisé est irrelevant. En introduisant une référence explicite aux supports informatiques dans cette disposition, on court le risque de créer une interprétation *a contrario* pour d'autres délits, comme la propagande raciste par exemple. Elle consisterait à dire que si une référence explicite n'est pas inscrite dans le texte, les supports informatiques ne sont pas visés. Or, il faut partir du principe que tout ce qui est punissable en général, l'est aussi sur les réseaux informatiques.

*Mme Jacqueline Herzet (PRL FDF MCC)* demande comment déterminer le responsable des délits commis sur des réseaux du type Internet.

*Le collaborateur du ministre* concède que l'application concrète de la loi sera difficile. Il est possible de définir en théorie les faits punissables, mais dans un réseau mondial, il devient extrêmement difficile d'en identifier et d'en poursuivre les auteurs. Ce sera la

ten te identificeren en de daders ervan te vervolgen. De onderzoeksdiensten zullen hun technische middelen voldoende bij de tijd moeten houden, willen zij in staat zijn het nodige speurwerk te verrichten.

De bekommernis van *de heer Erdman* om het strafbaar karakter van inhoudsgerelateerde misdrijven veilig te stellen, ook wanneer hierbij informatica als middel wordt gehanteerd, wordt door de regering volledig onderschreven (zie overigens ook de memorie van toelichting, blz. 4-6). Het uitgangspunt van het wetsontwerp informaticacriminaliteit is immers dat enkel in de gevallen van vastgestelde lacunes of waar rechtsonzekerheid heerst, een wettelijke ingreep vereist is.

Uit het beleidsvoorbereidende werk is gebleken dat de misdrijven in ons strafrecht die verwijzen naar een strafbare inhoud (bijvoorbeeld aanzetten tot racisme, negationisme, kinderpornografie, aanzetten tot misdaden, bekendmaken van bepaalde geheimen, …) op een voldoende technologieneutrale wijze zijn omschreven in de strafwet, opdat ook hun « telematische » variant onder de delictomschrijving zou kunnen worden ondergebracht. Of kinderpornografie nu via een tijdschrift of via het internet wordt verspreid, is irrelevant omdat de strafwet niet limitatief geformuleerd is ten aanzien van de wijze waarop dit materiaal wordt verspreid. Dit is eveneens het geval voor artikel 380*quinquies* van het Strafwetboek.

Er is evenwel een reëel juridisch risico dat het expliciet toevoegen van één mogelijke wijze om het voormelde misdrijf te plegen, via een *a contrario*-redenering aanleiding geeft tot betwisting. Indien immers de wetgever in dit bepaalde geval van oordeel is dat de rechtszekerheid vereist dat specifiek wordt verwezen naar informaticagegevens, zou daaruit afgeleid kunnen worden dat deze *modus operandi* niet strafbaar is voor andere misdrijven, waar deze verwijzing naar informaticagegevens niet uitdrukkelijk voorkomt. Dit effect lijkt volledig in te gaan tegen de wens van *de heer Erdman*.

In het licht van het voorgaande wordt dan ook voorgesteld om dit amendement niet aan te houden, ten einde de doelstelling ervan, namelijk het garanderen van de strafbaarheid van traditionele inhoudsgerelateerde misdrijven, wanneer zij via informaticasystemen worden gepleegd, niet in gevaar te brengen. De ondubbelzinnige wil van de wetgever terzake zal afdoende blijken uit de voorbereidende werken.

*
* *

Amendement *nr 4* van de heer Fred Erdman wordt ingetrokken.

responsabilité des services de recherche de tenir les moyens techniques suffisamment à jour pour pouvoir effectuer ces poursuites.

Le gouvernement souscrit pleinement à la préoccupation de *M. Erdman* visant à préserver le caractère punissable des délits portant sur le contenu, également lorsque l'informatique est utilisée comme moyen (voir par ailleurs l'exposé des motifs, pp. 4 à 6). Le point de départ du projet de loi relatif à la criminalité informatique est en effet qu'une intervention du législateur ne s'impose que lorsque des lacunes ont été constatées ou qu'il règne une insécurité juridique.

Il est ressorti du travail préparatoire à l'élaboration de la politique à suivre que la loi pénale donne des délits, renvoyant à un contenu punissable, prévus dans notre droit pénal (par exemple, l'incitation au racisme, le négationnisme, la pornographie enfantine, l'incitation aux crimes, la divulgation de certains secrets, …) une description suffisamment neutre sous l'angle de la technologie pour que leur variante « télématique » puisse également être couverte par cette description. Il importe peu que la pornographie enfantine soit diffusée par un magazine ou sur internet, étant donné que la loi pénale n'est pas limitative quant aux modes de diffusion des documents. Tel est également le cas de l'article 380*quinquies* du Code pénal.

Sur le plan juridique, il y a cependant tout lieu de craindre que l'ajout explicite d'un seul mode possible de commission du délit précité ne donne lieu à contestation sur la base d'un raisonnement *a contrario*. Si le législateur estime en effet que, dans ce cas précis, la sécurité juridique demande que l'on renvoie spécifiquement aux données informatiques, on pourrait en déduire que ce *modus operandi* n'est pas punissable pour d'autres délits dans lesquels il n'est pas renvoyé explicitement aux données informatiques. Cet effet paraît à l'opposé du souhait de *M. Erdman.*

À la lumière de ce qui précède, il est donc proposé de ne pas retenir cet amendement, afin de ne pas compromettre l'objectif poursuivi, à savoir préserver la possibilité d'incriminer les délits traditionnels axés sur le contenu lorsqu'ils sont commis à l'aide de systèmes informatiques. La volonté explicite du législateur ressortira suffisamment des travaux préparatoires.

*
* *

L'amendement *n° 4* de M. Fred Erdman est retiré.

C. KWALIFICERING

*De heer Fred Erdman (SP)*, voorzitter, stelt de kwalificering van sommige artikelen uit het ontwerp II (DOC 50 0214/001) ter discussie. De artikelen 8 en 9 die werden opgenomen in het als verplicht bicameraal gekwalificeerde ontwerp dienen als optioneel bicameraal te worden beschouwd en moeten bijgevolg uit dat ontwerp worden gelicht en in het voorliggende ontwerp worden opgenomen.

Hij stelt vast dat de Raad van State in zijn advies wel consequent is met reeds voorheen ingenomen standpunten, maar hij merkt op dat die zienswijze achterhaald is door het compromis dat terzake in de overlegcommissie tussen Kamer en Senaat werd bereikt.

De voorzitter legt aan de commissie het advies voor dat hij aan de juridische dienst van de Kamer hieromtrent heeft gevraagd (zie bijlage I).

Na kennis te hebben genomen van dit advies, stelt de voorzitter voor dat de commissie het standpunt zou innemen dat reeds ten tijde van de bespreking van de wet van 12 maart 1998 tot verbetering van de strafrechtspleging in het stadium van het opsporingsonderzoek en het gerechtelijk onderzoek (wet Franchimont) werd ingenomen en dat inhoudt dat beperkte wijzigingen in de bevoegdheid van de procureur of de onderzoeksrechter als optioneel bicameraal dienen te worden behandeld.

De minister antwoordt dat hij het ontwerp zal laten aanpassen conform het besluit van de nota van de juridische dienst waarin wordt voorgesteld om de artikelen 3, 4 en 7 gedeeltelijk naar het andere ontwerp over te hevelen.

De minister meent dat het beter zou zijn om de artikelen niet te splitsen om redenen van praktische en legistieke aard.

*De heer Geert Bourgeois (VU-ID)* stelt vast dat er een compromis was bereikt tijdens de vorige legislatuur dat afwijkt van datgene wat de grondwetgever oorspronkelijk had gewild met name dat de Senaat alleen bevoegd zou zijn voor institutionele aangelegenheden. Alles wat rechterlijke organisatie betreft, zou nog bicameraal zijn. Bevoegdheid en rechtspleging zouden optioneel bicameraal dienen te worden behandeld.

Het compromis dat werd bereikt, bestond erin dat ook structurele bevoegdheidswijzigingen volgens de volledig bicamerale procedure dienden te worden behandeld.

Ten gronde is de heer Bourgeois het niet met deze zienswijze eens, maar hij aanvaardt ze om pragmatische redenen.

*De heer Tony Van Parys (CVP)* deelt dit standpunt.

*De voorzitter* verwijst ten slotte nog naar het document nr 83/3-1995 van de Kamer dat verschenen is op 1 februari 1999 en dat een analyse geeft van de hoger

C. QUALIFICATION

*M. Fred Erdman (SP)*, président, met en question la qualification de certains articles du projet de loi II (DOC 50 0214/001). Les articles 8 et 9, repris dans le projet qualifié d'obligatoirement bicaméral doivent être considérés comme relevant de la procédure optionnellement bicamérale et doivent dès lors être soustraits de ce projet pour être insérés dans le projet à l'examen.

Il constate que, dans son avis, le Conseil d'État respecte certes la logique des points de vue adoptés précédemment, mais que cette vision n'est plus de mise entretemps en raison du compromis intervenu au sein de la commission de concertation entre la Chambre et le Sénat.

Le président soumet à la commission l'avis qu'il a demandé à ce sujet au service juridique de la Chambre (voir annexe I).

Après avoir pris connaissance de cet avis, le président propose que la commission s'en tienne au point de vue qu'elle a déjà adopté lors de l'examen de la loi du 12 mars 1998 relative à l'amélioration de la procédure pénale au stade de l'information et de l'instruction (loi Franchimont), point de vue selon lequel les modifications restreintes apportées à la compétence du procureur ou du juge d'instruction doivent être traitées selon la procédure optionnellement bicamérale.

Le ministre répond qu'il fera adapter le projet en fonction de la conclusion de la note du service juridique, qui propose de transférer partiellement les articles 3, 4 et 7 dans l'autre projet.

Le ministre estime que, pour des raisons d'ordre pratique et légistique, il serait préférable de ne pas scinder les articles.

*M. Geert Bourgeois (VU-ID)* constate qu'au cours de la législature précédente, on était parvenu à un compromis qui déroge à la volonté initiale du législateur, à savoir que le Sénat serait seul compétent pour les matières institutionnelles. Tout ce qui concerne l'organisation judiciaire resterait bicaméral, tandis que les dispositions ayant trait aux compétences et à la procédure devraient être traitées selon la procédure optionnellement bicamérale.

Le compromis auquel on était parvenu prévoyait de traiter aussi les modifications structurelles de compétences selon la procédure entièrement bicamérale.

S'il ne partage cet avis sur le fond, M. Bourgeois s'y rallie toutefois pour des raisons pragmatiques.

*M. Tony Van Parys (CVP)* partage cet avis.

Enfin, *le président* renvoie au document n° 83/3-1995 de la Chambre, qui a été publié le 1er février 1999 et qui contient une analyse de la loi Franchimont précitée. Il

vermelde wet Franchimont. Hij verwijst naar blz. 16 van dit document waarin het volgende standpunt wordt ingenomen :

*« Het voeren van het opsporings- en het gerechtelijk onderzoek maakt de essentiële opdracht uit van respectievelijk de procureur des Konings en de onderzoeksrechter. Door een wettelijke regeling dienaangaande in het leven te roepen, regelt het wetsontwerp met andere woorden de (meest wezenlijke) bevoegdheid van de procureur des Konings en de onderzoeksrechter. Van een « incidentele bevoegdheidswijziging » is er bijgevolg geen sprake, aangezien het de bevoegdheid zelf is die het voorwerp van de regeling uitmaakt. ».*

De voorzitter wenst van de minister te vernemen of hij het nodig vindt om ook artikel 2, dat de bevoegdheden van de onderzoeksrechter en van de procureur des Konings betreft uit het volledig bicamerale ontwerp te halen.

De minister antwoordt dat artikel 2 niet wordt vermeld in de nota van de juridische dienst en dat men zich dus zal beperken tot de artikelen 3, 4 en 7 van het tweede ontwerp.

*
* *

De commissie heeft op 29 februari 2000, bij brief aan de kamervoorzitter, gevraagd dat de overlegcommissie zich terzake zou uitspreken.

De overlegcommissie heeft het volgende beslist :

*Beslissing van 16 maart 2000* : het wetsontwerp inzake informaticacriminaliteit, DOC 50 0214/001-006, zoals geamendeerd door de commissie voor de Justitie van de Kamer van volksvertegenwoordigers, dient te worden behandeld overeenkomstig de procedure bepaald in de artikelen 78 en 79 van de Grondwet (DOC 50 0082/007 (Kamer); 2-82/7 (Senaat)).

De commissie heeft tijdens de vergadering van 21 maart 2000 kennis genomen van deze beslissing en heeft ermee ingestemd. De artikelen 2 tot 9 van het wetsontwerp nr 214 worden bijgevolg ingevoegd in het wetsontwerp nr 213.

De commissie heeft tijdens die vergadering eveneens ingestemd met de wetgevingstechnische verbeteringen aan de geamendeerde wetsontwerpen, die door de dienten werden voorgesteld.

Het gehele wetsontwerp wordt eenparig aangenomen. Bijgevolg wordt het ontwerp nr 214 zonder voorwerp.

*De rapporteur,* *De voorzitter,*

Servais VERHERSTRAETEN Fred ERDMAN

renvoie à la page 16 dudit document, où est explicité le point de vue ci-après :

*« Le procureur du Roi et le juge d'instruction sont chargés essentiellement de procéder à l'information et à l'instruction. En réglant cette matière, la loi en projet règle aussi la compétence (la plus essentielle) du procureur du Roi et du juge d'instruction. Il n'est dès lors question d'aucune « modification occasionnelle de la compétence », puisque c'est la compétence elle-même qui fait l'objet de la réglementation. ».*

Le président demande au ministre s'il estime nécessaire de disjoindre l'article 2, qui concerne les pouvoirs du juge d'instruction et du procureur du Roi, du projet de loi, qui relève intégralement de la procédure bicamérale.

Le ministre répond qu'il n'est pas question de l'article 2 dans la note du service juridique et que l'on se limitera dès lors aux articles 3, 4 et 7 du second projet.

*
* *

Le 29 février 2000, la commission a demandé, par lettre adressée au président de la Chamre, que la commission de concertation se prononce en la matière.

La commission de concertation a décidé ce qui suit :

*Décision du 16 mars 2000* : le projet de loi relatif à la criminalité informatique, DOC 50 0214/001-006, tel qu'amendé par la commission de la Justice de la Chambre des représentants, doit être examiné selon la procédure prévue aux articles 78 et 79 de la Constitution (DOC 50 0082/007 (Chambre); 2-82/7 (Sénat)).

La commission a pris connaissance de cette décision au cours de la réunion du 21 mars 2000 et a marqué son accord sur celle-ci. Les articles 2 à 9 du projet de loi n° 214 sont dès lors insérés dans le projet de loi n° 213.

Au cours de la même réunion, la commission a également marqué son accord sur les corrections d'ordre légistique que les services ont proposé d'apporter aux projets de loi amendés.

L'ensemble du projet de loi est adopté à l'unanimité. Le projet n° 214 devient dès lors sans objet.

*Le rapporteur,* *Le président,*

Servais VERHERSTRAETEN Fred ERDMAN

*Lijst van de bepalingen die uitvoeringsmaatregelen vergen (toepassing Rgt. artikel 18, 4. a), tweede lid) :*

Verordeningen en besluiten te nemen met toepassing van artikel 108 van de Grondwet :

Art. 13

— artikel 90*septies* van het Wetboek van strafvordering

Art. 14

— artikel 109*ter* E van de wet van 21 maart 1991

*Liste des dispositions qui nécessitent des mesures d'exécution (application de l'article 18, 4. a), alinéa 2 du Règlement :*

Règlements et arrêtés à prendre en application de l'article 108 de la Constitution :

Art. 13

— article 90*septies* du Code d'instruction criminelle

Art. 14

— article 109*ter* E de la loi du 21 mars 1991

BIJLAGE I

NOTA VAN DE JURIDISCHE DIENST TER ATTENTIE VAN DE HEER ERDMAN, VOORZITTER VAN DE COMMISSIE VOOR DE JUSTITIE

**Betreft : Uw verzoek om ter attentie van de commissie voor de Justitie een nota te redigeren over de kwalificering van de wetsontwerpen inzake informatiecriminaliteit (DOC 50 0213/001 en 0214/001)**

1. Het voorontwerp dat door de regering aan de Raad van State werd voorgelegd, was volledig als optioneel bicameraal (artikel 78 van de Grondwet) gekwalificeerd.

De Raad van State stelde in zijn advies dat « verschillende bepalingen van het ontwerp (…) betrekking (hebben) op de bevoegdheden van de procureur des Konings en op die van de onderzoeksrechter. Dat geldt inzonderheid voor de artikelen 5 tot 10 van het ontwerp ([1]) ». Artikel 1 van het ontwerp diende volgens de Raad bijgevolg te worden gewijzigd.

De Raad van State verantwoordt zijn standpunt door te verwijzen naar twee vorige adviezen. *We zullen hieronder zien dat die weliswaar het standpunt van de Raad van State vertegenwoordigen, maar niet dat van de overlegcommissie, die als enige bevoegd is voor het regelen van bevoegdheidsconflicten.*

De regering heeft het advies van de Raad van State volledig gevolgd. Ze heeft haar ontwerp gesplitst in twee ontwerpen : het ene verplicht bicameraal (artikel 77 van de Grondwet), het andere optioneel bicameraal (artikel 78 van de Grondwet)

In het verplicht bicamerale ontwerp heeft de regering alle artikelen ondergebracht die volgens de Raad van State verplicht bicameraal zijn. De artikelen 5 tot 10 van het voorontwerp zijn aldus de artikelen 2 tot 7 van het « ontwerp 77 » geworden.

De regering is echter verder gegaan dan de Raad van State vroeg. Zo brengt ze *zonder enige motivering* ook de artikelen 11 en 12 van het voorontwerp onder in het verplicht bicamerale ontwerp (als artikelen 8 en 9). Nochtans had de Raad van State geen enkel bezwaar geuit tegen de oorspronkelijke — optioneel bicamerale — kwalificering van die artikelen.

Het gaat hier manifest om een foute kwalificering, zoals we hieronder nog zullen zien.

([1]) DOC 50 0213/001, blz. 56.

ANNEXE I

NOTE DU SERVICE JURIDIQUE À L'ATTENTION DE M. ERDMAN, PRÉSIDENT DE LA COMMISSION DE LA JUSTICE

**Objet : Votre demande de rédiger à l'attention de la commission de la Justice une note relative à la qualification des projets de loi relatifs à la criminalité informatique (DOC 50 0213/001 et 0214/001)**

1. L'avant-projet de loi que le gouvernement a soumis pour avis au Conseil d'État avait été entièrement qualifié d'optionnellement bicaméral (article 78 de la Constitution).

Dans son avis, le Conseil d'État a estimé que « plusieurs dispositions du projet (...) concernent les compétences du procureur du Roi ainsi que celles du juge d'instruction. Il en va notamment ainsi des articles 5 à 10 du projet ([1]) ». Le Conseil d'État a estimé que l'article 1er devait par conséquent être modifié.

Le Conseil d'État justifie son point de vue en renvoyant à deux avis antérieurs. *Nous verrons ci-après que si ceux-ci reflètent, certes, le point de vue du Conseil d'État, ils ne reflètent aucunement celui de la commission de concertation, qui est seule compétente pour régler les conflits de compétence.*

Le gouvernement a suivi entièrement l'avis du Conseil d'État. Il a scindé son projet en deux projets : l'un obligatoirement bicaméral (article 77 de la Constitution) et l'autre optionnellement bicaméral (article 78 de la Constitution).

Le gouvernement a regroupé dans le projet obligatoirement bicaméral tous les articles considérés comme tels par le Conseil d'État. Les articles 5 à 10 de l'avant-projet sont ainsi devenus les articles 2 à 7 du « projet 77 ».

Le gouvernement a toutefois été au-delà des voeux du Conseil d'État. C'est ainsi qu'il a également inséré, *sans aucune motivation,* les articles 11 et 12 de l'avant-projet dans le projet obligatoirement bicaméral (dont ils deviennent les articles 8 et 9), alors que le Conseil d'État n'avait formulé aucune objection contre la qualification initiale — optionnellement bicamérale — de ces articles.

Il s'agit manifestement, en l'espèce, d'une qualification erronée, comme on le verra encore ci-après.

([1]) DOC 50 0213/001, p. 56.

2. Wil men dit probleem van kwalificering begrijpen, dan moet men zich herinneren wat de basisprincipes zijn van de bevoegdheidsverdeling tussen Kamer en Senaat sinds de hervorming van de wetgevingsprocedure.

2.1. Artikel 77, eerste lid, 9), van de Grondwet bepaalt dat « de organisatie van de hoven en rechtbanken » onder de verplicht bicamerale procedure ressorteert.

Over de interpretatie van dat artikel is de afgelopen vijf jaar al behoorlijk getwist. We vatten de standpunten hieronder samen.

2.1.1. Het eerste en oorspronkelijke standpunt is dat van de *Grondwetgever*, die een formeel criterium naar voren heeft geschoven : enkel de bepalingen van het tweede deel (« Rechterlijke organisatie ») van het Gerechtelijk Wetboek, evenals de bepalingen van het eerste deel (« Algemene beginselen ») waaraan het tweede deel concrete invulling geeft, vallen onder de verplicht bicamerale procedure ([2]).

Dat formele criterium was op zich al een compromis : de institutionele voorschriften inzake de rechterlijke macht zouden aldus verplicht bicameraal worden, « zonder dat evenwel de materiële en territoriale bevoegdheidsomschrijving van de gewone hoven en rechtbanken volledig bicameraal zou worden, laat staan de procedure die voor de gewone hoven en rechtbanken moet worden gevolgd ([3]) ».

Dit formele standpunt werd steeds verdedigd door de Kamer van volksvertegenwoordigers, omdat het zowel met de tekst als met de geest van de Grondwet overeenstemt ([4]).

2.1.2. Het tweede standpunt is dat van *de Raad van State*, die in zijn beginseladvies van 10 oktober 1995 artikel 77, eerste lid, 9), van de Grondwet combineert met twee bepalingen die voorkomen in artikel 77, eerste lid, 3), van de Grondwet, met name de artikelen 145 en 146 van de Grondwet. Uit die combinatie leidt de Raad van State af dat de organisatie *en de bevoegdheden* van alle rechtscolleges, met inbegrip van de gewone hoven en rechtbanken, verplicht bicameraal zijn.

Het is niet onze bedoeling hier opnieuw in de polemiek te gaan over de juistheid van die interpretatie. In

([2]) Verslag Erdman, Stuk Senaat nr 100-19/2-1991/1992, blz. 8, 18 en 28.

([3]) VAN NIEUWENHOVE, J., Naschrift : « De eerste ervaringen met de nieuwe wetgevende procedure », in LEUS, K; en VENY, L., Het federale België in de praktijk, 1996, Brugge, Die Keure, 139.

([4]) Merk op dat volgens dit formele criterium, de onderzochte bepalingen onbetwist optioneel bicameraal zijn, aangezien ze het Wetboek van strafvordering wijzigen en niet het Gerechtelijk Wetboek.

2. Pour comprendre ce problème de qualification, il faut se remémorer les principes de base qui régissent la répartition des compétences entre la Chambre et le Sénat depuis la réforme de la procédure législative.

2.1. L'article 77, alinéa 1er, 9), de la Constitution dispose que « l'organisation des cours et tribunaux » relève de la procédure obligatoirement bicamérale.

Au cours des cinq dernières années, l'interprétation de cet article a déjà souvent nourri la polémique. Nous résumons ci-après les avis en présence.

2.1.1. Le premier point de vue, qui est en même temps le point de vue initial, est *celui du Constituant*, qui a fait valoir un critère formel: seules les dispositions de la deuxième partie (« L'organisation judiciaire ») du Code judiciaire, ainsi que les dispositions de la première partie (« Principes généraux ») qui sont concrétisées par la deuxième partie, relèvent de la procédure obligatoirement bicamérale ([2]).

Ce critère formel était déjà, en soi, le résultat d'un compromis : les prescriptions institutionnelles concernant le pouvoir judiciaire deviendraient ainsi obligatoirement bicamérales, « sans que toutefois la définition des compétences matérielles et territoriales des cours et tribunaux ordinaires devienne entièrement bicamérale, ni *a fortiori* la procédure qui doit être suivie devant les cours et tribunaux ordinaires ([3]) ».

La Chambre des représentants a toujours défendu ce point de vue, parce qu'il correspond tant à l'esprit qu'à la lettre de la Constitution ([4]).

2.1.2. Le deuxième point de vue est celui du *Conseil d'État*, qui, dans son avis de principe du 10 octobre 1995, combine l'article 77, alinéa 1er, 9), de la Constitution avec deux dispositions visées à l'article 77, alinéa 1er, 3), de la Constitution, à savoir les articles 145 et 146 de la Constitution. Le Conseil d'État infère de cette combinaison que l'organisation *et les compétences* de toutes les juridictions, y compris celles des cours et tribunaux ordinaires, sont obligatoirement bicamérales.

Notre propos n'est pas de relancer la polémique sur le bien-fondé de cette interprétation. La doctrine a en

([2]) Rapport Erdman, DOC Sénat no 100-19/2-1991/1992, pp. 8, 18 et 28.

([3]) VAN NIEUWENHOVE, J., *Naschrift : De eerste ervaringen met de nieuwe wetgevende procedure*, dans LEUS, K. et VENY, L., *Het federale België in de praktijk*, 1996, Bruges, *Die Keure*, 139.

([4]) Il convient d'observer que sur la base de ce critère formel, les dispositions examinées sont indiscutablement optionnellement bicamérales, étant donné qu'elles modifient le Code d'instruction criminelle et non le Code judiciaire.

de rechtsleer is immers al op overtuigende wijze aangetoond dat de Raad van State systematisch alle elementen van de parlementaire voorbereiding die in een andere richting wezen, naast zich neer heeft gelegd ([5]).

De Senaat heeft zich in het verleden altijd aangesloten bij de extensieve interpretatie van de Raad van State, omdat hij aldus zijn bevoegdheden uitgebreid ziet. Bovendien moet worden toegegeven dat het zuiver formele criterium dat de Grondwetgever destijds voor ogen had, niet altijd tot een logisch resultaat leidt.

2.1.3. Een en ander heeft in de parlementaire overlegcommissie tot urenlange discussies geleid. Het is naar aanleiding van die discussies dat *de regering* een compromisvoorstel heeft geformuleerd dat het midden houdt tussen voornoemd principsadvies van de Raad van State (+ de Senaat) enerzijds en de restrictieve opvatting van de Grondwetgever (+ de Kamer) anderzijds. In een poging om beide standpunten te verzoenen stelde de regering voor dat *enkel structurele wijzigingen inzake de bevoegdheid* onder het begrip « rechterlijke organisatie » zouden vallen ([6]). Incidentele bevoegdheidswijzigingen zouden niet onder dat begrip vallen ([7]).

2.1.4. Uit die discussies is uiteindelijk een (niet geformaliseerde) synthese voortgesproten, in de vorm van een consensus binnen de overlegcommissie, die als volgt kan worden samengevat :

1. samenstelling en organisatie van de hoven en rechtbanken : artikel 77 van de Grondwet.

2. bevoegdheid :

— volgens de Raad van State en de Senaat : artikel 77 van de Grondwet;

— volgens de Kamer : artikel 78 van de Grondwet;

— compromis, voorgesteld door de regering, en aanvaard door de overlegcommissie;

— structurele wijzigingen van de bevoegdheid : artikel 77 van de Grondwet;

— andere bevoegdheidsbepalingen : artikel 78 van de Grondwet.

3. rechtspleging : artikel 78 van de Grondwet.

([5]) DEFOORT, P.J., « Over de interpretatie van artikel 77, 9), van de gecoördineerde Grondwet », TBP, 1996, 127-131; VAN NIEUWENHOVE, J., l.c., 140.

([6]) Als voorbeelden gaf de regering de oprichting van een verkeersrechtbank of de concentratie van alle huurgeschillen bij één (eventueel bestaande) rechtbank (Zie Stuk nr 83/1-1995, blz. 24).

([7]) Dit zou bijvoorbeeld het geval kunnen zijn indien een wetgevend initiatief zijdelings een weerslag heeft op de bevoegdheden van de rechtbank van eerste aanleg (*Ibid.*).

effet déjà démontré de manière convaincante que le Conseil d'État a systématiquement ignoré tous les éléments des travaux parlementaires préparatoires qui allaient dans un sens différent ([5]).

Le Sénat s'est toujours rallié, par le passé, à l'interprétation extensive adoptée par le Conseil d'État, car il voit ainsi ses compétences élargies. Qui plus est, il faut admettre que l'application du critère purement formel voulu, à l'époque, par le Constituant ne donne pas toujours un résultat logique.

2.1.3. Toutes ces questions ont donné lieu à de longues discussions au sein de la commission parlementaire de concertation. C'est à la suite de ces discussions que *le gouvernement* a formulé une proposition de compromis qui se situe en effet à mi-chemin entre l'avis de principe précité du Conseil d'État (+ Sénat), d'une part, et la conception restrictive du Constituant (+ Chambre), d'autre part. Dans une tentative de concilier les deux points de vue, le gouvernement a proposé de ne faire relever de la notion d'« organisation judiciaire » que *les modifications structurelles en matière de compétences* ([6]). Les modifications accessoires de compétences ne relèveraient pas de cette notion ([7]).

2.1.4. Les discussions ont finalement débouché sur une synthèse (non formalisée), sous la forme d'un consensus dégagé au sein de la commission de concertation et qui peut se résumer comme suit :

1. composition et organisation des cours et tribunaux : article 77 de la Constitution.

2. compétence :

— selon le Conseil d'État et le Sénat : article 77 de la Constitution;

— selon la Chambre : article 78 de la Constitution;

— compromis, proposé par le gouvernement, et accepté par la commission de concertation;

— modifications structurelles de la compétence : article 77 de la Constitution;

— autres dispositions relatives aux compétences : article 78 de la Constitution.

3. procédure : article 78 de la Constitution.

([5]) DEFOORT, P.J., « *Over de interpretatie van artikel 77, 9), van de gecoördineerde Grondwet* », TBP, 1996, 127-131; VAN NIEUWENHOVE, J., *l.c.*, 140.

([6]) Le gouvernement a cité comme exemples la création d'un tribunal compétent pour les litiges en matière de circulation routière ou la concentration de tous les litiges en matière de loyers auprès d'un tribunal (éventuellement existant) (Voir DOC no 83/1-1995, p. 24).

([7]) Tel pourrait par exemple être le cas si une initiative législative avait indirectement des répercussions sur les compétences du tribunal de première instance (*Ibid.*).

Dit compromis werd reeds bij diverse gelegenheden door de overlegcommissie toegepast ([8]).

3. Als we dit compromis toepassen op de voorliggende ontwerpen « inzake informaticacriminaliteit », komen we tot de volgende vaststellingen.

3.1. Artikel 2 van het « ontwerp 77 » heeft betrekking op de wijze waarop de procureurs des Konings handelen in de uitoefening van hun ambt. Het wordt dan ook terecht ingevoegd in afdeling II van Hoofdstuk IV van het Wetboek van strafvordering en niet in afdeling I (« Bevoegdheid van de procureurs des Konings betreffende de gerechtelijke politie »).

Deze bepaling kan dus geenszins worden beschouwd als een « structurele wijziging van de bevoegdheid van een hof of rechtbank ». Ten eerste omdat het niet om een bevoegdheidstoewijzing gaat, ten tweede omdat mocht het een bevoegdheidstoewijzing zijn — *quod non* —, deze zeker niet « structureel » te noemen is en ten derde omdat het allesbehalve evident is dat een bevoegdheid van een procureur des Konings zomaar kan worden gelijkgesteld met een bevoegdheid van een hof of een rechtbank (zie in dat verband onder meer het standpunt verdedigd door de Kamer en gevolgd door de parlementaire overlegcommissie met betrekking tot de bevoegdheden van de procureurs des Konings en de onderzoeksrechters in het kader van het bevoegdheidsconflict over het ontwerp-Franchimont) ([9]).

3.2. De artikelen 3, 4 en 7 van het « ontwerp 77 » hebben betrekking op de ambtsverrichtingen van de onderzoeksrechter.

Ze bevatten een mengeling van bepalingen. Sommige hebben helemaal niets te maken met de bevoegdheid van de onderzoeksrechter (bijvoorbeeld de §§ 3 tot 5 van het voorgestelde artikel 88*quater*, het derde en het vierde lid van de § 4 van het voorgestelde artikel 90*quater*…). Andere hebben louter te maken met zijn werkwijze (bijvoorbeeld § 3 van het voorgestelde artikel 88*ter* …). Sommige bepalingen betreffen echter wel degelijk

([8]) Zie bijvoorbeeld het wetsontwerp betreffende de teruggave van cultuurgoederen die op onrechtmatige wijze buiten het grondgebied van bepaalde buitenlandse Staten zijn gebracht (Stuk Kamer, nr 289/1-95/96 en stuk Senaat, nr 1-246/1-1995/1996). De overlegcommissie besloot eenparig dat de betwiste artikelen volgens de optioneel bicamerale procedure moesten worden behandeld, omdat ze « slechts partiële verschuivingen van de bevoegdheidsverdeling tussen de verschillende rechtbanken inhouden » (« Periodiek verslag », Stuk Kamer, nr 83/1-95 en stuk Senaat, nr 1-83/1-1995, 6). Zie ook Stuk Senaat, nr 1-589/1-1996/1997 en blz. 3 van de notulen van de vergadering van 30 juni 1996 van de parlementaire overlegcommissie.

([9]) Stuk Kamer nr 83/3-95 en stuk Senaat nr 1-83/3-1995, blz. 22-32; stuk Kamer nr 82/24-95.

Ce compromis a déjà été appliqué à plusieurs reprises par la commission de concertation ([8]).

3. Si nous appliquons ce compromis aux projets à l'examen « relatifs à la criminalité informatique », nous aboutissons aux constatations suivantes.

3.1. L'article 2 du « projet 77 » concerne la manière dont les procureurs du Roi agissent dans l'exercice de leur fonction. C'est par conséquent à juste titre qu'il est inséré dans la section II du Chapitre IV du Code d'instruction criminelle, et non dans la section Ire (« De la compétence des procureurs du Roi, relativement à la police judiciaire »).

Cette disposition ne peut donc en aucun cas être considérée comme « une modification structurelle de la compétence d'une cour ou d'un tribunal ». En premier lieu parce qu'il ne s'agit pas d'une attribution de compétence, en deuxième lieu parce que s'il s'agissait d'une attribution de compétence — *quod non* —, celle-ci ne pourrait être qualifiée de « structurelle » et, en troisième lieu, parce qu'il n'est pas du tout évident qu'une compétence d'un procureur du Roi puisse être assimilée purement et simplement à une compétence d'une cour ou d'un tribunal (voir, à ce propos, notamment le point de vue défendu par la Chambre et suivi par la commission parlementaire de concertation en ce qui concerne les compétences des procureurs du Roi et des juges d'instruction dans le cadre du conflit de compétence concernant le projet Franchimont) ([9]).

3.2. Les articles 3, 4 et 7 du « projet 77 » concernent les fonctions du juge d'instruction.

Ils contiennent des dispositions diverses. Certaines n'ont absolument rien à voir avec la compétence du juge d'instruction (par exemple, les §§ 3 à 5 de l'article 88*quater* proposé, les alinéas 3 et 4 du § 4 de l'article 90*quater* proposé...). D'autres concernent exclusivement sa manière de procéder (par exemple, le § 3 de l'article 88*ter* proposé). Certaines dispositions concernent cependant bel et bien ses compétences (par exem-

([8]) Voir par exemple le projet de loi relatif à la restitution de biens culturels ayant quitté illicitement le territoire de certains États étrangers (DOC Chambre, no 289/1-95/96 et DOC Sénat, no 1-246/1-1995/1996). La commission de concertation a décidé à l'unanimité que les articles incriminés devaient être examinés selon la procédure bicamérale optionnelle, car ils « n'impliquent en fait que des glissements partiels de compétences entre les différents tribunaux » (« Rapport périodique », DOC Chambre, no 83/1-95 et DOC Sénat, no 1-83/1-1995, 6). Voir également DOC Sénat, no 1-589/1-1996/1997 et p. 3 du procès-verbal de la réunion de la commission parlementaire de concertation du 30 juin 1996.

([9]) DOC Chambre no 83/3-95 et DOC Sénat no 1-83/3-1995, pp. 22-32; DOC Chambre, no 82/24-95.

zijn bevoegdheden (bijvoorbeeld § 1 van het voorgestelde artikel 88*ter*, §§ 1 en 2 van het voorgestelde artikel 88*quater*, het eerste en tweede lid van de § 4 van het voorgestelde artikel 90*quater* …).

Dat betekent echter nog niet dat die enkele bepalingen betreffende de bevoegdheid van de onderzoeksrechter onder de verplicht bicamerale procedure ressorteren.

Ten eerste omdat de Kamer in het verleden het standpunt heeft verdedigd dat de bevoegdheid van de onderzoeksrechter niet zomaar kan worden gelijkgesteld met die van een hof of rechtbank (cf. het standpunt verdedigd door de Kamer in het bevoegdheidsconflict met betrekking tot het ontwerp-Franchimont, dat is gevolgd door de parlementaire overlegcommissie ([10]).

Ten tweede omdat men — mocht men toch die gelijkstelling maken — bezwaarlijk kan beweren dat het hier gaat om een structurele wijziging in de zin van het hierboven vermelde compromis.

Binnen de logica die de Kamer tot nog toe verdedigd heeft, was het dus niet nodig deze artikelen als « verplicht bicameraal » te herkwalificeren .

3.3. De artikelen 5 en 6 van het « ontwerp 77 » zijn zuivere verwijzingsbepalingen. Zelfs al zouden die verwijzingen het gevolg zijn van de invoeging in het Wetboek van strafvordering van verplicht bicamerale bepalingen – *quod non* – dan nog is er geen enkele reden om ze enkel daarom volgens de verplicht bicamerale procedure te behandelen.

De tegengestelde redenering zou tot gevolg hebben dat iedere wetsbepaling waarin een verwijzing naar een verplicht bicamerale bepaling voorkomt, vanzelf ook verplicht bicameraal wordt, wat zeker niet de bedoeling was van de Grondwetgever, die meermaals heeft onderstreept dat de « materies van artikel 77 van de Grondwet » restrictief dienen te worden geïnterpreteerd.

4. Besluit :

4.1. De splitsing zoals ze door de regering is doorgevoerd is alleszins fout. Op zijn minst de artikelen 8 en 9 moeten uit het « ontwerp 77 » worden gelicht en naar het « ontwerp 78 » overgeheveld.

4.2. De kwalificering voorgesteld door de Raad van State is niet verrassend. De Raad van State blijft grosso modo perfect binnen de logica die hij enkele jaren terug heeft uitgestippeld, maar die haaks staat op de beslissingen van de overlegcommissie.

([10]) *Ibid.*

ple, le § 1er de l'article 88*ter* proposé, les §§ 1er et 2 de l'article 88*quater* proposé, les alinéas 1er et 2 du § 4 de l'article 90*quater* proposé).

Cela ne signifie cependant pas encore que ces quelques dispositions relatives à la compétence du juge d'instruction relèvent de la procédure obligatoirement bicamérale.

En premier lieu, parce que la Chambre a défendu par le passé le point de vue selon lequel la compétence du juge d'instruction ne peut être assimilée purement et simplement à celle d'une cour ou d'un tribunal (cf. le point de vue défendu par la Chambre concernant le projet Franchimont et suivi par la commission parlementaire de concertation) ([10]).

Deuxièmement parce que, même si la thèse de l'assimilation était malgré tout retenue, l'on pourrait difficilement prétendre qu'il s'agit en l'occurrence d'une modification structurelle au sens du compromis précité.

Selon la logique défendue jusqu'à ce jour par la Chambre, il n'était donc pas nécessaire de requalifier ces articles d'« obligatoirement bicaméraux ».

3.3. Les articles 5 et 6 du « projet 77 » sont de simples dispositions de renvoi. Même si ces renvois découlaient de l'insertion de dispositions obligatoirement bicamérales dans le Code d'instruction criminelle — *quod non* —, ce ne serait pas une raison suffisante pour les examiner selon la procédure bicamérale obligatoire.

Le raisonnement inverse aurait pour effet de rendre automatiquement obligatoirement bicamérale toute disposition législative comportant un renvoi à une disposition obligatoirement bicamérale, ce qui n'était assurément pas l'intention du constituant, qui a souligné à maintes reprises que les matières relevant de l'article 77 de la Constitution devaient s'interpréter de manière restrictive.

4. Conclusion :

4.1. La scission opérée par le gouvernement est en tout cas erronée. Les articles 8 et 9 doivent à tout le moins être disjoints du « projet 77 » et insérés dans le « projet 78 ».

4.2. La qualification proposée par le Conseil d'État n'est pas surprenante. Le Conseil d'État reste, en gros, parfaitement fidèle à la logique qu'il a définie il y a quelques années, mais qui est en contradiction avec les décisions de la commission de concertation.

([10]) *Ibid.*

De Raad van State is niet bevoegd om bevoegdheidsconflicten te regelen : dat kan alleen de parlementaire overlegcommissie. De commissie voor de Justitie zou deze zaak dus best aanhangig maken bij de overlegcommissie (en dit nog vooraleer de kwalificering te amenderen, cf. het *gentlemen's agreement* tussen Kamer en Senaat).

4.3. Wil de Kamer logisch blijven met zichzelf en met haar jurisprudentie, dan moet zij vragen dat alle artikelen overeenkomstig de optioneel bicamerale procedure worden behandeld. Dat betekent dat het ontwerp in zijn vroegere vorm wordt hersteld.

4.4. In ondergeschikte orde : als er in het kader van de regeling van het bevoegdheidsconflict door de parlementaire overlegcommissie, door de Kamer toegevingen zouden worden gedaan — de overlegcommissie is per slot van rekening een politiek orgaan en geen rechtbank … —, dan kunnen die hooguit betrekking hebben op *gedeelten* van de artikelen 3, 4 en 7.

Le Conseil d'État n'est pas habilité à régler des conflits de compétence, cette faculté étant réservée exclusivement à la commission parlementaire de concertation. La commission de la Justice ferait donc bien de saisir la commission de concertation de cette question (et ce, avant même de modifier la qualification, voir le *gentlemen's agreement* conclu entre la Chambre et le Sénat).

4.3. Si elle souhaite rester logique avec elle-même et fidèle à sa jurisprudence, la Chambre doit demander que *tous* les articles soient examinés selon la procédure optionnellement bicamérale, ce qui implique que le projet soit rétabli dans son ancienne version...

4.4. Subsidiairement, si, dans le cadre du règlement du conflit de compétence par la commission parlementaire de concertation, la Chambre devait faire des concessions — la commission de concertation est, après tout, un organe politique et non un tribunal —, celles-ci ne pourraient porter tout au plus que sur certaines *parties* des articles 3, 4 et 7.

BIJLAGE II

**Advies nr 33 / van 13 december 1999**

Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals gewijzigd door de wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens, inzonderheid op artikel 29;

Gelet op het verslag van de heren De Schutter en Poullet;

Brengt uit eigen beweging op 13 december 1999 het volgende advies uit :

1. **Voorgeschiedenis**

Op 30 november 1999 werd de voorzitter van de Commissie voor de bescherming van de persoonlijke levenssfeer uitgenodigd om zich uit te drukken op een hoorzitting in de Kamercommissie Justitie over twee, door de ministers van Justitie, van Telecommunicatie en Overheidsbedrijven en Participaties en van Economie gezamenlijk ingediende ontwerpen van wet inzake informaticacriminaliteit (DOC 50 0213/001 en 0214/001) (1). Voorliggend advies volgt op deze hoorzitting.

2. **Voorstelling van de wetsontwerpen**

De wetsontwerpen inzake informaticacriminaliteit beogen het strafbaar stellen van feiten die de vertrouwelijkheid, de integriteit en de beschikbaarheid aantasten van informaticasystemen of van gegevens die worden opgeslagen, verwerkt of overgedragen door middel van deze systemen (2).

Hiertoe wordt voorzien in het invoegen van een nieuwe titel in het Strafwetboek dat bepaalde wanbedrijven zoals de valsheid in informatica, de ongeoorloofde toegang tot een systeem of de data- en informaticasabotage strafbaar stelt.

Verder voorzien de wetsontwerpen in nieuwe opsporingstechnieken zoals databeslag, medewerkingsver-

(1) Hierna : nrs 213/1 en 214/1.

(2) Zie daaromtrent de werkzaamheden van de Raad van Europa (met name *La criminalité informatique*, voorwoord van August Bequai, Straatsburg, 1990) en van de Verenigde Naties.

ANNEXE II

**Avis n° 33 / du 13 décembre 1999**

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/EG du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, en particulier l'article 29;

Vu le rapport de MM. De Schutter et Poullet;

Émet d'initiative, le 13 décembre 1999, l'avis suivant :

1. **Antécédents**

Le 30 novembre 1999, le président de la Commission de la protection de la vie privée a été invité à s'exprimer devant la commission de la Justice du Parlement à propos de deux projets de loi relatifs à la criminalité informatique déposés conjointement par le ministre de la Justice, le ministre des Télécommunications et des Entreprises et Participations publiques et le ministre de l'Économie (DOC 50 0213/001 et 0214/001) (1). Le présent avis fait suite à cette audition.

2. **Présentation des projets de loi**

Les projets de loi relatifs à la criminalité informatique visent à ériger en infraction le fait de porter atteinte à la confidentialité, l'intégrité et la disponibilité des systèmes informatiques ou des données qui sont stockées, traitées ou transmises par le biais de ces systèmes (2).

À cet effet, il est prévu d'ajouter un nouveau titre au Code pénal incriminant certains délits comme le faux en informatique, l'accès non-autorisé à un système ou encore le sabotage de données informatisées.

Par ailleurs, les projets de loi prévoient de nouvelles techniques de dépistage comme la confiscation de don-

(1) Ci-après, n° 213/1 et n° 214/1.

(2) Voir à ce sujet les travaux du Conseil de l'Europe (notamment *La criminalité informatique*, préface d'August Bequai, Strasbourg, 1990) et des Nations Unies.

plichtingen, netwerkzoeking en interceptie van communicatie.

3. **Opmerkingen van de commissie**

A. *Algemene opmerkingen*

1. De commissie benadrukt dat de twee wetsontwerpen die in voorliggend advies worden besproken, een aanvulling zijn voor een reeks andere, reeds genomen bepalingen waarvoor haar advies werd gevraagd.

In het bijzonder vermelden we :

— de artikelen 202 en 203 van de wet van 21 december 1994, onder meer betreffende de technische medewerking van de operatoren met het oog op de uitvoering van gerechtelijke maatregelen van afluisteren (advies nr 17/97 van 9 juli 1997);

— het ontwerp van wet betreffende de toegang tot en het opsporen van nummers van communicatie- of telecommunicatiemiddelen en houdende wijziging van de artikelen 90*ter*, 90*quater*, 90*sexies*, en 90*septies* van het Wetboek van strafvordering (advies nr 09/97 van 20 maart 1997);

— de amendementen op de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie (advies nr 34/97 van 27 november 1997);

— het ontwerp van koninklijk besluit tot uitvoering van de bepalingen van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie en van artikel 109*ter* E, § 2 van de wet van 22 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (advies nr 12/99 van 24 maart 1999).

In deze context verwondert de commissie zich er over dat zij niet werd gevat betreffende de wetsontwerpen nrs 213/1 en 214/1 vóór de bespreking in het Parlement. De vorige adviezen die de commissie uitbracht, benadrukten immers het belang van sommige ontwerpbepalingen op het vlak van de persoonlijke levenssfeer ([3]).

De commissie wenst de aandacht van de wetgever te vestigen op het feit dat zowel sommige bepalingen van het wetsontwerp nr 213/1 als bijna alle bepalingen van het ontwerp nr 214/1 gevolgen kunnen hebben op het vlak van de bescherming van de persoonlijke le-

([3]) In het kader van de vernoemde adviezen inzake de teksten betreffende de interceptie van telecommunicatie en het afluisteren, heeft de commissie systematisch de wens uitgedrukt om hierover te worden geraadpleegd.

nées, l'obligation de coopération, la recherche de réseau et l'interception de communications.

3. **Observations de la commission**

A. *Observations générales*

1. La commission souligne que les deux projets de loi qui font l'objet du présent avis complètent une série d'autres dispositions déjà prises et pour lesquelles son avis avait été sollicité.

On citera en particulier :

— les articles 202 et 203 de la loi du 21 décembre 1994, relatifs entre autres à la collaboration technique des opérateurs à l'exécution de mesures judiciaires d'écoute (avis n° 17/97 du 9 juillet 1997);

— le projet de loi concernant l'identification et le repérage des numéros de postes de communication ou de télécommunication et portant modification des articles 90*ter*, 90*quater*, 90*sexties* et 90*septies* du Code d'instruction criminelle (avis n° 09/97 du 20 mars 1997);

— les amendements de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et télécommunications privées (avis n° 34/97 du 27 novembre 1997);

— le projet d'arrêté royal portant exécution des dispositions de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance, l'enregistrement de communications et télécommunications privées et l'article 109*ter*, E, § 2 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (avis n° 12/99 du 24 mars 1999).

Dans ce contexte, la commission s'étonne de ne pas avoir été saisie des projets de loi n° 213/1 et n° 214/1 à un stade antérieur à la discussion au Parlement. Les précédents avis émis par la commission soulignaient en effet l'importance des enjeux en termes de protection de la vie privée de certaines dispositions en projet ([3]).

La commission souhaite attirer l'attention du législateur sur le fait que tant certaines dispositions du projet de loi n° 213/1 que la quasi-totalité de celles du projet n° 214/1 peuvent avoir des implications en matière de protection de la vie privée. En effet, nombre de disposi-

([3]) Dans le cadre des avis cités sur les textes visant l'interception des télécommunications et des écoutes, la commission a systématiquement émis le désir d'être consultée.

venssfeer. Menige ontwerpbepalingen (zoeking en databeslag, opsporing en interceptie van telecommunicatie …) kunnen immers persoonsgegevens impliceren. De relevante bepalingen op het vlak van de persoonlijke levenssfeer zijn van toepassing op al deze gegevens.

2. Laten we vanaf het begin het belang van het proportionaliteitsbeginsel benadrukken.

Zowel de internationale teksten inzake de bescherming van de persoonsgegevens als ook de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna : de wet van 8 december 1992 ([4])) leggen de nadruk op de strikte eerbiediging van dit beginsel.

In dit opzicht, en in een gelijkaardige context, had de commissie reeds in herinnering gebracht dat « dergelijke technische maatregelen niet voor gevolg mogen hebben het opsporen of preventief onderscheppen te wettigen, dat ze er niet toe kunnen leiden dat de openbare overheden over informatie beschikken die niet evenredig is met deze nodig in het kader van het onderzoek, en, ten slotte, dat ze de strikt uitzonderlijke aard van de tap moeten eerbiedigen » (advies nr 09/97, nr 12/99). Deze opmerking geldt in het bijzonder voor de ontwerpartikelen 39*bis*, 88*ter*, 88*quater* en 109*ter* van het Wetboek van strafvordering (van het wetsontwerp nr 214/1, hieronder uiteengezet).

De commissie herinnert eraan dat de toegang tot informaticasystemen (artikel 88*ter*), tot informatie waardoor de methodes die de vertrouwelijkheid van de gegevens waarborgen, kunnen worden opgeheven (cryptografie) (artikel 88*quater*) of tot de gegevensbanken die het gebruik van de diensten bijhouden (artikel 109*ter,* E, ontwerp tot wijziging), niet mag leiden tot het verzamelen van meer informatie dan strikt noodzakelijk is voor een onderzoek; deze bepalingen staan niet toe dat er algemene toezichtmethodes worden gebruikt die losstaan van een onderzoek naar specifieke misdrijven. Zodoende zou het mogelijk zijn om door raadpleging van de gegevensbank waarin de toegangen van een persoon tot zijn *access provider* wordt bijgehouden, alle *sites* op te sporen die door deze

([4]) Deze wet werd gewijzigd door de wet van 11 december 1998 tot omzetting van de richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrij verkeer van die gegevens. Deze wet is momenteel nog niet in werking getreden maar de commissie beveelt aan om, gelet op het principe van directe werking van de Europese richtlijn, waarvan de omzettingstermijn verstreken is, zoveel mogelijk te anticiperen op bepaalde, door deze wet aangebrachte wijzigingen. In dit bijzonder geval gaat het hoofdzakelijk om een wijziging van de terminologie.

tions en projet (recherche et saisie de données, repérage et interception des télécommunications ...) peuvent impliquer des données à caractère personnel. Les dispositions pertinentes en matière de protection de la vie privée s'appliquent à toutes ces données.

2. Soulignons d'emblée l'importance du principe de proportionnalité.

Tant les textes internationaux relatifs à la protection des données à caractère personnel que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après, la loi du 8 décembre 1992 ([4])) mettent l'accent sur le respect strict de ce principe.

À cet égard, et dans un contexte similaire, la commission avait déjà rappelé que « les mesures à prévoir ne peuvent avoir pour effet de légitimer les pratiques de repérage ou d'interception préventives (…) elles ne peuvent conduire les autorités publiques à disposer d'informations disproportionnées par rapport à celles nécessaires dans le cadre de l'instruction, et (…) doivent respecter le caractère strictement d'exception de l'écoute » (avis n° 09/97, n° 12/99). Cette remarque vaut en particulier pour les articles 39*bis*, 88*ter*, 88*quater* et 109*ter* en projet du Code d'instruction criminelle (projet de loi n° 214/1, développement *infra*).

La commission rappelle que l'accès à des systèmes d'information (article 88*ter* en projet), à des informations permettant de lever les procédés garantissant la confidentialité des données (cryptographie) (article 88*quater* en projet) ou aux bases de données d'utilisation des services (article 109*ter*, E projet de modification) ne devrait pas permettre de rassembler quantité d'informations au-delà de ce qui est strictement nécessaire pour une instruction; ces dispositions n'autorisent pas des méthodes de surveillance globale indépendamment d'une instruction relative à des infractions précises. Ainsi, en consultant la base de données des accès d'une personne à son fournisseur d'accès, il est possible de retracer l'ensemble des sites visités par cette personne, alors que seule la question de sa con-

([4]) Cette loi a été modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/EG du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette loi n'est pas encore entrée en vigueur à cette date mais la commission préconise d'anticiper autant que possible certains changements apportés par cette loi, vu le principe de l'effet direct de la directive européenne dont le délai de transposition est dépassé. En particulier dans ce cas-ci, c'est essentiellement la terminologie qui se voit modifiée.

persoon werden bezocht, terwijl men slechts zijn verbinding met een specifieke *site* beoogt. Zo is het eveneens mogelijk om, als men beschikt over de door iemand gebruikte encryptiesleutel, toegang te hebben tot alle door deze persoon verstuurde berichten, of ook, als men beschikt over de toegangscode van een geneesheer, toegang te hebben tot alle gegevens voorkomende op een chipkaart in verband met gezondheid.

3. Het moet bovendien duidelijk zijn dat het geheel van bepalingen van de wet van 8 december 1992 van toepassing is op alle persoonsgegevens waarop de ontwerpbepalingen betrekking hebben. We vermelden hier niet alleen hetgeen door artikel 4 wordt bepaald (finaliteit, proportionaliteit, pertinentie, beperkte bewaartijd), maar ook door artikel 16 (veiligheid). De commissie is van oordeel dat men duidelijk in de ontwerptekst zou moeten vermelden dat deze wet van toepassing is ([5]). Deze vermelding zou op zijn minst in de memorie van toelichting moeten voorkomen. De commissie merkt niettemin op dat het ontwerp zelf onrechtstreeks het aspect « bescherming van persoonsgegevens » erkent, door in maatregelen te voorzien die de toegang beperken (artikel 39*bis*, § 2), en in waarborgen op het vlak van de integriteit en de confidentialiteit (artikel 39*bis*, § 6).

4. Met betrekking tot de toepasbaarheid van de wet van 8 december 1992 stelt zich nog de vraag van het gebruik van de concepten die in de ontwerptekst worden gebruikt in vergelijking met die van de wet van 8 december 1992 (zie *infra*) : hoe kunnen de door de ontwerpteksten geformuleerde wanbedrijven en de in de wet van 8 december 1992 vastgelegde en bestrafte wanbedrijven worden gearticuleerd ? ([6]) De commissie vraagt zich af of de wetgever de cumulatie van kwalificaties en misschien straffen op het oog heeft, of overweegt voorrang te geven aan één wetgeving, en in dat geval, aan welke.

5. Verder wenst de commissie de aandacht van de wetgever te vestigen op het feit dat de ontwerpteksten het volgende probleem niet regelen : in welke mate zullen bepaalde verantwoordelijken van informaticasystemen de regel van het beroepsgeheim (advocaten, geneesheren …) kunnen inroepen ? Het bewaren van

([5]) Cf. *infra* artikel 2.

([6]) Aldus zou de « valsheid in informatica » uit ontwerpartikel 210*bis* van het Strafwetboek, indien zij betrekking heeft op persoonsgegevens, kunnen overeenkomen met de verwerking van onjuiste persoonsgegevens (artikel 39, 1° van de wet van 8 december 1992), of met de verstrekking van onjuiste inlichtingen wanneer de betrokken persoon zijn recht van toegang uitoefent (artikel 39, 5°).

Informaticabedrog (ontwerpartikel 504*quater*) of *hacking* (ontwerpartikel 550*bis*) zouden kunnen overeenkomen met de indringing in een bestand, met een onwettige verwerking, of zelfs met een afwijking van finaliteit.

nexion à un site particulier serait visée. De la même manière, en disposant de la clé de cryptage utilisée par une personne, il est possible d'accéder à tous les messages émis par cette personne ou encore, en disposant du code d'accès d'un médecin, on peut avoir accès à toutes données figurant sur une « carte à puce » de santé.

3. De plus, il doit être clair que c'est l'ensemble des dispositions de la loi du 8 décembre 1992 qui s'applique à toutes les données à caractère personnel concernées par les dispositions en projet : non seulement le prescrit de l'article 4 (finalité, proportionnalité, pertinence, durée limitée de conservation), mais également celui de l'article 16 (sécurité). La commission est d'avis que l'applicabilité de cette loi devrait être clairement énoncée dans le texte en projet ([5]). À tout le moins, une telle mention devrait être reprise dans l'exposé des motifs. Elle note toutefois que le projet lui-même reconnaît indirectement l'aspect « protection des données à caractère personnel » en prévoyant des mesures limitant l'accès (article 39*bis*, § 2), ou encore de garanties en termes d'intégrité et de confidentialité (article 39*bis*, § 6).

4. Eu égard à l'applicabilité de la loi du 8 décembre 1992, se pose encore la question de l'utilisation des concepts utilisés dans le texte en projet par rapport à ceux de la loi du 8 décembre 1992 (cf. *infra*) ou de savoir comment articuler les délits prévus par les textes en projet et à ceux prévus et sanctionnés par la loi du 8 décembre 1992 ([6]). La commission se demande si le législateur envisage le cumul des qualifications et peut-être des peines ou s'il envisage d'accorder la priorité à une législation par rapport l'autre, et dans ce cas, à laquelle.

5. Par ailleurs, la commission souhaite attirer l'attention du législateur sur le fait que les textes en projet ne règlent pas la question de savoir dans quelle mesure certains responsables de systèmes informatiques pourront invoquer la règle du secret professionnel (avocats, médecins, ...). Les précautions particulières qu'impli-

([5]) Cf. *infra,* article 2.

([6]) Ainsi, le faux informatique de l'article 210*bis* du Code pénal en projet pourrait correspondre, s'il porte sur des données à caractère personnel, avec le traitement de données à caractère personnel inexactes (article 39, 1° de la loi du 8 décembre 1992), ou encore la communication de renseignements inexacts lorsque l'intéressé exerce sont droit d'accès (article 39, 5°).

La fraude informatique (article 504quater en projet) ou le *hacking* (article 550*bis* en projet) pourrait correspondre à une intrusion dans un fichier, à un traitement illicite, voire à un détournement de finalité.

het beroepsgeheim ten overstaan van een onderzoek waarvoor de toegang tot een informaticasysteem noodzakelijk is, impliceert specifieke voorzorgsmaatregelen waarvoor eveneens een regeling zou moeten worden getroffen.

In dit opzicht herinnert de commissie aan het voorschrift van artikel 90*octies* van het Wetboek van strafvordering : « de maatregel kan alleen betrekking hebben op de lokalen aangewend voor beroepsdoeleinden, de woonplaats of de communicatie- of telecommunicatiemiddelen van een advocaat of een arts, indien deze er zelf van worden verdacht een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd of eraan te hebben deelgenomen, of, indien precieze feiten doen vermoeden dat derden die ervan worden verdacht een van de strafbare feiten bedoeld in artikel 90*ter* te hebben gepleegd, gebruik maken van diens lokalen, woonplaats of communicatie- of telecommunicatiemiddelen. De maatregel mag niet ten uitvoer worden gelegd, zonder dat, naargelang van het geval, de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren ervan op de hoogte is. […] ».

De commissie is enerzijds van mening dat men zou moeten voorzien in dergelijke interventieprocedures — met inbegrip van de door beroepsverenigingen ondernomen interventies ([7]) — *in alle specifieke*, door de wetsontwerpen die het onderwerp van voorliggend advies uitmaken, *beoogde gevallen* (cf. *infra*). Anderzijds meent zij dat er voorzorgsmaatregelen moeten worden bepaald voor andere beroepscategorieën dan enkel de geneesheren en advocaten ([8]).

6. Kortom, de risico's op ontsporing en de mogelijkheid om een systeem van algemeen politietoezicht in te voeren op basis van de ontwerpbepalingen, maken een strikte herinnering aan de wettigheids- (cf. *infra*) en proportionaliteitsbeginselen noodzakelijk. Het lijkt eveneens wenselijk dat deze specifieke gerechtelijke praktijk wordt geëvalueerd en dat deze evaluatie wordt opgenomen in een binnen de drie jaar op te stellen verslag. Dit verslag zou aan de commissie moeten worden bezorgd, opdat zij hierop kan reageren op grond van de wettelijke beginselen waarover zij moet waken. De met deze evaluatie belaste instantie of dienst zou rekening moeten houden met specifieke, door de commissie vooraf te bepalen, criteria.

([7]) Zodoende zou men zich kunnen voorstellen dat een lid van de Raad van de Orde van geneesheren of van advocaten *aanwezig* is tijdens het optreden van de gerechtelijke instanties.

([8]) Zie niettemin in dit opzicht de rechtspraak van het Arbitragehof, dat de niet-uitbreiding van de bescherming tot andere, eveneens aan het beroepsgeheim onderworpen beroepen, in overeenstemming verklaarde met het gelijkheidsprincipe (arrest n[r] 26/96 van 27 maart 1996).

que la sauvegarde du secret professionnel face à une perquisition nécessitant l'accès à un système informatique devraient également être réglées.

À ce propos, la commission rappelle le prescrit de l'article 90*octies* du Code d'instruction criminelle libellé comme suit « la mesure ne pourra porter sur les locaux utilisés à des fins professionnelles, la résidence ou les moyens de communication ou de télécommunication d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90*ter* ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une des infractions visées à l'article 90*ter*, utilisent ses locaux, sa résidence ou ses moyens de communications ou de télécommunication. La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. (…) ».

La commission estime d'une part que des mécanismes d'intervention de ce type incluant les instances professionnelles ([7]) devraient être légalement prévus dans *tous les cas d'espèce* visés par les projets de loi qui font l'objet du présent avis (cf. *infra*) et d'autre part que des mesures de précautions devraient être prévues pour d'autres catégories professionnelles que les seuls médecins et avocats ([8]).

6. En bref, les risques de dérapage et la possibilité de mettre en place un système de surveillance policière générale sur la base des dispositions en projet nécessitent de rappeler strictement les principes de légalité (cf. *infra*) et de proportionnalité. Il paraît également souhaitable que cette pratique judiciaire spécifique fasse l'objet d'une évaluation et que celle-ci soit reprise dans un rapport à élaborer dans les trois ans, rapport qui devrait être communiqué à la commission afin de mettre celle-ci en état de réagir en fonction des principes légaux dont elle est instituée la gardienne. L'instance ou le service chargé de cette évaluation devrait tenir compte de critères spécifiques qu'il appartiendrait à la commission de formuler au préalable.

([7]) Ainsi, on pourrait imaginer qu'un membre du Conseil de l'Ordre des médecins ou des avocats soit *présent* lors de l'intervention des autorités judiciaires.

([8]) Voir toutefois à ce propos la jurisprudence de la Cour d'arbitrage qui a déclaré conforme au principe d'égalité la non extension de la protection à d'autres professions également soumises au secret professionnel (arrêt n° 26/96 du 27 mars 1996).

B. *Artikelsgewijze commentaar*

Betreffende het ontwerp nr 213/1 beperkt de commissie zich tot het benadrukken van het belang van dit wetsontwerp dat een bijdrage levert tot de bescherming van de persoonsgegevens en in het bijzonder tot de veiligheid van de persoonsgegevens.

De onder dit deel B door de commissie geformuleerde commentaar spitst zich toe op het ontwerp nr 214/1.

Art. 2

Artikel 2 van het ontwerp voegt een nieuw artikel 39*bis* in het Wetboek van strafvordering in.

Vanuit het standpunt van de bescherming van de persoonsgegevens, is de commissie van oordeel dat het probleem veroorzaakt door de inbeslagname of de kopie op bepaalde informatiedragers van de in een informaticasysteem opgeslagen gegevens, als volgt luidt. Het zal in de praktijk dikwijls moeilijk zijn om zich tijdens een inbeslagname of kopie te beperken tot enkel die gegevens betreffende vervolgde personen, zoals de strikte toepassing van het proportionaliteitsbeginsel het vereist.

De commissie meent bijgevolg dat het onontbeerlijk is dat :

1. de maatregel tot inbeslagname of kopie op nauwkeurige wijze de *misdrijven* aangeeft, waarvan de vervolging de inbeslagname of kopie vereist, alsmede, voorzover mogelijk, de verdachte personen;
2. voorzover mogelijk de kopie of inbeslagname beperkt zou moeten worden tot enkel die gegevens;
3. indien dat niet mogelijk is, de andere gegevens in de gerechtelijke gegevensbank zouden worden gewist, of dat wordt gewaarborgd dat deze gegevens niet zullen worden gebruikt door de gerechtelijke autoriteiten.

Bovendien stelt de commissie voor dat er in dit artikel uitdrukkelijk wordt verwezen naar de toepasbaarheid van de wet van 8 december 1992.

Art. 3

Artikel 3 voegt een artikel 88*ter* in het Wetboek van strafvordering in.

De commissie is van oordeel 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. Een motivatie van de aanwezigheid van deze drie voorwaarden zou moeten bestaan en onderzocht kunnen worden in de gevallen dat er betwisting zou bestaan over de uitbreidingsmaatregel.

B. *Observations par article*

En ce qui concerne le projet n° 213/1, la commission se contente de souligner l'importance de ce projet de loi qui contribue à la protection des données à caractère personnel et en particulier à leur sécurité.

Les observations de la commission effectuées sous cette partie B se concentrent sur le projet n° 214/1.

Art. 2

L'article 2 du projet insère un nouvel article 39*bis* dans le Code d'instruction criminelle.

Du point de vue de la protection des données à caractère personnel, la commission est d'avis que le problème créé par la saisie ou la copie de données stockées dans un système informatique sur certains supports est le suivant. En pratique, il sera souvent difficile lors d'une saisie ou d'une copie de se limiter aux seules données relatives aux personnes, objet des poursuites, comme l'exige l'application stricte du principe de proportionnalité.

La commission estime dès lors indispensable que :

1. la mesure ordonnant la saisie ou la copie indique précisément les *infractions* dont la poursuite requiert la saisie ou la copie ainsi que, dans toute la mesure du possible, les personnes soupçonnées;
2. dans toute la mesure du possible, la copie ou la saisie devraient être limitées à ces seules données;
3. si cela n'est pas possible, l'effacement des autres données devrait être opéré dans la banque de données judiciaires ou des garanties de non utilisation de celles-ci par les autorités judiciaires devraient être prévus.

La commission suggère en outre d'inclure dans cet article une référence explicite à l'applicabilité de la loi du 8 décembre 1992.

Art. 3

L'article 3 insère un article 88*ter* dans le Code d'instruction criminelle.

La commission est d'avis que l'extension de la perquisition à d'autres systèmes informatiques ne devrait pouvoir être effectuée que si les trois conditions énoncées dans la disposition proposée sont présentes de façon cumulative. Une motivation de la présence de ces trois conditions devrait être établie et pouvoir être examinée dans les cas où la mesure d'extension serait contestée.

De commissie merkt op dat het het tweede lid van dit artikel aan nauwkeurigheid ontbreekt voorzover de door dit lid beoogde personen via open systemen zoals het Internet toegang hebben tot een groot aantal *sites*. Het zou bijgevolg nuttig zijn om te preciseren dat men alleen de uitbreiding beoogt tot die systemen waartoe de gemachtigde personen « *in het bijzonder* » toegang hebben krachtens een bijzondere machtiging.

Het in het derde lid gebruikte begrip « *verantwoordelijke van het informaticasysteem* » wordt nergens omschreven. Een dergelijke onnauwkeurigheid zou onjuistheden en misverstanden kunnen scheppen. Gaat het om de technisch of burgerlijk verantwoordelijke of om de verantwoordelijke ten opzichte van een specifieke wetgeving zoals die betreffende de bescherming van persoonsgegevens ? Artikel 1, § 4 van de wet van 8 december 1992, zoals gewijzigd door de wet van 11 december 1998, omschrijft de verantwoordelijke voor de verwerking als « de natuurlijke persoon of rechtspersoon, de feitelijke vereniging of het openbaar bestuur […] die alleen of samen met anderen het doel en de middelen voor de verwerking van gegevens bepaalt ». De commissie is van mening dat het wetsontwerp aanwijzingen zou moeten leveren betreffende het begrip « verantwoordelijke van het informaticasysteem ».

De commissie merkt ten slotte op dat de uitbreiding van de zoeking toelaat om de « *nuttige* » gegevens te verzamelen voor dezelfde finaliteiten als voor de inbeslagname. Deze uitgebreide mogelijkheid tot verzameling van gegevens lijkt niet conform het proportionaliteitsbeginsel. De wet van 8 december 1992 bepaalt evenwel criteria van relevantie, toereikendheid en niet-overmatigheid die veeleisender lijken op het vlak van de bescherming van persoonsgegevens.

Art. 4

Artikel 4 voegt een artikel 88*quater* in het Wetboek van strafvordering in.

De commissie merkt op dat dit artikel voorziet in een opdracht door de onderzoeksrechter aan een officier van gerechtelijke politie. Zij stelt voor om eraan toe te voegen dat dit *schriftelijk* moet gebeuren.

Krachtens het tweede lid breidt de medewerkingsverplichting zich uit tot « iedere relevante persoon », uitgezonderd de verdachte en zijn naasten. De commissie vraagt zich af wat de gevolgen zullen zijn indien de verdachte een rechtspersoon is. Wordt een orgaan of een aangestelde beschermd door de regel van zelfin-

La commission relève que le deuxième alinéa de cet article manque de précision dans la mesure où via des réseaux ouverts comme Internet, les personnes visées par cet alinéa ont accès à une multitude de sites. Il serait par conséquent utile de préciser que seule est visée l'extension à des systèmes auxquels les personnes autorisées ont *« spécifiquement »* accès en vertu d'une autorisation particulière.

La notion de *« responsable du système informatique »* utilisée au troisième alinéa n'est définie nulle part. Pareille imprécision risque de créer des inexactitudes et des malentendus. S'agit-il du responsable technique, civil ou du responsable vis-à-vis d'une législation particulière comme celle relative à la protection des données à caractère personnel ? Ainsi, l'article 1er, § 4 de la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 définit le responsable du traitement comme « la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ». La commission estime que le projet de loi devrait fournir certaines indications à propos de la notion de « responsable du système informatique ».

La commission note enfin que l'extension de la recherche permettra de collecter des données *« utiles »* pour les mêmes finalités que celles prévues pour la saisie. Cette possibilité étendue de collecter des données ne paraît pas conforme au principe de proportionnalité. La loi du 8 décembre 1992 prévoit des critères de pertinence, d'adéquation et de non-excessivité qui paraissent plus exigeants en termes de protection des données à caractère personnel.

Art. 4

L'article 4 insère un article 88*quater* dans le Code d'instruction criminelle.

La commission note que cet article prévoit une délégation par le juge d'instruction à un officier de police judiciaire. Elle suggère d'ajouter qu'elle doit être faite *par écrit*.

En vertu du deuxième alinéa, l'obligation de collaboration s'étend « à toute personne pertinente », sauf l'inculpé et ses proches. La commission se demande quelles seront les conséquences si l'inculpé est une personne morale. Un organe ou un préposé est-il protégé par la règle de l'auto-incrimination ? Les exemples

criminatie ? De in de memorie van toelichting ([9]) gegeven voorbeelden zijn vaak extern aan een onderneming en de situatie van vernoemde personen blijft onduidelijk.

Ten slotte meent de commissie eveneens dat het, zowel wat het eerste als ook het tweede lid betreft, van belang zou zijn om te waken over de eerbiediging van het beroepsgeheim (cf. *supra*).

Art. 7

Artikel 7 vult artikel 90*quater* van het Wetboek van strafvordering aan door er een vierde lid in te voegen.

Deze bepaling regelt de medewerking van de personen verbonden aan een telecommunicatiedienst en die gevorderd kunnen worden om inlichtingen te verschaffen over de werking van het systeem of over de wijze om in een verstaanbare vorm toegang te verkrijgen tot de inhoud van de telecommunicatie. De tekst voegt er gelukkig aan toe dat dit moet gebeuren « *voorzover dit in hun mogelijkheden ligt* ». Men stuit hier op het probleem van een verplichting tot decrypteren die moeilijk zal kunnen worden nagekomen indien het initiatief tot encryptie niet van de operator maar wel van de gebruiker uitgaat (cf. advies nr 12/99, blz. 6).

Bovendien laat de bepaling, zoals deze is opgesteld ([10]) de onderzoeksrechter niet alleen toe om de voor de decodering of het decrypteren noodzakelijke gegevens betreffende de verdachte communicaties te verkrijgen, maar ook van alle telecommunicaties van alle gebruikers van de dienst die dossiers beschermt of encrypteert.

Bijgevolg is de commissie van mening dat men moet waken over de eerbiediging van het proportionaliteitsbeginsel en dat de decodering of het decrypteren moet worden uitgevoerd door de *persoon* die kennis heeft van de methode van encrypteren of codering zonder dat er noodzakelijkerwijze een overdracht is van de inlichtingen betreffende de decodering of het decrypteren.

([9]) DOC 50 0213/001 en 0214/001, blz. 27.

([10]) « De onderzoeksrechter kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van de telecommunicatiedienst waarop de bewakingsmaatregel betrekking heeft of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, vorderen in een verstaanbare vorm inlichtingen te verstrekken over de werking ervan en over de wijze om toegang te verkrijgen tot de inhoud van telecommunicatie die wordt of werd overgebracht.

Indien nodig, kan hij personen bevelen om zelf de inhoud van de telecommunicatie toegankelijk te maken in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt […]. »

donnés dans l'exposé des motifs ([9]) sont souvent externes à la société et la situation des personnes précitées reste peu claire.

Enfin, la commission estime également que, tant pour le premier que pour le second alinéa, il serait important de veiller au respect du secret professionnel (cf. *supra*).

Art. 7

L'article 7 complète l'article 90*quater* du Code d'instruction criminelle en ajoutant un quatrième alinéa.

Cette disposition règle la collaboration des personnes liées à un service de télécommunication, qui doivent fournir des informations afin d'informer sur le fonctionnement du système ou sur la manière d'accéder au contenu de la télécommunication, sous une forme compréhensible. Le texte ajoute heureusement *« dans la mesure où c'est dans leurs possibilités »*. On retrouve ici le problème d'une obligation de décryptage qui sera difficile à respecter lorsque l'initiative du cryptage n'émane pas de l'opérateur, mais de l'utilisateur (cf. avis n° 12/99, p. 6).

En outre, telle qu'elle est rédigée ([10]), la disposition permet au juge d'instruction d'obtenir les informations nécessaires au décodage ou au décryptage, non seulement des communications suspectes, mais de toutes les télécommunications de l'ensemble des utilisateurs du service de protection ou de cryptage des dossiers.

Dès lors, la commission estime qu'il faut veiller à ce que le principe de proportionnalité soit respecté et que le décodage ou décryptage soit fait par la *personne* qui a connaissance du procédé de cryptage ou de codage sans qu'il y ait nécessairement transmission des informations relatives au décodage ou au décryptage.

([9]) DOC 50 0213/001 et 0214/001, p. 27.

([10]) « Le juge d'instruction peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible.

Si nécessaire, il peut ordonner aux personnes de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure où c'est dans leurs possibilités. […] ».

Bovendien acht de commissie het nuttig dat enkel bepaalde personen binnen de instellingen die gegevens kunnen beschermen of encrypteren, door de onderzoeksrechter gecontacteerd kunnen worden, en dit op zodanige wijze dat de risico's op verspreiding van de genomen maatregelen en onderzoeksresultaten niet groter worden. Deze door de instellingen aangewezen personen zouden aan het beroepsgeheim onderworpen zijn (cf. de « Coördinatiecel Justitie » voorgesteld door het ontwerp van koninklijk besluit ter uitvoering van artikel 109*ter*, E van de wet van 21 maart 1991).

Bovendien werpt deze bepaling eveneens het probleem op van het beroepsgeheim dat bepaalde personen zouden kunnen inroepen ten overstaan van de onderzoeksrechter (cf. *supra*).

Art. 8

Artikel 8 breidt de modaliteiten uit van de bewaring van gegevens bij het parket.

Aangezien persoonsgegevens niet van deze bewaring worden uitgesloten, meent de commissie dat men bij voorkeur moet verduidelijken dat de middelen « *moeten* », en niet « *mogen* » aangewend worden voor de integriteit en de vertrouwelijkheid.

De commissie is van oordeel dat het gaat om een nieuwe, aan de wet van 8 december 1992 onderworpen, verwerking van persoonsgegevens. Bijgevolg zou, gelet op de aard van sommige te bewaren gegevens, het koninklijk besluit dat de middelen bepaalt aan het advies van de commissie moeten onderworpen worden.

Art. 9

Artikel 9 wijzigt artikel 109*ter*, E van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven.

De voorgestelde wettelijke bepaling vult een bepaling aan die recent werd gewijzigd door de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie. Deze bepaling stelt dat de Koning, na het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer te hebben ingewonnen, bij een in Ministerraad overlegd koninklijk besluit, « *de technische middelen [bepaalt] waarmee de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten, in voorkomend geval gezamenlijk, moeten instaan om het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-telecommunicatie […] mogelijk te maken* ».

De plus, la commission estime qu'il serait utile que seules certaines personnes au sein des organismes permettant de protéger ou de crypter des données, puissent être contactées par le juge d'instruction, et ce de manière à ne pas multiplier les risques de divulgation des mesures prises et des résultats de l'enquête. Ces personnes désignées par les organismes seraient soumises au secret professionnel (cf. la cellule « coordination Justice » proposée par le projet d'arrêté royal en application de l'article 109*ter*, E de la loi du 21 mars 1991).

Par ailleurs, cette disposition soulève également la question du secret professionnel que certaines personnes pourraient opposer au juge d'instruction (cf. *supra*).

Art. 8

L'article 8 étend les modalités de conservation des données au niveau du parquet.

Des données à caractère personnel n'étant pas exclues de cette conservation, la commission estime qu'il serait préférable de préciser que les moyens « *doivent* » être utilisés pour l'intégrité et la confidentialité, au lieu de « *peuvent* ».

La commission est d'avis qu'il s'agit d'un nouveau traitement de données à caractère personnel soumis à la loi du 8 décembre 1992. Dès lors, étant donné la nature de certaines données à conserver, l'arrêté royal déterminant les moyens devrait être soumis à l'avis de la commission.

Art. 9

L'article 9 modifie l'article 109*ter*, E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

La disposition légale proposée complète une disposition récemment modifiée par la loi du 10 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées. Cette disposition veut que le Roi détermine, après avis de la Commission de la protection de la vie privée, par arrêté délibéré en Conseil des ministres *« les moyens techniques par lesquels les opérateurs de réseaux et les fournisseurs de services de télécommunications doivent permettre le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement de télécommunications privées »*.

De commissie brengt in herinnering dat zij een haar voorgelegd ontwerp van koninklijk besluit tot omzetting van deze wettelijke bepaling streng had bekritiseerd (advies nr 12/99 van 24 maart 1999).

Bovendien waarborgt artikel 8 van het Europese Verdrag voor de bescherming van de rechten van de mens en de fundamentele vrijheden de vertrouwelijkheid van de telecommunicatie, met inbegrip van de gegevens betreffende het gebruik van telecommunicatiediensten ([11]). Artikel 5 van de richtlijn 97/66/EG ([12]) hanteert dezelfde logica. Het principe is dus het verbod op kennisneming behoudens uitzonderingen die strikt moeten worden afgebakend.

De door artikel 29 van de richtlijn 95/46/EG ([13]) opgerichte groep (hierna : groep 29) heeft de *in casu* toepasbare beginselen in herinnering gebracht in het kader van de aanbevelingen nrs 2/99 en 3/99 (cf. *supra*).

Op grond van de in deze verschillende teksten naar voren gebrachte commentaar en beginselen, meent de commissie dat de door ontwerpartikel 109*ter* ingevoerde maatregelen de verplichte oprichting van databanken van persoonsgegevens met zich mee zal brengen, en belangrijke gevolgen hebben op het vlak van de persoonlijke levenssfeer. De Raad van State had opmerkingen betreffende dit artikel.

1. *Wettelijke grondslag*

Artikel 22 van de Grondwet bepaalt dat « ieder recht heeft op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht ». Met andere woorden, alleen bij wet kunnen enige beperkingen op het recht op eerbiediging van het privé- en het gezinsleven worden ingesteld. De verschillende maatregelen die bijdragen tot het vergemakkelijken van de taak van de bevoegde overheid moeten bijgevolg hun rechtstreekse grondslag vinden in de wet (zie, in dezelfde zin, het advies van de Raad van State, DOC 50 0213/001 en 0214/001, blz. 55).

La commission rappelle qu'un projet d'arrêté royal relatif à la transposition de cette disposition, qui lui avait été soumis en son temps, avait fait l'objet de critiques sévères de sa part (dans son avis n° 12/99 du 24 mars 1999).

En outre, l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales garantit le caractère confidentiel des télécommunications en ce compris les données relatives à l'utilisation des services de télécommunication ([11]). L'article 5 de la directive 97/66/CE ([12]) s'inscrit dans la même logique. Le principe est donc l'interdiction de prise de connaissance, sauf exceptions, qui doivent être strictement délimitées.

Le groupe établi par l'article 29 de la directive 95/46/CE ([13]) (ci-après, le groupe 29) a rappelé les principes applicables en l'espèce dans le cadre des recommandations n° 2/99 et n° 3/99 (cf. *supra*).

Sur la base des critiques et principes énoncés par ces différents textes, la commission estime que les mesures instituées par l'article 109*ter* en projet entraîneront la création obligatoire de banques de données à caractère personnel et ont des conséquences importantes en matière de vie privée. Cet article a fait l'objet de remarques du Conseil d'État.

1. *Base légale*

L'article 22 de la Constitution énonce que « chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ». En d'autres termes, seule la loi peut apporter des restrictions au droit à la vie privée et familiale. Les différentes mesures contribuant à faciliter la tâche des autorités compétentes doivent dès lors trouver leur fondement direct dans la loi (dans le même sens, avis du Conseil d'État, DOC 50 0213/001 et 0214/001, p. 55).

---

([11]) Arrest Malone van 2 augustus 1984, *Publ. Cour,* Série A, nr 82, blz. 30 en volgende.

([12]) Richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (hierna : de richtlijn 97/66/EG).

([13]) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (hierna : de richtlijn 95/46/EG).

([11]) Arrêt Malone du 2 août 1984, publ. Cour, Série A, n° 82, pp. 30 et suivantes.

([12]) Directive 97/66/CE du 15 décembre 1997 du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (ci-après, la directive 97/66/CE).

([13]) Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, la directive 95/46/CE).

Deze verplichting blijkt eveneens uit verschillende internationale teksten. De toepassing van artikel 8 van voornoemd Europees verdrag alsmede van artikel 9, § 2 van het Verdrag nr 108 van de Raad van Europa, van artikel 13 van de richtlijn 95/46/EG, en van artikel 14 van de richtlijn 97/66/EG, heeft tot gevolg dat de lidstaten nauwkeurige voorwaarden moeten vastleggen om maatregelen van inmenging door de politie-, gerechtelijke en veiligheidsdiensten toe te laten. Drie criteria geven de doorslag : de wettelijke grondslag, de noodzakelijkheid in een democratische samenleving en het wettig doeleinde.

Op de kritiek van de Raad van State als zouden de inbreuken op de persoonlijke levenssfeer die voortvloeien uit de verplichting om de gegevens te registreren en te bewaren, hun grond moeten vinden in een wettekst, antwoordt de auteur van de tekst dat de techniciteit van de zaak een dergelijke oplossing in de weg staat.

Los van het risico dat een dergelijke keuze door het Arbitragehof wordt afgekeurd, wenst de commissie op te merken dat niets belet om de bewaartijd en de waarborgen op het vlak van de bescherming van de persoonlijke levenssfeer in een wettekst te gieten (wat niets technisch heeft en bijvoorbeeld reeds werd gedaan in de wet op het Centraal Strafregister) en om de middelen van uitsluitend « technische » aard te bepalen bij koninklijk besluit ([14]).

Indien men bij de huidige keuze blijft, zou het in ieder geval om een in Ministerraad overlegd koninklijk besluit moeten gaan en zou het advies van de commissie op zijn minst vereist moeten worden voor § 2 van artikel 109*ter* (verplichting voor de verstrekkers van telecommunicatiediensten om de gegevens te registreren en te bewaren) en niet alleen voor § 4 van dat artikel (modaliteiten en middelen om de vertrouwelijkheid en integriteit van de gegevens te waarborgen).

2. *Proportionaliteit*

i) Noodzakelijkheidscriterium

De beoogde gegevens maken het mogelijk om een gegevensbank van niet *a-priori* verdachte personen samen te stellen (zie naar analogie het advies nr 17/98 van de commissie houdende een wetsontwerp inzake DNA-onderzoek in strafzaken en het advies nr 40/97 inzake de proactieve recherche betreffende potentiële

Cette obligation ressort également de divers textes internationaux. L'application des articles 8 de la Convention européenne précitée, ainsi que de l'article 9, § 2 de la Convention n° 108 du Conseil de l'Europe, de l'article 13 de la directive 95/46/CE et de l'article 14 de la directive 97/66/CE, a pour conséquence que les États doivent établir des conditions précises pour permettre des mesures d'ingérence par les services de police, de justice et de sûreté. Trois critères prévalent : la base légale, la nécessité dans une société démocratique et la finalité légitime.

À la critique émise par le Conseil d'État tenant au fait que les atteintes à la vie privée résultant des obligations d'enregistrement et de conservation des données doivent trouver leur origine dans un texte de loi, le rédacteur du texte répond aux objections du Conseil d'État que la technicité de la question s'oppose à ce type de solution.

Indépendamment du risque de censure d'un tel choix par la Cour d'arbitrage, la commission souhaite faire remarquer que rien n'empêche de figer la durée et les garanties en termes de protection de la vie privée dans un texte légal (ce qui n'a rien de technique et a déjà été fait dans la loi sur le Casier judiciaire central, par exemple) et de prévoir les modalités de nature exclusivement « techniques » par arrêté royal ([14]).

Si le choix actuel devait être maintenu, il devrait s'agir en tout état de cause d'un arrêté royal délibéré en Conseil des ministres et l'avis de la commission devrait à tout le moins être requis pour le § 2 du 109*ter* (obligation pour les fournisseurs de services d'enregistrer et de conserver des données) et pas uniquement pour le § 4 de cet article (modalités et moyens de garantir la confidentialité et l'intégrité des données).

2. *Proportionnalité*

i) Critère de nécessité

Les données visées permettent de constituer des bases de données de personnes non soupçonnées *a priori* (voyez, pour analogie, l'avis n° 17/98 de la Commission portant sur un avant-projet de loi relatif à l'analyse ADN en matière pénale et l'avis n° 40/97 concernant un projet proactif relatif aux ravisseurs potentiels

([14]) In haar advies nr 12/99 betreffende het afluisteren van telecommunicatieverkeer had de commissie een wet voorgesteld, of een in Ministerraad overlegd en voorafgaand aan het advies van de commissie voorgelegd, koninklijk besluit.

([14]) Dans son avis n° 12/99 sur les écoutes téléphoniques, la commission avait suggéré une loi, ou un arrêté royal délibéré en Conseil des ministres et préalablement soumis à la commission.

ontvoerders van kinderen). Nu, de commissie brengt in herinnering dat noch de hierboven vermelde internationale teksten, noch de wet van 8 december 1992 (beginselen van proportionaliteit, beperkte bewaartijd, …) algemene toezichtsmethodes toestaan die losstaan van een onderzoek naar specifieke misdrijven (uitgezonderd het zeer specifieke geval van de proactieve recherche, die strikt omkaderd is).

In dit opzicht wenst de commissie nog te verwijzen naar de rechtspraak van het Europese Hof voor de rechten van de mens ([15]), die leidt tot het verbieden van de op grote schaal gehanteerde verkennende en algemene toezichtsmethodes op telecommunicatiediensten.

Aldus zou een *access provider* niet verplicht kunnen worden om systematisch alle oproepen uitgaande van zijn klanten te registreren, maar alleen wanneer een onderzoek wordt ingesteld naar een specifieke persoon. Hij zou ook niet mogen gedwongen worden om een logboek bij te houden van de toegangen die het onderzoek zouden kunnen sterken ([16]).

In deze context acht de commissie het eveneens nuttig om te herinneren aan artikel 2, § 2, 2° van aanbeveling n$^{r}$ R(95)4 van de Raad van Europa, krachtens hetwelk anonieme middelen voor toegang tot een netwerk en telecommunicatiediensten ter beschikking van de gebruikers zouden moeten worden gesteld.

ii) Toepassingsgebied

Het toepassingsgebied is zeer ruim : de beoogde gegevens slaan op iedereen die gebruik maakt van telecommunicatiediensten. Potentieel betreft het hier de hele bevolking en alle telecommunicatiediensten (een zeer ruime categorie : *access providers*, toegangspoorten, dienstenverleners, certificaatverstrekkers, de zogenaamde « anonimiserings »-*servers* …). In onze samenleving, die steeds meer naar een « informatiemaatschappij » evolueert, is het gebruik van telecommunicatiediensten immers steeds meer verbreid.

Bovendien zijn de gegevenscategorieën niet nauwkeurig afgebakend (cf. de memorie van toelichting die

([15]) Arrest Klass (arrest van 6 september 1978, *Publ. Cour*, Série A, n$^{r}$ 28, blz. 23 en volgende) en Malone (vernoemd). Zie op dit punt de aanbeveling n$^{r}$ 2/99 van de bij artikel 29 van de richtlijn 95/46/EG opgerichte groep, betreffende de bescherming van de persoonlijke levenssfeer in het kader van de interceptie van telecommunicatieverkeer.

([16]) Zie de uitzonderlijk ruime formulering in de memorie van toelichting, blz. 31.

d'enfants). Or, la commission rappelle que ni les textes internationaux mentionnés ci-dessus, ni la loi du 8 décembre 1992 (principes de proportionnalité, durée limitée, …) n'autorisent les méthodes de surveillance globale indépendamment d'instructions relatives à des infractions particulières (si l'on excepte le cas très particulier de la recherche proactive, qui est strictement encadrée).

À cet égard, la commission souhaite encore se référer à la jurisprudence de la Cour européenne des droits de l'homme ([15]) qui conduit à proscrire les mesures de surveillance exploratoire ou générale des télécommunications mises en œuvre sur une grande échelle.

Ainsi, il ne pourrait être question d'obliger un fournisseur d'accès à enregistrer systématiquement tous les appels en provenance de ses clients mais uniquement lorsqu'une instruction est ordonnée vis-à-vis d'une personne en particulier. Il ne pourrait non plus être question de contraindre un fournisseur d'accès à tenir un log book des accès susceptibles de conforter l'instruction ([16]).

Dans ce contexte, la Commission estime également utile de rappeler l'article 2, § 2, 2° de la recommandation n° R(95)4 du Conseil de l'Europe en vertu duquel des dispositifs anonymes d'accès au réseau et aux services de télécommunication devraient être mis à la disposition des utilisateurs.

ii) Champ d'application

Le champ d'application est très large : les données visées ont trait à quiconque utilise des services de télécommunication. Il s'agit potentiellement de toute la population, et l'ensemble des services de télécommunication est couvert (catégorie extrêmement large : fournisseurs d'accès, portails, services dits « intermédiaires », certificateurs, serveurs dits « d'anonymisation » …). En effet, dans notre société qui évolue de plus en plus vers une «société de l'information», l'utilisation des services de télécommunications est de plus en plus répandue.

De plus, les catégories de données ne sont pas circonscrites de manière précise (cf. l'exposé des mo-

([15]) Arrêts Klass (arrêt du 6 septembre 1978, Publ. Cour, Série A, n° 28, p. 23 et suivantes) et Malone (cité). Voir sur ce point la recommandation du groupe institué à l'article 29 de la directive 95/46/CE n° 2/99 concernant le respect de la vie privée dans le contexte de l'interception des télécommunications.

([16]) Voir la formulation extrêmement large de l'exposé des motifs, p. 31.

niet bijdraagt tot de duidelijkheid door *a-priori* bepaalde gegevens te vermelden zonder de andere definitief uit te sluiten ([17])).

iii) Bewaartijd

Aanbeveling nr 3/99 van de groep 29 vraagt om een bewaartijd vast te leggen die afgestemd wordt op de hoogste beschermingsnorm in de lidstaten ([18]). Een termijn van drie maanden, zoals toegepast in Duitsland, lijkt in de praktijk voldoende. De commissie zou zich in ieder geval moeten kunnen uitspreken over deze termijn.

Bovendien kan de commissie niet instemmen met de in de memorie van toelichting naar voren gebrachte criteria, namelijk enerzijds een uitzonderlijk breed criterium gevormd door de noden van de strafvordering, en anderzijds, de mogelijkheden van de dienstenverstrekkers op technisch en praktisch vlak. Dit laatste komt erop neer dat men een uitbreiding van de maatregelen toestaat op grond van de praktische en technische mogelijkheden. Twee karakteristieken zijn evenwel steeds kenmerkend geweest voor de evolutie van de informatie- en communicatietechnologieën : het toenemen van de snelheid van de informatieverwerking en de kleinere ruimte die noodzakelijk is om deze informatie te verwerken en te bewaren. Indien men deze redenering volgt, zou dus een langere bewaartijd moeten worden toegestaan van zodra de techniek dit mogelijk maakt.

3. *Aanzetten tot het opstarten van nieuwe verwerkingen*

Men dient op te merken dat de ontwerptekst toestaat dat dienstenverstrekkers worden verplicht de gegevens betreffende de oproepen (wie roept op, wie wordt opgeroepen, identificatiegegevens van de opgeroepene, Internetadres…) te *registreren*, die zij niet noodzakelijkerwijze zouden registreren voor de uitvoering van hun diensten (met inbegrip van hun facturering). Aldus zou-

([17]) Zie bijvoorbeeld de gegevens betreffende de door een Internetgebruiker bezochte *sites*, die slechts in bepaalde « uitzonderlijke » situaties zouden mogen worden bewaard. Bovendien zullen andere, *a-priori* uitgesloten gegevens, zoals de lokalisering in het geval van het gebruik van een GSM, over het algemeen worden bewaard tot op het moment dat de facturering niet meer betwist kan worden. Men kan bijgevolg niet definitief uitsluiten dat deze gegevens tijdens deze termijn aan de overheid worden medegedeeld.

([18]) Aanbeveling nr 3/99 van 7 september 1999 over de bewaring van verkeersgegevens door Internetdienstenaanbieders voor wetshandhavingsdoeleinden.

tifs, qui ne contribue pas à la clarté en mentionnant *a priori* certaines données sans exclure les autres de manière définitive ([17])).

iii) Durée de conservation

La recommandation n° 3/99 du groupe 29 demande de fixer un délai de conservation aligné sur la norme de protection la plus élevée observée dans les États membres ([18]). Il semble, par exemple, qu'un délai de trois mois, tel qu'appliqué en Allemagne, soit suffisant en pratique. La commission devrait en tout état de cause pouvoir se prononcer quant à ce délai.

En outre, la commission ne peut se rallier aux critères avancés dans l'exposé des motifs à savoir, d'une part, un critère extrêmement large constitué par les besoins de l'action publique et, d'autre part, les possibilités des fournisseurs de services sur les plans technique et pratique. Ce dernier critère équivaut à admettre une extension des mesures en fonction des possibilités pratique et technique. Or deux caractéristiques ont toujours marqué l'évolution des technologies de l'information et de la communication : l'augmentation de la rapidité de traitement de l'information et la réduction des espaces nécessaires pour la traiter et la conserver. Si l'on suit ce raisonnement, dès que la technique le permettra, une durée plus longue devrait être admise.

3. *Incitation à la création de nouveaux traitements*

On notera que le texte en projet permet de contraindre les fournisseurs de services à *enregistrer* des données relatives aux données d'appel (qui appelle, qui est appelé, données d'identification de l'appelé, adresse Internet, …) qu'ils n'enregistreraient pas forcément pour la mise en œuvre de leurs services (en ce compris leur facturation). Ainsi des services de mobilophonie

([17]) Voir par exemple les données relatives aux sites consultés par un Internaute qui ne devraient être conservées que dans certaines situations « exceptionnelles ». En outre, d'autres données *a priori* exclues, comme la localisation en cas d'utilisation d'un GSM seront généralement conservées jusqu'au moment où la facturation ne peut plus être contestée. On ne peut dès lors exclure de manière définitive leur communication aux autorités durant ce délai.

([18]) Recommandation n° 3/99 du 7 septembre 1999 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit.

den abonnementsloze mobilofoondiensten aan de registratieplicht onderworpen kunnen worden.

Deze evolutie werd reeds gebrandmerkt door de commissie in haar voorgaande adviezen (advies nr 34/97 en nr 12/99), erkennende dat « in het licht van de technologische evolutie, de medewerking van de operatoren van telecommunicatienetwerken en de leveranciers van diensten, voortaan vereist is om de bevolen maatregelen efficiënt te maken. Ze vestigt er echter de aandacht van de wetgever op dat een dergelijke samenwerking aanleiding kan geven tot nieuwe risico's voor de persoonlijke levenssfeer, in zoverre het antwoord op de verzoeken van de openbare overheid nieuwe verwerkingen kan vereisen in hoofde van de operatoren en leveranciers ».

De commissie merkt ook nog op dat de aan de memorie van toelichting toegevoegde rechtvaardigingen, in het bijzonder de mogelijkheid om de netwerken op anonieme wijze te gebruiken, haar niet voldoende lijken en niet met de werkelijkheid overeenkomen. Op dit moment bestaan er veel mogelijkheden om de gebruikers van telecommunicatiediensten op te sporen aan de hand van verschillende gebruikersidentificaties, met name verbonden aan het gebruik van het Internet.

Overeenkomstig zowel artikel 4 van de wet van 8 december 1992 als ook artikel 6, §§ 1 en 2 van de richtlijn 95/46/EG, moet de finaliteit van elke nieuwe verwerking voldoende en uitdrukkelijk gedefinieerd zijn en moet de verwerking proportioneel zijn ten overstaan van deze finaliteit.

Als besluit is de commissie van oordeel dat het proportionaliteitsbeginsel strikt zou moeten worden toegepast teneinde de oprichting van een opslagplaats te vermijden, waarin meer en meer gegevens verzameld zouden kunnen worden, volgens steeds diversere hypotheses.

**Conclusie**

De commissie is van mening :

— dat een wetgeving die de informaticacriminaliteit bestraft, onrechtstreeks meewerkt aan de bescherming van de persoonlijke levenssfeer voorzover zij bijdraagt tot een grotere veiligheid van de persoonsgegevens (inzonderheid het ontwerp nr 213/1);

— dat de teksten (inzonderheid het ontwerp nr 214/1) niettemin geamendeerd zouden moeten worden om rekening te houden met de in voorliggend advies gemaakte opmerkingen;

— dat er een uitdrukkelijke verwijzing naar de toepassing van de wet van 8 december 1992 zou moeten bestaan in het wetsontwerp of tenminste in de memorie van toelichting;

— dat een systeem van *follow-up* van de voorziene maatregelen zou moeten worden ingevoerd, waarbij de commissie betrokken wordt, en dat er in ieder geval binnen een termijn van drie jaar een evaluatie zou

sans abonnement pourraient être soumis à l'obligation d'enregistrement.

Cette évolution a été stigmatisée par la commission dans ses avis précédents (avis n° 34/97 et n° 12/99) qui a considéré « qu'au regard de l'évolution des technologies, la collaboration des opérateurs de réseaux de télécommunications et des fournisseurs de services sera dorénavant requise pour rendre efficaces les mesures ordonnées. Elle attire cependant l'attention du législateur sur le fait qu'une telle collaboration peut créer des risques nouveaux d'atteinte à la vie privée, dans la mesure où la réponse aux demandes de l'autorité publique peut requérir des traitements nouveaux dans le chef des opérateurs et des fournisseurs ».

La commission note encore que les justifications apportées dans l'exposé des motifs, et en particulier la facilité d'utiliser les réseaux de façon anonyme, ne lui apparaissent pas satisfaisantes et ne correspondent pas à la réalité. Il existe actuellement de nombreuses possibilités de repérer les utilisateurs de service de télécommunication sur la base des identifiants uniques, notamment dans le contexte d'Internet.

En application tant de l'article 4 de la loi du 8 décembre 1992 que de l'article 6, §§ 1er et 2 de la directive 95/46/CE, la finalité de tout nouveau traitement doit être suffisamment définie et explicite et le traitement doit être proportionnel par rapport à cette finalité.

En conclusion, la commission est d'avis que le principe de proportionnalité devrait être appliqué strictement afin d'éviter la création d'un réservoir dans lequel de plus en plus de données pourraient être collectées dans des hypothèses de plus en plus diverses.

**Conclusions**

La commission estime :

— qu'une législation réprimant la criminalité informatique participe indirectement à la protection de la vie privée dans la mesure où elle contribue à améliorer la sécurité des données à caractère personnel (en particulier, le projet n° 213/1);

— que les textes (en particulier, le projet n° 214/1) devraient néanmoins être amendés pour tenir compte des remarques énoncées dans le présent avis;

— qu'une référence explicite à l'application de la loi du 8 décembre 1992 devrait exister dans le projet de loi ou à tout le moins dans l'exposé des motifs;

— qu'un système de suivi des mesures envisagées devrait être mis en place incluant la commission et qu'en tout état de cause une évaluation devrait être réalisée dans un délai maximum de 3 ans, évaluation à

moeten plaatsvinden, waaraan de commissie zou moeten deelnemen (formuleren van specifieke criteria voor de instantie belast met de evaluatie, mededeling van het evaluatieverslag aan de commissie);

— dat zij dient geraadpleegd te worden betreffende ieder ontwerp van koninklijk besluit ter uitvoering van deze teksten.

*De secretaris,* *De voorzitter,*

(get.) M.- H. BOULANGER (get.) P. THOMAS

laquelle la commission devrait être associée (formulation de critères spécifiques à l'instance chargée de l'évaluation, communication du rapport d'évaluation à la commission) ;

— qu'elle devrait être saisie de tout projet d'arrêté royal adopté en exécution de ces textes.

*Le secrétaire,* *Le président,*

(sé) M.-H. BOULANGER (sé) P. THOMAS

Drukkerij-Imprimerie SCHAUBROECK — 9810 NAZARETH