

# SÉNAT DE BELGIQUE

---

SESSION DE 1999-2000

---

28 JUIN 2000

**Projet de loi relative  
à la criminalité informatique**

---

**AMENDEMENTS**

N° 1 DE MME NYSSSENS

Art. 14

**Au 1<sup>o</sup> de cet article, remplacer les mots « ne peut jamais être inférieur à 12 mois » par les mots « ne peut être supérieur à 12 mois ».**

Justification

Le texte prévoit l'obligation pour les opérateurs de conserver les données d'appel de moyens de télécommunications pendant un certain délai. Ce délai est déterminé par arrêté royal en Conseil des ministres et après avis de la Commission de la protection de la vie privée, et ne peut jamais être inférieur à 12 mois. Ce délai minimal d'un an est trop long. Il représente une charge trop lourde pour l'opérateur. En outre, il n'est pas sain de conserver aussi longtemps des données personnelles au regard de la protection de la vie privée.

---

*Voir:*

Documents du Sénat:

2-392 - 1999/2000:

N° 1: Projet transmis par la Chambre des représentants.

# BELGISCHE SENAAAT

---

ZITTING 1999-2000

---

28 JUNI 2000

**Wetsontwerp inzake  
informatiecriminaliteit**

---

**AMENDEMENTEN**

Nr. 1 VAN MEVROUW NYSSSENS

Art. 14

**In het 1<sup>o</sup> van dit artikel de woorden « en mag nooit minder zijn dan 12 maanden » vervangen door de woorden « en mag nooit meer zijn dan 12 maanden ».**

Verantwoording

De tekst bepaalt dat de operatoren verplicht zijn de oproepgegevens van telecommunicatiemiddelen gedurende een bepaalde termijn te bewaren. Deze termijn, die nooit minder mag zijn dan 12 maanden, wordt bepaald bij een koninklijk besluit vastgesteld na overleg in de Ministerraad en nadat het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer is ingewonnen. Deze minimumtermijn legt de operatoren een te zware last op want een jaar is te lang. Bovendien is het vanwege de bescherming van de persoonlijke levenssfeer niet wenselijk persoonlijke gegevens zo lang te bewaren.

---

*Zie:*

Stukken van de Senaat:

2-392 - 1999/2000:

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

## N° 2 DE M. VAN QUICKENBORNE

## Art. 14

**Au 1<sup>o</sup> de cet article, entre le mot «télécommunications.» et les mots «Ce délai est déterminé ...», insérer la phrase suivante :**

*«Les données d'appel et d'identification seront définies par arrêté délibéré en Conseil des ministres, sur avis de la Commission de la protection de la vie privée.»*

## Justification

Afin d'avoir l'assurance que la signification exacte des données précitées, telle qu'elle sera définie par le Roi, est compatible avec le respect de la vie privée, la Commission de la protection de la vie privée doit être consultée pour avis.

Le représentant du ministre a accepté de tenir compte de cette préoccupation, qui s'inscrit dans le droit fil du texte initial du projet de loi.

## N° 3 DE M. VAN QUICKENBORNE ET CONSORTS

## Art. 6

**Remplacer l'article 550bis, § 1<sup>er</sup>, proposé parce qu'il suit :**

*« § 1<sup>er</sup>. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, dans une intention frauduleuse ou à dessein de nuire, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement. »*

## Justification

1) Le chapitre II du projet de loi en discussion crée un certain nombre d'infractions. Pour être punissable, chacune de ces infractions nouvelles requiert explicitement une intention frauduleuse, le dessein de nuire ou une volonté d'enrichissement. Seul l'alinéa 1<sup>er</sup>, § 1<sup>er</sup>, de l'article 550bis nouveau ne prévoit pas cette condition. Il s'agit de l'infraction d'accès illicite à un système informatique.

2) En outre, le présent amendement crée un parallélisme avec le § 2 de l'article.

## Nr. 2 VAN DE HEER VAN QUICKENBORNE

## Art. 14

**In het 1<sup>o</sup> van dit artikel, tussen het woord «... Participaties.» en de woorden «Deze termijn wordt bepaald...» de volgende zin invoegen :**

*«De oproepingsgegevens en de identificatiegegevens worden bepaald bij een in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.»*

## Verantwoording

Teneinde zekerheid te bekomen dat de privacy wordt gerespecteerd bij de bepaling door de Koning van de exacte betekenis van genoemde gegevens, moet het advies ingewonnen worden van de Commissie voor de bescherming van de persoonlijke levenssfeer.

De vertegenwoordiger van de minister heeft zijn instemming met deze bekommernis laten blijken na verwijzing naar de oorspronkelijke tekst van het wetsontwerp.

Vincent VAN QUICKENBORNE.

## Nr. 3 VAN DE HEER VAN QUICKENBORNE C.S.

## Art. 6

**Het voorgestelde artikel 550bis, § 1, vervangen als volgt :**

*« § 1. Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, met bedrieglijk opzet of met het oogmerk om te schaden zich toegang verschafft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van drie maanden tot een jaar en met geldboete van zesentwintig frank tot vijfentwintigduizend frank of met een van die straffen alleen. »*

## Verantwoording

1) Hoofdstuk II van het voorliggend wetsontwerp voert een aantal nieuwe incriminaties in. Bij elk van deze nieuwe misdrijven wordt uitdrukkelijk een bedrieglijk opzet, een oogmerk om te schaden of een verrijking vereist teneinde de strafbaarheid toe te staan. Enkel bij het nieuwe artikel 550bis komt deze voorwaarde te vervallen in het eerste lid van de eerste paragraaf. Het betreft het misdrijf van de ongeoorloofde toegang tot een informaticasysteem.

2) Bovendien wordt een parallellisme ingebouwd met § 2 van het artikel.

Vincent VAN QUICKENBORNE.  
Nathalie de T'SERCLAES.  
Jean-François ISTASSE.

## N° 4 DU GOUVERNEMENT

## Art. 7

**L'article 39 bis proposé est remplacé comme suit :**

« Article 39bis. — § 1<sup>er</sup>. Sans préjudice des dispositions spécifiques de cet article, les règles de ce Code relatives à la saisie, y compris l'article 28sexies, sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données stockées dans un système informatique.

§ 2. Lorsque le procureur du Roi découvre dans un système informatique des données stockées qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, mais que la saisie du support n'est néanmoins pas souhaitable, ces données, de même que les données nécessaires pour les comprendre, sont copiées sur des supports qui appartiennent à l'autorité. En cas d'urgence ou pour des raisons techniques, il peut être fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

§ 3. Il utilise en outre les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

Si ces données 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, ces données sont seulement copiées et elles sont ensuite retirées du système informatique.

Il peut cependant, sauf dans le cas prévu à l'alinéa précédent, autoriser l'usage ultérieur de l'ensemble ou d'une partie de ces données, lorsque cela ne présente pas de danger pour l'exercice des poursuites.

§ 4. Lorsque la mesure prévue au § 2 n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens techniques appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui sont à la disposition de personnes autorisées à utiliser le système informatique, de même que pour garantir leur intégrité.

§ 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, rendues inaccessibles ou retirées.

## Nr. 4 VAN DE REGERING

## Art. 7

**Het voorgestelde artikel 39 bis vervangen als volgt :**

Artikel 39bis. — § 1. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels van dit Wetboek inzake inbeslagneming, met inbegrip van artikel 28sexies, van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van in een informaticasysteem opgeslagen gegevens.

§ 2. Wanneer de procureur des Konings in een informaticasysteem opgeslagen gegevens aantreft die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, maar de inbeslagneming van de drager daarvan evenwel niet wenselijk is worden deze gegevens, evenals de gegevens noodzakelijk om deze te kunnen verstaan, gekopieerd op dragers, die toebehoren aan de overheid. In geval van dringendheid of om technische redenen, kan gebruik gemaakt worden van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

§ 3. Hij wendt bovendien de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

Indien deze 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, worden deze gegevens enkel gekopieerd en worden zij daarna uit het informaticasysteem verwijderd.

Hij kan evenwel, behoudens in het geval bedoeld in het vorige lid, het verdere gebruik van het geheel of een deel van deze gegevens toestaan, wanneer dit geen gevaar voor de strafvordering oplevert.

§ 4. Wanneer de in § 2 vermelde maatregel niet mogelijk is om technische redenen of wegens de omvang van de gegevens, wendt hij de passende technische middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen en hun integriteit te waarborgen.

§ 5. De procureur des Konings brengt de verantwoordelijke van het informaticasysteem op de hoogte van de zoeking in het informaticasysteem en deelt hem een samenvatting mee van de gegevens die zijn gekopieerd, ontoegankelijk zijn gemaakt of verwijderd.

§ 6. *Le procureur du Roi utilise 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.*

*La même règle s'applique, lorsque des données qui sont stockées, traitées ou transmises dans un système informatique sont saisies avec leur support, conformément aux articles précédents. »*

#### Justification

Cet amendement du gouvernement vise à rendre la structure de la disposition plus claire et à en préciser le contenu sur un certain nombre de points, tenant compte de l'adoption de l'amendement n° 2 de M. Erdman.

1. L'applicabilité des règles de droit commun en matière de saisie est posée comme principe et précisée.

2. Concernant les données qui sont retirées du système, il est précisé qu'elles sont d'abord copiées.

3. En ce qui concerne le fait d'empêcher l'accès et de garantir l'intégrité, les formulations du projet initial sont maintenues, afin de clairement distinguer les différentes hypothèses.

4. Concernant la conservation au greffe, il n'est pas fait référence aux modalités de l'article 90septies du Code d'instruction criminelle en matière d'interception de communications, et en particulier à la conservation sous pli scellé et les mentions dans un registre spécial. L'article 13 du projet prévoit justement en la matière le remplacement de principe de ces moyens par des techniques adéquates plus modernes qui offrent d'ailleurs plus de garanties. Le projet impose néanmoins une responsabilité claire aux greffes de conserver les données saisies de façon adéquate afin de garantir la qualité des éléments de preuve.

*Le ministre de la Justice,*

Marc VERWILGHEN.

N° 5 DE M. VANDENBERGHE ET MME NYSSSENS

#### Art. 6

**À l'article 550bis, § 1<sup>er</sup>, proposé, apporter les modifications suivantes :**

**A. À l'alinéa 1<sup>er</sup>, insérer les mots « , avec une intention frauduleuse ou dans le but de nuire » entre les mots « Celui qui » et les mots « sachant qu'il n'y est pas autorisé ».**

**B. Supprimer l'alinéa 2.**

#### Justification

Quiconque accède à un système informatique en outrepassant son pouvoir n'est punissable que lorsqu'il agit avec une intention

§ 6. *De procureur des Konings wendt de passende technische middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen.*

*Gepaste technische middelen worden aangewend voor de bewaring hiervan op de griffie.*

*Hetzelfde geldt, wanneer gegevens die worden opgeslagen, verwerkt of overgedragen in een informatiesysteem, samen met hun drager in beslag worden genomen, overeenkomstig de vorige artikelen. »*

#### Verantwoording

Dit amendement van de regering strekt ertoe de structuur van de bepaling te verhelderen en de inhoud op een aantal punten duidelijker te maken, rekening houdend met de aanneming van het amendement nr. 2 van de heer Erdman.

1. De principiële toepasselijkheid van de gemeenrechtelijke regels inzake inbeslagneming wordt vooropgesteld en gepreciseerd.

2. Inzake de gegevens die uit het systeem worden verwijderd, wordt geëxpliciteerd dat deze eerst worden gekopieerd.

3. Wat het verhinderen van de toegang en het vrijwaren van de integriteit betreft, worden de formuleringen uit het oorspronkelijk ontwerp gehandhaafd, teneinde de verschillende hypothesen duidelijk te onderscheiden.

4. Inzake de bewaring ter griffie wordt niet verwezen naar de modaliteiten van artikel 90septies van het Wetboek van strafvordering met betrekking tot het afluisteren van communicatie, in het bijzonder het bewaren onder verzegelde omslag en het bijhouden van een register met een aantal vermeldingen. Artikel 13 van het ontwerp voorziet ter zake juist in de principiële vervanging hiervan door passende moderne technieken die overigens meer garanties bieden. Het ontwerp legt evenwel een duidelijke verantwoordelijkheid bij de griffies om de in beslag genomen data adequaat te bewaren teneinde de kwaliteit van het bewijsmateriaal te vrijwaren.

*De minister van Justitie,*

Nr. 5 VAN DE HEER VANDENBERGHE EN MEVROUW NYSSSENS

#### Art. 6

**In het voorgestelde artikel 550bis, § 1, de volgende wijzigingen aanbrengen :**

**A. In het eerste lid de woorden « , met bedrieglijk opzet of met het oogmerk om te schaden » invoegen tussen de woorden « Hij die » en de woorden « , terwijl hij weet dat ».**

**B. Het tweede lid doen vervallen.**

#### Verantwoording

Iemand die zich toegang verschafft tot het computersysteem door overschrijding van zijn bevoegdheid is slechts strafbaar

frauduleuse ou dans le but de nuire (voir le § 2 de l'article 550bis proposé). Celui qui n'a pas accès à un tel système mais qui force cet accès est par contre toujours punissable, même s'il n'agit pas avec une intention frauduleuse ou dans le but de nuire (§ 1<sup>er</sup> de l'article 550bis proposé).

Le Conseil d'État a relevé qu'il y a là «deux poids deux mesures» ce qui, vu l'absence de motifs objectifs, soulève la question de la compatibilité de cette disposition avec le principe d'égalité (voir doc. Chambre, 1999/2000, n° 213/001, p. 52).

De fait, aucun motif objectif ne paraît justifier cette distinction. Au contraire, le droit pénal punit souvent plus lourdement les personnes qui abusent de la confiance dont elles jouissent. C'est ainsi qu'un vol, par exemple, est sanctionné plus lourdement lorsqu'il est le fait d'un domestique ou d'un homme de service à gages envers son maître (article 64 du Code pénal). Par analogie, toute personne qui accède à un système informatique en abusant de ses droits d'accès doit être sanctionnée plus lourdement que la personne qui ne dispose pas de tel droit.

## N° 6 DE M. VANDENBERGHE ET MME NYSSSENS

### Art. 8

**À l'article 88ter, § 1<sup>er</sup>, deuxième tiret, proposé, remplacer les mots «ou s'il existe un risque que,» par les mots «et s'il existe un risque que».**

#### Justification

Voir l'avis de la Commission de la protection de la vie privée (doc. Chambre, 1999/2000, n° 213/004, p. 90):

«La commission est d'avis que l'extension de la perquisition à d'autres systèmes informatiques ne devrait pouvoir être effectuée que si les conditions énoncées dans la disposition proposée sont présentes de façon cumulative.»

Il convient dès lors de remplacer le mot «ou» figurant dans le texte par le mot «et».

## N° 7 DE M. VANDENBERGHE ET MME NYSSSENS

### Art. 8

**Supprimer le deuxième alinéa du § 3 de l'article 88ter proposé.**

#### Justification

Le deuxième alinéa du § 3 de l'article 88ter proposé autorise le juge d'instruction à copier des données qui ne se trouvent pas sur le territoire du Royaume.

Cette disposition est contraire au droit international, comme le relève l'avis du Conseil d'État:

«Parmi les règles fondamentales du droit international figure celle selon laquelle l'État exerce l'autorité étatique sur son propre

wanneer hij handelt met bedrieglijk opzet of met het oogmerk om te schaden (zie § 2 van het voorgestelde artikel 550bis). Diegene die geen toegang heeft maar zich deze toch verschafft is daarentegen steeds strafbaar, ook al handelt hij niet met bedrieglijk opzet of met het oogmerk om te schaden (§ 1 van het voorgestelde artikel 550bis).

De Raad van State heeft opgemerkt dat aldus «met twee maten wordt gemeten», waardoor, bij gebreke aan objectieve redenen, zich de vraag stelt naar het gelijkheidsbeginsel (Stuk Kamer, 1999/2000, nr. 213/001, blz. 52).

Objectieve redenen voor het onderscheid lijken inderdaad niet voorhanden te zijn. Integendeel het strafrecht bestraft personen die misbruik maken van het vertrouwen dat zij genieten veelal zwaarder. Zo bijvoorbeeld wordt een diefstal zwaarder gestraft wanneer deze gebeurt door een dienstbode of een loondienaar ten nadele van zijn meester (artikel 64 van het Strafwetboek). Naar analogie dient dan ook eerder de persoon die zich toegang verschafft tot een computersysteem door misbruik te maken van zijn toegangsbevoegdheid zwaarder te worden gestraft dan diegene die niet over een dergelijke bevoegdheid beschikt.

## Nr. 6 VAN DE HEER VANDENBERGHE EN MEVROUW NYSSSENS

### Art. 8

**In het voorgestelde artikel 88ter, § 1, tweede streepje, de woorden «of indien er een risico bestaat» vervangen door de woorden «en indien er een risico bestaat».**

#### Verantwoording

Zie het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer (Stuk Kamer, 1999/2000, nr. 213/004, blz. 90):

«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.»

Het woord «of» in de tekst dient derhalve te worden vervangen door het woord «en».

## Nr. 7 VAN DE HEER VANDENBERGHE EN MEVROUW NYSSSENS

### Art. 8

**Het tweede lid van § 3 van het voorgestelde artikel 88ter doen vervallen.**

#### Verantwoording

Het tweede lid van § 3 van het voorgestelde artikel 88ter laat aan de onderzoeksrechter toe gegevens te kopiëren die zich niet bevinden op het grondgebied van het Rijk.

Een dergelijke bepaling is strijdig met het internationaal recht, zoals aangegeven in het advies van de Raad van State:

«Een van de fundamentele regels van het internationaal recht bepaalt dat een Staat staatsgezag uitoefent op zijn eigen grondge-

territoire, et le fait seul, à l'exclusion de tout autre État. (...). Un État ne peut ainsi, en dehors de son territoire, ni procéder à une arrestation, ni dresser un procès-verbal constatant un délit, ni mener une enquête, etc. La jurisprudence internationale est, sur ce point, constante» (doc. Chambre, n° 213/001, 99/00, p. 45).

«L'obligation de se restreindre à la seule copie des données situées à l'étranger, et le devoir fait au juge d'informer le ministère de la Justice pour que ce dernier avise à son tour les autorités étrangères compétentes, ne suffisent pas à rendre une telle investigation compatible avec la règle de droit international ci-dessus rappelée. La «*hot pursuit*», institution traditionnelle du droit maritime international, à laquelle le commentaire de l'article 88<sup>ter</sup> fait une allusion, sans doute métaphorique, ne suffit pas davantage» (doc. Chambre, n° 213/001, 99/00, p. 46).

De plus, en vertu de l'article 4 du Code pénal, les infractions commises à l'étranger ne sont en principe pas punissables en Belgique. Comment justifier alors qu'un juge d'instruction puisse effectuer sur un système informatique étranger une recherche portant sur n'importe quel délit? Les délits «étrangers» que le juge d'instruction constaterait à l'occasion de cette recherche ne pourraient en effet pas être poursuivis par lui dès lors que l'intéressé ne pourra généralement pas être sanctionné à ce titre en application de l'article 4 du Code pénal.

Il convient dès lors de supprimer l'alinéa 2 du § 3 de l'article 88<sup>ter</sup> proposé.

## N° 8 DE MME TAELMAN

### Art. 14

**Au 1<sup>o</sup> de cet article, remplacer les mots «du Royaume» par les mots «de l'Union européenne».**

#### Justification

Il semble difficilement acceptable, à l'intérieur des frontières du marché unique européen, qu'un État membre prévienne que des données sont conservées sur son territoire.

L'Union doit anticiper dans le domaine de l'entraide judiciaire, afin que les autorités judiciaires aient facilement accès aux données nécessaires à la conduite d'une enquête pénale et ce, sur tout le territoire de l'Union.

## N° 9 DE M. VAN QUICKENBORNE

### Art. 6

**Remplacer l'article 550 bis, § 3, 1<sup>o</sup>, proposé, comme suit :**

«1<sup>o</sup> soit reprend de quelque manière que ce soit les données stockées, traitées ou transmises par le système informatique;»

bied, en dat alleen doet, zonder inmenging van enige andere Staat (...). Een Staat mag dus buiten zijn grondgebied geen arrestatie verrichten, noch een proces-verbaal opmaken waarbij een strafbaar feit wordt vastgesteld, noch een onderzoek doen, enz. Dit is vaste internationale rechtspraak» (Stuk Kamer, 1999/2000, nr. 213/001, blz. 45).

«De bepaling dat gegevens die zich in het buitenland bevinden, alleen mogen worden gekopieerd en dat de rechter het ministerie van Justitie dient te waarschuwen, dat op zijn beurt de bevoegde buitenlandse autoriteiten op de hoogte brengt, volstaat niet opdat zulk een onderzoek niet strijdig zal zijn met de regel van het internationaal recht waarnaar hierboven is verwezen. De *hot pursuit*, een traditionele rechtsinstelling in het internationale zeerecht, waarnaar, weliswaar op grond van analogie, in de bespreking van artikel 88<sup>ter</sup> verwezen wordt, is evenmin toereikend» (Stuk Kamer, 1999/2000, nr. 213/001, blz. 46).

Bovendien is het zo dat, blijkens artikel 4 van het Strafwetboek, in het buitenland gepleegde misdrijven in beginsel niet strafbaar zijn in België. Hoe kan men dan verantwoordelijk dat een onderzoeksrechter een zoeking zal mogen uitvoeren in een buitenlands informaticasysteem naar om het even welk misdrijf? De «buitenlandse» misdrijven die de onderzoeksrechter ter gelegenheid van de zoeking zou vaststellen, zullen door hem immers niet vervolgd kunnen worden vermits de betrokkene er in België, bij toepassing van artikel 4 van het Strafwetboek, in de regel niet voor kan worden gestraft.

Het tweede lid van § 3 van het voorgestelde artikel 88<sup>ter</sup> dient derhalve te worden geschrapt.

Hugo VANDENBERGHE.  
Clotilde NYSSSENS.

## Nr. 8 VAN MEVROUW TAELMAN

### Art. 14

**In het 1<sup>o</sup> van dit artikel de woorden «van het Rijk» vervangen door de woorden «van de Europese Unie».**

#### Verantwoording

Binnen de grenzen van de eengemaakte Europese markt lijkt het moeilijk aanvaardbaar dat een lidstaat bepaalt dat gegevens worden bewaard binnen zijn grenzen.

Door de Unie dient te worden vooruitgegaan op het vlak van wederzijdse rechtshulp, zodat op het hele grondgebied van de hele Unie, op een vlotte manier, de gerechtelijke autoriteiten de nodige gegevens in strafrechtelijke onderzoeken kunnen opvragen.

Martine TAELMAN.

## Nr. 9 VAN DE HEER VAN QUICKENBORNE

### Art. 6

**Het voorgestelde artikel 550 bis, § 3, 1<sup>o</sup>, vervangen als volgt :**

«1<sup>o</sup> hetzij de gegevens die worden opgeslagen, verwerkt of overgedragen via het informaticasysteem op enige manier overneemt;»

## Justification

Il ressort des questions au gouvernement que la circonstance aggravante prévue au 1<sup>o</sup> sera toujours réalisée dans les faits, dès lors que quiconque accède à un système informatique prend connaissance des données qui sont stockées, traitées ou transmises.

Cet amendement répond à la préoccupation du gouvernement pour ce qui est des personnes qui ont accédé à un système informatique et qui copient les données dont elles ont pris connaissance afin de pouvoir les réutiliser le cas échéant.

Cet amendement est parallèle à l'article 138a de la loi néerlandaise de 1993 relative à la criminalité informatique, qui qualifie également ce fait de circonstance aggravante.

N<sup>o</sup> 10 DE M. VAN QUICKENBORNE

## Art. 6

**Remplacer l'article 550bis, § 3, 2<sup>o</sup>, comme suit :**

« 2<sup>o</sup> soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert de ce système informatique pour accéder au système informatique d'un tiers; »

## Justification

Cet amendement formule plus clairement ce qui est visé par le gouvernement, à savoir l'auteur qui utilise un système dont il n'est pas propriétaire pour accéder de manière illicite au système informatique visé au § 1<sup>er</sup>. Un tel acte constitue une circonstance aggravante. Tel qu'il est libellé dans sa forme initiale, le texte donne l'impression que, dès l'instant où l'on se sert d'un système informatique, il y a lieu d'appliquer une peine aggravée. Or, le hacking et le cracking ne peuvent pas se faire sans ordinateur (F. Deryck, « *Is de wetgever met de wetsontwerpen inzake de informaticacriminaliteit on-line of off-line?* », studiedag VUB, mars 2000, à paraître).

De plus, par analogie avec la loi néerlandaise (article 138a), on a ajouté une circonstance aggravante dans le cas où l'accès illicite au système permet à son tour d'accéder au système d'un tiers.

N<sup>o</sup> 11 DE M. VAN QUICKENBORNE

## Art. 6

**Remplacer l'article 550bis, § 3, 3<sup>o</sup>, proposé, par la disposition suivante :**

« 3<sup>o</sup> soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées, traitées ou transmises par ce système informatique; »

## Justification

Cet amendement vise à apporter une petite modification au texte en renvoyant explicitement au système auquel on a accédé ou dans lequel on se maintient.

## Verantwoording

Uit de bevraging van de regering is gebleken dat de verzwarende omstandigheid voorzien in 1<sup>o</sup> de facto altijd zal gerealiseerd worden, aangezien eenieder die zich een toegang verschaft tot een informaticasysteem kennisneemt van gegevens die worden opgeslagen, verwerkt of overgedragen.

Dit amendement komt tegemoet aan de bezorgdheid van de regering tegenover personen die zich de toegang hebben verschaft en die de gegevens waarvan ze kennis hebben genomen, overnemen zodat ze desgevallend nog kunnen gebruikt worden.

Dit amendement loopt parallel met artikel 138a van de Nederlandse Wet computercriminaliteit van 1993 waar ook dit aange-merkt wordt als een verzwarende omstandigheid.

## Nr. 10 VAN DE HEER VAN QUICKENBORNE

## Art. 6

**Het voorgestelde artikel 550bis, § 3, 2<sup>o</sup>, vervangen als volgt :**

« 2<sup>o</sup> hetzij enig gebruik maakt van een informaticasysteem van een derde of door tussenkomst van het informaticasysteem de toegang verwerft tot een informaticasysteem van een derde; »

## Verantwoording

Dit amendement verwoordt op een duidelijker manier hetgeen de regering voor ogen heeft. Met name, de dader die gebruik maakt van een systeem waarvan hij geen eigenaar is om zich de ongeoorloofde toegang te verschaffen tot het informaticasysteem bedoeld in § 1. Dit maakt een verzwarende omstandigheid uit. De tekst zoals hij in de oorspronkelijke vorm gelibelleerd is, doet uitschijnen dat men vanaf het gebruik van een informaticasysteem verzwwaard gestraft moet worden. Hacking en cracking zonder computer bestaan echter niet (F. Deruyck, « *Is de wetgever met de wetsontwerpen inzake de informaticacriminaliteit on-line of off-line?* », studiedag VUB, maart 2000, te verschijnen).

Bovendien wordt, naar analogie met de Nederlandse wet (artikel 138a), een verzwarende omstandigheid toegevoegd in het geval dat de ongeoorloofde toegang tot het systeem op haar beurt toegang geeft tot een systeem van een derde.

## Nr. 11 VAN DE HEER VAN QUICKENBORNE

## Art. 6

**Het voorgestelde artikel 550bis, § 3, 3<sup>o</sup>, vervangen als volgt :**

« 3<sup>o</sup> hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die via het informaticasysteem worden opgeslagen, verwerkt of overgedragen; »

## Verantwoording

Dit amendement beoogt een kleine wijziging door expliciet te verwijzen naar het systeem waartoe men zich de toegang heeft verschaft of waarin men zich handhaaft.

On a choisi de maintenir la disposition concernant le dommage non intentionnel, étant donné que, par suite de l'amendement n° 3, il faut prouver que l'accusé a eu l'intention de nuire ou a agi par intention frauduleuse pour lui infliger la peine de base. Dans ce cas, l'intéressé doit se rendre compte que le dommage non intentionnel n'est pas excusable.

## N° 12 DE M. VAN QUICKENBORNE

### Art. 14

**Remplacer, au 1° de cet article, les mots « et ne peut jamais être inférieur à 12 mois » par les mots « et ne peut jamais être supérieur à 6 mois ».**

#### Justification

Le délai minimum doit devenir un délai maximum. Le texte en projet est diamétralement opposé à ce que dit l'avis du Conseil d'État. Le Conseil d'État souligne que les infractions au droit à la vie privée doivent être fondées sur un texte de loi et non pas sur un arrêté royal. Le projet de loi prévoit que les opérateurs doivent conserver les données pendant au moins 12 mois et implique que ce délai peut encore être prolongé par arrêté royal. Cet article ne limite donc aucunement la compétence du Roi d'imposer un délai de conservation. Au contraire, le texte permet au Roi de prolonger encore davantage le délai minimum légal.

En prévoyant un délai de conservation minimum de 12 mois, le législateur s'écarte des avis formulés par la Commission de la protection de la vie privée. Selon celle-ci, un délai de trois mois, comme on l'applique en Allemagne, est suffisant en pratique (avis n° 33/1999 du 13 décembre 1999). Le projet de loi prévoit que l'arrêté royal déterminant le délai de conservation final doit être soumis pour avis à la Commission de la protection de la vie privée. Comme celle-ci a déjà déclaré, dans son avis, qu'un délai de trois mois est suffisant, on peut en déduire que tout délai supérieur à 12 mois sera jugé trop long.

De plus, le délai de conservation proposé (12 mois) n'est pas du tout conforme au délai fixé dans les pays voisins. Le délai de conservation imposé par le législateur belge est nettement plus long que le délai imposé à cet effet par d'autres pays aux opérateurs de réseaux de télécommunications. À l'heure actuelle, peu de pays ont déjà défini dans quel délai les « données d'appel » doivent être conservées à des fins de maintien des lois. Les Pays-Bas sont le plus avancés en ce qui concerne l'emploi des données télécoms à des fins judiciaires. Cependant, le délai durant lequel les opérateurs doivent mettre les données à la disposition des autorités judiciaires n'est que de trois mois. En Allemagne aussi, on applique un délai de trois mois. En d'autres termes, en imposant un délai de 12 mois, la Belgique est leader absolu pour ce qui est de vider de son contenu le secret des télécommunications.

Ce délai de conservation ne tient pas compte des limites auxquelles sont soumis les opérateurs ni des dépenses que ceux-ci doivent consentir pour les surmonter. À l'heure actuelle, la plupart des opérateurs ne gardent pas leurs données plus de trois à six mois, comme l'a montré clairement l'audition des représentants des fournisseurs d'accès à l'internet.

Er is gekozen om de onopzettelijke schade die wordt veroorzaakt te behouden daar door amendement nr. 3, voor de basisstraf het oogmerk om te schaden of het bedrieglijk opzet in hoofde van de beschuldigde moet bewezen zijn. In dat geval moet hij of zij zich realiseren dat onopzettelijke schade niet verschoonbaar is.

## Nr. 12 VAN DE HEER VAN QUICKENBORNE

### Art. 14

**In het 1° van dit artikel de woorden « en mag nooit minder dan 12 maanden » vervangen door de woorden « en mag nooit meer zijn dan 6 maanden ».**

#### Verantwoording

De minimumtermijn moet een maximumtermijn worden. De ontwerp tekst staat haaks op het advies van de Raad van State. De Raad van State merkt op dat inbreuken op de persoonlijke levenssfeer hun grond moeten vinden in een wettekst en dus niet in een koninklijk besluit. Het wetsontwerp bepaalt dat de operatoren de gegevens minimum 12 maanden ter beschikking dienen te houden en impliceert dat deze termijn nog kan worden verlengd bij koninklijk besluit. Dit artikel formuleert dus op geen enkele wijze een beperking op de bevoegdheid van de Koning om een bewaartermijn op te leggen. Integendeel, de tekst verleent aan de Koning de bevoegdheid om de wettelijke minimumtermijn nog verder te verlengen.

Met het vaststellen van een minimumbewaartermijn van 12 maanden wijkt de wetgever af van de adviezen van de Privacy-Commissie. Volgens deze is een termijn van drie maanden zoals toegepast in Duitsland in de praktijk voldoende (advies nr. 33/1999 van 13 december 1999). Het wetsontwerp voorziet dat het koninklijk besluit dat de uiteindelijke bewaartermijn vaststelt dient te worden voorgelegd voor advies aan de Commissie voor de bescherming van de persoonlijke levenssfeer. Aangezien deze commissie reeds heeft geadviseerd dat een termijn van 3 maanden voldoende is, mag men ervan uitgaan dat iedere termijn langer dan 12 maanden te lang zal bevonden worden.

De vooropgestelde bewaartermijn (12 maanden) loopt bovendien helemaal niet parallel met hetgeen vastgelegd is in de andere naburige landen. De bewaartermijn die de Belgische wetgever oplegt gaat veel verder dan wat in andere landen voor deze doeleinden aan de telecomoperatoren wordt opgelegd. Weinig landen hebben op dit ogenblik reeds een termijn gedefinieerd gedurende dewelke « oproepgegevens » dienen bewaard te worden voor wetshandhavingsdoeleinden. Nederland staat vooraan in het gebruik van telecomgegevens voor gerechtelijke doeleinden. Niettemin bedraagt de termijn gedurende dewelke de operatoren hun gegevens ter beschikking dienen te houden van de gerechtelijke autoriteiten slechts drie maanden. Ook in Duitsland wordt een termijn van drie maanden toegepast. Met een termijn van 12 maanden, wordt België met andere woorden de absolute koploper op het vlak van de uitholling van het telecomgeheim.

De bewaartermijn houdt geen rekening met de beperkingen van de operatoren en de kosten die moeten worden gemaakt om deze beperkingen ongedaan te maken. Op dit ogenblik houden de meeste operatoren hun gegevens niet langer bij dan 3 tot 6 maanden. Dit is duidelijk gebleken uit de hoorzitting met de vertegenwoordigers van de Internet Service Providers.

Vincent VAN QUICKENBORNE.



## N° 13 DE MME de T'SERCLAES

## Art. 6

**À l'article 550bis, § 3, 3°, proposé, supprimer les mots « même non intentionnellement ».**

## Justification

À partir du moment où on se trouve dans le cas où l'intention est frauduleuse, il est inutile de prévoir le cas où le dommage créé pourrait être non intentionnel. Il est inutile de le préciser, cela va de soi.

Nathalie de T'SERCLAES.

## N° 14 DE MME KAÇAR

## Art. 14

**Au 1<sup>o</sup> de cet article, remplacer la dernière phrase de l'alinéa 1<sup>er</sup> comme suit :**

*« Ce délai est fixé à 12 mois. »*

## Justification

Pour la sécurité juridique, il y a lieu d'appliquer un délai minimum comme un délai maximum. Étant donné que la loi sur la protection de la vie privée est applicable également, la conservation des données en question pendant le délai de 12 mois n'est utile que dans le cadre d'une instruction judiciaire.

## N° 15 DE M. VAN QUICKENBORNE

(Sous-amendement à l'amendement n° 11)

## Art. 6

**Remplacer l'article 550bis, § 3, 3°, par le texte suivant :**

*« 3<sup>o</sup> soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées, traitées ou transmises par ce système, ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système. »*

## Justification

Ce sous-amendement répond à la nécessité d'explicitier le dommage possible, compte tenu de l'amendement n° 10.

## Nr. 13 VAN MEVROUW de T'SERCLAES

## Art. 6

**In § 3, 3°, van het voorgestelde artikel 50bis, de woorden « zelfs onopzettelijk » doen vervallen.**

## Verantwoording

Zodra er sprake is van bedrieglijk opzet, is het overbodig te bepalen wat er moet gebeuren indien de schade onopzettelijk zou zijn veroorzaakt. Zoiets moet niet worden bepaald. Het gaat immers om een vanzelfsprekende zaak.

## Nr. 14 VAN MEVROUW KAÇAR

## Art. 14

**In het 1<sup>o</sup> van dit artikel, de laatste zin van het eerste lid vervangen als volgt :**

*« Deze termijn wordt bepaald op 12 maanden. »*

## Verantwoording

Omwille van de rechtszekerheid dient zowel een minimum als een maximum termijn te worden gehanteerd. Aangezien de wet op bewaring van de privacygegevens ook hierop van toepassing is, is de bewaring van desbetreffende gegevens gedurende deze termijn van 12 maanden enkel dienstig in het kader van het gerechtelijk onderzoek.

Meryem KAÇAR.

## Nr. 15 VAN DE HEER VAN QUICKENBORNE

(Subamendement op amendement nr. 11)

## Art. 6

**Het voorgestelde artikel 550bis, § 3, 3°, vervangen als volgt :**

*« 3<sup>o</sup> hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan het informaticasysteem of aan de gegevens die via het informaticasysteem worden opgeslagen, verwerkt of overgedragen, of aan een informaticasysteem van een derde of aan de gegevens via laatstgenoemd informaticasysteem worden opgeslagen, verwerkt of overgedragen. »*

## Verantwoording

Dit subamendement komt tegemoet aan de nood aan explicitering van mogelijke schade ten gevolge van amendement nr. 10.

Vincent VAN QUICKENBORNE.

## N° 16 DE MME NYSSENS

(Sous-amendement à l'amendement n° 5)

## Art. 6

**À l'article 550bis, § 1<sup>er</sup>, proposé, apporter les modifications suivantes :**

**A. Remplacer les mots** « sachant qu'il n'y est pas autorisé » **par les mots** « avec une intention frauduleuse ou dans le but de nuire ».

**B. Remplacer les mots** « trois mois » **par les mots** « six mois » **et les mots** « un an » **par les mots** « deux ans ».

**C. Supprimer l'alinéa 2.**

## Justification

Le texte proposé vise à instaurer un seuil d'incrimination plus élevé dans le cas du hacker interne (qui possède certains pouvoirs d'accès) par opposition au hacker externe (doc. Chambre, n° 213-001, 99-00, p. 16).

Or, au niveau du texte légal, aucun élément objectif ne permet de justifier *a priori* cette différence de traitement (voy. aussi en ce sens l'avis du Conseil d'État, doc. Chambre, n° 52, 99-00).

L'élément moral constitutif de l'infraction pénale doit donc être défini dans les mêmes termes par le législateur (et les peines doivent être identiques). En revanche, cela n'empêche nullement les cours et tribunaux d'apprécier différemment, c'est-à-dire plus ou moins sévèrement, des comportements selon qu'ils émanent de hackers externes ou de hackers internes. À cet égard, les termes légaux doivent permettre l'appréciation la plus large possible. Les mots « avec une intention frauduleuse ou dans un but de nuire » remplissent précisément cette fonction. Ils rendent notamment punissable l'accès en toute connaissance de cause au système sans y avoir droit (en ce sens, *Lamy informatique 2000*, n° 3120, p. 1765).

Clotilde NYSSENS.

## N° 17 DE M. VAN QUICKENBORNE

(Sous-amendement à l'amendement n° 4 du gouvernement)

## Art. 7

**Remplacer le § 3, alinéa 2, de l'article 39bis proposé, comme suit :**

« § 3. Si les données constituent l'objet du délit ou son résultat et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité des systèmes informatiques ou pour des données stockées, traitées ou transmises par le biais de tels systèmes, le procureur du Roi utilise tous les moyens techniques appropriés pour rendre ces données inaccessibles. »

## Nr. 16 VAN MEVROUW NYSSENS

(Subamendement op amendement nr. 5)

## Art. 6

**In § 1 van het voorgestelde artikel 550bis de volgende wijzigingen aanbrengen :**

**A. De woorden** « terwijl het weet dat hij daartoe niet gerechtigd is » **vervangen door de woorden** « met bedrieglijk opzet of met het oogmerk om te schaden ».

**B. De woorden** « drie maanden » **vervangen door de woorden** « zes maanden » **en de woorden** « een jaar » **vervangen door de woorden** « twee jaar ».

**C. Het tweede lid doen vervallen.**

## Verantwoording

De voorgestelde tekst trekt ertoe de strafbaarheidsdrempel hoger te leggen voor insiders (die bepaalde toegangsbevoegdheden hebben) dan voor buitenstaanders (Stuk Kamer, nr. 213-001, 99-00, blz. 16).

Dit verschil in behandeling kan door geen enkel objectief gegeven worden verantwoord (zie ook het advies van de Raad van State, Stuk Kamer, nr. 52, 99-00).

Het moreel gegeven dat bepalend is voor de strafbaarstelling moet door de wetgever dus in dezelfde bewoordingen worden gedefinieerd (en de straffen moeten dezelfde zijn). Dit doet geenszins afbreuk aan de vrijheid van de hoven en rechtbanken die bepaalde gedragingen strenger of minder streng kunnen beoordelen naargelang het gaat om buitenstaanders of insiders die het systeem binnendringen. De formulering van de wet moet een zo ruim mogelijke beoordeling mogelijk maken. De woorden « met bedrieglijk opzet of met het oogmerk om te schaden » vervullen precies die functie. Zij maken de bewuste wederrechtelijke toegang tot het systeem strafbaar (zie hiervoor *Lamy informatique 2000*, nr. 3120, blz. 1765).

## Nr. 17 VAN DE HEER VAN QUICKENBORNE

(Subamendement op amendement nr. 4 van de regering)

## Art. 7

**Paragraaf 3, tweede lid, van het voorgestelde artikel 39bis vervangen als volgt :**

« § 3. Indien de gegevens het voorwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en indien de 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 deze gegevens ontoegankelijk te maken. »

## Justification

La modification proposée par l'amendement n° 4 du gouvernement semble porter atteinte au pouvoir de décision du juge indépendant lorsque celui-ci rend son jugement matériel final sur le fait, et ce, précisément à cause du mot «retirer». Dans ce sens, le sous-amendement rejoint la justification de M. Erdman relative à son amendement n° 2. Seul un juge indépendant peut annuler et supprimer des données.

De plus, l'expression «rendre inaccessible» a une acception suffisamment large pour autoriser le procureur du Roi à prendre diverses mesures. Nous renvoyons à cet égard au nouvel article 125o proposé du Code d'instruction criminelle néerlandais, où elle est considérée comme la plus neutre techniquement: «par les mots «rendre les données inaccessibles» il faut entendre la prise de mesures visant à éviter que le gestionnaire du système informatique ou des tiers ne prennent connaissance ou ne fassent usage de ces données ainsi que la prise de mesures visant à éviter la diffusion desdites données. «Rendre des données inaccessibles» englobe l'élimination (effacement) des fichiers concernés avec conservation d'une copie pour la Justice» (article 125o, alinéa 2).

Il s'agit de la mesure la plus évidente. La définition de l'expression «rendre des données inaccessibles» permet en outre de prendre toutes sortes d'autres mesures, pourvu qu'elles tendent à éviter toute nouvelle consultation, etc. de ces données. Une telle mesure consistera, par exemple, à installer, à l'aide des techniques d'encryptage, un véritable «cadenas» sur les fichiers concernés, de telle sorte que le gestionnaire et les autres utilisateurs de l'ordinateur n'y aient plus accès. Il est aussi imaginable, par exemple, que l'on rende le port d'accès à l'ordinateur concerné (momentanément) inutilisable. Dans chaque situation, il faudra apprécier quelle est la mesure la plus efficace.

N° 18 DE MME DE T'SERCLAES

## Art. 8

**À l'article 88ter, § 1<sup>er</sup>, proposé, remplacer les mots «soit dans le cadre d'une perquisition soit autrement» par les mots «dans le cadre d'une perquisition».**

## Justification

Si nous nous trouvons bien dans l'hypothèse d'un mandat de perquisition ordonné par un juge d'instruction et que le paragraphe vise la possibilité d'étendre la recherche vers un système informatique qui se trouve dans un autre lieu, les mots «soit autrement» n'ajoutent rien au texte. Ils permettraient par contre de couvrir des actes d'instruction non spécifiés, ce que l'on ne peut accepter sur le plan des principes.

Nathalie de T'SERCLAES.

N° 19 DE MME TAELMAN

## Art. 14

**Au 1<sup>o</sup> de cet article, supprimer le dernier alinéa proposé.**

## Verantwoording

De voorgestelde wijziging door het amendement nr. 4 van de regering lijkt afbreuk te doen aan de beslissingsmacht van de onafhankelijke rechter bij een materiële einduitspraak over het feit, precies door het woord «verwijderen». In die zin sluit het sub-amendement aan bij de verantwoording van de heer Erdman bij zijn amendement nr. 2. Enkel een onafhankelijke rechter kan gegevens vernietigen en verwijderen.

Bovendien zijn de woorden «ontoegankelijk maken» voldoende ruim om verschillende maatregelen toe te staan aan de procureur des Konings. Hiervoor zij gerefereerd aan het nieuw voorgestelde artikel 125o Strafvordering in Nederland waar men «ontoegankelijk maken» al meest technisch onafhankelijk aanziet: «Onder ontoegankelijkmaking van gegevens» wordt verstaan het treffen van maatregelen ter voorkoming dat de beheerder van dat geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen (wissen) van de betrokken bestanden, met behoud van een kopie voor Justitie (artikel 125o, tweede lid).

Dit is de meest voor de hand liggende maatregel. De definitie van ontoegankelijkmaking laat daarnaast echter allerlei andere maatregelen toe, mits die kunnen strekken ter voorkoming van de verdere kennisneming enz. van die gegevens. Een voorbeeld van zulke andere maatregelen is het met behulp van zogenaamde encryptietechnieken als het ware een «slot» zetten op de betrokken bestanden, zodat de beheerder en andere gebruikers van de computer er geen toegang meer toe hebben. Daarnaast is bijvoorbeeld denkbaar dat de toegangspoort van de betrokken computer (tijdelijk) onbruikbaar wordt gemaakt. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is.

Vincent VAN QUICKENBORNE.

Nr. 18 VAN MEVROUW DE T'SERCLAES

## Art. 8

**In § 1 van het voorgestelde artikel 88ter de woorden «hetzij in het kader van een huiszoeking, hetzij anderszins», vervangen door de woorden «in het kader van een huiszoeking».**

## Verantwoording

Indien de voorgestelde paragraaf, in geval van een huiszoeking bevolen door een onderzoeksrechter, voorziet in de mogelijkheid om de zoeking uit te breiden naar een informaticasysteem dat zich op een andere plaats bevindt, zijn de woorden «hetzij anderszins» overbodig. De toevoeging van die woorden zou niet nader gespecificeerde onderzoekshandelingen kunnen dekken, wat principieel onaanvaardbaar is.

Nr. 19 VAN MEVROUW TAELMAN

## Art. 14

**In het 1<sup>o</sup> van dit artikel het voorgestelde laatste lid doen vervallen.**

## Justification

Cet amendement vise à éviter d'imposer des restrictions inutiles à la vie économique. Il est néanmoins évident que les données visées doivent être mises à la disposition des autorités compétentes, quand une demande à cet effet est faite dans le cadre des mesures visées aux articles 46*bis* et 88*bis* du Code d'instruction criminelle.

## Verantwoording

Dit amendement strekt ertoe te vermijden dat nodeloze beperkingen aan het economische leven worden opgelegd. Het is evenwel vanzelfsprekend dat de bedoelde gegevens in België beschikbaar moeten worden gesteld aan de bevoegde overheden, wanneer hierom wordt verzocht in het kader van de maatregelen bedoeld in de artikelen 46*bis* en 88*bis* van het Wetboek van Strafvordering.

Martine Taelman.