DOC 50 **0213/001**
DOC 50 **0214/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

3 november 1999

WETSONTWERP

inzake informaticacriminaliteit
(Nr 213/1) (I)

WETSONTWERP

inzake informaticacriminaliteit
(Nr 214/1) (II)

DOC 50 **0213/001**
DOC 50 **0214/001**

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

3 novembre 1999

PROJET DE LOI

relatif à la criminalité informatique
(N° 213/1) (I)

PROJET DE LOI

relatif à la criminalité informatique
(N° 214/1) (II)

SAMENVATTING

De ministers van Justitie, van Telecommunicatie en Overheidsbedrijven en Participaties en van Economie dienen een wetsontwerp in inzake informaticacriminaliteit.

Het gaat hier om delicten die een inbreuk plegen op de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen of de gegevens die daarin worden opgeslagen, verwerkt of overgedragen.

Daartoe wordt een nieuwe titel toegevoegd aan het Strafwetboek waarin specifieke computer- en telecommunicatiemisdrijven strafbaar worden gesteld. Daaronder vallen de hoofdstukken valsheid in informatica, informaticabedrog, ongeoorloofde toegang tot het systeem en data- en informaticasabotage.

Er zijn ook nieuwe opsporingstechnieken voorzien zoals databeslag, medewerkingsverplichtingen, netwerkzoeking, interceptie van communicatie.

Inbreuken worden bestraft met geldboetes tussen de 26 Belgische frank en 200 000 Belgische frank (x 20) en/of gevangenisstraf tussen de 3 maand en 5 jaar.

Straffen worden verdubbeld indien ze worden begaan binnen de 5 jaar na een eerste veroordeling voor eenzelfde feit.

RÉSUMÉ

Le ministre de la Justice, le ministre des Télécommunications et des Entreprises et Participations publiques et le ministre de l'Économie déposent un projet de loi relatif à la criminalité informatique.

Ce projet englobe les délits qui constituent une infraction contre 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.

À cet effet, un nouveau titre est ajouté au Code pénal où les délits d'informatique et de télécommunications spécifiques sont pénalisés. Ce titre comprend les chapitres sur les faux en informatique, la fraude informatique et l'accès non-autorisé au système et le sabotage de données informatiques.

Des nouvelles techniques de dépistage comme la confiscation des données, l'obligation de coopération, la recherche de réseau et l'interception des communications sont également prévues.

Les auteurs de ces infractions sont punis d'une amende de 26 francs belges à 200 000 francs belges (x 20) et/ou d'un emprisonnement de trois mois à cinq ans.

Les peines sont doublées lorsque les infractions sont commises endéans une période de 5 ans après une première condamnation pour un même délit.

Wetsontwerp nr 213/001 : aangelegenheid bedoeld in artikel 78 van de Grondwet.
Wetsontwerp nr 214/001 : aangelegenheid bedoeld in artikel 77 van de Grondwet.

Projet de loi n° 213/001 : matière visée à l'article 78 de la Constitution.

Projet de loi n° 214/001 : matière visée à l'article 77 de la Constitution.

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

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

De ontwikkeling van de informatietechnologie (hierna : IT) heeft een steeds ingrijpender invloed op de wijze waarop de samenleving evolueert. Het is dan ook niet verwonderlijk dat op verschillende internationale fora over de jaren heen het bewustzijn van de verschillende juridische implicaties van de IT toeneemt. Zo moet worden vastgesteld dat men in verschillende rechtstakken verplicht is na te gaan of de klassieke juridische begrippen in staat zijn de nieuwe problemen die samenhangen met de IT op te vangen.

Dit geldt uiteraard ook voor het strafrecht. De mogelijkheden om gegevens massaal en zeer snel over te brengen van een locatie naar een andere of ze wereldwijd te verspreiden kunnen immers zowel voor legitieme als voor criminele doeleinden worden aangewend. De fysische grenzen van nationale staten vormen in dat opzicht geen obstakel voor de informatiesnelweg. Dit is echter wel het geval voor de diensten die belast zijn met de bestrijding van de criminaliteit. Hun bevoegdheden stoppen aan de landsgrenzen.

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

Het ontwerp van wet verzekert in dit verband de continuïteit met het wetgevend initiatief dat onder de vorige legislatuur door de toenmalige minister van Justitie werd genomen en waarover de Raad van State reeds een advies heeft uitgebracht. De regering is immers van oordeel dat de recente gebeurtenissen ten overvloede hebben aangetoond dat de strafrechtelijke bescherming van de netwerken zowel in het licht van de belangen van de overheid, de bedrijven en de particulieren een belangrijke beleidsprioriteit moet zijn die een dringend wetgevend optreden noodzakelijk maakt.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

L'évolution de la technologie de l'information influence de plus en plus la façon dont évolue la société. Il n'est dès lors pas étonnant d'assister au fil des différents forums internationaux de ces dernières années, à une véritable prise de conscience des différentes implications juridiques de la technologie de l'information. Force est de constater que nous sommes obligés d'examiner, dans le cadre de différentes branches juridiques, si les concepts juridiques classiques permettent de répondre aux nouveaux problèmes liés à la technologie de l'information.

Il en va évidemment de même pour le droit pénal. Les possibilités de transmission massive et très rapide de données d'un lieu à un autre ou de diffusion de ces données dans le monde entier peuvent, en effet, être utilisées, tant à des fins légitimes que criminelles. Dans cette optique, les frontières physiques des états nationaux ne constituent pas un obstacle aux autoroutes de l'information. Ceci est cependant le cas pour les services qui sont chargés de lutter contre la criminalité. Leurs compétences s'arrêtent aux frontières du pays.

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

À cet égard, le projet de loi assure la continuité par rapport à l'initiative législative prise sous la précédente législature par le ministre de la Justice de l'époque et qui a déjà fait l'objet d'un avis du Conseil d'État. Le gouvernement estime en effet que les récents événements ont démontré à suffisance que dans l'optique des intérêts de l'autorité, mais également des entreprises et des particuliers, la protection des réseaux d'un point de vue pénal doit constituer une priorité politique majeure qui requiert une intervention urgente sur le plan législatif.

A. ALGEMENE OVERWEGINGEN

1. **Het materieel strafrecht**

1.1. *Algemeen kader*

De vormen van criminaliteit waarbij gebruik wordt gemaakt van de meest moderne mogelijkheden van telecommunicatie en informatica zijn genoegzaam bekend. Hoewel er in deze sector waarschijnlijk een relatief hoog *« dark number »* is van misbruiken waarvan de slachtoffers om velerlei redenen geen aangifte doen bij de overheid, besteden de media in binnen- en buitenland geregeld ruime aandacht aan occasionele spectaculaire gevallen van computercriminaliteit. Overigens moet worden vastgesteld dat er in essentie voor heel wat « traditionele » misdrijven wel een « telematische » variant bestaat. Enkele voorbeelden kunnen dit illustreren. Zo kan het plaatsen van een « logische bom » in een vitaal computersysteem door terroristen worden aangewend als afpersingstechniek. Zo kunnen frauduleuze manipulaties van de doseringsgegevens voor het toedienen van geneesmiddelen in de computer van een ziekenhuis aan de basis liggen van het overlijden van patiënten. Zo kan eveneens het aanbieden van niet-bestaande diensten met de bedoeling geïnteresseerde klanten op te lichten, evenzeer plaatsvinden via telematicanetwerken als via meer klassieke praktijken.

Op internationaal vlak heeft men daarom reeds in de jaren ’80 onderzoek verricht om na te gaan of het bestaande materiële strafrecht soepel genoeg was om deze telematicacriminaliteit te absorberen. De werkzaamheden van de OESO en de Raad van Europa waren hier toonaangevend, en hebben ertoe geleid dat de meeste geïndustrialiseerde landen thans zijn overgegaan tot een herziening van hun nationale strafbepalingen. Daartoe werden bestaande bepalingen aangevuld of uitgebreid, of werden in sommige gevallen volledig nieuwe misdrijven voorzien.

In België werd vooralsnog niet overgegaan tot een algemene wettelijke revisie van de relevante strafbepalingen. Uit de bestaande rechtspraak en doctrine en uit specifiek beleidsvoorbereidend studiewerk blijkt evenwel dat hieruit niet mag worden afgeleid dat ons strafrecht op dit ogenblik volkomen machteloos staat tegenover vormen van criminaliteit die gericht zijn tegen of zich bedienen van de IT. Sectorieel, in het bijzonder op het domein van de sociale zekerheid en inzake de bescherming van persoonsgegevens, bestaan er bepalingen die gedurende het laatste decennium werden ingevoerd en die reeds een zekere bescherming bieden op dit domein. Op sommige andere gebieden blijken de bestaande incriminaties te volstaan, maar zijn het de opsporingsmogelijkheden die niet afdoende zijn; het gaat hier vooral om inhoudsgerichte delicten zoals expressie-

A. CONSIDÉRATIONS GÉNÉRALES

1. **Le droit pénal matériel**

1.1. *Cadre général*

Les formes de criminalité s’appuyant sur le recours aux moyens de télécommunication et informatiques aux possibilités plus modernes sont suffisamment connues. Bien qu’il y ait probablement dans ce secteur un « chiffre inconnu » relativement élevé de délits dont les victimes ne font pas de déposition auprès des autorités pour de multiples raisons, les médias prêtent régulièrement une grande attention à des cas spectaculaires occasionnels de criminalité informatique, tant en Belgique qu’à l’étranger. Par ailleurs, l’on doit constater qu’il existe une variante « télématique » pour bon nombre de délits « traditionnels ». Quelques exemples suffisent à illustrer cette réalité. Ainsi, le placement d’une «bombe logique» dans un système informatique vital peut être utilisé par des terroristes comme technique de chantage. De même, toute manipulation frauduleuse de données de dosage pour l’administration de médicaments, dans l’ordinateur d’un hôpital, peut provoquer le décès de patients. Enfin, l’offre de services non-existants dans l’intention d’escroquer des clients intéressés, peut être formulée aussi bien via des réseaux de télématique que par le biais de pratiques plus classiques.

Sur le plan international, une enquête a dès lors été menée dans les années 80 pour déterminer si le droit pénal matériel existant était suffisamment souple que pour absorber cette criminalité télématique. Les travaux de l’OCDE et du Conseil de l’Europe ont fait autorité en la matière et ont incité les pays les plus industrialisés à procéder à une révision de leurs dispositions pénales nationales. À cet effet, des dispositions existantes ont été complétées ou étendues et, dans certains cas, des nouvelles qualifications de délit ont été prévues.

À ce jour, la Belgique n’a pas encore procédé à une révision légale générale des dispositions pénales concernées. Il ressort cependant de la jurisprudence et de la doctrine existantes ainsi que du travail d’étude spécifiquement préparatoire à la définition de la politique à suivre, qu’il ne faut pas en déduire que notre droit pénal est aujourd’hui entièrement impuissant face à certaines formes de criminalité qui sont dirigées contre la technologie de l’information ou qui se servent de cette technologie. Dans certains secteurs, notamment dans le domaine de la sécurité sociale et en matière de protection de données à caractère personnel, il existe des dispositions qui ont été introduites durant cette dernière décennie et qui offrent une certaine protection sur ce plan. Dans certains autres domaines, les incriminations existantes semblent suffire, mais ce sont les possibili-

vormen die strijdig zijn met de goede zeden of aanzetten tot rassendiscriminatie. In een aantal andere gevallen rijzen er interpretatieproblemen inzake de toepasselijkheid van bestaande strafbepalingen (bijvoorbeeld schriftvervalsing, oplichting). Voor sommige strafwaardige specifieke telematicamisbruiken ten slotte wordt evenwel aanvaard dat het huidige strafrecht deficiënt is.

De conclusie in dit verband moet derhalve luiden dat voor de gevallen waar twijfel heerst en ten aanzien van de lacunes in de bestaande regelgeving het aan de wetgever toekomt om op te treden.

1.2. *Aanpassingen op het vlak van de strafbaarstellingen*

Traditioneel wordt inzake de mogelijke misbruiken van de IT een onderscheid gemaakt tussen de gevallen waar de IT in essentie nieuwe modaliteiten biedt om traditionele misdrijven te plegen — informatica als middel voor de criminaliteit — en de gevallen waar de inbreuken gericht zijn tegen het systeem of de gegevens zelf — informatica als doel van de criminaliteit. Hoewel deze grens in de praktijk niet scherp valt te trekken, is het conceptueel onderscheid nuttig, omdat het toelaat vast te stellen dat er in het laatste geval sprake is van het ontstaan van een nieuw rechtsbelang.

1.2.1. Informatica als middel om klassieke misdrijven te plegen

Inderdaad, zo roept de verspreiding van kinderpornografie op het internet in wezen geen nieuw probleem van materieel strafrecht op, in de mate dat dergelijke gedragingen reeds strafbaar zijn wanneer het meer traditionele media betreft. De inbreuken op de auteursrechten door het illegaal aanbieden van beschermde computerprogramma's via netwerken, blijft ook op de informatiesnelweg strafbaar. En dit is eveneens het geval met de hierboven vermelde voorbeelden inzake bedrog of het aanbieden van verboden diensten. De vraag die voor de « telematische » varianten van de thans voorziene misdrijven vooral rijst, is of de constitutieve bestanddelen van traditionele delicten voldoende technologie-neutraal zijn, om in de context van de IT onverkort te kunnen worden toegepast. Het verschil met de klassieke verschijningsvormen van deze misdrijven ligt immers elders, namelijk vooral in een dubbele evolutie die kan worden vastgesteld. Enerzijds is de omvang van het probleem sterk toegenomen : netwerken laten toe om goedkoop, wereldwijd strafbare

tés de recherche qui ne sont pas efficaces; ceci concerne avant tout les délits axés sur le contenu tels que des formes d'expression qui sont contraires aux bonnes moeurs ou qui incitent à la discrimination raciale. Dans une série d'autres cas, des problèmes d'interprétation se posent en ce qui concerne l'applicabilité des dispositions pénales existantes (par exemple en cas de faux en écritures ou d'escroquerie). Enfin, pour certains délits télématiques spécifiques punissables, il est concédé que le droit pénal actuel est déficient.

Il faut donc en conclure qu'il appartient au législateur de réagir à l'égard des lacunes dans la réglementation existante.

1.2. *Adaptation dans le domaine des incriminations*

Concernant les possibilités de délits liés à la technologie de l'information, une distinction est traditionnellement établie entre les cas où la technologie de l'information permet fondamentalement de commettre des délits traditionnels selon des modalités nouvelles — l'informatique comme outil pour la criminalité — et les cas où les infractions sont dirigées contre le système ou contre les données elles-mêmes — l'informatique comme but de la criminalité. Bien que dans la pratique il peut y avoir des chevauchements, la distinction conceptuelle est indispensable, parce qu'elle permet de constater, dans le second cas, l'apparition d'un nouvel intérêt juridique.

1.2.1. L'informatique comme moyen de commettre des délits classiques

La diffusion de la pornographie enfantine sur internet ne crée pas de nouveaux problèmes en termes de droit pénal matériel, dans la mesure où de tels comportements sont déjà punissables lorsqu'ils utilisent des médias plus traditionnels. Enfreindre les droits d'auteur en proposant illégalement des programmes informatiques protégés via des réseaux, demeure également punissable sur les autoroutes de l'information, ce qui est également le cas pour les exemples cités ci-dessus en matière de fraude ou d'offre de services interdits. La question essentielle concernant les variantes « télématiques » des délits actuellement prévus, est de savoir si les éléments constitutifs des délits traditionnels sont suffisamment neutres d'un point de vue technologique que pour pouvoir être intégralement transférés au contexte de la technologie de l'information. La différence avec les formes dans lesquelles ces délits se présentent classiquement réside en effet ailleurs, à savoir au niveau d'une double évolution qui peut être constatée. D'une part, l'ampleur du problème a fortement aug-

boodschappen te verspreiden die gemakkelijk toegankelijk zijn of complexe frauduleuze constructies op te zetten. Anderzijds rijzen enorme opsporingsproblemen gezien de moeilijkheden om de oorsprong van de delictueuze tussenkomsten te achterhalen, evenals de identiteit van de daders.

De conclusie van het beleidsvoorbereidende werk luidt dat het strafrecht in zijn huidige vorm in dit opzicht globaal gezien geen lacunes vertoont voor wat een aantal inhoudsdelicten betreft (pornografie, racisme, aanzetten tot misdaden, …).

Bij een aantal andere misdrijven, en met name daar waar in de omschrijving naar specifieke concrete begrippen of een menselijke tussenkomst wordt gerefereerd, is er in de doctrine en de rechtspraak geen duidelijkheid of de bestaande bepalingen ook in een geïnformatiseerde omgeving volledig toepasselijk blijven. In die gevallen komt het erop aan dat hetzelfde rechtsbelang (bijvoorbeeld openbare trouw, eigendom) ook in een IT-context gewaarborgd blijft. Deze onzekerheid is in het bijzonder prangend voor twee misdrijven die in het kader van de strijd tegen de financieel-economische criminaliteit zeer belangrijk zijn, namelijk valsheid in geschrifte en oplichting.

1.2.2. Informatica als doel van de criminaliteit

Naast de vermelde criminele fenomenen die uiteindelijk hoofdzakelijk uitingen zijn van nieuwe *modi operandi* van misdrijven gericht tegen bestaande beschermde rechtsbelangen, zijn er een aantal misbruiken inzake IT waar op dat vlak een kwalitatieve sprong moet worden gemaakt. Het gaat hier om delicten die een inbreuk plegen op de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen of de gegevens die daarin worden opgeslagen, verwerkt of overgedragen. Het onderzoek heeft uitgewezen dat het op dit domein is dat innoverende wetgevende wijzigingen aan het strafwetboek op een aantal punten noodzakelijk zijn.

Gedragingen zoals het ongeoorloofd binnendringen in een computersysteem, het blokkeren van de toegang tot een computersysteem of onderdelen daarvan, het bedrieglijk consulteren of kopiëren van bestanden, het inbrengen van schadelijke programma's en de verspreiding ervan via netwerken, het onderscheppen van telecommunicatie, het berokkenen van schade of overlast aan dienstenaanbieders of gebruikers van netwerken, … kunnen niet worden herleid tot de traditionele misdrijven tegen personen of eigendommen, zonder de feitelijke en juridische realiteit geweld aan te doen.

menté : les réseaux permettent de diffuser mondialement des messages punissables peu onéreux qui sont facilement accessibles ou qui reposent sur des constructions frauduleuses complexes. D'autre part, d'énormes problèmes de recherche surgissent étant donné les difficultés rencontrées pour déterminer l'origine des interventions délictueuses, ainsi que l'identité des auteurs des délits.

Le travail préparatoire à l'élaboration d'une politique en arrive à la conclusion que le droit pénal dans sa forme actuelle ne présente globalement aucune lacune en ce qui concerne une série de délits portant sur le contenu (pornographie enfantine, racisme, incitation aux délits, …).

Dans le cas d'une série d'autres délits, et notamment ceux dont la définition renvoie à des concepts concrets spécifiques ou à une intervention humaine, la doctrine et la jurisprudence n'établissent pas clairement si les dispositions existantes restent également totalement applicables dans un environnement informatisé. Dans ces cas, il importe que le même intérêt juridique (par exemple fidélité publique, propriété) demeure également garanti dans un contexte de technologie de l'information. Cette incertitude est particulièrement préoccupante pour deux délits primordiaux dans le cadre de la lutte contre la criminalité financière et économique, à savoir, les faux en écriture et l'escroquerie.

1.2.2. L'informatique comme but de la criminalité

Outre les phénomènes criminels mentionnés qui sont finalement principalement l'expression de nouveaux *modi operandi* de délits visant les intérêts juridiques actuellement protégés, un certain nombre d'abus en matière de technologie de l'information nécessitent une amélioration qualitative sur ce plan. Il s'agit de délits qui enfreignent la confidentialité, l'intégrité et la disponibilité des systèmes de télématique ou des données qui y sont répertoriées, traitées ou transférées. La recherche a permis d'établir que c'est dans ce domaine qu'il convient d'apporter des modifications législatives innovatrices au code pénal sur un certain nombre de points.

Des comportements tels que pénétrer illicitement dans un système informatique, bloquer l'accès à un système informatique ou à des parties de système, consulter ou copier des fichiers de manière frauduleuse, encoder des programmes nuisibles et les diffuser via des réseaux, intercepter les télécommunications, causer des dégâts et du dérangement à des fournisseurs de services ou à des utilisateurs de réseaux, … ne peuvent pas être réduits à des délits traditionnels contre des personnes ou propriétés, sans que soit porté atteinte à la réalité physique et juridique.

Hier kan derhalve niet worden volstaan met een aantal toevoegingen in de bestaande hoofdstukken van boek II van het Strafwetboek. Een nieuwe benadering is vereist die ten volle tegemoet komt aan de legitieme verwachtingen van dienstenaanbieders en gebruikers om zich veilig op de informatiesnelweg te kunnen begeven. Daarom wordt een nieuwe titel toegevoegd aan het Strafwetboek waarin de specifieke computer- en telecommunicatiemisdrijven kunnen worden geïntegreerd.

2. **Strafprocesrecht**

2.1. *Algemeen kader*

Het aandachtsveld van beleidsverantwoordelijken en juristen was in het verleden haast exclusief gericht op de omschrijving van de strafbaar te stellen telematicamisdrijven. Nochtans komt bij alle vormen van criminaliteit die gelieerd zijn aan de IT steeds weer de problematiek van het gebrek aan effectiviteit van de opsporing en de bewijsvoering aan de orde. Naast de mogelijkheden die de IT biedt om misdrijven te plegen, kan de IT immers ook door criminelen worden aangewend om de sporen van hun activiteiten uit te wissen of te verhullen en als hulpmiddel om hun criminele plannen voor te bereiden en uit te voeren. Het is derhalve niet verwonderlijk dat opsporing en bewijsvoering thans algemeen als het voornaamste probleem worden ervaren bij de bestrijding van de criminaliteit op de informatiesnelweg. Dit hangt voor een deel samen met de techniciteit van de materie en de nood aan specialisatie bij de politionele en gerechtelijke diensten. De ongrijpbaarheid van geïnformatiseerde gegevens en de snelheid waarmee dergelijke gegevens die relevant kunnen zijn voor de waarheidsvinding, verplaatst of vernietigd kunnen worden, zijn hieraan niet vreemd. Niettemin vloeien een aantal problemen ook voort uit het feit dat het bestaande strafprocesrecht op sommige punten niet is aangepast aan de noden van een effectieve criminaliteitsbestrijding in de informatiemaatschappij.

De problemen van de strafprocedure die verband houden met de IT zijn, internationaal gezien, eigenlijk pas sinds de jaren ’90 ten gronde besproken. De Raad van Europa heeft hier pionierswerk verricht. Het is dan ook niet verwonderlijk dat heelwat staten op dit vlak nog niet over een omvattende regeling beschikken.

Hoewel dit domein derhalve minder is uitgekristalliseerd dan het materiële strafrecht, is het noodzakelijk ook in ons land de nodige aanpassingen door te voeren om een adequate opsporing en bewijsvoering in een telematische omgeving te waarborgen. Gezien het bewijsrecht *stricto sensu* in strafzaken relatief soepel is,

Dans ce cas, l’on peut donc se contenter d’une série d’ajouts dans les chapitres existants du livre II du Code pénal. Une nouvelle approche est requise qui réponde pleinement aux attentes légitimes des fournisseurs et des utilisateurs de services désireux de s’aventurer en toute sécurité sur les autoroutes de l’information. Un nouveau titre intégrant les délits d’informatique et de télécommunication spécifiques est dès lors ajouté au Code pénal.

2. **Procédure pénale**

2.1. *Cadre général*

Dans le passé, les responsables politiques et les juristes n’avaient d’attention que pour la définition des délits de télématique à considérer comme punissables. Pourtant, toutes les formes de criminalité liées à la technologie de l’information posent toujours la problématique du manque d’efficacité de la recherche et celle de l’établissement de la preuve. Outre les possibilités offertes par la technologie de l’information pour commettre des délits, celle-ci peut en effet également être utilisée par des criminels pour effacer ou pour cacher les traces de leurs activités, et comme instrument servant à exécuter leurs plans criminels. Il n’est donc pas étonnant que les problèmes de la recherche et de l’établissement de la preuve sont aujourd’hui généralement considérés comme étant les plus importants dans la lutte contre la criminalité commise sur les autoroutes de l’information. Ceci est partiellement dû à la technicité de la matière et au besoin de spécialisation au niveau des services policiers et judiciaires. Le caractère insaisissable des données informatisées et la rapidité avec laquelle de telles données, peut-être pertinentes pour établir la vérité, peuvent être déplacées ou détruites, ne sont pas étrangers à cela. Une série de problèmes découlent néanmoins aussi du fait que sur certains points la procédure pénale existante n’est pas adaptée aux besoins d’une lutte effective contre la criminalité dans la société d’information.

Au niveau international, les problèmes de procédure pénale liés à la technologie de l’information ont seulement été soumis à une discussion approfondie depuis les années 90. Le Conseil de l’Europe a accompli une œuvre de pionnier sur ce plan. Il n’est dès lors pas étonnant que bon nombre d’états ne disposent pas encore d’une réglementation globale dans ce domaine.

Bien que ce domaine soit moins affiné que celui du droit pénal matériel, il est indispensable que les adaptations nécessaires soient également apportées dans notre pays afin de garantir une recherche et une argumentation adéquates dans l’environnement télématique. Étant donné que le droit relatif à la preuve est, au sens

rijzen de meeste juridische problemen in het kader van de opsporings- en onderzoekshandelingen tijdens het strafrechtelijk vooronderzoek.

2.2. *Opsporing en onderzoek inzake criminaliteit op de informatiesnelweg*

Verschillende domeinen binnen het huidige strafprocesrecht zijn in het licht van de IT aan actualisatie toe.

Het gaat hier in de eerste plaats om de problematiek van de zoeking in computersystemen. In een geïnformatiseerde omgeving is er immers een bijzondere deskundigheid vereist om snel de gegevens op te sporen die relevant zijn voor het strafonderzoek. In het bijzonder moet er in het geval van met elkaar verbonden computersystemen aan worden gedacht de mogelijkheid te voorzien om de zoeking uit te breiden naar systemen die zich op andere locaties bevinden dan waar de zoeking fysisch plaatsgrijpt.

Daarnaast rijzen ook vragen aangaande de huidige modaliteiten van de inbeslagneming. Wanneer de gerechtelijke overheid met name wil overgaan tot de inbeslagneming van de gegevens zelf, onafhankelijk van hun drager, ontbreekt hiervoor thans een adequate juridische basis.

Het opsporen en onderscheppen van (tele)communicatie zijn thans reeds mogelijk als onderzoeksmaatregelen. De bepalingen hierover in het Wetboek van strafvordering zijn juridisch gezien in principe ook toepasselijk in de context van telematicanetwerken. Op een aantal punten moet de regelgeving evenwel verder worden bijgeschaafd, in het licht van de ontwikkelingen inzake telecommunicatie en informatica. Zo zal onder meer de identificatie van gebruikers van netwerkdiensten in de toekomst meer en meer problemen scheppen.

In het licht van de toenemende liberalisering van de telecommunicatiemarkten, werden de bestaande medewerkingsverplichtingen van operatoren in een recente wetswijziging uitgebreid tot aanbieders van netwerkdiensten. In dit ontwerp worden deze mogelijkheden verder gepreciseerd en bovendien wordt in het algemeen in de mogelijkheid voorzien om de medewerking te vorderen van personen die over een bijzondere kennis beschikken van de computersystemen of -netwerken die het voorwerp van de opsporingen uitmaken, of van de toegang tot deze systemen of netwerken en de gegevens die zich daarin bevinden.

In verband hiermee moet er worden gewezen op het steeds toenemende gebruik van versleutelingstechnieken die vanuit justitieel oogpunt problemen met zich meebrengen, niet enkel inzake het onderscheppen van

strict, relativement souple en matière pénale, la plupart des problèmes juridiques surgissent dans le cadre des actes de recherche et d'enquête posés lors de l'instruction pénale préparatoire.

2.2. *Recherches et enquêtes en matière de criminalité sur les autoroutes de l'information*

Divers domaines au sein de la procédure pénale actuelle doivent être actualisés à la lumière de la technologie de l'information.

Il s'agit en premier lieu de la problématique de la recherche dans les systèmes informatiques. En effet, dans un environnement informatisé, une expertise particulière est requise afin de détecter rapidement les données qui sont pertinentes pour l'instruction pénale. Dans le cas de systèmes informatiques liés entre eux, il convient en particulier de penser à prévoir la possibilité d'étendre l'enquête à des systèmes qui se trouvent à d'autres endroits que ceux où la recherche a physiquement lieu.

Complémentairement à cela, surgissent également des questions concernant les modalités actuelles en matière de saisie. Ainsi, une base juridique adéquate fait actuellement défaut lorsque les autorités judiciaires souhaitent procéder à la saisie des données elles-mêmes, indépendamment de leur support.

Le repérage et l'interception de (télé)communications sont actuellement déjà possibles en tant que mesures d'instruction. Les dispositions à ce propos, contenues dans le Code d'instruction criminelle, sont, d'un point de vue juridique, en principe également applicables dans le contexte des réseaux de télématique. Cependant, il convient d'affiner la régulation en cette matière sur certains points à la lumière des développements en matière de télécommunication et d'informatique. En effet, l'identification des utilisateurs de services de réseaux, par exemple, posera de plus en plus problème à l'avenir.

À la lumière de la libéralisation croissante des marchés de télécommunication, les obligations de collaboration existantes dans le chef des opérateurs ont déjà été étendues aux fournisseurs de services de réseaux dans le cadre d'une modification législative récente. Dans ce projet de loi-ci, ces possibilités sont précisées davantage et, en outre, on prévoit la possibilité, d'une manière générale, de requérir la collaboration de personnes qui disposent d'une connaissance particulière des systèmes ou réseaux informatiques qui font l'objet de recherches, ou de l'accès à ces systèmes ou réseaux ainsi qu'aux données qui s'y trouvent.

À ce propos, il y a lieu de souligner l'utilisation toujours croissante de techniques de verrouillage qui, d'un point de vue judiciaire, posent des problèmes, non seulement pour l'interception du contenu de télécommuni-

de inhoud van telecommunicatie, maar ook wat de toegang in « klare tekst » betreft tot gegevens die zich in *stand alone*-computersystemen bevinden. De problematiek van cryptografie overstijgt echter het kader van de criminaliteitsbestrijding. Het gaat hier immers om een technisch middel dat enorme mogelijkheden biedt om het vertrouwen van de overheid, de commerciële wereld en het publiek in het algemeen in het gebruik van de telematica te versterken. Sommigen durven zelfs te gewagen van een « recht op cryptografie ». In deze context komt het er derhalve op aan om de negatieve effecten van het gebruik van versleutelingstechnieken op strafrechtelijke onderzoeken te minimaliseren. Overigens biedt cryptografie ook interessante perspectieven in verband met het voorkomen van misdrijven (bijvoorbeeld fraude) en in verband met de beveiliging van de resultaten van onderscheppingsmaatregelen en de transcriptie, bewaring en exploitatie daarvan.

3. **Algemene benadering van het voorontwerp**

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

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

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

Hierbij werden de relevante internationaalrechtelijke instrumenten in rekening gebracht. Met name werd inspiratie geput uit twee belangrijke aanbevelingen die werden uitgewerkt in het kader van de Raad van Europa : de aanbeveling n^{r} R(89)9 van 13 september 1989 inzake computergerelateerde criminaliteit en de aanbeveling n^{r} R(95)13 van 11 september 1995 inzake problemen van strafprocesrecht die gelieerd zijn aan de informatietechnologie.

Deze documenten werden in rekening gebracht om de oriëntaties van het voorontwerp te bepalen. Het gaat evenwel om niet-bindende instrumenten die overigens niet in alle opzichten werden gevolgd. De kritiek van de Raad van State dat deze of gene aanbeveling (of elementen uit het verklarend verslag) niet worden gevolgd, is derhalve minder pertinent.

Voor de strafbaarstellingen is dit vaak een gevolg van het feit dat de aanbeveling R(89)9 deels achterhaald is door de evolutie.

cation, mais également au niveau de l'accès « en clair » aux données qui se trouvent dans des systèmes informatiques isolés. La problématique de la cryptographie dépasse cependant le cadre de la lutte contre la criminalité. En effet, il s'agit d'un moyen technique qui offre de nombreuses possibilités en vue de renforcer la confiance des autorités, du monde commercial et du public en général en ce qui concerne l'usage de la télématique. Certains osent même évoquer un « droit à la cryptographie ». Dans ce contexte, il convient par conséquent de minimaliser les effets négatifs du recours aux techniques cryptographiques sur les enquêtes pénales. La cryptographie offre d'ailleurs également d'intéressantes perspectives pour la protection des résultats des mesures d'interception ainsi que pour la transcription, la conservation et l'exploitation des résultats.

3. **Approche générale de l'avant-projet**

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

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

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

À cet égard, il a été tenu compte des instruments de droit international pertinents. L'inspiration a notamment été puisée dans deux recommandations importantes élaborées dans le cadre du Conseil de l'Europe : la recommandation n° R(89)9 du 13 septembre 1989 en matière de criminalité informatique et la recommandation n° R(95)13 du 11 septembre 1995 relative aux problèmes de droit de procédure pénale liés à la technologie de l'information.

Ces documents ont été pris en considération pour déterminer les orientations de l'avant-projet. Il s'agit toutefois d'instruments non contraignants qui d'ailleurs n'ont pas été suivis en tout point. Par conséquent, la critique du Conseil d'État selon laquelle l'une ou l'autre recommandation (ou certains éléments du rapport déclaratif) ne sont pas suivis est moins pertinente.

Pour ce qui regarde des incriminations, cela résulte souvent du fait que la recommandation R(89)9 est partiellement dépassée.

Inzake het strafprocesrecht integreert het voorontwerp belangrijke suggesties uit de aanbeveling R(95)13 in de Belgische rechtsorde; het is evenwel onjuist om te stellen dat de uitleg in het verklarend verslag als zodanig een vertolking is van vaststaande internationaal publiekrechtelijke principes : de discussies ter zake zijn eigenlijk pas dan op gang gekomen.

In het licht van het voorgaande streeft het voorontwerp er vooreerst naar om twee centrale traditionele beschermde rechtsbelangen, de openbare trouw en het vermogen, ook in een IT-context te waarborgen, niet in het minst omwille van de twijfel die in dat verband in doctrine en rechtspraak heerst. Er worden derhalve nieuwe bepalingen inzake valsheid in informatica en informaticabedrog ingevoegd in de hoofdstukken van het strafwetboek die op de voormelde rechtsbelangen betrekking hebben, zonder evenwel te raken aan de opbouw van die hoofdstukken en de bepalingen daarvan.

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

Het uitgangspunt van het voorontwerp inzake strafbaarstellingen is : *off-line = on-line*. Er is inderdaad geen reden om bijvoorbeeld kinderporno strenger te beteugelen als die wordt verspreid op internet dan wel via andere media. Inzake gegevensbescherming beoogt het voorontwerp dan ook geen bijzondere categorieën van gegevens, die buiten de geïnformatiseerde context geen strafrechtelijke bescherming genieten, louter en alleen omwille van hun geïnformatiseerde vorm een bijzondere bescherming te bieden.

In tegenstelling tot wat de Raad van State stelt, is er geen discriminerende onderscheiden behandeling van gedragingen in het voorontwerp, naargelang ze al dan niet via informatica worden gepleegd. Het voorontwerp gaat immers uit van de specificiteit van informaticanetwerken die niet kan worden gereduceerd tot het soort van analogieën vermeld in het advies (bijvoorbeeld de brandkast). De nieuwe, in het geding zijnde rechtsbelangen werden overigens reeds aangehaald : de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en data. De regering wenst derhalve de nieuwe realiteit van de informaticanetwerken ten volle te onderkennen.

Sur le plan du droit de procédure pénale, en se fondant sur la recommandation R(95)13, l'avant-projet intègre d'importantes suggestions dans le droit belge; il est toutefois inexact de dire que l'explication donnée dans le rapport déclaratif est en soi une interprétation des principes bien établis du droit international public : les débats sur la question sont en fait à peine entamés.

À la lumière de ce qui précède, l'avant-projet de loi vise principalement à garantir, y compris dans le contexte de la technologie de l'information, deux intérêts juridiques traditionnellement protégés, à savoir la foi publique et le patrimoine, surtout en raison du doute qui règne à cet égard au niveau de la doctrine et de la jurisprudence. C'est la raison pour laquelle de nouvelles dispositions relatives au faux en informatique et à la fraude informatique sont insérées dans les chapitres du Code pénal qui portent sur les intérêts juridiques précités, sans toutefois toucher à la structure de ces chapitres ni à leurs dispositions.

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

En ce qui concerne les incriminations, le point de départ de l'avant-projet est : *off-line = on-line*. Il n'y a en effet aucune raison de réprimer plus sévèrement la pornographie enfantine, par exemple, selon qu'elle est diffusée sur Internet ou via d'autres médias. Dès lors, en ce qui concerne la protection des données, l'avant-projet ne prévoit pas d'offrir une protection particulière à des catégories de données spécifiques, qui en dehors du contexte informatisé ne bénéficient d'aucune protection sur le plan pénal, simplement en raison de leur forme informatisée.

Contrairement à ce qu'affirme le Conseil d'État, aucun comportement n'est traité de manière discriminatoire dans l'avant-projet, qu'il soit commis ou non à l'aide de l'informatique. L'avant-projet se base en effet sur la spécificité des réseaux informatiques qui ne peut être réduite au type d'analogies mentionné dans l'avis (par exemple, le coffre-fort). Les nouveaux intérêts juridiques en cause ont d'ailleurs déjà été cités : la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données. Le gouvernement souhaite par conséquent reconnaître pleinement la nouvelle réalité que constituent les réseaux informatiques.

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

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

De Raad van State is van oordeel dat de internationale aspecten van informaticacriminaliteit een totaal andere benadering vereisen dan degene waarvoor de regering heeft geopteerd. Deze kritiek gaat evenwel in belangrijke mate voorbij aan de bedoelingen van de ontwerptekst, evenals aan de draagwijdte ervan.

De problematiek van de lokalisering van het misdrijf en de internationale rechtsmacht, aangehaald door de Raad van State, rechtvaardigen geen van het gemeenrecht afwijkende regeling in het intern Belgisch recht. De vragen ter zake rijzen immers vrijwel in dezelfde termen voor niet-computer gerelateerde criminaliteit, zoals vormen van economische criminaliteit, bijvoorbeeld fraude, corruptie of witwassen.

Inzake de problematiek van de toepassing van opsporingsmiddelen met een grensoverschrijdende dimensie moet worden benadrukt dat, in tegenstelling tot de lectuur van de Raad van State, het ontwerp geenszins beoogt op unilaterale basis de bevoegdheid te verlenen aan de gerechtelijke instanties om zich onbeperkt toegang te verschaffen tot in het buitenland opgeslagen gegevens.

Het voorontwerp laat in dat opzicht de principes van het internationaal publiek recht onverlet, principes waarvan de juiste draagwijdte thans overigens ter discussie staat gezien de specificiteit van de netwerken. Er worden derhalve geen bevoegdheden gecreëerd die een intentionele schending van de soevereiniteit van een andere staat beogen.

De problematiek van de internationale effecten van onderzoeksmaatregelen op het Internet wordt derhalve door de Raad van State in de context van het voorontwerp niet in het juiste perspectief geplaatst : de kwestie betreft niet het wetsontwerp in zijn geheel, maar komt enkel specifiek aan de orde in artikel 88*ter* (netwerkzoeking), en dan nog slechts om, met respect van het internationaal publiek recht, een handelwijze voor te schrijven, indien blijkt dat de netwerkzoeking effecten in het buitenland heeft gesorteerd. Over de uit-

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 à l'égard des fournisseurs de services de télécommunications, en ce qui concerne l'utilisation des services de télécommunications. Le non respect de ces obligations est sanctionné pénalement.

Le Conseil d'État considère que les aspects internationaux de la criminalité informatique requièrent une toute autre approche que celle choisie par le gouvernement. Toutefois, cette critique ignore dans une large mesure les objectifs ainsi que la portée du texte du projet.

Les questions de la localisation du délit et de la compétence internationale, citées par le Conseil d'État, ne justifient pas l'introduction en droit belge de dispositions dérogatoires du droit commun. En effet, les questions en la matière se présentent à peu près dans les mêmes termes pour la criminalité qui n'est pas liée à l'informatique, comme, par exemple, certaines formes de criminalité économique telles que la fraude, la corruption ou le blanchiment d'argent.

En ce qui concerne la problématique liée à l'application des moyens de recherche dotés d'une dimension transfrontière, il faut insister sur le fait que, contrairement à la lecture du Conseil d'État, le projet ne vise aucunement à octroyer unilatéralement la compétence aux instances judiciaires afin qu'elles se procurent un accès illimité aux données enregistrées à l'étranger.

À cet égard, l'avant-projet conserve dans leur intégralité les principes de droit public international, principes dont la portée exacte fait d'ailleurs l'objet actuellement d'une discussion vu la spécificité des réseaux. Par conséquent, aucune compétence visant à violer intentionnellement la souveraineté d'un autre État n'est créée.

Dans le contexte de l'avant-projet de loi, le Conseil d'État ne considère donc pas la problématique des effets internationaux des mesures de recherche sur Internet sous le bon angle : le problème ne concerne pas le projet de loi dans son ensemble, il ne se pose de façon spécifique qu'au niveau de l'article 88*ter* (recherche sur un réseau) et encore uniquement pour prescrire, dans le respect du droit public international, une manière d'agir s'il s'avère que la recherche sur un réseau a eu des effets à l'étranger. L'avant-projet de loi

eindelijke bewijswaarde van aldus bekomen data spreekt het voorontwerp zelf zich niet uit : dit zal *in concreto* beoordeeld moeten worden onder andere in het licht van de houding van de andere betrokken staat (vergelijk de rechtspraak van het Hof van Cassatie inzake in het buitenland afgeluisterde telefoongesprekken).

4. **Terminologie**

In het voorontwerp worden geen definities opgenomen. Dit past niet in onze juridische traditie en zou overigens contraproductief zijn. De gehanteerde terminologie beoogt in het bijzonder technologie-neutraal te zijn, om aldus te vermijden dat de concepten al te snel achterhaald worden door de evolutie van de informatietechnologie.

De hieronder vermelde begrippen worden gehanteerd :

— Informaticasysteem

Hiermee wordt gedoeld op alle systemen voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT.

— Gegevens

Hiermee wordt gedoeld op voorstellingen van informatie die geschikt zijn voor opslag, verwerking en overdracht via een informaticasysteem. Overigens wordt die laatste zinsnede in het voorontwerp telkens toegevoegd, waar verwarring met de veel ruimere, dagdagelijkse betekenis van het begrip « gegevens » mogelijk is.

De materiële vormgeving van deze gegevens — electro-magnetisch, optisch of anderszins — is irrelevant voor het wetsontwerp.

Het begrip wordt steeds in het meervoud gebruikt — de vraag of malversaties betrekking kunnen hebben op één informatietechnisch gegeven is louter theoretisch : het is in de context van de strafbepaling dat moet blijken welk conglomeraat van gegevens relevant is. Zo is het voor het voorontwerp niet relevant om een onderscheid te maken tussen een willekeurig geheel van gegevens en een bijzondere configuratie van gegevens die een computerprogramma vormt.

De Raad van State meent dat het begrip « gegevens » in het wetsontwerp zelf moet worden gedefinieerd. Deze opmerking is onterecht : het begrip « gegevens » heeft in de tekst steeds ondubbelzinnig betrekking op de specifieke notie « data », omdat steeds de link wordt ge-

ne se prononce pas sur la force probante finale des données ainsi obtenues : concrètement, il devra en être jugé notamment à la lumière de l'attitude adoptée par l'autre État impliqué (cf. la jurisprudence de la Cour de cassation en matière d'écoute de conversations téléphoniques à l'étranger).

4. **Terminologie**

L'avant-projet de loi ne contient aucune définition. Cela ne correspond pas à notre tradition juridique et produirait d'ailleurs un effet contreproductif. Aussi la terminologie employée est-elle particulièrement neutre du point de vue technologique afin d'éviter que les concepts soient trop rapidement dépassés par l'évolution de la technologie de l'information.

Les notions suivantes sont utilisées :

— Système informatique

Par système informatique, on entend tout système permettant le stockage, le traitement ou la transmission de données. À ce propos, on pense principalement aux ordinateurs, aux cartes à puce etc., mais également aux réseaux et à leurs composants ainsi qu'aux systèmes de télécommunication ou à leurs composants qui font appel à la technologie de l'information.

— Données

Par données, on entend les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique. Ce dernier morceau de phrase est ajouté dans l'avant-projet de loi chaque fois qu'une confusion est possible avec la signification générale et beaucoup plus large de la notion de « données ».

La forme matérielle que revêtent ces données — qu'elle soit électromagnétique, optique ou autre — n'a pas d'importance pour l'avant-projet de loi.

Le terme est toujours utilisé au pluriel — la question de savoir si des malversations peuvent se rapporter à une seule donnée dans le sens donné précédemment est purement théorique : c'est dans le contexte de la disposition pénale que doit apparaître le type de données pertinent. Dès lors, il n'est pas utile dans le cadre de l'avant-projet de loi d'établir une distinction entre un ensemble de données pris au hasard et une configuration de données particulière constituant un programme informatique.

Le Conseil d'État estime que dans la version néerlandaise du projet de loi, le concept de « *gegevens* » lui-même doit être défini. Cette remarque n'est pas fondée : dans le texte néerlandais, le concept de « *gegevens* » se rapporte toujours explicitement à la no-

legd tussen « gegevens » en « die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem ». Er valt niet in te zien welk soort verwarring er derhalve zou kunnen ontstaan. Men zou dan overigens soortgelijke vragen kunnen opwerpen ten aanzien van vele concepten die in het Strafwetboek worden gehanteerd.

De Raad van State stelt bovendien een aantal wijzigingen voor in de benaming van de misdrijven : « informatica » wordt « computer »; « bedrog » wordt « fraude » en « ongeoorloofde toegang » wordt « computervredebreuk ». De benaming « informatica » werd evenwel juist gekozen om de verregaande integratie van communicatie- en informatietechnologieën weer te geven, evenals de realiteit van de netwerken die daaruit resulteert, daar waar het begrip « computer » nog te veel de connotatie van een *stand alone* systeem heeft.

De benadering « computervredebreuk » creëert een onterechte analogie met huisvredebreuk, dat een misdrijf tegen de personen is. Het beschermde rechtsgoed is niet hetzelfde.

B. ARTIKELSGEWIJZE BESPREKING VAN HET ONTWERP ARTIKEL 78 (N^{r} 213/1)

Artikel 1

Dit artikel bepaalt de constitutionele bevoegdheidsgrondslag.

Art. 2

In het Strafwetboek wordt een nieuw artikel 210*bis* ingevoegd, dat betrekking heeft op valsheid in informatica.

In rechtspraak en rechtsleer heerst onduidelijkheid over de vraag of « elektronische gegevens » onder de bescherming van de traditionele valsheidsdelicten vallen. Een loutere assimilatie van elektronische gegevens met geschriften zou evenwel tot niet te overziene consequenties aanleiding kunnen geven inzake de draagwijdte van de bestaande bepalingen. Zo kunnen data ook spraak en beeld voorstellen, die als zodanig niet onder de bescherming van de bepalingen inzake schriftvervalsing ressorteren. Bovendien zou dit een wettelijke omschrijving van het begrip « geschrift » vereisen die het bestek van dit wetsontwerp te buiten gaat (vergelijk de uitvoerige rechtspraak inzake de artikelen 193 en volgende van het Strafwetboek in dit verband).

Aangezien het niet de bedoeling is in het kader van dit voorontwerp de basisbeginselen inzake schriftvervalsing in het algemeen te herzien, wordt er derhalve

tion spécifique de « *data* », car le rapport est toujours établi entre « *gegevens* » et « *die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem* ». On ne voit dès lors pas quelle confusion pourrait être engendrée par ces deux termes. Sinon, on pourrait alors soulever des questions similaires à l'égard de nombreux concepts qui sont utilisés dans le Code pénal.

En outre, le Conseil d'État propose un certain nombre de modifications relatives à la dénomination des délits dans le texte néerlandais : « *informatica* » devient «*computer* »; « *bedrog* » devient « fraude » et « *ongeoorloofde toegang* » devient « *computervredebreuk* ». Cependant, la dénomination « *informatica* » a précisément été adoptée pour refléter l'intégration extrême des technologies en matière de communication et d'informatique, ainsi que la réalité des réseaux qui en résultent vu que le concept « *computer* » a encore trop souvent une connotation de système *stand alone*.

L'approche « *computervredebreuk* » crée à tort une analogie avec « *huisvredebreuk* », qui est un délit contre les personnes. Le bien juridique protégé n'est pas le même.

B. COMMENTAIRE DES ARTICLES DU PROJET ARTICLE 78 (N° 213/1)

Article 1er

Le présent article détermine la base constitutionnelle de compétence.

Art. 2

Il est inséré dans le Code pénal un nouvel article 210*bis* qui a trait au faux en informatique.

La confusion règne tant dans la jurisprudence que dans la doctrine quant à la question de savoir si la protection contre les délits traditionnels en matière de faux s'applique aux « données électroniques ». Une assimilation pure et simple des données électroniques aux données scripturales pourrait toutefois entraîner des conséquences incalculables sur la portée des dispositions existantes. Ainsi, les données peuvent également prendre la forme de paroles et d'images, lesquelles ne tombent pas en tant que telles sous la protection des dispositions en matière de faux en écritures. En outre, cela nécessiterait une définition légale du terme « écriture », ce qui sort du cadre du présent avant-projet de loi (cf. à cet égard l'importante jurisprudence concernant les articles 193 et suivants du Code pénal).

Comme le but du présent avant-projet de loi n'est pas une révision générale des principes de base en matière de faux en écritures, on a décidé d'incriminer en tant

voor geopteerd om het opzettelijk vermommen van de waarheid via datamanipulatie met betrekking tot juridisch relevante gegevens als afzonderlijk misdrijf strafbaar te stellen, evenals de poging tot dergelijke valsheid. In tegenstelling tot de gemeenrechtelijke valsheid in geschrifte wordt geen bijzonder opzet vereist. De reden hiervoor is dat, enerzijds het oogmerk van bedrieglijke verrijking reeds wordt geviseerd door de voorgestelde bepaling inzake informaticafraude (zie hieronder, artikel 504*quater*), en anderzijds datamanipulatie met het specifieke doel schade te berokkenen geviseerd wordt door de bepalingen inzake informatica- en datasabotage (zie hieronder, artikel 550*ter*). Overigens wordt voor de toepassing van artikel 210*bis* ook vereist dat de juridische draagwijdte van de data is gewijzigd, wat beschouwd kan worden als de effectieve realisatie van een specifiek nadeel. Of deze data überhaupt een juridische draagwijdte hebben, en zich derhalve aan het openbaar vertrouwen opdringen, is een feitenkwestie die door de rechter ten gronde moet worden beoordeeld. De manipulaties van de data moeten op de meest ruime wijze worden opgevat.

In tegenstelling tot de indruk gewekt door de opmerkingen van de Raad van State wordt voor het nieuwe delict heel duidelijk wel degelijk het algemeen opzet vereist. De bedenkingen inzake de verschillen tussen de gemeenrechtelijke valsheid in geschrifte en het nieuwe misdrijf valsheid in informatica kunnen niet worden gedeeld. In de lijn van de hoger aangegeven reden, moet benadrukt worden dat het ontwerp :

— een duidelijke verhouding tussen de verschillende vormen van strafbare datamanipulaties wil bepalen, zonder terug te vallen op de ambigue verhouding tussen traditionele valsheid in geschrifte en oplichting;

— bewust wil afwijken van de achterhaalde complexiteit van de gemeenrechtelijke bepalingen over valsheid (onderscheiden tussen categorieën personen, ook verschillende misdaden, onderscheiden tussen aard van de documenten) : het herzien van het volledige hoofdstuk over de valsheden gaat evenwel het kader van dit voorontwerp te buiten.

Op die wijze wordt in het kader van dit wetsontwerp niet geraakt aan het bestaande evenwicht inzake de valsheidsbepalingen en heeft de gerechtelijke overheid een duidelijk houvast om moderne vormen van valsheid aan te kunnen pakken, zoals het vervalsen of namaken van kredietkaarten of valsheid inzake « digitale contracten » waar de juridisch relevante documenten niet meer op papier worden geprint en *de manu* worden ondertekend. Het toepassingsgebied van de nieuwe bepaling op dit ogenblik moet evenwel niet overschat worden : waar administratie en bedrijfswereld meer en meer gebruik maken van informatica als hulpmiddel, blijven meestal de juridisch relevante documenten toch nog degene die op papier worden uitgedrukt en *de manu* worden ondertekend.

que délit à part entière le fait, et la tentative, de dissimuler intentionnellement la vérité par le biais de manipulations informatiques de données pertinentes sur le plan juridique. Contrairement au faux en écritures de droit commun, aucune intention particulière n'est requise vu que, d'une part, l'intention d'enrichissement frauduleux est déjà visée dans la proposition de disposition en matière de fraude informatique (voir *supra*, article 504*quater*) et que, d'autre part, la manipulation de données dans le but spécifique de nuire est visée dans les dispositions relatives au sabotage informatique et au sabotage de données (voir *supra*, article 550*ter*). Du reste, l'application de l'article 210*bis* requiert également que la portée juridique des données soit modifiée, ce qui peut être considéré comme la réalisation effective d'un inconvénient spécifique. Que ces données aient réellement une portée juridique et qu'elles s'imposent dès lors à la foi publique sont des questions de fait qu'il appartient au juge du fond d'apprécier. Les manipulations des données doivent être envisagées de la manière la plus large qui soit.

Contrairement à l'impression donnée par les remarques du Conseil d'État, l'intention générale est clairement et nettement requise pour le nouveau délit. Les considérations quant aux différences entre le faux en écriture de droit commun et le nouveau délit que représente le faux en informatique ne peuvent être partagées. Dans le cadre de la raison susmentionnée, il faut insister sur le fait que le projet :

— veut déterminer un rapport clair entre les différentes formes de manipulations de données punissables, sans retomber dans le rapport ambigu entre le faux en écriture traditionnel et l'escroquerie;

— tient à s'écarter de la complexité dépassée des dispositions de droit commun en matière de faux (différences entre catégories de personnes, différents crimes, différences entre la nature des documents) : la révision du chapitre complet sur les faux s'écarte trop du cadre de cet avant-projet.

De cette manière et dans le cadre de ce projet de loi, on ne touche pas à l'équilibre existant au niveau des dispositions relatives au faux et les autorités judiciaires disposent d'une base claire pour pouvoir aborder les formes modernes de faux, comme la fabrication de cartes de crédit fausses ou falsifiées ou le faux en matière de « contrats numériques » où les documents pertinents sur le plan juridique ne sont plus imprimés sur papier, ni signés *de manu*. À ce stade, le champ d'application de la nouvelle disposition ne doit toutefois pas être surestimé : alors que l'administration et l'industrie ont recours de plus en plus souvent à l'informatique, la plupart des documents pertinents sur le plan juridique sont toujours imprimés sur papier et signés *de manu*.

Zoals voor andere valsheidsdelicten worden zowel de valsheid zelf, als het gebruik van de valse gegevens bestraft.

Er wordt een bijzonder regime voorzien, ingeval van herhaling, dat strenger is dan het gemeenrechtelijke. Dit wordt ingegeven door de grote risico's die dergelijke delicten, die relatief eenvoudig kunnen worden gerealiseerd en vrij moeilijk op te sporen zijn, met zich meebrengen.

Art. 3

In het Strafwetboek wordt een nieuw artikel 504*quater* ingevoegd, dat betrekking heeft op informaticabedrog.

De nieuwe incriminatie « informaticabedrog » stelt gegevensmanipulatie met het oogmerk voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel te verwerven, evenals de realisatie van dit oogmerk strafbaar.

De bepaling wordt losgekoppeld van artikel 496 (oplichting), dat in essentie bedrieglijke manœuvres viseert die het vertrouwen van personen schenden. Computerfraude betreft ongeoorloofde manipulaties van data ten aanzien van een machine, en is in dat opzicht wezenlijk verschillend.

De specifieke strafbaarstelling laat bovendien toe om een andere structuur te geven aan het delict dan aan sommige bestaande vermogensdelicten. Zo is het voor het nieuwe delict irrelevant of er voor of na de manipulatie afgifte is geweest van een vermogensonderdeel, terwijl dit essentieel is voor het onderscheid tussen misbruik van vertrouwen en oplichting. Ook zullen een aantal gevallen van misbruiken die door een extensieve interpretatie van de rechtspraak als diefstal, eventueel met gebruik van valse sleutels, werden gekwalificeerd, thans duidelijk onder informaticabedrog ressorteren.

Voorbeelden van gevallen die geviseerd worden door de nieuwe bepaling 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.

Er wordt eveneens een bijzonder, strenger regime voorzien, ingeval van herhaling.

À l'instar des autres délits en matière de faux, tant le faux que l'usage de données fausses sont punis.

En cas de récidive, il est prévu un régime particulier plus stricte que celui de droit commun, étant donné les risques importants occasionnés par ces délits qui peuvent être commis assez facilement, mais dépistés plus difficilement.

Art. 3

Un nouvel article 504*quater* relatif à la fraude informatique est inséré dans le Code pénal.

La nouvelle incrimination « fraude informatique » punit la manipulation de données en vue de se procurer pour son propre compte ou pour le compte d'autrui un avantage patrimonial frauduleux ainsi que la réalisation de cette intention.

La disposition est séparée de l'article 496 (escroquerie), laquelle vise essentiellement les manœuvres frauduleuses qui portent atteinte à la confiance de tiers. La fraude informatique concerne des manipulations illicites de données sur une machine et est donc dans cette optique profondément différente.

En outre, l'incrimination spécifique permet de conférer au délit une structure autre que celle conférée à certains délits patrimoniaux existants. Ainsi, en ce qui concerne le nouveau délit, il n'est pas important de savoir s'il y a eu remise d'un bien patrimonial avant ou après la manipulation, alors que c'est essentiel pour faire la distinction entre l'abus de confiance et l'escroquerie. Désormais un certain nombre de cas d'infractions qui par l'interprétation étendue de la jurisprudence sont qualifiées de vol, éventuellement à l'aide de fausses clés, relèvent clairement de la fraude informatique.

Parmi les exemples de cas visés par la nouvelle disposition, peuvent être cités l'utilisation d'une carte de crédit volée pour retirer de l'argent à un guichet automatique, le dépassement illicite du crédit par le biais de sa propre carte de crédit, l'introduction d'instructions informatiques pour modifier le résultat de certaines opérations en vue d'obtenir un avantage financier illicite, le détournement motivé par l'appât du gain de fichiers ou de programmes confiés dans un but bien précis.

Il est également prévu un régime particulier plus strict en cas de récidive.

Art. 4

Er wordt in het Strafwetboek een nieuwe Titel IX*bis* ingevoegd inzake de misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen. De redenen voor het creëren van deze nieuwe titel, die twee bepalingen bevat, werden in het algemene gedeelte van de memorie toegelicht.

— Ongeoorloofde toegang tot een informaticasysteem

De eerste strafbepaling van Titel IX*bis* is artikel 550*bis*, dat betrekking heeft op de ongeoorloofde toegang tot een informaticasysteem (« *hacking* »).

Centraal hierbij is de bestraffing van het wederrechtelijk toegang bekomen tot een informaticasysteem of een deel daarvan waartoe men niet is gerechtigd.

Hierbij wordt een onderscheid gemaakt tussen aantastingen van buiten het systeem (§ 1) en aantastingen door gebruikers die bepaalde toegangsbevoegdheden hebben (§ 2).

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

Voor insiders wordt de strafbaarheidsdrempel hoger gelegd : het overschrijden van het verleende autorisatieniveau moet plaatsvinden met een bijzonder opzet, namelijk onrechtmatig winstbejag of kwaadwillige bedoelingen. Het louter onrechtmatig betreden van delen van het systeem moet via minder ingrijpende mechanismen worden aangepakt (interne sancties, arbeidsrecht, burgerlijk recht, …).

De Raad van State betwist dit onderscheid inzake de strafwaardigheid van « *hacking* » door buitenstaanders, dan wel door « *insiders* ». De logica van het voorontwerp houdt rekening met de realiteit dat het binnen een organisatie frequenter zal voorkomen dat er een ongeoorloofde toegang is tot bepaalde delen van het netwerk omwille van allerhande factoren (persoonlijke contacten, structuur van het netwerk, werkomgeving). Deze inbreuken kunnen weliswaar intentioneel zijn, maar worden slechts strafwaardig geacht als er een bijzondere negatieve bedoeling achterzit (strafrecht als *ultima ratio*) : interne controlemechanismen moeten voor de minder ingrijpende gevallen volstaan. Deze situatie is verschillend ten aanzien van derden die buiten het netwerk zitten : hun transgressie brengt op zichzelf de veiligheid van het interne netwerk in gevaar. De veralgemeende introductie van netwerken maakt dat analogieën met de « papieren » wereld (brandkasten, en

Art. 4

Il est inséré 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 par le biais de ces systèmes. Les raisons qui ont motivé la création de ce nouveau titre, qui compte deux dispositions, sont commentées dans la partie générale de l'exposé.

— Accès illicite à un système informatique

La première disposition du Titre IX*bis* est l'article 550*bis* qui porte sur l'accès illicite à un système informatique (« *hacking* »).

Élément central à ce propos : le fait de punir l'obtention illégale de l'accès à l'entièreté ou à une partie d'un système informatique.

À cet égard, une distinction est établie entre les atteintes portées à partir de l'extérieur du système (§ 1er) et les atteintes portées par des utilisateurs qui possèdent certains pouvoirs d'accès (§ 2).

Les personnes étrangères au système sont punissables si elles savent qu'elles ne sont pas autorisées à y accéder ou à s'y maintenir. Dans ce cas, une peine plus sévère est prévue si l'infraction est réalisée avec intention frauduleuse.

Pour les autres personnes visées, le seuil d'incrimination est plus élevé : le dépassement du niveau d'autorisation accordé doit être accompli dans une intention particulière, à savoir l'appât du gain illicite ou la malveillance. Le simple fait d'entrer illicitement dans des parties du système doit être abordé par le biais de mécanismes moins radicaux (sanctions internes, législation du travail, droit civil, ...).

Le Conseil d'État conteste cette distinction au niveau du caractère punissable du « *hacking* » selon qu'il est perpétré par des personnes étrangères au système ou par des « *insiders* ». L'avant-projet de loi repose sur la logique que dans la réalité, l'accès illégal à certaines parties du réseau sera constaté plus fréquemment au sein d'une organisation du fait de facteurs des plus divers (contacts personnels, structure du réseau, environnement de travail). Ces infractions peuvent certes être intentionnelles, mais ne sont réputées punissables que si elles résultent d'une intention négative particulière (droit pénal en guise d'*ultima ratio*) : des mécanismes de contrôle internes doivent s'avérer suffisants pour les cas moins graves. La situation est différente à l'égard de tiers qui se trouvent en dehors du réseau en soi, la transgression dont ils se rendent coupables met en danger la sécurité du réseau interne. Vu l'introduction généralisée de réseaux, cela n'a pas de sens d'établir des

dergelijke) niet opgaan : « *hacking* » moet beschouwd worden als een gevaarzettingsdelict dat als zodanig strafwaardig is, ongeacht de bijzondere kwaadwillige bedoelingen of de gerealiseerde effecten.

De eis dat een beveiligingssysteem werd doorbroken, wordt niet als constitutief element voor de strafbaarstelling gehanteerd, omdat deze een aantal complicaties met zich meebrengt (welk niveau van beveiliging wordt vereist, openbaar worden van de beveiligingsvoorzieningen naar aanleiding van de bewijsvoering, …) en wellicht zonder veel inhoud wordt, nu systeembeveiliging meer en meer standaard wordt.

Bovendien moet erop worden gewezen dat deze bepaling de ongeoorloofde toegang tot het systeem als zodanig beteugelt. Wanneer een persoon zich op ongeoorloofde wijze toegang verschaft tot persoonsgegevens, zijn de strafbepalingen van de wet van 8 december 1992 op de bescherming van persoonsgevens reeds van toepassing. Overigens blijven, onverminderd deze nieuwe strafbepaling, ook strafbepalingen uit andere beschermingsregimes voor bepaalde categorieën van gegevens toepasselijk. De filosofie die ten grondslag ligt aan het ontwerp houdt immers in dat, wanneer bepaalde inlichtingen omwille van hun aard zelf een bijzondere bescherming rechtvaardigen, dit het voorwerp moet uitmaken van een apart beschermingsregime : het feit of deze inlichtingen vastgelegd zijn op papier of op een geïnformatiseerde drager, is ter zake irrelevant (*off-line = on-line*). Het door de nieuwe bepalingen beschermde rechtsbelang is op de eerste plaats de integriteit van het systeem.

Naast de centrale basisgedragingen worden eveneens een aantal gevolghandelingen strafbaar gesteld (§ 3), in de vorm van verzwarende omstandigheden bij het basismisdrijf in zijn beide varianten (§§ 1 en 2). Het gaat om de volgende gedragingen : naar aanleiding van het hacken,

-— hetzij kennisnemen of overnemen van gegevens (bijvoorbeeld het stelen van industriële geheimen in het kader van bedrijfsspionage);

— hetzij gebruikmaken van het systeem (bijvoorbeeld het benutten van de capaciteit van het systeem waardoor de mogelijkheden van andere gebruikers tijdelijk beperkt worden);

— hetzij veroorzaken van schade uit onvoorzichtigheid (opzettelijke sabotage wordt in het kader van artikel 550*ter* zwaarder bestraft).

Deze drie gedragingen worden in de context van het voorontwerp enkel strafwaardig geacht, omdat zij terzelfdertijd of na de « *hacking* » worden gepleegd. De Raad van State acht deze bepaling onduidelijk, omdat ze niet beantwoordt aan de definities van R(89)9.

analogies avec le monde du « papier » (coffres-forts, etc.) : le « *hacking* » doit être considéré comme un délit de mise en danger punissable en tant que tel, quels que soient les intentions malveillantes particulières ou les effets atteints.

La condition d'effraction d'un système de protection n'est pas utilisée comme élément constitutif de l'incrimination parce qu'elle entraîne un certain nombre de complications (quel est le niveau de protection requis, nécessité de révéler les systèmes de protection lors de l'établissement de la preuve, ...) et qu'elle est probablement devenue sans objet maintenant que les protections de systèmes sont de plus en plus standard.

En outre, il faut noter que cette disposition sanctionne l'accès non autorisé en tant que tel. Lorsqu'une personne accède de façon illicite à des données à caractère personnel, les dispositions de la loi du 8 décembre 1992 sur la protection des données à caractère personnel sont également d'application. Par ailleurs, sans préjudice de cette disposition, les dispositions pénales d'autres régimes de protection concernant des catégories particulières de données restent d'application. En effet, la philosophie à la base du projet de loi repose sur l'idée que lorsque certaines informations justifient une protection spéciale du fait même de leur nature, il y a lieu de prévoir un régime de protection séparé : le fait que ces informations soient consignées sur papier ou sur un support informatique est non pertinent à cet égard (*off-line = on-line*). L'intérêt juridique protégé par les nouvelles dispositions est en premier lieu l'intégrité du système.

Outre les comportements de base centraux, un certain nombre d'actes qui en découlent sont également punis (§ 3) sous la forme de circonstances aggravantes du délit de base dans ses deux variantes (§§ 1er et 2). Il s'agit des comportements suivants : à la suite de l'accès illicite,

— soit prendre connaissance ou s'emparer de données (par exemple, vol de secrets d'entreprise dans le cadre de l'espionnage industriel);

— soit faire usage du système (par exemple, utilisation de la capacité du système, entraînant une limitation temporaire des possibilités d'autres utilisateurs);

— soit causer un dommage par imprudence (le sabotage intentionnel est puni plus sévèrement dans le cadre de l'article 550*ter*).

Dans le contexte du présent avant-projet de loi, ces trois comportements sont considérés comme punissables uniquement parce qu'ils sont adoptés en même temps que ou après le « *hacking* ». Le Conseil d'État juge cette disposition confuse parce qu'elle ne répond pas aux définitions du R(89)9.

Vooreerst hebben de voormelde aanbevelingen van de Raad van Europa een ander en ruimer toepassingsgebied waarvan het niet de bedoeling was het over te nemen in het voorontwerp. Bovendien worden in § 2 enkel drie specifieke verzwarende omstandigheden omschreven van een reeds als zodanig strafbare gedraging. De verwijzingen naar spionage of tijdsdiefstal dienen enkel als voorbeelden.

Een andere gevolghandeling die wordt strafbaar gesteld is het « helen » van de naar aanleiding van de « *hacking* » bekomen gegevens (§ 7). Aangezien het misdrijf heling traditioneel enkel materiële voorwerpen kan betreffen, is deze bepaling vooral voor de context van spionagebestrijding belangrijk. De formulering is gelijklopend met een soortgelijke bepaling inzake het onderscheppen van communicatie (zie met name artikel 314*bis*, § 2, van het Strafwetboek).

Naast de basisgedraging en de gevolghandelingen, wordt eveneens de poging om zich onrechtmatig toegang te verschaffen tot een informaticasysteem of een deel daarvan, strafbaar gesteld (§ 4). Gezien de ernst van deze gedragingen wordt dezelfde strafmaat voorzien als voor het voltooide misdrijf. Men kan hierbij met name denken aan het geautomatiseerd uitproberen van lange listings van mogelijke paswoorden. Niet alleen kan dit een zekere tijd in beslag nemen met alle risico's vandien voor het systeem, maar bovendien zal de dader vaak eerder geïnteresseerd zijn in het bekomen van de toegangscode op zich dan in het effectief binnenbreken in de computer.

Daarnaast wordt er eveneens een specifieke bepaling ingevoerd die een aantal voorbereidingshandelingen tot « *hacking* » beteugelt (§ 5), met name het opsporen, verzamelen, ter beschikking stellen, verspreiden of verhandelen van bepaalde middelen om te kunnen « hacken ». Hierbij worden in de eerste plaats de handel in « *hackertools* » en de toegangscodezwendel geviseerd. Om te vermijden dat deze bepaling een hinderpaal zou kunnen vormen voor de vrije verspreiding van algemene informatie inzake beveiligingstechnieken, wordt een bijzonder opzet vereist.

Bovendien wordt de opdrachtgever of aanzetter tot « *hacking* » zwaarder gestraft dan degene die het misdrijf effectief uitvoert (§ 6). De reden hiervoor is dat, waar vroeger « *hacking* » in veel gevallen een tijdverdrijf was voor jonge computerfreaks, thans professionele criminelen dergelijke personen inschakelen om hun plannen uit te voeren.

Er wordt eveneens een bijzonder, strenger regime voorzien, ingeval van herhaling.

— Data- en informaticasabotage

Het nieuwe artikel 550*ter* van het Strafwetboek heeft betrekking op data- en informaticasabotage.

Tout d'abord, les recommandations précitées du Conseil de l'Europe couvrent un champ d'application différent et plus large qu'il n'était pas prévu de reprendre dans le projet de loi. Ensuite, le § 2 énonce seulement trois circonstances aggravantes spécifiques d'un comportement déjà punissable en tant que tel. L'espionnage ou le vol de temps sont uniquement évoqués à titre d'exemples.

Autre acte rendu punissable : le « recel » de données obtenues à la suite d'un « *hacking* » (§ 7). Comme traditionnellement le délit de recel peut uniquement concerner des objets matériels, cette disposition est importante principalement dans le contexte de la lutte contre l'espionnage. La formulation est analogue à celle d'une disposition similaire concernant l'interception de communications (voir notamment l'article 314*bis*, § 2, du Code pénal).

Outre le comportement de base et les actes qui en découlent, la tentative d'accéder à l'ensemble ou à une partie d'un système informatique sans y être autorisé est également rendue punissable (§ 4). Vu la gravité de ces comportements, il est prévu la même peine que celle qui vise l'accomplissement du délit. On peut ici penser notamment à l'essai automatisé de longues listes de mots de passe. Non seulement cette opération peut prendre un certain temps avec les risques qui en découlent pour le système, mais en outre, l'auteur sera souvent plus intéressé par l'obtention du code d'accès pour lui-même que par l'accès effectif au système informatique.

De plus, il est également inséré une disposition spécifique en vue de réprimer un certain nombre de comportements préparatoires au « *hacking* » (§ 5), à savoir le fait de rechercher, de rassembler, de mettre à disposition, de diffuser ou de commercialiser certains moyens permettant le « *hacking* ». À cet égard, on vise en premier lieu le commerce de « *hackertools* » et l'escroquerie en matière de codes d'accès. Une intention particulière est requise afin d'éviter que cette disposition puisse constituer une entrave à la libre diffusion d'informations générales en matière de techniques de protection.

Enfin, le commanditaire ou l'instigateur du « *hacking* » est puni plus sévèrement que la personne qui a effectivement commis le délit (§ 6). La raison est la suivante : si auparavant le « *hacking* » constituait dans bien des cas un divertissement pour les jeunes fanatiques d'informatique, aujourd'hui des criminels professionnels engagent de telles personnes pour accomplir leurs desseins.

Il est également prévu un régime particulier plus strict en cas de récidive.

— Sabotage de données et sabotage informatique

L'article 550*ter* nouveau du Code pénal concerne le sabotage de données et le sabotage informatique.

Deze bepaling beoogt, net als de voorgaande, een manifeste lacune in ons strafrecht in te vullen. Vernielingen en beschadigingen worden traditioneel in het strafrecht enkel in aanmerking genomen wanneer ze betrekking hebben op tastbare voorwerpen. Dit is het geval wanneer het schade betreft aan een informaticasysteem zelf, maar het is duidelijk dat het beschadiging van data *as such* niet rechtstreeks wordt geviseerd door de bepalingen van het Strafwetboek. Daarom wordt in de nieuwe bepaling elke kwaadwillige manipulatie van gegevens strafbaar gesteld (§ 1).

Indien hierdoor schade ontstaat, wordt ook het veroorzaken van schade aan informaticasystemen opgenomen, omdat in de praktijk schade aan data en schade aan het computersysteem zelf vaak samen zullen voorkomen en technisch niet altijd strict te scheiden zijn. Niettemin is het wenselijk een juridisch onderscheid te maken tussen de gevolgen voor de data en voor een informaticasysteem. Gezien het belang dat informaticasystemen in onze samenleving innemen, wordt het belemmeren van de correcte werking van een informaticasysteem (§ 3) zwaarder bestraft dan het louter berokkenen van schade aan de data (§ 2).

Naast de delicten die kwaadwillige manipulaties en de gevolgen die daaruit voortvloeien viseren, wordt ook een strafbaarstelling voorzien inzake bepaalde voorbereidingshandelingen. Hierbij wordt gedacht aan de ontwikkeling en de verspreiding van schadelijke gegevens en computerprogramma's zoals virussen of programma's om dergelijke virussen te genereren (§ 4).

Voor de strafbaarheid wordt een bijzonder opzet vereist : het opzet te bedriegen of te schaden. Aldus wordt vermeden dat de commercialisering van data of programma's waarvan een legitieme aanwending mogelijk is, maar die evenwel ook misbruikt kunnen worden, in het algemeen zou worden verboden.

Er wordt eveneens een bijzonder, strenger regime voorzien, ingeval van herhaling (§ 5).

C. ARTIKELSGEWIJZE BESPREKING VAN HET ONTWERP ARTIKEL 77 (Nr 214/1)

Artikel 1

Dit artikel bepaalt de constitutionele bevoegdheidsgrondslag.

Art. 2

In het Wetboek van strafvordering worden een aantal vernieuwingen ingevoerd inzake opsporings- en

Cette disposition, tout comme la précédente, vise à combler une lacune manifeste de notre droit pénal. Traditionnellement, celui-ci ne prend en compte les destructions et les dommages que lorsqu'ils se rapportent à des objets tangibles. C'est le cas lorsque le dommage concerne un système informatique mais il est clair que les dommages occasionnés aux données en tant que telles ne sont pas directement visés par les dispositions de notre Code pénal. C'est la raison pour laquelle la nouvelle disposition punit toute manipulation de données effectuée dans le but de nuire (§ 1er).

Si des dommages en résultent, les causes des dommages occasionnés au système informatique sont également reprises parce que dans la pratique, les dommages causés aux données et au système informatique même se produiront souvent simultanément et que, d'un point de vue technique, on ne peut pas toujours les différencier de manière stricte. Toutefois, il est souhaitable d'établir une distinction juridique entre les conséquences sur les données et celles qui concernent le système informatique. Compte tenu de l'importance que prennent les systèmes informatiques dans notre société, le fait d'empêcher le bon fonctionnement d'un système informatique (§ 3) est puni plus sévèrement que le simple fait de causer des dommages aux données (§ 2).

Outre les délits qui visent les manipulations effectuées en vue de nuire et les conséquences qui en découlent, une incrimination est également prévue en ce qui concerne certains actes préparatoires. On pense à cet égard à l'élaboration et à la diffusion de données pouvant causer des dommages et de programmes informatiques tels que des virus ou de programmes visant à développer pareils virus (§ 4).

L'incrimination requiert une intention particulière, à savoir l'intention de frauder ou de nuire. Cela permet, d'un point de vue général, de ne pas interdire la commercialisation de données ou de programmes dont il peut être fait légitimement usage mais qui peuvent néanmoins être utilisés de manière abusive.

Un régime particulier, plus sévère, est également prévu en cas de récidive (§ 5).

C. COMMENTAIRE PAR ARTICLES DU PROJET ARTICLE 77 (N° 214/1)

Article 1er

Le présent article détermine la base constitutionnelle de compétence.

Art. 2

Un certain nombre d'innovations relatives aux actes d'information et d'instruction posés dans un contexte

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 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 daarvan (bijvoorbeeld de computer, optische schijven, diskettes, …).

Als de gerechtelijke overheid enkel over de data wil beschikken, maar het informaticasysteem of andere dragers ter plaatse wil laten, is de juridische situatie verschillend, met name vooral omdat inbeslagneming de onttrekking van het betreffende voorwerp aan de beschikking van degene die het onder zich houdt, vereist, en het kopiëren van data derhalve niet als zodanig kan worden geassimileerd met de inbeslagneming van materiële voorwerpen.

De nieuwe bepaling creëert bijgevolg een adequate rechtsbasis voor een nieuw dwangmiddel met dezelfde finaliteiten als de inbeslagneming. Voor zover in deze nieuwe bepaling geen afwijkende regels worden bepaald, is het derhalve logisch dat de regels inzake inbeslagneming op het databeslag van toepassing zijn. De nieuwe maatregel moet evenwel onderscheiden worden van het onderscheppen van telecommunicatie, dat betrekking heeft op het capteren van data in transmissie.

De 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 gevallen, namelijk dringendheid of 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 versleutelingstechnieken). Aldus benadert men het dichtst de situatie van een klassieke inbeslagneming. Er kan evenwel beslist worden om gegevens of een deel daarvan niet te blokkeren, bijvoorbeeld om de continuïteit van de werking van een systeem of een organisatie niet in het gedrang te brengen.

3) Het blokkeren van de gegevens kan worden vervangen door het wissen ervan, in twee gevallen :

— de procureur des Konings acht de gegevens strijdig met de openbare orde of de goede zeden (bijvoorbeeld kinderpornografie, racistische pamfletten);

informatisé sont insérées dans le Code d'instruction criminelle. La première d'entre elles est contenue à l'article 39*bis* (*nouveau*) du Code d'instruction criminelle et concerne la saisie des données.

La saisie de données pertinentes pour l'instruction, stockées, traitées ou transmises par le biais d'un système informatique, peut s'effectuer intégralement conformément à la procédure traditionnelle dans la mesure où elle s'accompagne de la saisie du support matériel sur lequel elles se trouvent (par exemple l'ordinateur, des disques optiques, des disquettes, …).

Lorsque les autorités judiciaires veulent disposer uniquement des données et ne pas saisir le système informatique ou les autres supports, la situation juridique se présente différemment, principalement parce que la saisie requiert la soustraction de l'objet en question à celui qui le détient. Par conséquent, la copie de données ne peut pas être assimilée en tant que telle à la saisie d'objets matériels.

La nouvelle disposition crée par conséquent une base juridique adéquate pour un nouveau moyen coercitif ayant les mêmes finalités que la saisie. Dans la mesure où aucune dérogation n'est prévue dans cette nouvelle disposition, il est logique que les règles en matière de saisie s'appliquent à la saisie de données. La nouvelle mesure doit cependant être distinguée de l'interception de télécommunications, qui a trait au captage de données en cours de transmission.

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

1) En principe, les données pertinentes sont copiées sur des supports de l'autorité. Les supports dont disposent les personnes compétentes pour utiliser le système ne peuvent être employés que dans deux cas, à savoir en cas d'urgence ou de problèmes techniques.

2) En outre, l'accès à ces données qui se trouvent dans le système informatique qui fait l'objet de la recherche ou sur les supports présents sur place est en principe bloqué (par exemple au moyen de techniques de cryptage). On se rapproche ainsi le plus possible de la situation d'une saisie classique. Il peut toutefois être décidé de ne pas bloquer les données en tout ou partie, par exemple pour ne pas nuire à la poursuite du fonctionnement d'un système ou d'une organisation.

3) Au blocage des données peut se substituer leur retrait du système informatique, ce dans deux cas :

— le procureur du Roi estime que les données sont contraires à l'ordre public et aux bonnes mœurs (par exemple de la pornographie enfantine, des pamphlets à caractère raciste);

— 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.

4) Wanneer kopiëren niet mogelijk is, bijvoorbeeld omdat de toepassingsprogrammatuur zeer complex is en elders niet beschikbaar is of omdat de hoeveelheid data te omvangrijk is, worden de gegevens enkel geblokkeerd, wat in feite neerkomt op de informatische variant van verzegeling.

5) 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.

De Raad van State meent dat deze « verantwoordelijke van het informaticasysteem » in de tekst van het voorontwerp zelf moet worden omschreven. De bedoeling van het op de hoogte brengen van de maatregel is evenwel duidelijk te stellen dat het niet gaat om een geheime maatregel (vergelijk met de huiszoekingsbevoegdheid). De terminologie in het voorontwerp behoudt in dat opzicht enige flexibiliteit aangaande de te contacteren persoon : het kan inderdaad niet in alle gevallen *a priori* eenduidig vastgesteld worden wie de reële of juridische controle heeft over het systeem.

Inzake het vrijwaren van rechten van derden ingeval van databeslag, vult het wetsontwerp op verschillende punten het gemeen recht ter zake aan :

— artikel 39, § 2, eerste lid, en § 5 : een specifieke zorgplicht voor de procureur des Konings voor de bewaring van de data; dit is in het belang van de strafvordering, maar ook in het belang van de rechthebbenden;

— artikel 39, § 2, tweede lid : mogelijkheid voor de procureur des Konings om de betrokkenen in het bezit te laten van de data (in het bijzonder om disproportionele benadeling te voorkomen, bijvoorbeeld de continuïteit van een bedrijf);

— artikel 39, § 4 : een specifieke informatieplicht.

Daarnaast, is het gemeen recht inzake rechtsmiddelen uiteraard onverkort van toepassing. In het bijzonder artikel 28*sexies* en artikel 61*quater* van het Wetboek van strafvordering. Er wordt ter zake niet anders gehandeld dan bijvoorbeeld bij de inbeslagneming van een boekhouding, klanten- en leveranciersdossiers, beslag op bankrekeningen.

6) Gezien de vluchtigheid van data en de risico's dat op de « inbeslaggenomen » data ongeoorloofde manipulaties zouden plaatsvinden die hun bewijswaarde in het gedrang kunnen brengen, wordt een beveiligings-

— le procureur du Roi considère que les données risquent d'endommager le système (par exemple des virus informatiques).

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

4) Lorsque la copie n'est pas possible, par exemple parce que le programme d'application est très complexe et qu'il n'est pas disponible autrement ou en raison du volume des données, ces dernières sont seulement bloquées, ce qui équivaut en fait à une variante informatique de la mise sous scellés.

5) L'obligation d'informer le responsable du système informatique constitue une garantie générale. À cet égard, il est communiqué un résumé des opérations effectuées concernant ces données. En effet, dans un environnement informatique, vouloir dresser un inventaire exhaustif relève souvent de l'utopie.

Le Conseil d'État estime que le texte de l'avant-projet de loi doit lui-même contenir une définition du « responsable du système informatique ». Le but de la communication de la mesure est toutefois d'établir clairement qu'il ne s'agit pas d'une mesure secrète (cf. la compétence de perquisitionner). La terminologie de l'avant-projet comporte dans cette optique une certaine souplesse pour ce qui est de la personne à contacter : en effet, il n'est pas possible de déterminer *a priori* pour tous les cas et de manière univoque qui exerce le contrôle réel ou juridique sur le système.

En ce qui concerne la préservation des droits de tiers en cas de saisie de données, le projet de loi complète le droit commun en la matière sur différents points :

— article 39, § 2, alinéa 1er, et § 5 : obligation spécifique pour le procureur du Roi de veiller à la conservation des données, ce dans l'intérêt de l'action publique, mais également des ayants droit;

— article 39, § 2, alinéa 2 : possibilité pour le procureur du Roi de laisser les données en la possession des intéressés (en particulier pour éviter un préjudice disproportionné, par exemple au niveau de la continuité d'une entreprise);

— article 39, § 4 : devoir d'information spécifique.

En outre, il va de soi que le droit commun relatif aux voies de recours est d'application dans son intégralité, en particulier les articles 28*sexies* et 61*quater* du Code d'instruction criminelle. En l'occurrence, l'attitude adoptée ne diffère pas de celle qui prévaut par exemple à l'occasion de la saisie d'une comptabilité, de dossiers de clients ou de fournisseurs, ou encore d'une saisie sur des comptes bancaires.

6) Étant donné le caractère volatile des données et le risque de voir les données « saisies » subir des manipulations illicites susceptibles de nuire à leur valeur de preuve, une condition de protection est posée

eis ingesteld teneinde de vertrouwelijkheid en de integriteit van de gegevens die het voorwerp uitmaken van de nieuwe dwangmaatregel te waarborgen.

Deze beveiligingseis wordt logischerwijze ook uitgebreid tot de gegevens, die samen met hun materiële drager in beslag worden genomen.

De Raad van State is van oordeel dat « de gepaste middelen » die de procureur des Konings hiertoe moet aanwenden in de tekst moeten worden aangegeven. Dit advies gaat evenwel voorbij aan de specificiteit van de evolutie van de informatietechnologie :

— het gaat om technische middelen, en derhalve is de aard daarvan afhankelijk van de stand van de technologie, evenals van de specifieke vereisten van de data;

— deze middelen hebben als zodanig geen effect op de *bewijswaarde* van de data, maar betreffen de modaliteiten van de onttrekking of bewaring van de data, waardoor nodeloze bewijsbetwistingen voor de rechter kunnen worden voorkomen;

— bovendien gaat het hier om een wettelijke vereiste met het oog op het beschermen van het bewijsmateriaal; deze bestaat zelfs niet in het gemeen recht, en werd ingevoegd omwille van de eigenheid van de geïnformatiseerde omgeving.

Art. 3

Deze bepaling voert een nieuw artikel 88*ter* in in het Wetboek van strafvordering, dat betrekking heeft op de netwerkzoeking.

Een beperking bij een traditionele dwangmaatregel zoals de huiszoeking is dat ze, per definitie, enkel mag worden uitgevoerd ten aanzien van de plaats waarvoor ze wordt bevolen. Kenmerkend voor informaticasystemen — of het nu gaat om grote systemen binnen bedrijven of om handige draagbare computers — is dat ze meer en meer verbonden zijn in netwerken.

Wanneer de informaticasystemen waarin onderzoek noodzakelijk blijkt te zijn, zich op verschillende locaties bevinden, zijn derhalve in de bestaande context meerdere bevelen tot huiszoeking of inbeslagneming vereist. Het is duidelijk dat een dergelijke benadering problematisch is : niet alleen bestaat het risico dat bij niet gelijktijdig optreden bewijsmateriaal verloren gaat, maar bovendien zal in veel gevallen niet *a priori* vastgesteld kunnen worden op welke plaatsen de zoeking moet plaatsvinden, welke bestanden relevant zijn, of zelfs waar de computers geografisch gesitueerd zijn.

Om hieraan te verhelpen bepaalt het nieuwe artikel de voorwaarden waarin de uitbreiding van de zoeking in een informaticasysteem naar elders gesitueerde systemen toegelaten is. Hierbij moet het gaan om onderling verbonden systemen.

afin de garantir la confidentialité et l'intégrité des données qui font l'objet de la nouvelle mesure coercitive.

Cette condition de protection est logiquement étendue aux données saisies avec leur support matériel.

Le Conseil d'État est d'avis que les « moyens appropriés » à mettre en œuvre par le procureur du Roi doivent être indiqués dans le texte. Cet avis ne tient toutefois pas compte de la spécificité de l'évolution de la technologie de l'information :

— il s'agit de moyens techniques; par conséquent, leur nature dépend de l'état d'avancement de la technologie ainsi que des exigences spécifiques des données;

— ces moyens n'influencent en soi pas la *validité* des données en tant *qu'éléments de preuve* mais se rapportent aux modalités relatives à la soustraction ou à la conservation des données, ce qui permet d'éviter de saisir inutilement le juge pour des contestations en matière de preuve;

— de plus, il s'agit dans ce cas d'une exigence légale destinée à protéger les éléments de preuve; cette exigence n'existe même pas en droit commun, elle a été insérée en raison de la spécificité de l'environnement informatisé.

Art. 3

Cette disposition insère dans le Code d'instruction criminelle un nouvel article 88*ter* qui concerne les recherches sur les réseaux.

Une mesure coercitive traditionnelle, telle que la perquisition, est restrictive en ce sens que, par définition, elle ne peut être effectuée que sur le lieu pour lequel elle a été ordonnée. Ce qui caractérise les systèmes informatiques — qu'il s'agisse de systèmes importants dans des sociétés ou d'ordinateurs portables — c'est qu'ils sont de plus en plus connectés en réseaux.

Dans le contexte actuel, lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en divers endroits, plusieurs mandats de perquisition ou de saisie doivent être délivrés. Pareille approche suscite bien évidemment des problèmes : on court non seulement le risque de voir des éléments de preuve disparaître si l'intervention n'est pas simultanée mais en outre dans de nombreux cas, il ne sera pas possible *a priori* de déterminer les endroits où doivent s'effectuer les recherches, les fichiers pertinents ou même la localisation géographique des ordinateurs.

Pour pallier ces problèmes, le nouvel article fixe les conditions qui permettent l'extension de la recherche dans un système informatique vers des systèmes situés ailleurs. Il doit s'agir de systèmes liés entre eux.

De maatregel moet vooreerst noodzakelijk zijn voor de waarheidsvinding, en bovendien moet, hetzij een risico bestaan dat de bewijsgaring in het gedrang komt, hetzij het nemen van andere maatregelen (bijvoorbeeld meerdere huiszoekingsbevelen) disproportioneel zijn. Het komt aan de onderzoeksrechter toe om dit in redelijkheid te beoordelen. Omwille van het uitzonderlijke karakter van de uitbreiding van de zoeking in een informacticasysteem, meer bepaald het mogelijke extraterritoriale effect ervan, mag een dergelijke zoeking enkel uitgebreid worden inzoverre dit noodzakelijk is in het kader van de concrete strafzaak waarmee de onderzoeksrechter is gelast.

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. De maatregel gaat inderdaad niet zo ver dat de overheid gerechtigd zou worden om onbeperkt alle systemen die mogelijk met het onderzochte computersysteem in verbinding staan of kunnen gebracht worden, te doorzoeken. De technische verbinding via de netwerken moet een element van permanentie en stabiliteit inhouden, en niet louter occasioneel zijn.

Het is evenmin toegelaten dat de overheidsdiensten bijvoorbeeld via 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 derhalve verboden.

Daarbij moet er bovendien op worden gewezen dat in de context van de netwerkzoeking dezelfde regels gelden inzake personen die onderworpen zijn aan een beroepsgeheim als in het geval van een klassieke huiszoeking.

De internationale verwevenheid van de netwerken zal wellicht onvermijdelijk aanleiding geven tot gevallen, waar tijdens de netwerkzoeking bestanden worden bevraagd of zouden moeten worden geconsulteerd die zich, zonder dat de gerechtelijke diensten zich dit tijdig realiseren, in het buitenland zijn gesitueerd. De mogelijkheden om als zodanig doelbewust de zoeking uit te breiden naar systemen die in het buitenland zijn gesitueerd, roepen in de huidige stand van het internationale publiekrecht een aantal juridische vragen op. De bevoegdheden waarover de overheid beschikt om onderzoekshandelingen te stellen in het kader van een strafprocedure kunnen immers in principe enkel worden uitgeoefend op het nationale territorium waarover die overheid gezag heeft. Dit houdt ongetwijfeld verband met het feit dat het strafrecht zeer sterk verbonden is met de notie van staatssoevereiniteit. Het hangt eveneens samen met het beginsel van de goede trouw in de

La mesure doit avant tout être nécessaire à la manifestation de la vérité et il faut en outre qu'il y ait un risque de perdre des éléments de preuve ou que la prise d'autres mesures (par exemple plusieurs mandats de perquisition) soit disproportionnée. Il appartient au juge d'instruction d'apprécier raisonnablement ces considérations. En raison du caractère exceptionnel de l'extension de la recherche dans un système informatique, notamment en raison de ses éventuels effets extra-territoriaux, une telle recherche ne pourra être étendue que si elle apparaît nécessaire dans le cadre d'une affaire pénale concrète dont le juge est saisi.

L'exercice de cette nouvelle compétence se limite aux personnes autorisées à utiliser le système informatique qui fait l'objet de la recherche. En effet, la mesure ne permet pas aux autorités d'effectuer des recherches de manière illimitée dans tous les systèmes susceptibles d'être en relation ou d'être mis en relation avec le système informatique qui fait l'objet de la mesure. La liaison technique par le biais d'un réseau doit présenter un élément de permanence et de stabilité et ne peut être purement occasionnelle.

De même, les services publics ne sont pas autorisés à effectuer, via leurs propres systèmes informatiques, des recherches dans d'autres systèmes non accessibles au public et à propos desquels on suppose qu'ils sont utilisés à des fins criminelles. Par conséquent, l'utilisation par les autorités d'une mesure de surveillance nouvelle et secrète telle que le « *hacking* » est interdite.

Il faut en outre ajouter qu'en ce qui concerne les personnes qui sont soumises à un secret professionnel, les mêmes règles s'appliquent dans le contexte de la recherche sur réseau que dans le cadre d'une perquisition classique.

Le caractère international des réseaux engendrera inévitablement des situations dans lesquelles, lors de la recherche sur réseau, des fichiers seront ou devront être consultés avant même que les services judiciaires n'aient le temps de réaliser que ces fichiers proviennent de l'étranger. Les possibilités d'étendre de manière consciente la recherche à des systèmes se trouvant à l'étranger suscitent un certain nombre de questions juridiques compte tenu de l'état actuel du droit public international. La compétence des autorités de poser des actes d'instruction dans le cadre d'une procédure pénale ne peut être exercée, en principe, que sur le territoire national placé sous leur autorité. Ceci est certainement dû au fait que le droit pénal est étroitement lié avec les principes de souveraineté nationale et de bonne foi dans les relations interétatiques. De même, l'interprétation classique du concept de souveraineté est influencée par l'internationalisation sans cesse croissante

interstatelijke betrekkingen. Tegelijk komt de klassieke invulling van het concept soevereiniteit in deze context onder druk te staan, enerzijds omwille van de toenemende internationalisering van de financieel-economische criminaliteit, en anderzijds door de enorme vlucht die de informatietechnologie heeft genomen. Men is er zich meer en meer van bewust dat de traditionele vormen van internationale gerechtelijke samenwerking, die juist in het leven werden geroepen om aan de beperkingen van de nationale opsporings- en onderzoeksbevoegdheden te remediëren, niet enkel moeten worden gemoderniseerd, maar op sommige punten moeten worden geïnnoveerd. Vandaar dat thans met name inzake opsporingen en onderzoek in een IT-context op internationaal vlak naar oplossingen wordt gezocht in diverse fora (Europese Unie, Raad van Europa, blz. 8).

Het huidige ontwerp kan derhalve niet eenzijdig oplossingen aanreiken voor alle vragen die kunnen rijzen inzake de internationale netwerkzoeking. Een aantal punten zullen onmiskenbaar via internationale instrumenten of overleg met andere staten moeten worden behandeld. Dit neemt evenwel niet weg dat de problemen vandaag bestaan, en dat derhalve een juridisch houvast moet worden geboden aan de mensen die op het terrein naar aanleiding van een zoeking in een computersysteem met de problematiek van op internationale schaal verbonden informaticasystemen worden geconfronteerd. Er moet immers een antwoord geboden worden aan de noden van een effectieve criminaliteitsbestrijding op de informatiesnelwegen.

Daarom wordt in dit ontwerp in deze materie een voorzichtige, maar pragmatische positie ingenomen. Het is duidelijk dat de grensoverschrijdende zoeking niet als regel kan worden gesteld. Er kunnen immers ernstige problemen rijzen, wanneer de gerechtelijke overheden van een staat eenzijdig en welbewust een netwerkzoeking uitbreiden naar het buitenland zonder de bevoegde buitenlandse autoriteiten hierin te kennen. Wanneer derhalve voldoende tijd en kennis voorhanden is, moet de weg van de klassieke internationale rogatoire commissies worden gevolgd, bij ontstentenis van juridisch adequate alternatieven op dit ogenblik.

De wijze waarop computers, evenals de verbindingen daartussen, functioneren, kan zeer complex zijn. Daardoor zijn er situaties denkbaar waar tijdens een zoeking in een computersysteem data worden bekomen die niet zijn opgeslagen op de plaats waar de zoeking plaatsvindt (elders in het land of in het buitenland), maar waar de speurders zich hiervan niet bewust zijn of er niet in slagen de exacte lokatie van de data te bepalen.

Wanneer per toeval of onopzettelijk data uit het buitenland worden bekomen, staat de rechtmatigheid van het strafprocessueel optreden van de overheid niet prin-

de la criminalité économico-financière, d'une part, et par la rapidité avec laquelle la technologie de l'information évolue, d'autre part. On est de plus en plus conscient du fait qu'il est nécessaire de moderniser et, sur certains points, d'innover les formes traditionnelles d'entraide judiciaire internationale mises en place justement pour pallier les lacunes sur le plan des compétences en matière d'information et d'instruction au niveau national. D'où la raison d'organiser différents forums pour apporter la solution aux problèmes rencontrés, dans le contexte de la technologie de l'information, en matière d'instruction et d'information au niveau international (Union européenne, Conseil de l'Europe, p. 8).

Par conséquent, le présent projet n'offre pas de réponses unilatérales à toutes les questions qui peuvent se poser en matière de recherche internationale sur réseau. Un certain nombre de points devront indéniablement être traités à l'aide d'instruments internationaux ou en concertation avec d'autres États. Néanmoins, les problèmes se posent aujourd'hui et il est dès lors indispensable d'offrir des points d'appui juridiques aux personnes qui, à la suite d'une recherche dans un système informatique, sont confrontées sur le terrain à la problématique des systèmes informatiques en réseau. Il convient de répondre de manière satisfaisante aux besoins en matière de lutte contre la criminalité sur les autoroutes de l'information.

C'est pour cette raison qu'a été adoptée, dans le présent projet, une attitude prudente mais pragmatique en la matière. Il est clair que les recherches effectuées en dehors des frontières doivent rester exceptionnelles. Des problèmes peuvent néanmoins surgir lorsque les autorités judiciaires d'un État étendent unilatéralement et consciemment leurs recherches sur réseau à l'étranger sans en informer les autorités étrangères compétentes. Si le temps et les connaissances le permettent, et à défaut de solutions alternatives adéquates sur le plan juridique à l'heure actuelle, il convient de suivre la procédure classique des commissions rogatoires internationales.

Le mode de fonctionnement ainsi que les connexions des ordinateurs peuvent être très complexes. C'est pourquoi on peut envisager des situations dans lesquelles il est possible, lors d'une recherche dans un système informatique, d'obtenir des données qui ne sont pas stockées à l'endroit où s'effectue la recherche (c'est-à-dire ailleurs dans le pays ou à l'étranger), et dont les enquêteurs ignorent l'existence ou ne parviennent pas à localiser l'origine avec exactitude.

Lorsque des données sont recueillies à l'étranger par hasard ou involontairement, le bien-fondé de l'action pénale menée par les autorités ne peut en principe pas

cipieel ter discussie en is er derhalve geen aanleiding om de bekomen gegevens internrechtelijk *a priori* als bewijsmateriaal uit te sluiten. Nadat is vastgesteld dat de data in het buitenland werden bekomen, is het evenwel in het kader van goede interstatelijke betrekkingen aangewezen contact te nemen met de overheid van de andere betrokken staat waar de data gelokaliseerd zijn, als deze redelijkerwijze kan worden bepaald, teneinde deze staat toe te laten een standpunt ter zake in te nemen.

Ingeval de speurders tijdens de zoeking wel kennis hebben van het feit dat de gezochte bestanden in het buitenland gesitueerd zijn, maar er redelijkerwijze niet in slagen de betrokken staat te identificeren, wordt dezelfde oplossing als hiervoor vermeld weerhouden, aangezien ook internationaal overleg deze situatie niet kan oplossen.

Daarnaast moet tegelijk vastgesteld worden dat een impasse dreigt te ontstaan, omdat de logica die geldt voor een louter nationale uitbreiding van een zoeking in een informaticasysteem, onverkort en misschien nog sterker geldt in een « *global village* ». Het belang om in dringende gevallen de teloorgang van computerbestanden te vrijwaren voor de bewijsvoering botst hier op de thans nog algemeen verspreide traditionele invulling van het concept soevereiniteit. Men denke hier bijvoorbeeld aan het geval waar tijdens de zoeking wordt vastgesteld dat de relevante files zich op een welbepaalde plaats in het buitenland bevinden. Het stopzetten van de zoeking en het instellen van een internationale rogatoire commissie om ter plekke een huiszoeking te laten uitvoeren biedt de betrokkenen alle mogelijkheden om via de telecommunicatiekanalen ondertussen de data zelf te laten verdwijnen.

Vandaar de nood om in spoedeisende gevallen, naar analogie met de regelingen inzake « *hot pursuit* » over te kunnen gaan tot het nemen van voorlopige maatregelen om de teloorgang van het bewijsmateriaal te vrijwaren (kopiëren, maar niet blokkeren van de data). Het belang van de waarheidsvinding in gevallen van ernstige criminaliteit kan een dergelijke grensoverschrijdende zoeking uitzonderlijk rechtvaardigen. In dergelijke gevallen is het evenwel onontbeerlijk om de betrokken andere staat te informeren teneinde deze toe te laten na te gaan of al dan niet een inbreuk op de rechtsorde werd gemaakt. Internationaalrechtelijk kan hierbij onder andere het element reciprociteit een rol spelen. Op deze wijze is, los van een verdragsrechtelijke basis, een vorm van wederzijdse steun mogelijk, die van geval tot geval voor alle betrokken staten nuttig kan zijn. Niettemin is het in het bijzonder betreffende dergelijke situaties dat in de huidige stand van het internationaal publiekrecht geen klare invulling bestaat van wat de draagwijdte van het concept soevereiniteit in de « cyberruimte » nog kan zijn.

être mis en doute et il n'y a donc aucune raison d'exclure *a priori* les données recueillies par voie intrajudiciaire comme étant des éléments de preuve. Après qu'il a été constaté que les données ont été recueillies à l'étranger, il est indiqué de contacter les autorités du pays dans lequel les données ont été localisées, du moins si celui-ci peut être déterminé avec précision, afin de maintenir de bonnes relations interétatiques et permettre à ce pays d'adopter un point de vue à ce propos.

Lorsque les enquêteurs apprennent, au cours des recherches, que les fichiers recherchés se trouvent à l'étranger et qu'ils ne parviennent pas à identifier le pays concerné avec certitude, on opte pour la solution déjà mentionnée précédemment étant donné qu'aucune concertation internationale n'est à même d'apporter une solution à cette situation.

De plus, il faut également préciser que l'on risque d'aboutir sur une impasse parce que la logique sur laquelle repose une extension purement nationale d'une recherche dans un système informatique s'applique également de manière intégrale et peut-être encore plus intensivement au « *global village* ». Dans ces cas urgents, l'intérêt de préserver des fichiers informatiques pouvant servir d'éléments de preuve entre en conflit avec le concept traditionnel de souveraineté encore très largement répandu à l'heure actuelle. On pense, par exemple, au cas dans lequel il est établi, au cours des recherches, que le fichier pertinent se trouve à l'étranger dans un endroit bien déterminé. L'arrêt des recherches et la mise sur pied d'une commission rogatoire internationale en vue d'effectuer une perquisition sur place laisse aux intéressés suffisamment de temps pour faire disparaître les données via les canaux de télécommunication.

D'où la nécessité, dans des cas urgents, d'agir par analogie aux règles en matière de « *hot pursuit* », c'est-à-dire de pouvoir prendre des mesures destinées à empêcher la disparition des éléments de preuve (en copiant les données et non en les bloquant). L'importance de la vérité dans des cas de grande criminalité justifie que de telles recherches soient menées à l'étranger exceptionnellement. Dans ces cas, il semble toutefois essentiel d'informer l'État concerné afin de permettre à celui-ci de vérifier si une infraction à l'ordre juridique a été commise ou non. D'un point de vue judiciaire et international, la réciprocité, par exemple, peut jouer un certain rôle. Ainsi, il est possible, indépendamment de toute convention sur le plan juridique, de mettre sur pied une forme d'appui réciproque qui, selon les cas, peut être utile à tous les États concernés. Toutefois, le droit public international ne donne, à l'heure actuelle, aucune interprétation précise quant à l'importance que peut avoir le concept de souveraineté dans le « cyberespace », surtout dans ce genre de situations.

In de voormelde gevallen vereist een optreden « te goeder trouw » ten aanzien van andere staten, evenals de zorg voor het vrijwaren van de rechtmatigheid van het bewijs dat door de gerechtelijke overheden redelijke inspanningen worden gedaan om de data zo exact mogelijk te lokaliseren. Aldus wordt eveneens vermeden dat men het verwijt zou kunnen opperen dat de opsporingsdiensten nalatig geweest zijn om inbreuken op de rechtsorde van andere staten te vermijden.

Dit zijn de — beperkte — gevallen met internationale ramificaties waarvoor de ontwerptekst een houvast beoogt aan te reiken.

Paragraaf 4 bepaalt, zoals voorzien is inzake huiszoeking en inbeslagneming, de mogelijkheid voor de onderzoeksrechter om zijn bevoegdheid inzake netwerkzoeking te delegeren aan een officier van gerechtelijke politie, hulpofficier van de procureur des Konings.

Voorts gelden de regels inzake databeslag (artikel 39*bis* van het Wetboek van strafvordering) in principe ook voor de gegevens die via de netwerkzoeking voor gerechtelijke doeleinden worden verzameld.

Art. 4

Deze bepaling voert een nieuw artikel 88*quater* in het Wetboek van strafvordering in dat een aantal bijzondere medewerkingsverplichtingen in een geïnformatiseerde omgeving voorziet.

Het Belgische strafprocesrecht kent vooralsnog weinig mogelijkheden om personen die geen deel uitmaken van het gerechtelijk apparaat, te verplichten mee te werken aan de bewijsgaring (zie bijvoorbeeld het getuigenverhoor). In een snel evoluerende hoogtechnologische context, waar de overheid zelf vaak niet over voldoende expertise beschikt of deskundigen weinig beschikbaar zijn, is het onontbeerlijk om personen die het te onderzoeken informaticasysteem kennen of over een bijzondere expertise beschikken inzake bepaalde aspecten daarvan (bijvoorbeeld inzake beveiliging of cryptografie), te kunnen verplichten de gerechtelijke overheid bij te staan.

Dat is het oogmerk van de nieuwe bepaling, zonder dewelke een effectief onderzoek in informaticasystemen onmogelijk dreigt te worden. 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.

In dit opzicht worden derhalve verdergaande verplichtingen opgelegd aan particulieren om met het gerecht mee te werken, dan in de context van een traditionele

Dans les cas précités, une action menée « de bonne foi » par un État dans d'autres pays ainsi que le souci de garantir le bien-fondé de la preuve exigent des efforts importants de la part des autorités judiciaires pour localiser les données autant que possible. Cela permettra également de reprocher aux services de recherches d'avoir été négligents et de pas avoir été capables d'empêcher la perpétration des infractions à l'ordre juridique d'autres pays.

Voici les cas — peu nombreux — qui ont des ramifications internationales et pour lesquels le texte du projet de loi tente de servir de point d'appui.

Le § 4 prévoit, comme dans le cas d'une perquisition ou d'une saisie, la possibilité pour le juge d'instruction de déléguer sa compétence en matière de recherche sur réseau à un officier de police judiciaire, auxiliaire du procureur du Roi.

Désormais, les règles relatives à la saisie de données (article 39*bis* du Code d'instruction criminelle) seront également applicables aux données récoltées par le biais de la recherche sur réseau à des fins judiciaires.

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.

Dans le droit de procédure pénale belge, il n'existe, à l'heure actuelle, que peu de possibilités de contraindre des personnes n'appartenant pas à l'appareil judiciaire à coopérer à la collecte de preuves (voir l'audition de témoin, par exemple). Dans un contexte de haute technologie en évolution rapide, où il arrive fréquemment que les autorités ne disposent pas de moyens d'expertise suffisants ou que les experts ne soient pas disponibles, il est indispensable de contraindre les personnes ayant une connaissance du système informatique faisant l'objet de la recherche ou ayant d'une connaissance particulière de certains aspects de ce système (en matière de protection ou de cryptage, par exemple) d'assister les autorités judiciaires.

Tel est l'objectif de la nouvelle disposition sans laquelle une recherche efficace dans des systèmes informatiques semble impossible. Afin de s'assurer du caractère contraignant de cette mesure, le non-respect des obligations prévues ainsi que le fait de faire obstacle à la recherche dans un système informatique sont sanctionnés pénalement.

Dans cette perspective, des obligations de coopération avec la justice plus étendues sont imposées aux particuliers qu'en ce qui concerne les traditionnelles

huiszoeking en inbeslagneming. Om de hogervermelde redenen is dit evenwel onontbeerlijk. Overigens is men zich ook internationaal bewust van het belang om in deze problematiek specifieke maatregelen te nemen (zie met name R(95)13 van de Raad van Europa van 11 september 1995, principe nr 10).

Het ontwerp voorziet twee soorten verplichtingen.

Enerzijds wordt een informatieverplichting ten aanzien van de onderzoeksrechter gecreëerd voor personen die over een bijzondere kennis beschikken inzake specifieke technische aspecten van informatica (§ 1). Hierbij wordt onder andere gedacht aan de toegangsmogelijkheden, de configuratie, de beveiliging en de cryptografische sleutels.

Anderzijds wordt een verplichting gecreëerd voor personen die daartoe in staat zijn, om zelf, op bevel van de onderzoeksrechter, bepaalde operaties uit te voeren (bijvoorbeeld het doen functioneren van de computer, het opvragen van bepaalde *files*, …) (§ 2). Deze verplichting wordt evenwel niet als algemene regel gesteld : enkel wanneer het noodzakelijk is, kan de onderzoeksrechter dit bevelen. Dat is bijvoorbeeld het geval, wanneer het systeem te complex is, er onvoldoende gekwalificeerd politiepersoneel ter plaatse is, wanneer aldus minder risico's voor de bewijsgaring of voor het toebrengen van schade bestaan, … De onderzoeksrechter kan hierbij aangeven in welke vorm het resultaat van de operatie wordt verstrekt : naargelang het geval kan het bijvoorbeeld gaan om een papieren uitdruk, om een kopie van de data op diskette of CD-ROM.

In antwoord op de Raad van State moet gesteld worden dat de kring van personen die geviseerd worden door artikel 88*quater* niet *in abstracto* kan worden omschreven : het kan gaan om importeurs/verdelers van computers of software, « *trusted third parties* », dienstenverstrekkers, operatoren, bedrijfsingenieurs die een specifieke informaticaconfiguratie hebben uitgewerkt, beveiligingsspecialisten, … De onderzoeksrechter zal dit geval per geval moeten nagaan.

Bovendien gaat het uiteraard slechts om een inspanningsverbintenis : men kan immers niet meer van iemand verlangen dan hij zelf vermag.

De verplichting om bepaalde data te zoeken kan evenwel niet worden opgelegd aan de verdachte, gezien de bescherming tegen zelf-incriminatie.

De verdachte moet hier immers, zoals in de context van de getuigenverklaring, zijn zwijgrecht kunnen laten gelden. De andere verplichtingen zijn in dit opzicht evenwel niet onverenigbaar met de vereisten die worden gesteld door het EVRM (zie bijvoorbeeld het arrest Saunders tegen het Verenigde Koninkrijk van 17 decem-

perquisitions et saisies. Pour les raisons évoquées plus haut, c'est inévitable. Pour le surplus, il y a une prise de conscience sur le plan international de l'importance de prendre des mesures spécifiques à l'égard de cette problématique (voir notamment la résolution R(95)13 du Conseil de l'Europe du 11 septembre 1995, principe n° 10).

Le projet prévoit deux types d'obligations.

D'une part, il est créé une obligation d'information à l'égard du juge d'instruction, qui vise les personnes ayant une connaissance particulière des aspects pratiques et spécifiques de l'informatique (§ 1er). À cet égard, on pense notamment aux possibilités d'accès, à la configuration, à la protection et aux clés de cryptage.

D'autre part, il est créé une obligation destinée aux personnes capables d'exécuter, d'elles-mêmes ou sur ordre d'un juge d'instruction, certaines opérations (la mise en marche de l'ordinateur, la recherche de certains fichiers, …) (§ 2). Cette obligation ne constitue toutefois pas la règle générale : le juge d'instruction peut ordonner une telle mesure uniquement lorsque c'est nécessaire. C'est notamment le cas lorsque le système est trop complexe, lorsqu'il n'y a pas suffisamment d'agents de police qualifiés sur les lieux et que les risques liés à la collecte de preuve ou la détérioration des données, … sont moindres. Le juge d'instruction peut à cet égard indiquer la forme dans laquelle le résultat de l'opération est fourni : selon le cas, il peut par exemple s'agir d'une impression sur papier, d'une copie des données pertinentes sur disquette ou sur CD-ROM.

En réponse à l'avis du Conseil d'État, il y a lieu de préciser que le cercle de personnes visées par l'article 88*quater* ne peut être décrit *in abstracto* : il peut s'agir d'importateurs/de distributeurs d'ordinateurs ou de logiciels, de « *trusted third parties* », de fournisseurs de service, d'opérateurs, d'ingénieurs d'entreprise ayant élaboré une configuration informatique spécifique, de spécialistes de la sécurité, … Le juge d'instruction devra faire les vérifications au cas par cas.

De plus, il ne s'agit, bien évidemment, que d'un engagement à fournir des efforts : on ne peut attendre d'une personne qu'elle fournisse des efforts qu'elle est incapable de fournir.

Il n'est cependant pas possible de soumettre l'inculpé à l'obligation d'effectuer des recherches à propos de certaines données compte tenu du principe de protection contre l'auto-incrimination.

L'inculpé doit pouvoir faire valoir son droit au silence, comme c'est d'ailleurs le cas dans le contexte des déclarations de témoin. À cet égard, les autres obligations ne sont néanmoins pas incompatibles avec les conditions posées par la CEDH (voir, par exemple, l'arrêt Sauders contre le Royaume-Uni du 17 décembre 1996).

ber 1996). Wat betreft de personen die gehouden zijn aan het beroepsgeheim, kan hier worden verwezen naar de regels van het gemeen recht.

Evenmin kan deze verplichting worden opgelegd aan naaste familieleden van de verdachte. Er kan immers moeilijk worden aanvaard dat deze, onder dreiging van een strafsanctie, verplicht zouden worden bewijsmateriaal te verzamelen tegen een van hun naaste verwanten.

Ter zake wordt in de tekst, teneinde gevolg te geven aan het advies van de Raad van State, gerefereerd naar de bloed- en aanverwanten bedoeld in artikel 156 van het Wetboek van strafvordering.

Inzake de beroepsgeheimhouders is het niet de bedoeling om af te wijken van het gemeen recht inzake het respect van het beroepsgeheim : dragers van het beroepsgeheim handelend binnen de grenzen van dat beroepsgeheim, volgen hetzelfde regime als wanneer deze personen als getuige in rechte worden gehoord; dit impliceert dus een medewerkingsrecht maar geen verplichting, wanneer het erom gaat specifieke data zelf te zoeken.

De onderzoeksrechter kan deze bevoegdheid enkel delegeren aan officieren van gerechtelijke politie, hulpofficieren van de procureur des Konings. Dit is dezelfde regeling als inzake huiszoeking en inbeslagneming (artikel 89*bis* van het Wetboek van strafvordering) en netwerkzoeking (voorgesteld artikel 88*ter* van het Wetboek van strafvordering).

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 (§ 4).

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 gesteld zouden kunnen worden, tenzij zij opzettelijk schade zouden berokkenen. Daarom wordt expliciet voorzien dat de Staat aansprakelijk is voor onopzettelijk toegebrachte schade in het kader van het nakomen van de medewerkingsverplichting (§ 5).

Art. 5

Deze bepaling voert een legistieke aanpassing door in artikel 89 van het Wetboek van strafvordering. Aldus wordt geëxpliciteerd dat ook de onderzoeksrechter gebruik kan maken van het nieuwe artikel 39*bis*, wat overigens sowieso het geval is, overeenkomstig het gemeen recht.

En ce qui concerne les personnes tenues au secret, il peut être renvoyé aux règles de droit commun.

Les proches de l'inculpé ne peuvent pas non plus être soumis à cette obligation. Il est en effet difficilement acceptable que ces personnes soient obligées à rassembler des éléments de preuve contre leur proche, sous la contrainte de sanctions pénales.

À cet égard, le texte réfère aux parents et alliés visés à l'article 156 du Code d'instruction criminelle pour répondre à l'avis du Conseil d'État.

En ce qui concerne les personnes tenues au secret, le but n'est pas de déroger au droit commun en matière de respect du secret professionnel : les personnes tenues par le secret professionnel et agissant dans le cadre du secret professionnel suivent le même régime que si elles étaient appelées à témoigner en justice; ceci implique donc un droit et pas une obligation de coopérer lorsqu'elles doivent rechercher elles-mêmes des données spécifiques.

Le juge d'instruction ne peut déléguer cette compétence qu'aux officiers de police judiciaire, auxiliaires du procureur du Roi. C'est la même règle que celle qui est d'application en matière de perquisition et de saisie (article 89*bis* du Code d'instruction criminelle) et de recherche sur réseau (article 88*ter* proposé du Code d'instruction criminelle).

Afin de protéger le secret de l'instruction dans cette matière, une obligation au secret a été insérée à l'égard des personnes ayant connaissance de la mesure ou capables de prêter leur concours (§ 4).

Les citoyens tenus, dans le cadre de cette disposition, de prêter leur concours dans une enquête judiciaire peuvent, ce faisant, endommager des systèmes informatiques ou des données. Dans ce cas, il serait injuste de tenir ces personnes civilement responsables sauf si le dommage a été causé intentionnellement. C'est la raison pour laquelle il est explicitement prévu que l'État est responsable du dommage causé involontairement dans le cadre du respect de l'obligation de collaborer (§ 5).

Art. 5

Cette disposition introduit une adaptation légistique dans l'article 89 du Code d'instruction criminelle. Cette disposition prévoit que le juge d'instruction également peut invoquer le nouvel article 39*bis*, comme c'est déjà le cas conformément au droit commun.

Art. 6, 7 en 8

Deze bepalingen beogen een aanpassing van de modaliteiten van het regime van het gerechtelijk onderscheppen van telecommunicatie.

Er worden met name drie wijzigingen doorgevoerd, respectievelijk aan artikel 90*ter*, *quater* en *septies* van het Wetboek van strafvordering.

1) Artikel 6 :

De lijst van misdrijven waarvoor een tapmaatregel mogelijk is, wordt uitgebreid met de bestaande misdrijven inzake het aftappen van telecommunicatie (artikelen 259*bis* en 314*bis* van het Strafwetboek), met de nieuwe delicten valsheid in informatica (artikel 210*bis* van het Strafwetboek) en informaticabedrog (artikel 50*4quater* van het Strafwetboek), evenals met de twee nieuwe kerndelicten tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en data : « *hacking* » (artikel 550*bis* van het Strafwetboek) en computer- en datasabotage (artikel 550*ter* van het Strafwetboek). Het opsporen van deze misdrijven waarbij in de praktijk veelal telecommunicatie wordt benut, zou anders sterk worden bemoeilijkt.

2) Artikel 7 :

De bijzondere medewerkingsverplichtingen die in artikel 8 werden vermeld, worden *mutatis mutandis* ook ingevoerd inzake het onderscheppen van telecommunicatie. Inderdaad, het is juist in deze context dat de kritiek wordt geuit dat de tapmaatregelen in een *high-tech*-context onwerkzaam dreigen te worden. Er wordt derhalve verwezen naar de toelichting bij deze bepaling.

In antwoord op de opmerking van de Raad van State inzake het onderscheid in de strafmaat voor operatoren/dienstenverstrekkers die in het kader van een interceptie reeds moeten meewerken en de nieuwe medewerkingsverplichtingen in het ontwerp, wordt de zwaardere strafmaat voor onwillige « personen met een bijzondere kennis » gerechtvaardigd op grond van het feit dat het hier principieel om om het even wie kan gaan. De operatoren/dienstenverstrekkers zijn evenwel de institutionele medespelers van de overheid in de problematiek van interceptie, waarvan in principe meer goodwill kan worden verwacht.

3) Artikel 8 :

De beveiligings- en versleutelingstechnieken die thans beschikbaar zijn, kunnen ook door de gerechte-

Art. 6, 7 et 8

Ces dispositions visent une adaptation des modalités du mode d'interception de la télécommunication par les autorités judiciaires.

Trois modifications ont été apportées respectivement aux articles 90*ter*, 90*quater* et 90*septies* du Code d'instruction criminelle.

1) Article 6 :

La liste des infractions pour lesquelles une mesure d'écoute est possible est élargie aux infractions existantes en matière d'écoute de télécommunication (articles 259*bis* et 314*bis* du Code pénal), aux nouveaux délits de faux en informatique (article 210*bis* du Code pénal) et de fraude informatique (article 504*quater* du Code pénal) ainsi qu'à deux nouveaux délits primordiaux contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données : le « *hacking* » (article 550*bis* du Code pénal), le sabotage informatique et le sabotage de données (article 550*ter* du Code pénal). La recherche de ces délits pour laquelle on fait beaucoup appel à la télécommunication dans la pratique serait une tâche fort difficile à mener autrement.

2) Article 7 :

Les obligations particulières de collaborer mentionnées dans l'article 8 sont également insérées *mutatis mutandis* en ce qui concerne l'interception de la télécommunication. En effet, c'est justement dans ce contexte qu'une critique est émise selon laquelle les mesures d'écoute dans un contexte *high-tech* risquent d'être inefficaces. Il est dès lors renvoyé à l'exposé en ce qui concerne cette disposition.

En réponse à l'avis du Conseil d'État concernant, d'une part, la distinction à marquer entre le montant de la peine prononcée à l'égard des opérateurs et des fournisseurs de service qui doivent déjà collaborer dans le cadre d'une interception et, d'autre part, les nouvelles obligations de coopérer prévues dans le projet, la peine plus lourde destinée aux personnes récalcitrantes possédant une connaissance particulière est justifiée sur la base du fait qu'il peut s'agir en principe de n'importe quelle personne. Les opérateurs/fournisseurs de service, de la part desquels on peut en principe attendre plus de bonne volonté, sont toutefois les auxiliaires institutionnels des autorités dans la problématique de l'interception.

3) Article 8 :

Les techniques de protection et de cryptage disponibles à l'heure actuelle peuvent également être em-

lijke overheid worden aangewend om de vertrouwelijkheid en de integriteit van het tapmateriaal (dat meer en meer digitaal zal worden) te waarborgen, met inbegrip van de bewaringsmodaliteiten op de griffie. Hierbij kan meer bepaald gedacht worden aan de mogelijkheden die de digitale handtekening biedt. In de toekomst zal de informatietechnologie ook inzake de transcriptie en de eventuele vertaling mogelijkheden bieden. Het voorontwerp schept daarom de principiële mogelijkheid om hiervan gebruik te maken, maar houdt er tegelijk rekening mee dat de implementatie hiervan enige tijd zal vergen. Omwille van de technische en infrastructurele aanpassingen die nodig zullen zijn om het systeem van bewaring op de griffie onder verzegelde omslag en het bijzondere, « fysische » register te vervangen door hun digitale tegenhangers — die overigens meer veiligheid zullen bieden —, wordt het bepalen van de specifieke modaliteiten en de datum van toepassing hiervan gedelegeerd aan de Koning.

Art. 9

Deze bepaling brengt een aantal wijzigingen aan in artikel 109*ter* E 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, …) van telecommunicatie te kunnen achterhalen, en anderzijds gebruikers die informatie aan het publiek aanbieden, te kunnen identificeren, en deze inlichtingen te bewaren. Het betreft derhalve zowel gegevens die betrekking hebben op privételecommunicatie als op openbare telecommunicatie. Het begrip « oproepgegevens » wordt aangewend, omdat in de context van computernetwerken niet louter met traditionele telefoonnummers wordt gewerkt, maar ook bijvoorbeeld met internetadressen. In eerste instantie worden evenwel de verbindingen tussen de gebruiker en de *access provider* geviseerd. Niettemin kan het in bepaalde gevallen voor de bevoegde magistraat ook nodig zijn om bijvoorbeeld precies na te kunnen gaan welke internetadressen werden gecontacteerd. De Koning zal bepalen op welke types van operatoren van telecommunicatienetwerken en telecommunicatiediensten deze verplichting betrekking heeft. Wat de telefonie in de klassieke zin betreft, heeft de bepaling om gegevens in een register te bewaren *a priori* enkel

ployées par les autorités judiciaires pour garantir la confidentialité et l'intégrité du matériel d'écoute (qui prend de plus en plus souvent une forme numérique), y compris les modalités de sauvegarde au greffe. On peut penser ici en particulier aux possibilités que fournit la signature digitale. Dans l'avenir, la technologie de l'information offrira également des possibilités en matière de transcription et éventuellement de traduction. L'avant-projet permet en principe l'utilisation de cette technologie mais tient compte en même temps du fait que la mise en œuvre nécessitera un certain temps. En raison des adaptations techniques et infrastructurelles nécessaires pour faire fonctionner le système de sauvegarde des données sous plis scellés au greffe et remplacer le registre particulier et « physique » par son équivalent numérique, qui offrira plus de sécurité, le Roi est chargé de déterminer les modalités spécifiques et la date d'application du présent article.

Art. 9

Cette disposition apporte plusieurs modifications à l'article 109*ter* E de la loi du 21 mars 1991 relative à la réforme de certaines entreprises publiques.

Les nouvelles obligations pour les fournisseurs de service qui devront être précisées par le Roi concernent l'inobservation de l'obligation d'identification en ce qui concerne l'utilisation des services de télécommunications.

Cette disposition crée des obligations pour les fournisseurs de services de télécommunication, lesquels sont tenus de prendre des mesures pour pouvoir retrouver les données d'appel de télécommunication (origine, destination, localisation, durée, …), d'une part, identifier les utilisateurs qui fournissent ces informations au public, d'autre part, et conserver ces renseignements. Il s'agit par conséquent tant de données qui concernent la télécommunication privée que la télécommunication publique. Le concept « données d'appel » est utilisé, parce que dans le contexte des réseaux d'ordinateurs on ne travaille pas seulement avec des numéros de téléphone traditionnels, mais également avec par exemple des adresses « internet ». Néanmoins, on vise en premier lieu les connections entre l'utilisateur et le fournisseur d'accès. Dans certains cas il peut s'avérer nécessaire pour le magistrat compétent de vérifier par exemple les adresses « internet » qui ont été contactées. Le Roi devra déterminer les types des opérateurs de réseaux de télécommunication et de services de télécommunications auxquels cette obligation s'applique. En ce qui concerne la téléphonie au sens classique du terme, *a priori* seuls les numéros d'appel devront être

betrekking op de oproepgegevens. Het is dus niet de bedoeling om andere telecommunicatiegegevens te registreren en te bewaren zoals lokalisatiegegevens bij mobiel telefoonverkeer. Wat de gegevens omtrent internetverkeer betreft, behoort het register niet automatisch de gegevens te bevatten over de door de netwerkgebruiker geraadpleegde internetsites. Nochtans, laat de bepaling toe dat de Koning, op voorstel van de minister van Justitie en de minister van Telecommunicatie en Overheidsbedrijven en Participaties om specifieke maatregelen uit te vaardigen om bijvoorbeeld Internettoegangsleveranciers te verplichten bepaalde informatie te bewaren in uitzonderlijke gevallen en in functie van de technologie waarover zij redelijkerwijze kunnen beschikken. Als uitzonderlijk geval wordt bijvoorbeeld beschouwd de hypothese waarbij een onderzoek naar een persoon wordt gevoerd.

Deze verplichting is ingegeven door de problemen die rijzen bij moderne vormen van telecommunicatie en bij nieuwe media, zoals het Internet, waarbij het inderdaad zeer eenvoudig is om anoniem gebruik te maken van de netwerken.

Eerder dan in dit stadium van de internationale discussie de weg op te gaan van een van het gemeen recht afwijkend strafrechtelijk aansprakelijkheidsregime voor *providers*, wordt in deze bepaling geopteerd voor het opleggen van een inspanningsverplichting voor de *providers*, die de noodzakelijke tussenpersonen zijn voor elke activiteit op de computernetwerken die worden aangewend voor dienstverlening aan het publiek. De problemen inzake identificatie en lokalisatie van criminele gebruikers vormen immers een van de voornaamste knelpunten bij opsporingen op het Internet. In dat opzicht is deze bepaling complementair aan de bepalingen in het Wetboek van strafvordering die juist de gevallen regelen waarin de bevoegde gerechtelijke instanties deze inlichtingen kunnen opeisen (zie op de eerste plaats de artikelen 46*bis* en 88*bis* van het Wetboek van strafvordering inzake privé-communicatie, en de mogelijkheden inzake zoeking en vereiste medewerking inzake openbare communicatie (cf. *supra*)). Opdat de oorsprong van telecommunicatie opgespoord zou kunnen worden, is er immers noodzakelijk de voorafgaande voorwaarde dat de daarop betrekking hebbende inlichtingen ook technisch beschikbaar kunnen zijn.

De Koning zal de bewaarperiode van de gegevens moeten bepalen. Hierbij moet rekening worden gehouden met hetgeen redelijk is in het licht van, enerzijds de noden van de strafvordering om een zekere tijd nadat de feiten werden gepleegd, bepaalde opsporingen te kunnen doen, en anderzijds, de technische en praktische haalbaarheid voor de dienstenverstrekkers.

conservés dans le registre. Il n'est donc pas question de conserver dans ce registre les autres données de télécommunications comme par exemple les données relatives à la localisation de l'utilisateur dans le cadre de la téléphonie mobile. En ce qui concerne les données en rapport avec le réseau Internet, le registre ne pourra contenir de manière automatique les données relatives aux sites consultés par l'utilisateur du réseau. Toutefois, cette disposition habilite le Roi, sur proposition du ministre de la Justice et du ministre des Télécommunications et des Entreprises et Participations publiques, à arrêter des dispositions particulières afin, par exemple, de contraindre les *access providers*, en fonction des moyens technologiques dont ils peuvent raisonnablement disposer, à conserver ce type de données dans certaines situations exceptionnelles. Par situation exceptionnelle, on vise par exemple l'hypothèse dans laquelle une instruction serait dirigée à l'encontre d'une personne.

Cette obligation est inspirée par les problèmes suscités par les formes modernes de télécommunication et par les nouveaux médias comme Internet, par le biais desquels il est très facile d'utiliser des réseaux de façon anonyme.

À ce stade du débat international, plutôt que d'opter à l'égard des fournisseurs pour un des régimes de responsabilité pénale différant du droit commun, on a choisi dans cette disposition d'imposer une obligation d'effort aux fournisseurs qui sont les intermédiaires incontournables pour toutes les activités sur les réseaux informatiques utilisés en matière d'assistance au public. Les problèmes liés à l'identification et à la localisation des utilisateurs criminels constituent en effet l'une des principales pierres d'achoppement dans le cadre des recherches sur Internet. Dans cette optique, cette disposition est complémentaire aux dispositions du Code d'instruction criminelle qui règlent uniquement les cas où les instances judiciaires compétentes peuvent exiger ces informations (voir en première instance les articles 46*bis* et 88*bis* du Code d'instruction criminelle concernant les communications privées ainsi que les possibilités relatives à la recherche et de la collaboration requise en matière de communications privées (cf. *supra*)). En effet, pour que l'origine de la télécommunication puisse être retrouvé, il est essentiel que les conditions préalables ayant trait aux informations en la matière puissent également être remplies sur le plan technique.

Le Roi devra déterminer la période de conservation de ces données. Pour cette détermination, il faudra tenir compte de ce qui paraît raisonnable à la lumière, d'une part, des besoins pour l'action publique de pouvoir procéder à certaines investigations et, d'autre part, des possibilités des fournisseurs de services sur les plans technique et pratique.

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

De Raad van State is van oordeel dat de delegatie inzake de voormelde registratie- en bewaringsverplichtingen aan de Koning onverenigbaar is met de grondwettelijke vereiste van wettelijke beperkingen op het recht op privacy. Gezien de techniciteit die met de implementatie van deze verplichtingen gepaard gaat, is het evenwel zeer moeilijk, zo niet onmogelijk om de concrete invulling ervan in de wet in formele zin te regelen. Overigens zouden dergelijke wettelijke bepalingen snel door de technologische evolutie achterhaald zijn. De bovenvermelde principes vormen evenwel een duidelijk wettelijk kader waardoor de Koning gebonden is. Derhalve kan het argument van de ongrondwettelijkheid niet worden aanvaard.

*
* *

Ziedaar de strekking van het ontwerp van wet dat de regering aan uw beraadslaging voorlegt.

De minister van Justitie,

M. VERWILGHEN

De minister van Telecommunicatie en Overheidsbedrijven en Participaties,

R. DAEMS

De minister van Economie en Wetenschappelijk Onderzoek,

R. DEMOTTE

Outre cette obligation sanctionnée pénalement pour les fournisseurs de services de télécommunication, il est également prévu que les données que ceux-ci sont tenus de conserver doivent bénéficier d'une protection technique suffisante dans un souci de confidentialité et d'intégrité.

Le Conseil d'État est d'avis que la délégation de compétence relative aux obligations d'enregistrement et de conservation susmentionnées donnée au Roi est incompatible avec l'exigence constitutionnelle de prévoir des restrictions légales en matière de droit au respect de la vie privée. Compte tenu de la technicité qui est liée à la mise en œuvre de ces obligations, il est très difficile, voire impossible, de traduire dans la loi le contenu concret de celles-ci de manière formelle. Du reste, de telles dispositions légales seraient vite dépassées par l'évolution technologique. Les principes mentionnés plus haut constituent néanmoins un cadre légal clair auquel le Roi est tenu. Par conséquent, l'argument de l'inconstitutionnalité ne peut être admis.

*
* *

Telle est la portée du projet de loi que le gouvernement soumet à votre délibération.

Le ministre de la Justice,

M. VERWILGHEN

Le ministre des Télécommunications et des Entreprises et Participations publiques,

R. DAEMS

Le ministre de l'Économie et de la Recherche scientifique,

R. DEMOTTE

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

_____

Voorontwerp van wet inzake informaticacriminaliteit

_____

Artikel 1

Deze wet regelt een aangelegenheid zoals bedoeld in artikel 78 van de Grondwet.

Art. 2

In hoofdstuk IV van Titel V van Boek II van het Strafwetboek wordt een nieuwe afdeling II*bis* ingevoegd, houdende een artikel 210*bis*, luidend als volgt :

« Afdeling II*bis*. — Valsheid in informatica

Art. 210*bis*. — § 1. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met één van die straffen alleen.

§ 2. Hij die, terwijl hij weet dat aldus bekomen gegevens vals zijn, hiervan gebruik maakt, wordt gestraft alsof hij de dader van de valsheid was.

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

§ 4. 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 een 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. ».

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

_____

Avant-projet de loi relatif à la criminalité informatique

_____

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2

Il est inséré, au chapitre IV, Titre V, Livre II du Code pénal une nouvelle section II*bis*, contenant un article 210*bis*, rédigée comme suit :

« Section II*bis*. — Faux en informatique

Art. 210*bis*. — § 1er. 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, 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.

§ 2. 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.

§ 3. La tentative de commettre l'infraction prévue 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.

§ 4. 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* de ce Code. ».

Art. 3

In hoofdstuk II van Titel IX van Boek II van het Strafwetboek wordt een nieuwe afdeling III*ter*, houdende een artikel 504*quater* ingevoegd, luidend als volgt :

« Afdeling III*bis*. — Informaticabedrog

Art. 504*quater*. — § 1. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 50 000 Belgische frank of met een van die straffen alleen.

§ 2. Hij die, door het misdrijf bedoeld in § 1 te plegen, voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwerft, 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.

§ 3. 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 een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis* of in Titel IX*bis* van dit Wetboek. ».

Art. 4

In Boek II van het Strafwetboek wordt een nieuwe Titel IX*bis*, houdende de artikelen 550*bis* en 550*ter*, ingevoegd, luidend als volgt :

« Titel IX*bis*. — Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen

Art. 550*bis*. — § 1. Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van 3 maanden tot 1 jaar en met geldboete van 26 Belgische frank tot 25 000 Belgische frank of met een van deze straffen alleen.

Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, is de gevangenisstraf van 6 maanden tot 2 jaar.

§ 2. Hij die, met bedrieglijk opzet of met het oogmerk te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van 6 maanden tot 2 jaar en met geldboete van 26 Belgische frank tot 25 000 Belgische frank of met een van deze straffen alleen.

Art. 3

Il est inséré, au chapitre II, Titre IX, Livre II du Code pénal une nouvelle section III*ter*, contenant un article 504*quater*, rédigée comme suit :

« Section III*bis.* — Fraude informatique

Art. 504*quater*. — § 1er. 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, est puni 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.

§ 2. Celui qui, par la commission de l'infraction visée au § 1er, obtient pour soi-même ou pour autrui un avantage patrimonial frauduleux 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.

§ 3. 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* de ce code. ».

Art. 4

Il est inséré dans le Livre II du Code pénal un nouveau Titre IX*bis*, contenant les articles 550*bis* et 550*ter*, rédigé comme suit :

« Titre IX*bis*. — Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par le biais de ces systèmes

Art. 550*bis*. — § 1er. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de 26 francs belges à 25 000 francs belges ou d'une de ces peines.

Si l'infraction visée au premier alinéa, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§ 2. Celui qui, avec intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de 26 francs belges à 25 000 francs belges ou d'une de ces peines.

§ 3. Hij die zich in één van de gevallen van de §§ 1 en 2 bevindt, en, naar aanleiding daarvan :

1° hetzij kennisneemt van gegevens die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem of deze op enige manier overneemt,

2° hetzij enig gebruik maakt van een informaticasysteem,

3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan een informaticasysteem of aan gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen,

wordt gestraft met gevangenisstraf van 1 jaar tot 3 jaar en met geldboete van 26 Belgische frank tot 50 000 Belgische frank of met een van die straffen alleen.

§ 4. Poging tot het plegen van één van de misdrijven, bedoeld in de §§ 1 en 2, wordt gestraft met de straffen gesteld op het misdrijf zelf.

§ 5. 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 de §§ 1 tot 4, gepleegd kunnen worden, opspoort, verzamelt, ter beschikking stelt, verspreidt of verhandelt, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met één van die straffen alleen.

§ 6. Hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven, bedoeld in de §§ 1 tot 5, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 100 Belgische frank tot 200 000 Belgische frank of één van die straffen.

§ 7. Hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van één van de misdrijven bedoeld in de §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen.

§ 8. De straffen gesteld in de §§ 1 tot 7 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 een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of in een van de andere artikelen van deze Titel.

Art. 550*ter*. — § 1. 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, wordt gestraft met gevangenisstraf van 6 maanden tot

§ 3. Celui qui se trouve dans une des situations prévues par les §§ 1er et 2 et qui, à cette occasion :

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,

2° soit fait tout usage d'un système informatique,

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,

est puni d'un emprisonnement de un an à trois ans et d'une amende de 26 francs belges à 50 000 francs belges ou d'une de ces peines.

§ 4. La tentative de commettre une des infractions prévues aux §§ 1er et 2 est punie des mêmes peines que l'infraction elle-même.

§ 5. 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, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 6. Celui qui ordonne la commission d'une des infractions prévues aux §§ 1er à 5 ou qui y incite est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 100 francs belges à 200 000 francs belges ou d'une de ces peines.

§ 7. 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 fait un usage quelconque des données ainsi obtenues est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 8. Les peines portées par les §§ 1er à 7 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*, 504*quater* ou dans un des articles du présent Titre.

Art. 550*ter*. — § 1er. 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, est puni d'un emprisonnement de six mois à trois ans et

3 jaar en met geldboete van 26 Belgische frank tot 25 000 Belgische frank of met een van die straffen alleen.

§ 2. Hij die, tengevolge van het plegen van het misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 26 Belgische frank tot 75 000 Belgische frank of met een van die straffen alleen.

§ 3. 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, wordt gestraft met gevangenisstraf van 1 jaar tot 5 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met één van die straffen alleen.

§ 4. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen.

§ 5. De straffen gesteld in de §§ 1 tot 4 worden verdubbeld indien een overtreding van een 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*, 504*quater* of in een van de andere artikelen van deze Titel. ».

d'une amende de 26 francs belges à 25 000 francs belges ou d'une de ces peines.

§ 2. 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, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs belges à 75 000 francs belges ou d'une de ces peines.

§ 3. 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, est puni d'un emprisonnement de un an à cinq ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 4. 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, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 5. Les peines portées par les §§ 1er à 4 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*, 504*quater* ou dans un des articles du présent Titre. ».

Art. 5

In het Wetboek van strafvordering wordt een artikel 39*bis* ingevoegd, luidend als volgt :

« Art. 39*bis*. — § 1. 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. Indien het gebruik van dergelijke dragers wegens de dringendheid of de techniciteit niet mogelijk is, wordt gebruik gemaakt van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

§ 2. Hij wendt bovendien de aangepaste middelen aan om de toegang tot deze gegevens in het informaticasysteem, evenals tot de kopieën daarvan die ter beschik-

Art. 5

Il est inséré dans le Code d'instruction criminelle un article 39*bis* rédigé comme suit :

« Art. 39*bis*. — § 1er. 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. Si l'utilisation de tels supports n'est pas possible en raison de l'urgence ou pour des raisons techniques, il est fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

§ 2. Il utilise en outre les moyens appropriés pour empêcher l'accès à ces données dans le système informatique, de même qu'aux copies de ces données qui

king staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken, te verhinderen.

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

§ 3. Indien de gegevens het onderwerp van het misdrijf vormen of voortgekomen zijn uit het misdrijf en 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, kan de procureur des Konings deze gegevens uit het informaticasysteem verwijderen.

Wanneer de in § 1 vermelde maatregel niet mogelijk is omwille van technische redenen of omwille van de omvang van de gegevens, wendt de procureur des Konings de aangepaste 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.

§ 4. 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 werden gekopieerd, ontoegankelijk werden gemaakt of verwijderd.

§ 5. De procureur des Konings wendt de aangepaste middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen. Dezelfde middelen worden aangewend voor de bewaring hiervan op de griffie.

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

§ 6. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels inzake inbeslagneming van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van gegevens. ».

Art. 6

In hetzelfde Wetboek wordt een artikel 88*ter* ingevoegd, luidend als volgt :

« Art. 88*ter*. — § 1. Wanneer de onderzoeksrechter onderzoek verricht in een informaticasysteem, hetzij in het kader van een huiszoeking, hetzij anderszins, kan hij dit onderzoek uitbreiden naar een informaticasysteem dat zich op een andere plaats bevindt dan daar waar dit onderzoek plaatsvindt, indien :

— hij van oordeel is dat deze uitbreiding noodzakelijk is voor de waarheidsvinding ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking en

sont à la disposition de personnes autorisées à utiliser le système informatique.

Il peut cependant 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.

§ 3. Si les données forment l'objet de l'infraction ou ont été produites par l'infraction et si elles 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 peut retirer ces données du système informatique.

Lorsque la mesure prévue au § 1er n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens 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.

§ 4. 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.

§ 5. Le procureur du Roi utilise les moyens appropriés pour garantir l'intégrité et la confidentialité de ces données. Les mêmes moyens 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.

§ 6. Sans préjudice des dispositions spécifiques de cet article, les règles relatives à la saisie sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données. ».

Art. 6

Il est inséré dans le même Code un article 88*ter* rédigé comme suit :

« Art. 88*ter*. — § 1er. Lorsque le juge d'instruction procède à une recherche dans le cadre d'un système informatique, soit dans le cadre d'une perquisition, soit autrement, il peut étendre cette recherche vers un système informatique qui se trouve dans un autre lieu que celui où la recherche est effectuée, si :

— il estime que cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la perquisition, et

— er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan, of

— hij van oordeel is dat andere maatregelen disproportioneel zijn.

§ 2. De uitbreiding van het onderzoek in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, toegang hebben.

§ 3. Inzake de door uitbreiding van het onderzoek in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in artikel 39*bis*. De onderzoeksrechter brengt de verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet kan worden achterhaald.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden deze enkel gecopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze bepaald kan worden.

§ 4. Artikel 89*bis* is van toepassing op de uitbreiding van het onderzoek in een informaticasysteem. ».

Art. 7

In hetzelfde Wetboek wordt een artikel 88*quater* ingevoegd, luidend als volgt :

« Art. 88*quater*. — § 1. De onderzoeksrechter, evenals in zijn opdracht een officier van de gerechtelijke politie, hulpofficier van de procureur des Konings, kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van een informaticasysteem dat het voorwerp uitmaakt van onderzoek of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verlenen over de werking ervan en over de wijze om er toegang toe te verkrijgen of in een verstaanbare vorm toegang te verkrijgen tot de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen.

§ 2. Indien nodig, kan de onderzoeksrechter iedere relevante persoon bevelen om zelf het informaticasysteem te bedienen of de pertinente gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voor zover dit in hun mogelijkheden ligt.

— il existe un risque que, sans cette extension, des éléments de preuve soient perdus ou

— il estime que d'autres mesures seraient disproportionnées.

§ 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure, ont accès.

§ 3. En ce qui concerne les données rassemblées par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39*bis* s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire belge, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique immédiatement cette information au ministère de la Justice, qui en informe les autorités compétentes de l'État concerné, si celui-ci peut raisonnablement être déterminé.

§ 4. L'article 89*bis* est applicable à l'extension de la recherche dans un système informatique. ».

Art. 7

Il est inséré dans le Code d'instruction criminelle un article 88*quater* rédigé comme suit :

« Art. 88*quater*. — § 1er. Le juge d'instruction, ainsi qu'un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des 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'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible.

§ 2. Si nécessaire, le juge d'instruction peut ordonner à toute personne pertinente de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure où c'est dans leurs possibilités.

Het bevel om zelf de pertinente gegevens te zoeken kan niet aan de verdachte en aan zijn naaste familieleden worden gegeven.

§ 3. Degene die weigert de in §§ 1 en 2 gevorderde technische medewerking te verlenen, waarvan de modaliteiten worden vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, of het onderzoek in een informaticasysteem hindert, wordt gestraft met gevangenisstraf van 6 maanden tot een jaar en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met een van die straffen alleen.

§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. De Staat is burgerlijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt. ».

Art. 8

In artikel 89 van hetzelfde Wetboek worden de woorden « en 39, » vervangen door « , 39 en 39*bis*, ».

Art. 9

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 …, worden een 1°*bis*, *ter* en *quater*, een 10°*bis* en een 13°*bis* ingevoegd, luidend als volgt :

« 1°*bis*. Artikel 210*bis* van hetzelfde Wetboek; »;

« 1°*ter*. Artikel 259*bis* van hetzelfde Wetboek; »;

« 1°*quater*. Artikel 314*bis* van hetzelfde Wetboek; »;

« 10°*bis*. Artikel 504*quater* van hetzelfde Wetboek; »;

« 13°*bis*. Artikelen 550*bis* en 550*ter* van hetzelfde Wetboek; ».

Art. 10

In artikel 90*quater* van hetzelfde Wetboek wordt een § 4 toegevoegd, luidend als volgt :

§ 4. De onderzoeksrechter kan van 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

L'ordonnance de rechercher soi-même les données pertinentes ne peut être prise à l'égard de l'inculpé et à l'égard de ses proches.

§ 3. Celui qui refuse de prêter son concours technique aux réquisitions visées aux §§ 1er et 2, concours dont les modalités sont déterminées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications ou qui fait obstacle à la recherche dans le système informatique, est puni d'un emprisonnement de six mois à un an et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

§ 4. Toute personne qui, du chef de sa fonction, a connaisance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 5. L'État est civilement responsable pour le dommage causé par les personnes requises de façon non intentionnelle à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système. ».

Art. 8

À l'article 89 du même Code, les mots « et 39 » sont remplacés par « , 39 et 39*bis* ».

Art. 9

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 ..., sont insérés un 1°*bis*, *ter* et *quater*, un 10°*bis* et un 13°*bis*, rédigés comme suit :

« 1°*bis*. L'article 210*bis* du même Code; »;

« 1°*ter*. L'article 259*bis* du même Code; »;

« 1°*quater*. L'article 314*bis* du même Code; »;

« 10°*bis*. L'article 504*quater* du même Code; »;

« 13°*bis*. Les articles 550*bis* et 550*ter* du même Code; ».

Art. 10

L'article 90*quater* du même Code est complété par un § 4, rédigé comme suit :

§ 4. 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

versleutelen, vorderen inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm 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.

Degene die weigert de in de vorige leden gevorderde medewerking te verlenen, medewerking waarvan de modaliteiten worden vastgesteld door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met gevangenisstraf van 6 maanden tot een jaar en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met een van die straffen alleen.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. ».

Art. 11

In artikel 90*septies* van hetzelfde Wetboek wordt tussen het vierde en het laatste lid een nieuw lid ingevoegd, luidend als volgt :

« De aangepaste middelen kunnen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen of 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 deze middelen en het ogenblik waarop deze middelen de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en vierde lid, vervangen. ».

Art. 12

In artikel 109*ter* E van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de wet van 21 december 1994, hernummerd bij de wet van 19 december 1997 en gewijzigd bij de wet van …, worden de volgende wijzigingen aangebracht :

— 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

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.

Celui qui refuse de fournir le concours requis par les alinéas précédents, concours dont les modalités sont déterminées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, est puni d'un emprisonnement de six mois à un an et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. ».

Art. 11

À l'article 90*septies* du même code, il est inséré entre le quatrième et le dernier alinéa un alinéa nouveau rédigé comme suit :

« Les moyens appropriés peuvent être utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée ou 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 ces moyens et le moment où ces moyens remplacent la conservation sous pli scellé ou le registre spécial prévus aux troisième et quatrième alinéas. ».

Art. 12

À l'article 109*ter* E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, inséré par la loi du 21 décembre 1994, rénuméroté par la loi du 19 décembre 1997 et modifié par la loi du …, sont apportées les modifications suivantes :

— 1° le premier alinéa du § 2 est complété comme suit :

« , ainsi que les obligations pour les opérateurs de réseaux de télécommunication et les fournisseurs de service d'enregistrer et de conserver dans les cas et pendant un délai à déterminer par le Roi, les données

van gebruikers van telecommunicatiediensten te registreren en, in de gevallen en gedurende een termijn door de Koning te bepalen, te bewaren, te bepalen bij een in Ministerraad overlegd besluit en op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie. »;

— 2° artikel 109*ter* E wordt als volgt aangevuld :

« § 3. Hij die de verplichtingen door de Koning krachtens de vorige paragrafen bepaald, niet nakomt, wordt gestraft met gevangenisstraf van 3 tot 6 maanden en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met een van die straffen alleen.

§ 4. De Koning bepaalt bij in Ministerraad overlegd besluit en na advies van de commissie voor de bescherming van de persoonlijke levenssfeer de modaliteiten en de middelen om de vertrouwelijkheid en de integriteit van de oproep- en identificatiegegevens bedoeld in § 2 te waarborgen. ».

d'appel de moyens de télécommunication et les données d'identification d'utilisateurs de services de télécommunication à déterminer par le Roi, par arrêté délibéré en Conseil des ministres et sur proposition du ministre de la Justice et du ministre compétent pour les Télécommunications. »;

— 2° l'article 109*ter* E est complété comme suit :

« § 3. Celui qui ne respecte pas les obligations prévues par le Roi en vertu des paragraphes précédents est puni d'un emprisonnement de trois à six mois et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

§ 4. Le Roi par arrêté délibéré en Conseil des ministres et après avis de la commission pour la protection de la vie privée prévoit les modalités et les moyens appropriés pour garantir la confidentialité et l'intégrité des données d'appels et d'identification visées au § 2. ».

ADVIES VAN DE RAAD VAN STATE

De RAAD VAN STATE, afdeling wetgeving, tweede kamer, op 13 juli 1998 door de minister van Justitie verzocht hem van advies te dienen over een ontwerp van wet « inzake informaticacriminaliteit », heeft, na de zaak te hebben onderzocht op de zittingen van 26 en 29 april, 17 en 31 mei 1999, op laatstvermelde datum het volgende advies gegeven :

ONDERWERP VAN HET ONTWERP

Zoals in de memorie van toelichting is aangegeven, wordt met de ontworpen wet gepoogd :

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

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

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

Hierbij werden de relevante internationaalrechtelijke instrumenten in rekening gebracht. Met name werd inspiratie geput uit twee belangrijke aanbevelingen die werden uitgewerkt in het kader van de Raad van Europa : de aanbeveling nr R(89)9 van 13 september 1989 inzake computergerelateerde criminaliteit en de aanbeveling nr R(95)13 van 11 september 1995 inzake problemen van strafprocesrecht die gelieerd zijn aan de informatietechnologie. ».

Met het ontwerp worden aldus twee precieze doelstellingen nagestreefd, namelijk enerzijds aanpassing van de strafbepalingen, wanneer de klassieke rechtsbegrippen niet meer de mogelijkheid bieden in te spelen op de specifieke noden in verband met computercriminaliteit, anderzijds wijziging van de strafrechtelijke procedure om de politiediensten en gerechtelijke diensten aangepaste juridische middelen ter beschikking te stellen ter bestrijding van computercriminaliteit.

In het Strafwetboek worden aldus ingevoerd de « valsheid in informatica » (lees : valsheid in computerbestanden) (ontworpen artikel 210*bis*), het « informaticabedrog » (lees : de computerfraude (ontworpen artikel 504*quater*) en de « misdrijven tegen de vertrouwelijkheid, integriteit en be-

AVIS DU CONSEIL D'ÉTAT

Le CONSEIL D'ÉTAT, section de législation, deuxième chambre, saisi par le ministre de la Justice, le 13 juillet 1998, d'une demande d'avis sur un projet de loi « relative à la criminalité informatique », après avoir examiné l'affaire en ses séances des 26 et 29 avril, 17 et 31 mai 1999, a donné, à cette dernière date, l'avis suivant :

OBJET DU PROJET

Comme l'indique l'exposé des motifs, la loi en projet tente :

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

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

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

À cet égard, il a été tenu compte des instruments de droit international pertinents. L'inspiration a notamment été puisée dans deux recommandations importantes élaborées dans le cadre du Conseil de l'Europe : la recommandation n° R(89)9 du 13 septembre 1989 en matière de criminalité informatique et la recommandation n° R(95)13 du 11 septembre 1995 relative aux problèmes de droit de procédure pénale liés à la technologie de l'information. ».

Le projet poursuit ainsi deux objectifs précis, à savoir, d'une part, une adaptation des dispositions pénales lorsque les concepts juridiques classiques ne permettent pas de répondre aux spécificités de la criminalité informatique et, d'autre part, une modification de la procédure pénale afin de permettre aux services policiers et judiciaires de disposer de moyens juridiques appropriés pour lutter contre la criminalité informatique.

Font ainsi leur apparition dans le Code pénal, le « faux en informatique » (article 210*bis* en projet), « la fraude informatique » (article 504*quater* en projet) ainsi que « les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données

schikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen » (ontworpen artikelen 550*bis* en 550*ter*).

In het Wetboek van Strafvordering moet de « inbeslagneming van gegevens » tijdens het onderzoek (ontworpen artikel 39*bis*) worden geregeld, de opsporing worden aangepast aan de eisen inzake computercriminaliteit (ontworpen artikel 88*ter*) en worden voorzien in de mogelijkheid om bepaalde personen die een bijzondere kennis hebben van de onderzochte computersystemen, te dwingen politie en gerecht bij te staan (ontworpen artikel 88*quater*).

De lijst van strafbare feiten waarvoor interceptiemaatregelen kunnen worden uitgevaardigd, wordt verruimd tot strafbare feiten terzake van telecommunicatie, tot de nieuwe strafbare feiten « valsheid in informatica » (lees : valsheid in computerbestanden), « informaticabedrog » (lees : computerfraude), « ongeoorloofde toegang tot een informaticasysteem » (lees : computervredebreuk, « data- en informaticasabotage » (lees : « data- en computersabotage) (ontworpen artikel 90*ter*).

Ten slotte brengt het ontwerp ook wijzigingen aan in de wet van 21 maart 1991 tot hervorming van sommige economische overheidsbedrijven, door nieuwe verplichtingen op te leggen aan de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten (ontworpen artikel 109*ter* E). Volgens de memorie van toelichting « zullen de verstrekkers van telecommunicatiediensten structurele maatregelen moeten nemen om, enerzijds, de oproepgegevens (oorsprong, bestemming, localisatie, duur, …) van telecommunicatie te kunnen achterhalen, en anderzijds gebruikers die informatie aan het publiek aanbieden, te kunnen identificeren, en deze inlichtingen te bewaren. Het betreft derhalve zowel gegevens die betrekking hebben op privé-telecommunicatie als op openbare telecommunicatie ».

qui sont stockées, traitées ou transmises par le biais de ces systèmes » (articles 550*bis* et 550*ter* en projet).

Quant au Code d'instruction criminelle, il s'agit d'organiser « la saisie de données » au cours de l'instruction (article 39*bis* en projet), d'adapter la perquisition aux exigences de la criminalité informatique (article 88*ter* en projet) et de contraindre certaines personnes ayant une connaissance particulière des systèmes informatiques faisant l'objet d'enquêtes, à assister les autorités policières et judiciaires (article 88*quater* en projet).

La liste des infractions pour lesquelles une mesure d'interception est possible, est élargie aux infractions en matière de télécommunications, aux nouveaux délits de « faux en informatique », de « fraude informatique », « d'accès illicite à un système informatique », de « sabotage informatique et de données » (article 90*ter* en projet).

Enfin, le projet apporte également des modifications à la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques en créant de nouvelles obligations dans le chef des opérateurs de réseaux et des fournisseurs de services de télécommunications (article 109*ter* E en projet). Ceux-ci seront notamment, aux termes de l'exposé des motifs, « tenus de prendre des mesures pour pouvoir retrouver les données d'appel de télécommunication (origine, destination, localisation, durée, …), d'une part, identifier les utilisateurs qui fournissent ces informations au public, d'autre part, et conserver ces renseignements. Il s'agit par conséquent tant de données qui concernent la télécommunication privée que la télécommunication publique ».

ALGEMENE OPMERKINGEN

I. **De internationale aspecten van computercriminaliteit**

In een door de algemene vergadering van de Raad van State van Frankrijk op 2 juli 1998 goedgekeurde studie is de volgende diagnose gesteld :

« La coopération judiciaire internationale est indispensable pour assurer une action efficace contre des sites ou des comportements litigieux dans l'espace mondial des réseaux; les progrès sont fort lents et les réticences des États qui craignent une perte de souveraineté importantes; même entre pays démocratiques comparables comme ceux du Conseil de l'Europe, les différences de sensibilité restent fortes et donc la définition des infractions communes délicate; dès lors, seule la

OBSERVATIONS GÉNÉRALES

I. **Les aspects internationaux de la criminalité informatique**

Dans une étude adoptée le 2 juillet 1998, l'assemblée générale du Conseil d'État de France a posé le diagnostic suivant :

« La coopération judiciaire internationale est indispensable pour assurer une action efficace contre des sites ou des comportements litigieux dans l'espace mondial des réseaux; les progrès sont fort lents et les réticences des États qui craignent une perte de souveraineté importantes; même entre pays démocratiques comparables comme ceux du Conseil de l'Europe, les différences de sensibilité restent fortes et donc la définition des infractions communes délicate; dès lors, seule la

détermination politique des États à mener une action contre les « paradis virtuels » et la délinquance de haute technologie peut les conduire à accepter l'abandon d'une partie de leur souveraineté afin de garantir l'efficacité de l'action répressive internationale. » ([1]).

Het is nuttig zich te bezinnen op deze tekst, die onverbloemd aantoont dat het noodzakelijk is de computercriminaliteit aan te pakken en dat wat elke Staat hiertoe kan ondernemen, beperkt is.

A. *De wetgevende en rechterlijke bevoegdheid*

a) Uit artikel 3 van het Strafwetboek kan worden afgeleid dat de Belgische autoriteiten de daders van in België gepleegde misdrijven, ongeacht of zij Belg of vreemdeling zijn, kunnen opsporen, vervolgen en bestraffen. Het Hof van Cassatie heeft van zijn kant geoordeeld dat een misdrijf in België is gepleegd, als een van de bestanddelen ervan of van de bezwarende omstandigheden waarin het is gepleegd, er is gelokaliseerd. Dezelfde autoriteiten mogen daarentegen de dader van een in het buitenland gepleegd misdrijf, ongeacht of hij Belg of vreemdeling is, niet vervolgen of straffen dan in de gevallen bij de wet bepaald (artikel 4 van het Strafwetboek).

Een kenmerk van computercriminaliteit is dat ze betrekking heeft op een computernetwerk dat niet door staatsgrenzen is beperkt; de bestanddelen van een strafbaar feit en de bezwarende omstandigheden waarin het wordt gepleegd, kunnen dus gemakkelijk tegelijkertijd op het grondgebied van verschillende staten gelokaliseerd zijn. Er mag dan ook worden van uitgegaan dat de territoriale aanknopingspunten niet altijd adequaat genoeg zijn om de specifieke handelingen in de computercriminaliteit doeltreffend te vervolgen en te bestraffen.

b) In de aanbevelingen van de Raad van Europa, waarop het ontwerp beoogt te steunen, wordt ervan uitgegaan dat de verdeling van de bevoegdheid van de Staten niet meer moet berusten op de goede wil van elke staat om zijn bevoegdheid te beperken, maar op gemeenschappelijk in internationale verdragen vastgelegde regels waarbij aanknopingspunten zouden worden bepaald. Dit zou zonder twijfel het beste middel zijn om de delicate vragen op te lossen die de keuze van die aanknopingen doet rijzen. Zulke verdragen bestaan evenwel nog niet. Zolang dat niet het geval is, mag het ontwerp echter niet aan die vragen voorbijgaan, omdat als in de wet hierover niets wordt gesteld, het aan de rechter wordt overgelaten om alleen en in de grootste

([1]) Zie in dit verband de studie die door de algemene vergadering van de Raad van State van Frankrijk op 2 juli 1998 goedgekeurd is en die gepubliceerd is in *« Internet et les réseaux numériques »*, *La Documentation française*, 1998, blz. 200.

détermination politique des États à mener une action contre les « paradis virtuels » et la délinquance de haute technologie peut les conduire à accepter l'abandon d'une partie de leur souveraineté afin de garantir l'efficacité de l'action répressive internationale. » ([1]).

Il est utile de méditer ce texte qui révèle sans illusion la nécessité autant que les limites de ce que chaque État peut entreprendre pour s'attaquer à la criminalité informatique.

A. *La compétence législative et judiciaire*

a) Il se déduit de l'article 3 du Code pénal que les autorités belges peuvent rechercher, poursuivre et punir les auteurs, qu'ils soient belges ou étrangers, des infractions commises en Belgique. La Cour de cassation a, pour sa part, considéré qu'une infraction est commise en Belgique si l'un de ses éléments constitutifs ou aggravants y est localisé. En revanche, les mêmes autorités ne peuvent poursuivre ou punir l'auteur, belge ou étranger, d'une infraction commise à l'étranger que dans les cas déterminés par la loi (article 4 du Code pénal).

Une caractéristique de la criminalité informatique est le fait qu'elle concerne un réseau informatique qui n'est pas limité par les frontières étatiques; les éléments constitutifs des infractions et les circonstances aggravantes peuvent facilement prendre place dans plusieurs États à la fois. Aussi peut-on penser que les critères de rattachement territoriaux ne sont pas toujours bien adaptés pour poursuivre et punir efficacement les comportements spécifiques de la criminalité informatique.

b) Les recommandations du Conseil de l'Europe précitées, dont le projet entend s'inspirer, estiment que la répartition des compétences des États ne doit plus reposer sur le bon vouloir de chacun d'eux de limiter la sienne, mais sur des règles arrêtées en commun par des conventions internationales qui fixeraient des critères de rattachement. Ce serait assurément le meilleur moyen de résoudre les questions délicates que le choix de ces rattachements soulève. Il reste cependant que de telles conventions n'existent pas encore. Tant qu'elles demeurent absentes, le projet ne peut, toutefois, rester muet sur ces questions, car alors, le silence de la loi revient à laisser au juge le soin de trancher seul dans la plus grande insécurité juridique les difficultés touchant

([1]) Voir à ce propos l'étude adoptée par l'assemblée général du Conseil d'État de France le 2 juillet 1998 et publiée dans « Internet et les réseaux numériques », La Documentation française, 1998, p. 200.

rechtsonzekerheid de problemen te beslechten die verband houden met de vraag of moet worden aangenomen dat een of ander bestanddeel van een computermisdrijf of een of andere bezwarende omstandigheid, al dan niet geacht moet worden in België gelokaliseerd te zijn.

B. *Het opsporen van strafbare feiten en het vervolgen van de daders ervan*

a) Een van de fundamentele regels van het internationaal recht bepaalt dat een Staat staatsgezag uitoefent op zijn eigen grondgebied, en dat alleen doet, zonder inmenging van enige andere Staat. Hieruit volgt dat een Staat in vredestijd absoluut geen dwangmiddelen mag gebruiken op het grondgebied van een andere Staat. Dit geldt inzonderheid voor alle handelingen van de uitvoerende macht, die al dan niet betrekking hebben op justitie. 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 ([1]).

Het is evenwel niet eenvoudig de precieze strekking van die regel te bepalen ten aanzien van het optreden van justitie of politie in verband met computergegevens, inzonderheid wat betreft bevelen tot opsporing en inbeslagneming van zulke gegevens. Dat probleem is niet alleen het gevolg van de blijvende onzekerheid die soms bestaat over de vraag waar computergegevens precies te vinden zijn; het houdt ook verband met het feit dat een autoriteit, precies dankzij de informatica, gegevens in het buitenland kan navorsen zonder daarom het grondgebied van de staat waaronder ze ressorteert, in stoffelijke zin te verlaten.

De meeste Staten zijn het er thans blijkbaar nog altijd over eens dat alleen het louter aanwezig zijn van gerechtelijke of politieautoriteiten op hun eigen grondgebied hun niet toestaat hun optreden uit te breiden tot alle gegevens; deze gegevens kunnen nochtans verschijnen op het scherm van een computer, die zich eveneens op datzelfde grondgebied bevindt. Om het onderzoek wettig te laten verlopen, is het bovendien noodzakelijk dat de gegevens (die de overheid aldus kan « zien », en eventueel kan bemachtigen) zich dus niet op het grondgebied van een vreemde Staat bevinden.

Die algemene opvatting van de Staten is onlangs uiteengezet in de voornoemde aanbeveling nr R(95)13 van het Ministercomité van de Raad van Europa aan de lidstaten.

Daarin staat te lezen dat wat betreft de « gegevens die in een ander land opgeslagen zijn …, de meeste

([1]) Paul Reuter, « *Droit international public* », blz. 165.

à la question de savoir s'il faut considérer que tel ou tel élément constitutif d'une infraction informatique, ou tel ou tel élément aggravant, doit ou non être considéré comme localisé en Belgique.

B. *La recherche des infractions et la poursuite de leurs auteurs*

a) Parmi les règles fondamentales du droit international figure celle selon laquelle l'État exerce l'autorité étatique sur son propre territoire, et le fait seul, à l'exclusion de tout autre État. Il en découle qu'en temps de paix, il est absolument interdit à un État de procéder à une fonction de contrainte sur le territoire d'un autre État. Ceci concerne notamment tous les actes de la fonction exécutive, liés ou non à la justice. 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 ([1]).

Il n'est, toutefois, pas simple de déterminer la portée exacte que revêt cette règle quant aux actions judiciaires ou policières touchant à des données informatiques, notamment les mandats de perquisition et de saisie qui concernent de telles données. La difficulté ne résulte pas seulement de l'incertitude persistante qui peut parfois planer sur la question de savoir où sont exactement localisées des données informatiques; elle tient encore au fait que, grâce précisément à l'informatique, une autorité est capable, sans pour autant quitter physiquement le territoire de l'État dont elle relève, d'investiguer sur des données situées à l'étranger.

Il semble bien que la plupart des États s'accordent encore aujourd'hui pour estimer que le seul fait de la présence de l'autorité judiciaire ou policière sur le territoire de son propre État ne suffit pas à lui permettre d'étendre son action sur n'importe laquelle des données qui, cependant, peuvent apparaître sur l'écran d'un ordinateur se trouvant, lui aussi, sur ce même territoire. Encore faut-il, pour rendre l'investigation licite, que les données (que l'autorité peut ainsi « voir », et dont elle peut éventuellement « s'emparer ») ne se trouvent pas localisées sur le territoire d'un État étranger.

Cette opinion générale des États a été récemment exposée dans la recommandation n° R(95) 13 précitée, du Comité des ministres du Conseil de l'Europe aux États membres.

On peut y lire qu'à l'égard des « données stockées dans un autre pays ... la plupart des États membres ten-

([1]) Paul Reuter, « Droit international public », p. 165.

lidstaten ervan lijken uit te gaan dat een opsporing op het netwerk over de grenzen heen door de overheden die belast zijn met het onderzoek, zonder toestemming van de bevoegde autoriteiten van het betrokken land, een schending van de soevereiniteit en van het internationaal recht zou kunnen vormen, alsmede een gedeeltelijk omzeilen van het traditionele middel van de wederzijdse rechtshulp ». In dezelfde aanbeveling wordt ook verklaard dat dat ook beschouwd zou kunnen worden als een overtreding van de wetgeving van het land (waar de gegevens zich bevinden) en er zelfs een strafbaar feit zou kunnen zijn » (nr 189, blz. 76).

Het is dus op zijn minst twijfelachtig of het ontwerp niet strijdig zal zijn met de aldus bepaalde regel van internationaal recht.

b) De bepaling van het ontworpen artikel 88*ter* breekt immers duidelijk met die regel, doordat ze toestaat een opsporing te verruimen vanaf het systeem aangewezen in het bevel tot opsporing, dus vanaf de plaats waar het systeem zich bevindt, tot een ander systeem, dat dan weer elders, in voorkomend geval in het buitenland, gelokaliseerd is.

Doordat het ontworpen artikel 88*ter*, § 1, de onderzoeksrechter aldus machtigt zijn onderzoek te verruimen, laat het ook aan hem over te oordelen over de opportuniteit van die verruiming; in dezelfde paragraaf 1, *in fine*, van dat artikel worden trouwens de criteria genoemd op basis waarvan de rechter hierover dient te beslissen. Die criteria zijn niet verschillend naargelang het gaat om een overschrijding van de grenzen van de territoriale bevoegdheid van de onderzoeksrechter, dan wel van de grenzen van de Staat waaraan de rechter zijn rechtsmacht ontleent.

De enige regel die in het bijzonder betrekking heeft op het probleem van internationaal recht, is vervat in paragraaf 3, tweede lid, van artikel 88*ter*, waar sprake is van door uitbreiding van het onderzoek (...) aangetroffen gegevens, maar « die zich niet op het grondgebied van het Rijk bevinden ». Deze enige regel bepaalt alleen dat die buitenlandse gegevens « enkel gekopieerd worden » en dat de onderzoeksrechter via het openbaar ministerie het ministerie van Justitie hiervan op de hoogte moet brengen.

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 internationaal recht waarnaar hierboven verwezen is. De « *hot pursuit* », een traditionele rechtsinstelling in het internationale zeerecht, waarnaar, weliswaar op grond van analogie, in de bespreking van artikel 88*ter* verwezen wordt, is evenmin toereikend.

In de bepaling van het ontwerp wordt stellig uitgegaan van bepaalde, in de voormelde aanbeveling geuite

dent à considérer qu'une perquisition transfrontalière sur réseau menée par les autorités chargées de l'enquête sans l'autorisation des autorités compétentes du pays concerné pourrait constituer une violation de la souveraineté et du droit international, ainsi qu'un contournement partiel de la voie traditionnelle d'entraide judiciaire ». La même Recommandation ajoute encore que « cela pourrait être considéré aussi comme une violation de la législation du pays (où les données se trouvent) et même y constituer une infraction pénale » (n° 189, p. 76).

La compatibilité du projet avec la règle de droit international ainsi identifiée est dès lors, pour le moins, problématique.

b) En effet, le texte de l'article 88*ter* en projet s'affranchit nettement de cette règle en ce qu'il permet d'étendre une perquisition depuis le système désigné par le mandat qui l'autorise et donc depuis le lieu où ce système est situé, vers un autre système, situé, pour sa part, en un autre lieu et, le cas échéant, à l'étranger.

Le texte de l'article 88*ter*, § 1er, en projet, en conférant ainsi au juge d'instruction le pouvoir d'étendre sa recherche, lui confie aussi le soin d'apprécier l'opportunité de l'extension; cet article précise d'ailleurs, au même paragraphe 1er, *in fine*, les critères d'après lesquels le juge doit en décider. Ces critères ne sont pas différents selon qu'il s'agit de franchir les limites de la compétence territoriale du juge d'instruction, ou qu'il s'agit de franchir les frontières de l'État dont le juge tient son pouvoir de juridiction.

La seule règle qui concerne spécialement le problème de droit international se rencontre au paragraphe 3, alinéa 2, de l'article 88*ter*, où il est question des données rassemblées par l'extension de la recherche, mais « qui ne se trouvent pas sur le territoire belge ». Cette unique règle se borne à préciser que ces données étrangères « peuvent seulement être copiées » et que le juge d'instruction doit en informer, par l'intermédiaire du ministère public, le ministère de la Justice.

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*ter* fait une allusion, sans doute métaphorique, n'y suffit pas davantage.

La règle du projet s'inspire assurément de certains vœux formulés par la recommandation précitée. Il faut

wensen. Er dient evenwel te worden opgemerkt dat in het ontwerp geen sprake is van het expliciete onderscheid dat in die aanbeveling is gemaakt tussen de gegevens die zich in het geheugen van de computer bevinden, en waarop de opsporing betrekking heeft, en die welke zich elders bevinden. In het bijzonder ten aanzien van gegevens die zich niet bevinden in het systeem waarvoor een opsporingsbevel gegeven is, maar die elders, op het grondgebied van een andere staat, opgeslagen zijn, is de aanbeveling duidelijk door te stellen dat « in dat geval alleen de traditionele weg van de wederzijdse rechtshulp overblijft »; die aanbeveling wijst aldus impliciet, maar stellig, van de hand dat een Staat, zonder voorafgaande toestemming, zulke gegevens kan navorsen. Zoals in de bespreking trouwens gepreciseerd wordt, beoogt de ontworpen tekst evenwel precies zulk een navorsing toe te staan in de gevallen waarin de onderzoeksrechter dit noodzakelijk acht; doordat het ontwerp hem alleen een verplichting tot kennisgeving *a posteriori* oplegt, is hij krachtens de tekst niet gebonden door de beperkingen die internationale wederzijdse rechtshulp meebrengen.

De beperkingen die de naleving van het beginsel van de territoriale soevereiniteit van de Staten meebrengen, kunnen buitensporig lijken en van die aard zijn dat ze het verloop van een doeltreffende nasporing door de politie te zeer bemoeilijken. De door de gemachtigde ambtenaar geuite wil om degenen die onderzoekingen van die aard moeten verrichten « inzonderheid juridisch te beschermen », mag er evenwel niet toe leiden dat in België een wet wordt gemaakt op grond waarvan een vreemde Staat, die zich door het optreden van een Belgische autoriteit benadeeld acht, zelfs zou kunnen pogen België internationaal aansprakelijk te stellen en van België compensatie te eisen.

c) Een Belgische wet mag vanzelfsprekend niet in strijd zijn met het internationale recht door de Belgische gerechtelijke autoriteiten toe te staan op het grondgebied van een ander land ambtsdaden te stellen.

België mag evenmin met een eigen wet een bijzondere vorm van samenwerking tussen de Belgische gerechtelijke overheid of politieautoriteiten en die van andere Staten vaststellen. Die nadere regels voor samenwerking tussen België en talrijke andere Europese landen zijn immers bepaald in verdragen, die stuk voor stuk uitzonderingen vormen op het beginsel van de exclusieve territorialiteit. Die verdragen bevestigen dus tegelijkertijd het bestaan van dat beginsel en de verwachting van de Staten dat het nageleefd wordt, behalve in uitzonderlijke gevallen waarin die verdragen voorzien en volgens de nadere regels die ze bepalen.

Dit geldt aldus inzonderheid voor de twee verdragen waarbij België zich tegenover bepaalde Europese Staten verbonden heeft : het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken, opgemaakt te

cependant observer que les distinctions explicites faites par cette dernière — entre les données se trouvant dans la mémoire de l'ordinateur, objet de la perquisition, et celles qui se trouvent ailleurs —, ne sont pas reproduites dans le projet. En particulier, à l'égard de données qui ne sont pas dans le système visé par le mandat de perquisition, mais sont stockées ailleurs, sur le territoire d'un autre État, la recommandation tranche clairement en affirmant qu' « il ne subsiste alors que la voie traditionnelle de l'entraide judiciaire »; elle exclut ainsi, implicitement mais sûrement, qu'un État puisse, sans accord préalable, investiguer sur de telles données. Or, c'est précisément une telle investigation que, comme l'explique d'ailleurs son commentaire, le texte en projet entend permettre dans les cas où le juge d'instruction l'estime nécessaire; le texte le libère des contraintes de l'entraide judiciaire internationale en lui imposant seulement une obligation d'information *a posteriori*.

Certes, les rigueurs qu'impose le respect du principe de la souveraineté territoriale des États peuvent sembler excessives et propres à entraver trop le cours d'une investigation policière efficace. Il n'en reste pas moins vrai que le souci, exposé par le fonctionnaire délégué, de « protéger notamment juridiquement » ceux qui sont amenés à conduire des recherches de ce type, ne doit pas aller jusqu'à faire élaborer en Belgique une loi sur laquelle il se pourrait même qu'un État étranger, s'estimant lésé par l'action d'une autorité belge, tente de se fonder pour dénoncer la responsabilité internationale de la Belgique et en exiger réparation.

c) Une loi belge ne peut évidemment pas violer le droit international en permettant aux autorités judiciaires belges d'accomplir des actes de leur fonction sur le territoire d'un pays étranger.

La Belgique ne peut pas non plus par une loi propre établir un mode particulier de coopération entre ses autorités judiciaires ou policières et celles des autres États. Ces modalités de la coopération entre la Belgique et de nombreux autres pays européens ont, en effet, été arrêtées par des traités qui constituent autant d'exceptions au principe de la territorialité exclusive. Ces traités attestent donc à la fois l'existence de ce principe et le fait que les États tiennent à ce qu'il soit respecté, sauf dans les cas exceptionnels que ces traités prévoient et selon les modalités qu'ils précisent.

Il en est ainsi notamment des deux traités par lesquels la Belgique s'est liée à certains États européens : la Convention européenne d'entraide judiciaire en matière pénale faite à Strasbourg le 20 avril 1959 et ap-

Straatsburg op 20 april 1959 en goedgekeurd bij de wet van 14 juli 1975 en de Overeenkomst ter uitvoering van het Akkoord van Schengen van 14 juni 1985 tussen de regeringen van de Staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek, betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen, gedaan op 18 juni 1990 en goedgekeurd bij de wet van 18 maart 1993. Met het eerste van deze verdragen wordt de rogatoire commissie het belangrijkste instrument van de wederzijdse rechtshulp; de overeenkomst ter uitvoering van het Akkoord van Schengen, van haar kant, berust voornamelijk op een wederzijdse informatieplicht en stelt een regeling van toestemming in wanneer de politieautoriteiten van een Staat de grenzen van een andere Staat overschrijden.

Uit de uitleg die voorafgaat volgt dat de bepalingen van het ontwerp die een internationale draagwijdte hebben, moeten worden herdacht om zowel het internationale gemeen recht als de in België vigerende verdragen na te leven.

d) Of het verzamelen van gegevens die zich op buitenlands grondgebied bevinden al dan niet onwettig is uit het oogpunt van het internationale recht, moet vanzelfsprekend ook worden bezien ten aanzien van de eventuele weerslag van die mogelijke onwettigheid op de bewijskracht die de strafrechtbanken aan dat materiaal kunnen toekennen of ontzeggen.

Bovendien rijst nog de vraag of de rechter zijn opvatting mag gronden op gegevens die bijzonder beschermd worden volgens het recht van de staat waar ze verzameld zijn, inzonderheid omdat ze beschouwd worden als persoonsgegevens, omdat ze beschermd zijn wegens het beroepsgeheim, of nog omdat ze betrekking hebben op de fundamentele belangen van de Staat (veiligheid, landsverdediging, enz.). Er mag immers niet uit het oog worden verloren dat, al berust de bewijsvoering in ons strafrechtelijk systeem op het vrijheidsbeginsel zodat de rechter zijn opvatting mag gronden op alle gegevens die hem ter kennis zijn gebracht, die gegevens niettemin regelmatig moeten zijn verkregen en de partijen ze vrij moeten kunnen tegenspreken.

De Belgische rechtbanken kunnen zich in dit opzicht wellicht laten leiden door de rechtspraak van het Hof van Cassatie (1) toen het afluisteren van telefoongesprekken in België nog niet toegestaan was. Het Hof was van oordeel dat gegevens verkregen door het afprouvée par la loi du 14 juillet 1975 et la Convention d'application de l'Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française, relatif à la suppression graduelle des contrôles aux frontières communes, faite le 18 juin 1990 et approuvée par la loi du 18 mars 1993. La première de ces conventions fait de la commission rogatoire l'instrument essentiel de l'entraide judiciaire; quant à la convention d'application de l'Accord de Schengen, elle repose principalement sur un devoir d'information réciproque et institue un régime d'autorisation lorsque les autorités policières d'un État franchissent les frontières d'un autre.

Il résulte des explications qui précèdent que les dispositions du projet revêtant une portée internationale doivent être repensées en vue de respecter autant le droit international commun que les traités en vigueur en Belgique.

d) Une éventuelle illicéité de droit international commise en recueillant des données situées en territoire étranger doit évidemment être aussi envisagée du point de vue des conséquences qu'elle peut avoir sur la valeur probatoire que les tribunaux répressifs pourraient reconnaître ou dénier à ces documents.

Du reste, il faudra encore s'interroger sur la question de savoir si le juge pourra asseoir sa conviction sur des données qui font l'objet d'une protection particulière selon le droit de l'État où elles ont été recueillies, notamment parce qu'elles sont tenues pour des données à caractère personnel, parce qu'elles sont protégées par le secret professionnel ou encore parce qu'elles concernent les intérêts fondamentaux de l'État (sûreté, défense nationale, etc.). Il faut, en effet, ne pas perdre de vue que si, dans notre système pénal, l'administration de la preuve repose sur un principe de liberté en sorte que le juge peut fonder sa conviction sur tous les éléments portés à sa connaissance, encore faut-il que ceux-ci aient été régulièrement obtenus et que les parties puissent les contredire librement.

Sans doute les juridictions belges pourraient-elles à cet égard s'inspirer de la jurisprudence élaborée par la Cour de cassation (1) à l'époque où les écoutes téléphoniques n'étaient pas encore autorisées en Belgique. La Cour avait estimé que des données fournies par de

(1) Cass. AR 7913, 24 mei 1983, Arr. Cass. 1982-1983, 1169; Cass. AR 7240, 26 januari 1993, Arr. Cass. 1992-1993, 108; Cass. AR 6420, 12 oktober 1993, Arr. Cass. 1993-1994, 830. Zie eveneens Brussel 30 november 1984, J.T., 1985, blz. 729 en volgende en de opmerkingen van D. Garabedian.

(1) Cass. 24 mai 1983, Pas. I, 1063; Cass. 26 janvier 1993, Pas., I, 101; Cass. 12 octobre 1993, Pas., I, 816; voir également Bruxelles 30 novembre 1984, J.T., 1985, pp. 729 et suivantes et les observations de D. Garabedian.

luisteren van telefoongesprekken door de rechter in aanmerking mochten worden genomen indien ze waren verkregen overeenkomstig de buitenlandse wet van het land waar was afgeluisterd, indien die wet tenminste in overeenstemming was met artikel 8, lid 1, van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

II. **De grondwettelijke aspecten van computercriminaliteit**

A. *Het gelijkheidsbeginsel : computercriminaliteit en traditionele criminaliteit*

Zoals uit het rapport van het Europees Comité voor strafrechtelijke vraagstukken blijkt, mag de omstandigheid dat een strafbaar feit met computers te maken heeft, niet als een verzwarende omstandigheid worden beschouwd (1).

Hoewel de notie computercriminaliteit vaag is, wordt er algemeen van uitgegaan dat ze twee categorieën van strafbare feiten omvat : enerzijds de strafbare feiten die tegen het computernetwerk zelf worden gepleegd — het gaat meer bepaald om een inbreuk op de integriteit van het computersysteem, de integriteit van de gegevens die dat systeem bevat en de vertrouwelijkheid van die gegevens — en anderzijds de strafbare feiten die door middel van de computer worden gepleegd, waar het namelijk gaat om klassieke strafbare feiten, die reeds buiten de context van de informatica bestaan (2).

Al dienen in het strafrecht bepaalde wijzigingen te worden aangebracht om rekening te houden met de specifieke aard van computercriminaliteit en het grondwettelijk beginsel « *Nullum crimen sine lege* » in acht te nemen, toch mogen die aanpassingen van het strafrecht aan de technologische vooruitgang er niet toe leiden dat een bepaald gedrag wordt bestraft, terwijl datzelfde gedrag misschien niet zou zijn bestraft zonder het gebruik van de computer.

Het volgende mag niet uit het oog worden verloren :

« ... *les données confidentielles intégrées sur un support informatique n'ont, en soi, pas plus de valeur que les données figurant sur tout support quelconque tenu secret par son placement dans une salle forte, un coffre-fort, voire une simple enveloppe.* » (3).

(1) Rapport gevoegd bij Aanbeveling nr R(89)9 inzake computergerelateerde criminaliteit, Straatsburg, 1990, blz. 23.

(2) Zie in dit verband de studie die door de algemene vergadering van de Raad van State van Frankrijk op 2 juli 1998 goedgekeurd is en die gepubliceerd is in « *Internet et les réseaux numériques* », blz. 169.

(3) P. Glineur, « *Droit et éthique de l'informatique* », gepolykopieerde syllabus van het licentiaat informatica (cursus 1e licentiaat — faculteit wetenschappen) en van het licentiaat informatica en menswetenschappen (cursus 2e licentiaat — faculteit sociale, politieke en economische wetenschappen) van de « *Université libre de Bruxelles* », 1999, blz. 186.

II. **Les aspects constitutionnels de la criminalité informatique**

A. *Le principe d'égalité : la criminalité informatique et la criminalité traditionnelle*

Ainsi qu'il ressort du rapport du Comité européen pour les problèmes criminels, « la dimension informatique d'un délit ne doit pas être considérée en tant que telle comme une circonstance aggravante de celui-ci » (1).

Si la notion de criminalité informatique est floue, généralement on considère qu'elle recouvre deux catégories d'infractions : il y a, d'une part, les infractions commises contre le réseau informatique lui-même — il s'agit notamment de porter atteinte à l'intégrité du système informatique, à l'intégrité des données qu'il contient, à la confidentialité de celles-ci — et il y a, d'autre part, les infractions commises grâce à l'informatique, c'est-à-dire qu'il s'agit d'infractions classiques qui existent déjà en dehors du contexte de l'informatique (2).

Si le droit pénal nécessite certaines modifications pour tenir compte des spécificités de la criminalité informatique et ce afin de respecter le principe constitutionnel « *Nullum crimen sine lege* », il ne faudrait cependant pas que ces adaptations du droit pénal aux progrès technologiques aboutissent à sanctionner un type de comportement alors que si ce même comportement avait été commis sans l'aide de l'informatique, il n'aurait peut-être pas donné lieu à une répression pénale.

Il convient de ne pas perdre de vue que :

« ... les données confidentielles intégrées sur un support informatique n'ont, en soi, pas plus de valeur que les données figurant sur tout support quelconque tenu secret par son placement dans une salle forte, un coffre-fort, voire une simple enveloppe. » (3).

(1) Rapport accompagnant la Recommandation n° R(89)9 sur la criminalité en relation avec l'ordinateur, Strasbourg, 1990, p. 23.

(2) Voir à ce propos l'étude précitée, adoptée par l'assemblée générale du Conseil d'État de France le 2 juillet 1998 et publiée dans « Internet et les réseaux numériques », p. 169.

(3) P. Glineur, « Droit et éthique de l'informatique », cours polycopié de la licence en informatique (cours de 1re licence — Faculté des sciences) et de la licence en informatique et sciences humaines (cours de 2e licence — Faculté des sciences sociales, politiques et économiques) de l'Université libre de Bruxelles, 1999, p. 186.

Pol Glineur wijst op het volgende :

« *... l'adoption d'un Code pénal de l'informatique présente donc le risque de voir, par exemple, ériger en infraction l'accès non désiré par son titulaire à un agenda électronique alors que l'accès non désiré à un agenda « papier », tout aussi confidentiel, demeurerait impuni. Il est douteux que la différence objective de support des données supposées confidentielles (l'agenda électronique ou l'agenda papier) justifie la différence de traitement au niveau pénal : l'atteinte à la confidentialité par l'auteur de l'acte est moralement, socialement et économiquement condamnable de la même manière et avec la même intensité dans les deux cas.* » ([1]).

a) Zo straft het ontworpen artikel 550*bis*, § 1, van het Strafwetboek degene die, zonder daartoe gerechtigd te zijn, zich toegang heeft verschaft tot een computersysteem, of bij vergissing in dat systeem is binnengedrongen, maar besluit om het niet te verlaten, ongeacht wat die persoon wil doen met de gegevens die hij heeft kunnen raadplegen.

In de context van computercriminaliteit kan loutere nieuwsgierigheid een strafbaar feit opleveren.

Uit de uitleg van de gemachtigde ambtenaar blijkt dat het beschermde rechtsbelang in het onderhavige geval de beveiliging van het computersysteem is; zulk een ongeoorloofd binnendringen kan tot gevolg hebben dat aan de computersystemen, en zelfs aan de gegevens die ze bevatten, schade wordt toegebracht.

Als zodanig beschouwd, is het strafbaar feit reeds duidelijker omschreven, aangezien het impliceert dat het binnendringen aan het computersysteem schade heeft toegebracht.

De formulering van het ontworpen artikel 550*bis*, § 1, is echter veel ruimer en vergt niet zulk een schade om strafrechtelijke bestraffing mogelijk te maken.

Uit het rapport van het Europees Comité voor strafrechtelijke vraagstukken blijkt ([2]) het volgende :

« *il y a peu de pays dont la législation permette de sanctionner un comportement qui consiste purement et simplement dans l'accès non autorisé à un réseau informatique.* ».

Bepaalde staten hebben ongeoorloofd binnendringen in een computersysteem bestraft wanneer dit interceptie van persoonsgegevens tot gevolg heeft of schade veroorzaakt aan het computersysteem of de gegevens die het bevat.

Andere landen, zoals Frankrijk, hebben subjectieve criteria opgelegd in verband met het gedrag van de delinquent.

([1]) *Ibidem*.
([2]) Zie de bladzijden 54 tot 56.

Ainsi que le démontre Pol Glineur,

« ... l'adoption d'un Code pénal de l'informatique présente donc le risque de voir, par exemple, ériger en infraction l'accès non désiré par son titulaire à un agenda électronique alors que l'accès non désiré à un agenda « papier », tout aussi confidentiel, demeurerait impuni. Il est douteux que la différence objective de support des données supposées confidentielles (l'agenda électronique ou l'agenda papier) justifie la différence de traitement au niveau pénal : l'atteinte à la confidentialité par l'auteur de l'acte est moralement, socialement et économiquement condamnable de la même manière et avec la même intensité dans les deux cas. » ([1]).

a) Ainsi, l'article 550*bis*, § 1er, en projet du Code pénal punit celui qui a accédé à un système informatique sans y être autorisé ou celui qui, par erreur, a accédé à un tel système mais décide de s'y maintenir, peu importe les intentions de cette personne par rapport aux données qu'elle a pu consulter.

Dans un contexte informatique, la simple curiosité peut susciter un délit pénal.

Il ressort des explications du fonctionnaire délégué que l'intérêt juridique protégé est, dans le cas d'espèce, la sécurité du système informatique; de tels accès non autorisés peuvent avoir pour conséquence d'endommager les systèmes informatiques, voire même les données contenues dans ces systèmes.

Envisagée comme telle, l'infraction est déjà plus précise puisqu'elle implique que l'accès a occasionné un préjudice au système informatique.

Or, l'article 550*bis*, § 1er, en projet, est beaucoup plus large dans sa formulation et ne nécessite pas un tel préjudice pour qu'une répression pénale puisse être mise en œuvre.

Il ressort du rapport du Comité européen pour les problèmes criminels ([2]) qu'

« il y a peu de pays dont la législation permette de sanctionner un comportement qui consiste purement et simplement dans l'accès non autorisé à un réseau informatique. ».

Certains États ont sanctionné des accès non autorisés lorsqu'ils ont pour effets d'intercepter des données à caractère personnel ou encore lorsqu'ils engendrent des dommages au système informatique ou aux données qu'il contient.

D'autres pays comme la France, ont imposé des critères subjectifs relatifs au comportement du délinquant.

([1]) *Ibidem*.
([2]) Voir les pages 54 à 56.

Zo worden in artikel 323-1 van het Franse strafwetboek straffen gesteld op het bedrieglijk volledig of gedeeltelijk binnendringen in een systeem van automatische gegevensverwerking of op het niet verlaten van dat systeem.

De Belgische wetgever moet er dus op toezien dat hij bij het bestraffen van een gedrag geen discriminaties creëert.

b) Een opmerking van dezelfde aard dient te worden gemaakt in verband met het ontworpen artikel 210*bis*.

Uit de bespreking van die bepaling blijkt het volgende : « In tegenstelling tot de gemeenrechtelijke valsheid in geschrifte wordt geen bijzonder opzet vereist. De reden hiervoor is dat, enerzijds het oogmerk van bedrieglijke verrijking reeds wordt geviseerd door de voorgestelde bepaling inzake informaticafraude (... ontworpen artikel 504*quater*), en anderzijds datamanipulatie met het specifieke doel schade te berokkenen geviseerd wordt door de bepalingen inzake informatica- en datasabotage (... ontworpen artikel 550*ter*) ».

Hieruit volgt dat valsheid in computerbestanden als moreel bestanddeel uitsluitend algemeen opzet vereist. Dat strafbaar feit kan worden toegeschreven aan een persoon indien die persoon dat feit willens en wetens heeft gepleegd.

Wanneer het gaat om manipulaties van gegevens, zijn vergissingen frequent en niet noodzakelijk opzettelijk.

Het kan gaan om een onoplettendheid, een gewone fout of een nalatigheid.

In verband met deze essentiële kwestie van het moreel bestanddeel van een strafbaar feit is het de Raad van State niet duidelijk om welke reden voor valsheid in computerbestanden aan geheel andere voorwaarden dient te worden voldaan dan voor gemeenrechtelijke valsheid in geschrifte.

Evenzo wordt in de artikelen 193 en volgende van het strafwetboek een onderscheid gemaakt naargelang de personen die het valsheiddelict plegen, ambtenaren of openbare officieren zijn, of naargelang de vervalste akte een openbaar, authentiek, handels- of privaat geschrift is. In de ontworpen bepaling daarentegen wordt aan dat onderscheid geen aandacht meer geschonken.

Bepaalde gegevens, inzonderheid betreffende de staat van personen, worden momenteel beheerd door een computersysteem dat onder het toezicht van de openbare besturen staat; denk aan het rijksregister van de natuurlijke personen, aan de kruispuntbank van de sociale zekerheid of nog aan het nationale strafregister.

Ook hier is het de Raad van State niet duidelijk om welke reden die fundamentele verschillen uit het strafrecht in dezen niet worden gemaakt.

c) Dezelfde opmerking dient te worden gemaakt in verband met het ontworpen artikel 550*bis*.

Ainsi, l'article 323-1 du Code pénal français incrimine le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données.

Le législateur belge doit donc veiller à ne pas créer de discriminations lorsqu'il réprime un comportement.

b) Une observation du même ordre doit être formulée en ce qui concerne l'article 210*bis* en projet.

En effet, il ressort du commentaire de cette disposition que, « contrairement au faux en écritures de droit commun, aucune intention particulière n'est requise vu que, d'une part, l'intention d'enrichissement frauduleux est déjà visée dans la proposition de disposition en matière de fraude informatique (... article 504*quater* en projet) et que, d'autre part, la manipulation de données dans le but spécifique de nuire est visée dans les dispositions relatives au sabotage informatique et au sabotage de données (... article 550*ter* en projet) ».

Il en résulte que le faux en informatique requiert uniquement comme élément moral le dol général. Cette infraction sera imputable à une personne si celle-ci l'a commise avec connaissance et volonté.

S'agissant de manipulations informatiques, les erreurs sont fréquentes et pas nécessairement volontaires.

Il peut s'agir d'une inattention, d'une simple faute ou d'une négligence.

Sur cette question essentielle qu'est l'élément moral de l'infraction, le Conseil d'État n'aperçoit pas la raison pour laquelle le faux en informatique répond à de toutes autres conditions que le faux en écriture de droit commun.

De même, les articles 193 et suivants du Code pénal font une distinction suivant que les personnes qui commettent l'infraction de faux sont des fonctionnaires ou officiers publics ou suivant que l'acte falsifié est un acte public, authentique, de commerce de banque ou un acte privé. Par contre, la disposition en projet ne se soucie plus de ces distinctions.

Or, certaines données concernant notamment l'état des personnes sont actuellement gérées par un système informatique sous le contrôle des administrations; il suffit de penser au registre national des personnes physiques, à la banque-carrefour en matière de sécurité sociale ou encore au casier judiciaire national.

Ici également, le Conseil d'État n'aperçoit pas la raison pour laquelle ces distinctions fondamentales en droit pénal ne sont pas opérées en la matière.

c) Une observation identique doit être formulée en ce qui concerne l'article 550*bis* en projet.

Paragraaf 2 van dat artikel betreft een persoon die recht op toegang tot een computersysteem heeft, maar van dat recht misbruik maakt met het oogmerk te schaden of met bedrieglijk opzet.

De Raad van State ziet niet in waarom in het onderhavige geval bedrieglijk opzet of het oogmerk te schaden vereist is, terwijl het louter ongeoorloofd binnendringen in een computersysteem reeds een strafbaar feit oplevert overeenkomstig paragraaf 1, eerste lid, van het ontworpen artikel 550*bis*.

Eenieder die toegang heeft tot het computersysteem en uit loutere nieuwsgierigheid misbruik maakt van zijn recht op toegang, zou niet strafbaar zijn, terwijl degene die er geen toegang toe heeft strafbaar is ... . Hier wordt « met twee maten gemeten », wat de wetgever objectief moet kunnen wettigen.

d) De Raad van State heeft ook vragen bij de interne samenhang van artikel 90*quater* van het Wetboek van Strafvordering.

Zo is bij 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, in paragraaf 2 van artikel 90*quater* een nieuw lid ingevoegd dat bepaalt dat « iedere persoon die zijn technische medewerking weigert aan de vorderingen bedoeld in dit artikel, medewerking waarvan de modaliteiten vastgesteld worden door de Koning, op voorstel van de minister van Justitie en de minister bevoegd voor Telecommunicatie, wordt gestraft met een geldboete van zesentwintig Belgische frank tot tienduizend Belgische frank ».

De in die bepaling bedoelde personen zijn de operatoren van communicatienetwerken en de verstrekkers van telecommunicatiediensten.

Paragraaf 4 van het ontworpen artikel 90*quater* heeft dan weer betrekking op iedere persoon die de gerechtelijke en politie-autoriteiten kan helpen, en in het derde ontworpen lid ervan wordt bepaald dat ze, indien ze weigeren hun medewerking te verlenen, worden gestraft met gevangenisstraf van zes maanden tot een jaar en met geldboete van zesentwintig tot twintigduizend frank.

Het is de Raad van State niet duidelijk om welke objectieve reden die personen strenger dan de operatoren en de verstrekkers van diensten worden gestraft.

De steller van het ontwerp dient die keuze te rechtvaardigen.

B. *Het beginsel van de wettelijkheid van de strafbaarstellingen*

a) Benevens het bezwaar dat in de vorige opmerking is geopperd, doet het ontworpen artikel 210*bis* een bezwaar rijzen inzake de wettelijkheid van de strafbaarstellingen.

Le paragraphe 2 de cet article concerne une personne qui est autorisée à accéder au système informatique, mais qui abuse de son pouvoir d'accès dans le but de nuire ou avec une intention frauduleuse.

Le Conseil d'État n'aperçoit pas pour quelle raison, dans ce cas d'espèce, l'on exige une intention frauduleuse ou un but de nuire alors que le simple accès non autorisé donne déjà lieu à une infraction conformément au paragraphe 1er, alinéa 1er, de l'article 550*bis* en projet.

Quiconque a accès au système informatique et qui abuse de son pouvoir d'accès par simple curiosité ne serait pas punissable, alors que celui qui n'y a pas accès est punissable ... Il y a là « deux poids deux mesures » que le législateur doit pouvoir justifier objectivement.

d) Le Conseil d'État s'interroge également sur la cohérence interne de l'article 90*quater* du Code d'instruction criminelle.

Ainsi, 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 a introduit dans le paragraphe 2 de l'article 90*quater* un nouvel alinéa prévoyant que « toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, concours dont les modalités sont déterminées par le Roi, sur la proposition du ministre de la justice et du ministre compétent pour les télécommunications, est punie d'une amende de vingt-six francs belges à dix mille francs belges ».

Les personnes visées par cette disposition sont les opérateurs des réseaux de communication et les fournisseurs du service de télécommunication.

Le paragraphe 4 de l'article 90*quater* en projet vise quant à lui toute personne susceptible d'aider les autorités judiciaires et policières et le troisième alinéa en projet dispose que si elles refusent de prêter leur concours, elles seront punies d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs belges à vingt mille francs belges.

Le Conseil d'État n'aperçoit pas pour quelle raison objective ces personnes sont plus sévèrement punies que les opérateurs et les fournisseurs de services.

Il appartient à l'auteur du projet de justifier ce choix.

B. *Le principe de la légalité des incriminations*

a) Outre la critique formulée dans l'observation précédente, l'article 210*bis* en projet appelle une objection au regard du principe de la légalité des incriminations.

In dat artikel wordt het begrip « gegevens » op zich niet gedefinieerd.

In de memorie van toelichting wordt aangegeven dat daarmee « wordt gedoeld op voorstellingen van informatie die geschikt zijn voor opslag, verwerking en overdracht via een informaticasysteem ».

Zodra de steller van het ontwerp die « gegevens » strafrechtelijk wil beschermen, dient in het dispositief duidelijk te worden gedefinieerd wat juist onder die benaming valt. Met uitleg in de memorie van toelichting kan in dezen niet worden volstaan.

b) Het ontworpen artikel 550*bis* geeft aanleiding tot een soortgelijke opmerking.

De ontworpen paragraaf 3 is volstrekt onduidelijk.

Uit de bespreking van die bepaling in de memorie van toelichting blijkt dat de ontworpen paragraaf 1 verwijst naar spionage, paragraaf 2 naar het veroorzaken van tijdverlies en paragraaf 3 naar het veroorzaken van schade, hetzij aan het computersysteem zelf, hetzij aan de daarin vervatte gegevens.

Volgens de voormelde aanbeveling n^{r} R(89)9 beantwoordt computerspionage echter aan een heel andere definitie.

Computerspionage bestaat in het wederrechtelijk verkrijgen of in het verspreiden, overdragen of gebruiken zonder recht of enige andere wettige reden, van een bedrijfs- of handelsgeheim met de bedoeling de persoon die recht heeft op het geheim economische schade te berokkenen of voor zichzelf of voor een derde een onwettig economisch voordeel te verkrijgen (1).

Als de bedoeling van de steller van het ontwerp erin bestaat een straf te stellen op het ongeoorloofd intercepteren van gegevens, wordt eveneens verwezen naar de voormelde aanbeveling R(89)9, die daarvan een nauwkeurige definitie geeft (2).

De ontworpen paragraaf 1 dient grondig te worden herzien teneinde de inhoud ervan te verduidelijken.

De ontworpen paragraaf 2 is nauwelijks duidelijker. In de voormelde aanbeveling n^{r} R(89)9 is sprake van het strafbaar feit van het ongeoorloofde gebruik van een computersysteem of een computernetwerk.

Ook hier echter verschilt de door de aanbeveling voorgestelde tekst grondig van de ontworpen tekst.

Ook paragraaf 2 behoort grondig te worden herzien, doordat zulk een onnauwkeurigheid een schending inhoudt van het beginsel van de wettelijkheid van de strafbaarstellingen en van de straffen.

(1) Zie blz. 69-70 van het rapport bij aanbeveling n^{r} R(89)9.

(2) Zie blz. 59 van het rapport.

Dans cet article, la notion de « données » n'est pas définie en tant que telle.

L'exposé des motifs indique que « par données, on entend les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique ».

Dès l'instant où l'auteur du projet entend, sur le plan pénal, protéger ces « données », il convient que le dispositif définisse clairement ce qu'elles recouvrent exactement. Un exposé des motifs ne peut suffire.

b) L'article 550*bis* en projet appelle une observation du même ordre.

Le paragraphe 3 en projet manque totalement de clarté.

Le commentaire de cette disposition fait apparaître que le paragraphe 1er en projet constituerait de l'espionnage, le paragraphe 2 impliquerait un vol en termes de temps et le paragraphe 3 serait la provocation d'un dommage soit au système informatique lui-même, soit aux données qu'il contient.

Si l'on s'en réfère à la recommandation n° R(89)9, précitée, l'espionnage informatique répond à une toute autre définition.

Constitue un espionnage informatique, « l'obtention par des moyens illégitimes ou la divulgation, le transfert ou l'utilisation sans droit ni autre justification légale d'un secret commercial ou industriel, dans l'intention de causer un préjudice économique à la personne ayant droit au secret, ou d'obtenir pour soi-même ou pour autrui un avantage économique illicite » (1).

Si l'intention de l'auteur du projet est de punir l'interception non autorisée de données, il est également renvoyé à la recommandation n° R(89)9, précitée, qui en donne une définition précise (2).

Le paragraphe 1er en projet doit être fondamentalement revu afin d'en clarifier le contenu.

Le paragraphe 2 en projet n'est guère plus précis. La recommandation n° R(89)9, précitée, envisage l'infraction d'utilisation non autorisée d'un système ou d'un réseau informatique.

Mais, une nouvelle fois, le texte proposé par la recommandation est fort différent de celui qui est en projet.

Le paragraphe 2 doit, lui aussi, être fondamentalement revu, dans la mesure où un tel manque de précision constitue une violation du principe de la légalité des incriminations et des peines.

(1) Voir p. 69-70 du rapport accompagnant la recommandation n° R(89)9.

(2) Voir p. 59 du rapport.

c) Het ontworpen artikel 39*bis* geeft aanleiding tot een soortgelijke opmerking.

In de ontworpen paragraaf 2 wordt de procureur des Konings ertoe gemachtigd « de aangepaste middelen aan (te wenden) om de toegang tot (in beslag genomen) gegevens ... te verhinderen ». In de ontworpen tekst wordt echter niet gepreciseerd wat onder « aangepaste middelen » moet worden verstaan.

Bovendien zou het beter zijn om in het Nederlands in plaats van het woord « aangepaste » het woord « passende » te gebruiken als equivalent voor het Franse « appropriés ».

In de bespreking van deze bepaling in de memorie van toelichting is echter sprake van « techniques de cryptage » en « versleutelingstechnieken », terwijl in de voormelde aanbeveling nr R(95)13 gebruik wordt gemaakt van de term « chiffrement » (vercijfering).

Aangezien het *in casu* gaat om een regeling die verband houdt met de strafrechtelijke procedure, zouden die « aanpaste (of passende) middelen » duidelijker moeten worden gedefinieerd.

Deze opmerking geldt ook voor paragraaf 3 (die de ontworpen paragraaf 4 wordt) en voor paragraaf 5 (die de ontworpen paragraaf 6 wordt).

Paragraaf 4 (die de ontworpen paragraaf 5 wordt) bepaalt dat de procureur des Konings verplicht is « de verantwoordelijke van het informaticasysteem » in te lichten.

Die bepaling geeft echter niet aan wat onder « de verantwoordelijke van het informaticasysteem » moet worden verstaan.

In de zin van de voormelde aanbeveling nr R(95)13 geldt het begrip « persoon die voor een computersysteem verantwoordelijk is » voor alle personen die bij een opsporingsactie of een inbeslagneming formeel of werkelijk controle blijken uit te oefenen op het computersysteem waarop de opsporing betrekking heeft. Het kan gaan om de eigenaar van het systeem, om een operateur van dat systeem of zelfs om de bewaker (huurder of bewoner) van de lokalen waarin het computersysteem zich bevindt (1).

In de ontworpen bepaling dient bijgevolg uitdrukkelijk te worden bepaald welke personen moeten worden ingelicht.

Overigens kan de inbeslagneming van gegevens ook van belang zijn voor derden. Zo worden de lidstaten in de voormelde aanbeveling nr R(95)13 verzocht dit verstrekken van inlichtingen te regelen met oog voor de noden van het onderzoek (2).

Dat vereiste is van belang, aangezien eenieder die zich door een opsporingshandeling of een onderzoeks-

(1) Zie blz. 34 van het rapport bij aanbeveling nr R(95)13.

(2) Zie blz. 35 van het rapport.

c) L'article 39*bis* en projet suscite une critique analogue.

Au paragraphe 2 en projet, le procureur du Roi est habilité à prendre « les moyens appropriés pour empêcher l'accès » aux données qui sont saisies. Le texte en projet ne précise cependant pas ce qu'il faut entendre par « moyens appropriés ».

Dans le texte néerlandais du paragraphe 2, il vaudrait mieux, en outre, remplacer le mot « *aangepaste* » par le mot « *passende* ».

Le commentaire de cette disposition fait par contre référence à la technique du cryptage, la recommandation n° R(95)13, précitée, parle quant à elle du chiffrement.

S'agissant d'un texte touchant à la procédure pénale, il conviendrait d'identifier plus clairement ces « moyens appropriés ».

La même remarque vaut pour les paragraphes 3 (devenant le paragraphe 4 en projet) et 5 (devenant le paragraphe 6 en projet).

Le paragraphe 4 (devenant le paragraphe 5 en projet) contient une obligation d'information à charge du procureur du Roi et destinée au « responsable du système informatique ».

Mais la disposition ne donne pas une définition de ce qu'il faut entendre par « le responsable du système informatique ».

Au sens de la recommandation n° R(95)13, précitée, la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition. Il peut s'agir du propriétaire du système, d'un opérateur de ce système ou même du gardien (locataire ou occupant) des locaux abritant le système informatique (1).

La disposition en projet doit, en conséquence, définir expressément les personnes concernées par l'information.

Par ailleurs, la saisie de données peut également concerner des tierces personnes. C'est ainsi que la recommandation n° R(95)13, précitée, invite les États membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête (2).

Cette exigence est importante car, en vertu des articles 28*sexies* et 61*quater* du Code d'instruction

(1) Voir p. 34 du rapport accompagnant la recommandation n° R(95)13.

(2) Voir p. 35 du rapport.

handeling met betrekking tot zijn goederen geschaad acht, krachtens de artikelen 28*sexies* en 61*quater* van het Wetboek van strafvordering aan de procureur des Konings of aan de onderzoeksrechter de opheffing ervan kan vragen.

In dat verband biedt de ontworpen paragraaf 2, tweede lid, nauwelijks duidelijkheid doordat daarin wordt bepaald dat de procureur des Konings « evenwel het verdere gebruik van het geheel of een deel van deze gegevens (kan) toestaan, wanneer dit geen gevaar voor de Strafvordering oplevert. ».

d) Het ontworpen artikel 88*quater* staat bloot aan dezelfde kritiek.

De ontworpen bepaling levert immers geen enkele precisering op omtrent de personen die aldus zouden kunnen worden gedwongen hun medewerking te verlenen. In de ontworpen paragraaf 2, tweede lid, worden weliswaar de verdachte en zijn naaste familieleden uitgesloten teneinde het recht om het stilzwijgen te bewaren, te garanderen.

Het begrip « naaste familieleden » wordt echter niet gepreciseerd. Het zou gaan om personen die met de verdachte verwant zijn. Als zulks de bedoeling van de steller van het ontwerp is, behoort die bepaling in die zin te worden herzien.

Opdat artikel 458 van het Strafwetboek niet volledig wordt uitgehold, behoort overigens, overeenkomstig de voormelde aanbeveling R(95)13, te worden bepaald dat dit dwangmiddel evenmin kan worden toegepast op personen die aan het beroepsgeheim zijn gehouden.

Een soortgelijke opmerking dient te worden gemaakt over het ontworpen artikel 90*quater.*

e) Het ontworpen artikel 90*septies* bevat een onaanvaardbare opdracht van bevoegdheid aan de Koning.

Aangezien het hier om de bewijsvoering gaat, moet in de wet worden aangegeven wat onder « aangepaste (of passende) middelen » dient te worden verstaan. In dit verband wordt verwezen naar algemene opmerking nr I.

C. *Het recht op eerbiediging van het privé-leven*

De steller van het ontwerp wordt eraan herinnerd dat 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 ordonnantie moeten de bescherming van dat recht waarborgen.

Alleen bij wet kunnen dan ook enige beperkingen op het recht op eerbiediging van het privé- en het gezinsleven worden gesteld.

Wat het ontworpen artikel 109*ter*, E, betreft, gaat het voor de operatoren van telecommunicatienetwerken en verstrekkers van telecommunicatiediensten om het registreren en bewaren van « oproepgegevens ». Volgens

criminelle, toute personne qui s'estime lésée par un acte d'information ou par un acte d'instruction relatif à ses biens peut en demander la levée soit au procureur du Roi, soit au juge d'instruction.

À cet égard, le paragraphe 2, alinéa 2, en projet, n'est guère explicite lorsqu'il dispose que le procureur du Roi « peut cependant 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. ».

d) L'article 88*quater* en projet s'expose à la même critique.

La disposition en projet n'apporte, en effet, aucune précision sur les personnes qui pourraient ainsi être contraintes de collaborer. Le paragraphe 2, alinéa 2, en projet, exclut cependant l'inculpé et ses proches et ce afin de préserver le droit au silence.

La notion de « proches » n'est toutefois pas précisée. Il s'agirait des personnes qui ont un lien de parenté avec l'inculpé. Si telle est la volonté de l'auteur du projet, la disposition doit être revue en ce sens.

Par ailleurs, ainsi que le suggère la recommandation n° R(95)13, précitée, il convient d'exclure également de ce pouvoir de contrainte, les personnes soumises au secret professionnel sous peine de vider l'article 458 du Code pénal de tout son sens.

Une observation similaire doit également être faite au sujet de l'article 90*quater* en projet.

e) L'article 90*septies* en projet comporte une délégation au Roi qui n'est point admissible.

La loi doit spécifier ce qu'il y a lieu d'entendre par « moyens appropriés », s'agissant de l'administration de la preuve. Sur ce point, il est fait référence à l'observation générale I.

C. *Le droit au respect de la vie privée*

Il est rappelé à l'auteur du projet qu'en vertu de l'article 22 de la Constitution, 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 et l'ordonnance doivent garantir la protection de ce droit.

Seule la loi peut ainsi apporter certaines restrictions au droit à la vie privée et familiale.

En ce qui concerne l'article 109*ter*, E, en projet, il s'agit pour les opérateurs de réseaux de télécommunication et les fournisseurs de service d'enregistrer et de conserver des « données d'appel ». En vertu du com-

de bespreking van deze bepaling in de memorie van toelichting verwijst dit begrip naar alle informatie betreffende de oorsprong, de bestemming, de « lokalisatie » en de duur van telecommunicatie. Naast die gegevens zullen ook de gegevens voor de identificatie van de gebruikers van telecommunicatiediensten moeten worden geregistreerd en bewaard.

Dat zijn gegevens die deel uitmaken van het privéleven van de betrokkenen.

Bijgevolg staat het alleen aan de wetgever om duidelijk te vermelden 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.

Bijgevolg dient deze bepaling grondig te worden herwerkt.

III. DE KWALIFICATIE VAN HET ONTWERP

Volgens artikel 1 van de ontworpen wet geldt daarvoor de procedure van het onvolledige bicamerisme, bepaald in artikel 78 van de Grondwet.

Verscheidene bepalingen van het ontwerp hebben echter betrekking 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.

De afdeling wetgeving van de Raad van State heeft in haar adviezen over een wetsontwerp « betreffende de internationale samenwerking inzake de tenuitvoerlegging van inbeslagnemingen en verbeurdverklaringen » (1) en over een wetsontwerp « betreffende de toegang tot en het opsporen van nummers van communicatie- en telecommunicatiemiddelen en houdende wijziging van de artikelen 90*ter*, 90*quater*, 90*sexies* en 90*septies* van het Wetboek van strafvordering » (2), geoordeeld dat voor de bepalingen betreffende de bevoegdheden van de onderzoeksrechter de procedure van het volledige bicamerisme, bedoeld in artikel 77 van de Grondwet, behoort te worden gevolgd.

Bijgevolg dient artikel 1 van het ontwerp te worden gewijzigd.

Gelet op de voorgaande fundamentele opmerkingen, dient het ontwerp dan ook volledig te worden herwerkt.

Naar aanleiding van het herzien van het ontwerp zou in gedachte moeten worden gehouden dat de Nederlandse tekst van verscheidene bepalingen van het ontmentaire de cette disposition, ce concept recouvre toute information relative à l'origine, la destination, la localisation et la durée de la télécommunication. Outre ces données, devront être enregistrées et conservées les « données d'identification » concernant les utilisateurs.

Il s'agit là d'éléments participant à la vie privée de chacun.

En conséquence, il appartient au législateur seul d'identifier clairement 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.

En conséquence, cette disposition sera fondamentalement complétée.

III. QUANT À LA QUALIFICATION DU PROJET

Selon son article 1er, la loi en projet devrait être soumise à la procédure bicamérale incomplète consacrée à l'article 78 de la Constitution.

Or, 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.

En ses avis concernant d'une part, un projet de loi « sur la coopération internationale en ce qui concerne l'exécution de saisies et de confiscations » (1) et, d'autre part, un projet de loi « concernant l'identification et le repérage des numéros des postes de communication ou de télécommunication et portant modification des articles 90*ter*, 90*quater*, 90*sexies* et 90*septies* du Code d'instruction criminelle » (2), la section de législation du Conseil d'État a considéré que les dispositions relatives aux compétences du juge d'instruction relèvent de la procédure bicamérale complète visée à l'article 77 de la Constitution.

En conséquence, l'article 1er du projet sera modifié.

En conclusion, compte tenu des observations fondamentales qui précèdent, le projet doit être entièrement revu.

À l'occasion de cette révision, le texte néerlandais du projet ainsi que celui de l'exposé des motifs doivent également être revus du point de vue de la correction

(1) Gedr. St. Kamer, 1995-1996, nr 427/1, blz. 15.
(2) Gedr. St. Kamer, 1996-1997, nr 1075/1, blz. 17.

(1) Doc. parl. Chambre, 1995-1996, n° 427/1, p. 15.
(2) Doc. parl. Chambre, 1996-1997, n° 1075/1, p. 17.

werp uit een oogpunt van correct taalgebruik voor verbetering vatbaar is. Zo bijvoorbeeld schrijve men, onder voorbehoud van de hiervoren gemaakte inhoudelijke opmerkingen, in artikel 4, het ontworpen artikel 550*bis*, § 1, tweede lid, « bedraagt de gevangenisstraf zes maanden … » in plaats van « is de gevangenisstraf van 6 maanden … », in artikel 5, het ontworpen artikel 39*bis*, § 3, « om technische redenen of vanwege de omvang van de gegevens » in plaats van « omwille van technische redenen of omwille van de omvang van de gegevens » alsook « wendt de procureur des Konings de passende middelen aan … » in plaats van « wendt hij de, in de aangepaste middelen aan … » en in § 4 « de opsporing … de gegevens die zijn gekopieerd, ontoegankelijk zijn gemaakt of verwijderd » in plaats van « de zoeking … de gegevens die werden gekopieerd, ontoegankelijk werden gemaakt of verwijderd ».

Ook de Nederlandse tekst van de memorie van toelichting zou uit een oogpunt van correct taalgebruik en uit een oogpunt van consistent gebruik van de terminologie moeten worden herzien.

De Kamer was samengesteld uit

HH. :

Y. KREINS, *staatsraad, voorzitter;*

P. LIENARDY,
P. QUERTAINMONT, *staatsraden;*

P. GOTHOT,
J. van COPPENOLLE, *assessoren van de afdeling wetgeving;*

Mevr. :

J. GIELISSEN, *griffier.*

Het verslag werd uitgebracht door mevrouw P. VANDERNACHT, auditeur. De nota van het Coördinatiebureau werd opgesteld en toegelicht door de heer P. BROUWERS, referendaris.

De overeenstemming tussen de Franse en de Nederlandse tekst werd nagezien onder toezicht van de heer P. LIENARDY.

De griffier, *De voorzitter,*

J. GIELISSEN Y. KREINS

de la langue, en tenant compte des observations faites dans la version néerlandaise du présent avis.

La Chambre était composée de

MM. :

Y. KREINS, *conseiller d'État, président de chambre;*

P. LIENARDY,
P. QUERTAINMONT, *conseillers d'État;*

P. GOTHOT,
J. van COPPENOLLE, *assesseurs de la section de législation;*

Mme :

J. GIELISSEN, *greffier.*

Le rapport a été présenté par MME P. VANDERNACHT, auditeur. La note de Bureau de coordination a été rédigée et exposée par M. P. BROUWERS, référendaire.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de M. P. LIENARDY.

Le greffier, *Le président,*

J. GIELISSEN Y. KREINS

WETSONTWERP I
(Nr 213/1)

———

ALBERT II, KONING DER BELGEN

Aan allen die nu zijn en hierna wezen zullen,
ONZE GROET.

Op de voordracht van Onze minister van Justitie, Onze minister van Telecommunicatie en Overheidsbedrijven en Participaties en Onze minister van Economie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ :

Onze minister van Justitie, Onze minister van Telecommunicatie en Overheidsbedrijven en Participaties en Onze minister van Economie zijn gelast het wetsontwerp waarvan de tekst volgt, in Onze naam aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen :

Artikel 1

Deze wet regelt een aangelegenheid zoals bedoeld in artikel 78 van de Grondwet.

Art. 2

In hoofdstuk IV van titel V van boek II van het Strafwetboek wordt een nieuwe afdeling II*bis* ingevoegd, houdende een artikel 210*bis*, luidend als volgt :

« Afdeling II*bis*. — Valsheid in informatica

Art. 210*bis*. — § 1. 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, 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.

§ 2. Hij die, terwijl hij weet dat aldus bekomen gegevens vals zijn, hiervan gebruik maakt, wordt gestraft alsof hij de dader van de valsheid was.

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

§ 4. De straffen gesteld in de §§ 1 tot 3 worden verdubbeld indien een overtreding van een van die bepa-

PROJET DE LOI I
(N° 213/1)

———

ALBERT II, ROI DES BELGES

À tous, présents et à venir,
SALUT.

Sur la proposition de Notre ministre de la Justice, de Notre ministre des Télécommunications et des Entreprises et Participations publiques et de Notre ministre de l'Économie,

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

Notre ministre de la Justice, Notre ministre des Télécommunications et des Entreprises et Participations publiques et Notre ministre de l'Économie sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit :

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

Art. 2

Il est inséré, au chapitre IV, titre V, IIe livre du Code pénal une nouvelle section II*bis*, contenant un article 210*bis*, rédigée comme suit :

« Section II*bis*. — Faux en informatique

Art. 210*bis*. — § 1er. 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, 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.

§ 2. 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.

§ 3. La tentative de commettre l'infraction prévue 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.

§ 4. Les peines portées par les §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est

lingen wordt begaan binnen 5 jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 259*bis*, 314*bis*, 504*quater* of in titel IX*bis* van dit Wetboek. ».

Art. 3

In hoofdstuk II van titel IX van boek II van het Strafwetboek wordt een nieuwe afdeling III*ter*, houdende een artikel 504*quater* ingevoegd, luidend als volgt :

« Afdeling III*bis*. — Informaticabedrog

Art. 504*quater*. — § 1. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 50 000 Belgische frank of met een van die straffen alleen.

§ 2. Hij die, door het misdrijf bedoeld in § 1 te plegen, voor zichzelf of voor een ander een bedrieglijk vermogensvoordeel verwerft, 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.

§ 3. De straffen gesteld in §§ 1 en 2 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen 5 jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis* of in titel IX*bis* van dit Wetboek. ».

Art. 4

In boek II van het Strafwetboek wordt een nieuwe titel IX*bis*, houdende de artikelen 550*bis* en 550*ter*, ingevoegd, luidend als volgt :

« Titel IX*bis*. — Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen

Art. 550*bis*. — § 1. Hij die, terwijl hij weet dat hij daartoe niet gerechtigd is, zich toegang verschaft tot een informaticasysteem of zich daarin handhaaft, wordt gestraft met gevangenisstraf van 3 maanden tot 1 jaar en met geldboete van 26 Belgische frank tot 25 000 Belgische frank of met een van deze straffen alleen.

Wanneer het misdrijf, bedoeld in het eerste lid, gepleegd wordt met bedrieglijk opzet, bedraagt de gevangenisstraf van 6 maanden tot 2 jaar.

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* de ce Code. ».

Art. 3

Il est inséré, au chapitre II, titre IX, II^e^ livre du Code pénal une nouvelle section III*ter*, contenant un article 504*quater*, rédigée comme suit :

« Section III*bis*. — Fraude informatique

Art. 504*quater*. — § 1^er^. 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, est puni 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.

§ 2. Celui qui, par la commission de l'infraction visée au § 1^er^, obtient pour soi-même ou pour autrui un avantage patrimonial frauduleux 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.

§ 3. Les peines portées par les §§ 1^er^ 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* de ce Code. ».

Art. 4

Il est inséré dans le II^e^ livre du Code pénal un nouveau titre IX*bis*, contenant les articles 550*bis* et 550*ter*, rédigé comme suit :

« Titre IX*bis*. — Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par le biais de ces systèmes

Art. 550*bis*. — § 1^er^. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de 26 francs belges à 25 000 francs belges ou d'une de ces peines.

Si l'infraction visée au premier alinéa, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.

§ 2. Hij die, met bedrieglijk opzet of met het oogmerk te schaden, zijn toegangsbevoegdheid tot een informaticasysteem overschrijdt, wordt gestraft met gevangenisstraf van 6 maanden tot 2 jaar en met geldboete van 26 Belgische frank tot 25 000 Belgische frank of met een van deze straffen alleen.

§ 3. Hij die zich in een van de gevallen van §§ 1 en 2 bevindt, en, naar aanleiding daarvan :

1° hetzij kennisneemt van gegevens die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem of deze op enige manier overneemt;

2° hetzij enig gebruik maakt van een informaticasysteem;

3° hetzij enige schade, zelfs onopzettelijk, veroorzaakt aan een informaticasysteem of aan gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen;

wordt gestraft met gevangenisstraf van 1 jaar tot 3 jaar en met geldboete van 26 Belgische frank tot 50 000 Belgische frank of met een van die straffen alleen.

§ 4. Poging tot het plegen van een van de misdrijven, bedoeld in §§ 1 en 2, wordt gestraft met de straffen gesteld op het misdrijf zelf.

§ 5. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen.

§ 6. Hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven, bedoeld in §§ 1 tot 5, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 100 Belgische frank tot 200 000 Belgische frank of een van die straffen.

§ 7. Hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen.

§ 8. De straffen gesteld in de §§ 1 tot 7 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 een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of in een van de andere artikelen van deze titel.

Art. 550*ter*. — § 1. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en

§ 2. Celui qui, avec intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de 26 francs belges à 25 000 francs belges ou d'une de ces peines.

§ 3. Celui qui se trouve dans une des situations prévues par les §§ 1er et 2 et qui, à cette occasion :

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;

2° soit fait tout usage d'un système informatique;

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;

est puni d'un emprisonnement de un à trois ans et d'une amende de 26 francs belges à 50 000 francs belges ou d'une de ces peines.

§ 4. La tentative de commettre une des infractions prévues aux §§ 1er et 2 est punie des mêmes peines que l'infraction elle-même.

§ 5. 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, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 6. Celui qui ordonne la commission d'une des infractions prévues aux §§ 1er à 5 ou qui y incite est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 100 francs belges à 200 000 francs belges ou d'une de ces peines.

§ 7. 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 fait un usage quelconque des données ainsi obtenues est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 8. Les peines portées par les §§ 1er à 7 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*, 504*quater* ou dans un des articles du présent titre.

Art. 550*ter*. — § 1er. 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, est puni d'un emprisonnement de six mois à trois ans et

met geldboete van 26 Belgische frank tot 25 000 Belgische frank of met een van die straffen alleen.

§ 2. Hij die, tengevolge van het plegen van het misdrijf bedoeld in § 1, schade berokkent aan gegevens in dit of enig ander informaticasysteem, wordt gestraft met gevangenisstraf van 6 maanden tot 5 jaar en met geldboete van 26 Belgische frank tot 75 000 Belgische frank of met een van die straffen alleen.

§ 3. 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, wordt gestraft met gevangenisstraf van 1 jaar tot 5 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen.

§ 4. 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, wordt gestraft met gevangenisstraf van 6 maanden tot 3 jaar en met geldboete van 26 Belgische frank tot 100 000 Belgische frank of met een van die straffen alleen.

§ 5. De straffen gesteld in de §§ 1 tot 4 worden verdubbeld indien een overtreding van een van die bepalingen wordt begaan binnen 5 jaar na de uitspraak van een vonnis of een arrest houdende veroordeling wegens een van die strafbare feiten of wegens een van de strafbare feiten bedoeld in de artikelen 210*bis*, 259*bis*, 314*bis*, 504*quater* of in een van de andere artikelen van deze titel.

Gegeven te Brussel, 28 oktober 1999.

ALBERT

VAN KONINGSWEGE :

De minister van Justitie,

M. VERWILGHEN

De minister van Telecommunicatie en Overheidsbedrijven en Participaties,

R. DAEMS

De minister van Economie en Wetenschappelijk Onderzoek,

R. DEMOTTE

d'une amende de 26 francs belges à 25 000 francs belges ou d'une de ces peines.

§ 2. 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, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de 26 francs belges à 75 000 francs belges ou d'une de ces peines.

§ 3. 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, est puni d'un emprisonnement de un an à cinq ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 4. 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, est puni d'un emprisonnement de six mois à trois ans et d'une amende de 26 francs belges à 100 000 francs belges ou d'une de ces peines.

§ 5. Les peines portées par les §§ 1er à 4 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*, 504*quater* ou dans un des articles du présent titre.

Donné à Bruxelles, le 28 octobre 1999.

ALBERT

PAR LE ROI :

Le ministre de la Justice,

M. VERWILGHEN

Le ministre des Télécommunications et des Entreprises et Participations publiques,

R. DAEMS

Le ministre de l'Économie et de la Recherche scientifique,

R. DEMOTTE

DOC 50 **0213/001**
DOC 50 **0214/001**

WETSONTWERP II
(Nr 214/1)

———

ALBERT II, KONING DER BELGEN

Aan allen die nu zijn en hierna wezen zullen,
ONZE GROET.

Op de voordracht van Onze minister van Justitie, Onze minister van Telecommunicatie en Overheidsbedrijven en Participaties en Onze minister van Economie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ :

Onze minister van Justitie, Onze minister van Telecommunicatie en Overheidsbedrijven en Participaties en Onze minister van Economie zijn gelast het wetsontwerp waarvan de tekst volgt, in Onze naam, aan de Wetgevende Kamers voor te leggen en bij de Kamer van Volksvertegenwoordigers in te dienen :

Artikel 1

Deze wet regelt een aangelegenheid zoals bedoeld in artikel 77 van de Grondwet.

Art. 2

In het Wetboek van Strafvordering wordt een artikel 39*bis* ingevoegd, luidend als volgt :

« Art. 39*bis*

§ 1. 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. Indien het gebruik van dergelijke dragers wegens de dringendheid of de techniciteit niet mogelijk is, wordt gebruik gemaakt van dragers, die ter beschikking staan van personen die gerechtigd zijn om het informaticasysteem te gebruiken.

§ 2. Hij wendt bovendien de passende 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.

PROJET DE LOI II
(N° 214/1)

———

ALBERT II, ROI DES BELGES

À tous, présents et à venir,
SALUT.

Sur la proposition de Notre ministre de la Justice, de Notre ministre des Télécommunications et des Entreprises et Participations publiques et de Notre ministre de l'Économie,

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

Notre ministre de la Justice, Notre ministre des Télécommunications et des Entreprises et Participations publiques et Notre ministre de l'Économie sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit :

Article 1er

La présente loi règle une matière visée à l'article 77 de la Constitution.

Art. 2

Il est inséré dans le Code d'Instruction criminelle un article 39*bis* rédigé comme suit :

« Art. 39*bis*

§ 1er. 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. Si l'utilisation de tels supports n'est pas possible en raison de l'urgence ou pour des raisons techniques, il est fait usage de supports qui sont disponibles pour des personnes autorisées à utiliser le système informatique.

§ 2. Il utilise en outre les moyens 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.

Indien hij echter van oordeel is dat 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, kan hij deze gegevens uit het informaticasysteem verwijderen.

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

§ 3. Wanneer de in § 1 vermelde maatregel niet mogelijk is om technische redenen of omwille van de omvang van de gegevens, wendt hij de passende 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.

§ 4. 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.

§ 5. De procureur des Konings wendt de passende middelen aan om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen. Dezelfde middelen worden aangewend voor de bewaring hiervan op de griffie.

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

§ 6. Onverminderd de specifieke bepalingen van dit artikel, zijn de regels inzake inbeslagneming van toepassing op het kopiëren, ontoegankelijk maken en verwijderen van gegevens. ».

Art. 3

In hetzelfde Wetboek wordt een artikel 88*ter* ingevoegd, luidend als volgt :

« Art. 88*ter*. — § 1. Wanneer de onderzoeksrechter een zoeking verricht in een informaticasysteem, hetzij in het kader van een huiszoeking, hetzij anderszins, kan hij deze zoeking uitbreiden naar een informaticasysteem dat zich op een andere plaats bevindt dan daar waar deze zoeking plaatsvindt, indien :

— hij van oordeel is dat deze uitbreiding noodzakelijk is voor de waarheidsvinding ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking; en

— er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan, of

— hij van oordeel is dat andere maatregelen disproportioneel zijn.

S'il estime que 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, il peut retirer ces données 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.

§ 3. Lorsque la mesure prévue au § 1er n'est pas possible, pour des raisons techniques ou à cause du volume des données, le procureur du Roi utilise les moyens 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.

§ 4. 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.

§ 5. Le procureur du Roi utilise les moyens appropriés pour garantir l'intégrité et la confidentialité de ces données. Les mêmes moyens 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.

§ 6. Sans préjudice des dispositions spécifiques de cet article, les règles relatives à la saisie sont applicables aux mesures consistant à copier, rendre inaccessibles et retirer des données. ».

Art. 3

Il est inséré dans le même Code un article 88*ter* rédigé comme suit :

« Art. 88*ter*. — § 1er. Lorsque le juge d'instruction procède à une recherche dans un système informatique, soit dans le cadre d'une perquisition, soit autrement, il peut étendre cette recherche vers un système informatique qui se trouve dans un autre lieu que celui où la recherche est effectuée, si :

— il estime que cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et

— il existe un risque que, sans cette extension, des éléments de preuve soient perdus ou

— il estime que d'autres mesures seraient disproportionnées.

§ 2. De uitbreiding van de zoeking in een informaticasysteem mag zich niet verder uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, toegang hebben.

§ 3. Inzake de door uitbreiding van de zoeking in een informaticasysteem aangetroffen gegevens, die nuttig zijn voor dezelfde doeleinden als de inbeslagneming, wordt gehandeld zoals bepaald in artikel 39*bis*. De onderzoeksrechter brengt de verantwoordelijke van dit informaticasysteem op de hoogte, tenzij diens identiteit of woonplaats redelijkerwijze niet achterhaald kan worden.

Wanneer blijkt dat deze gegevens zich niet op het grondgebied van het Rijk bevinden, worden deze enkel gekopieerd. In dat geval deelt de onderzoeksrechter dit, via het openbaar ministerie, onverwijld mee aan het ministerie van Justitie, dat de bevoegde overheid van de betrokken Staat hiervan op de hoogte brengt, indien deze redelijkerwijze kan worden bepaald.

§ 4. Artikel 89*bis* is van toepassing op de uitbreiding van de zoeking in een informaticasysteem. ».

Art. 4

In hetzelfde Wetboek wordt een artikel 88*quater* ingevoegd, luidend als volgt :

« Art. 88*quater*. — § 1. De onderzoeksrechter, evenals in zijn opdracht een officier van gerechtelijke politie, hulpofficier van de procureur des Konings, kan personen waarvan hij vermoedt dat ze een bijzondere kennis hebben van een informaticasysteem dat het voorwerp uitmaakt van onderzoek of van diensten om gegevens, die worden opgeslagen, verwerkt of overgedragen via een informaticasysteem, te beveiligen of te versleutelen, bevelen inlichtingen te verlenen over de werking ervan en over de wijze om er toegang toe te verkrijgen of in een verstaanbare vorm toegang te verkrijgen tot de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen.

§ 2. Indien nodig, kan de onderzoeksrechter iedere relevante persoon bevelen om zelf het informaticasysteem te bedienen of de pertinente gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, naargelang het geval, te zoeken, toegankelijk te maken, te kopiëren, ontoegankelijk te maken of te verwijderen, in de door hem gevorderde vorm. Deze personen zijn verplicht hieraan gevolg te geven, voorzover dit in hun mogelijkheden ligt.

Het bevel om zelf de pertinente gegevens te zoeken kan niet worden gegeven aan de verdachte en aan de personen bedoeld in artikel 156.

§ 3. Degene die weigert de in §§ 1 en 2 gevorderde medewerking te verlenen of de zoeking in een informaticasysteem hindert, wordt gestraft met gevan-

§ 2. L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont accès.

§ 3. En ce qui concerne les données rassemblées par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39*bis* s'appliquent. Le juge d'instruction informe le responsable du système informatique, sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire belge, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction, par l'intermédiaire du ministère public, communique immédiatement cette information au ministère de la justice, qui en informe les autorités compétentes de l'État concerné, si celui-ci peut raisonnablement être déterminé.

§ 4. L'article 89*bis* est applicable à l'extension de la recherche dans un système informatique. ».

Art. 4

Il est inséré dans le Code d'Instruction criminelle un article 88*quater* rédigé comme suit :

« Art. 88*quater*. — § 1er. Le juge d'instruction, ainsi qu'un officier de police judiciaire auxiliaire du procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des 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'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible.

§ 2. Si nécessaire, le juge d'instruction peut ordonner à toute personne pertinente de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure où c'est dans leurs possibilités.

L'ordonnance de rechercher soi-même les données pertinentes ne peut être prise à l'égard de l'inculpé et à l'égard des personnes visées à l'article 156.

§ 3. Celui qui refuse de fournir la collaboration ordonnée conformément aux §§ 1er et 2 ou qui fait obstacle à la recherche dans le système informatique, est

genisstraf van 6 maanden tot één jaar en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met een van die straffen alleen.

§ 4. Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek.

§ 5. De Staat is burgerlijk aansprakelijk voor de schade die onopzettelijk door de gevorderde personen aan een informaticasysteem of de gegevens, die door middel daarvan worden opgeslagen, verwerkt of overgedragen, wordt veroorzaakt. ».

puni d'un emprisonnement de six mois à un an et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

§ 4. Toute personne qui, du chef de sa fonction, a connaisance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 5. L'État est civilement responsable pour le dommage causé par les personnes requises de façon non intentionnelle à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système. ».

Art. 5

In artikel 89 van hetzelfde Wetboek worden de woorden « en 39, » vervangen door « , 39 en 39*bis*, ».

Art. 5

À l'article 89 du même Code, les mots « et 39 » sont remplacés par «, 39 et 39*bis* ».

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 een 1°*bis*, *ter* en *quater*, een 10°*bis* en een 13°*bis* ingevoegd, luidend als volgt :

« 1°*bis*. Artikel 210*bis* van hetzelfde Wetboek; »;

« 1°*ter*. Artikel 259*bis* van hetzelfde Wetboek; »;

« 1°*quater*. Artikel 314*bis* van hetzelfde Wetboek; »;

« 10°*bis*. Artikel 504*quater* van hetzelfde Wetboek; »;

« 13°*bis*. Artikelen 550*bis* en 550t*er* van hetzelfde Wetboek; ».

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 juni 1998, sont insérés un 1°*bis*, *ter* et *quater*, un 10°*bis* et un 13°*bis*, rédigés comme suit :

« 1° *bis*. L'article 210*bis* du même Code; »;

« 1°*ter*. L'article 259*bis* du même Code; »;

« 1°*quater*. L'article 314*bis* du même Code; »;

« 10°*bis*. L'article 504*quater* du même Code; »;

« 13°*bis*. Les articles 550*bis* et 550*ter* du même Code. ».

Art. 7

In artikel 90*quater* van hetzelfde Wetboek wordt een § 4 toegevoegd, luidend als volgt :

« § 4. 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 inlichtingen te verlenen over de werking ervan en over de wijze om in een verstaanbare vorm 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.

Art. 7

L'article 90*quater* du même Code est complété par un § 4, rédigé comme suit :

« § 4. 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.

Degene die weigert de in de vorige leden gevorderde medewerking te verlenen, wordt gestraft met gevangenisstraf van 6 maanden tot een jaar en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met een van die straffen alleen.

Iedere persoon die uit hoofde van zijn bediening kennis krijgt van de maatregel of daaraan zijn medewerking verleent, is tot geheimhouding verplicht. Iedere schending van het geheim wordt gestraft overeenkomstig artikel 458 van het Strafwetboek. ».

Art. 8

In artikel 90*septies* van hetzelfde Wetboek wordt tussen het vierde en het laatste lid een nieuw lid ingevoegd, luidend als volgt :

« De passende middelen kunnen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen of 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 deze middelen en het ogenblik waarop deze middelen de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en vierde lid, vervangen. ».

Art. 9

In artikel 109*ter*, E, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de wet van 21 december 1994, hernummerd bij de wet van 19 december 1997 en gewijzigd bij de wet van 10 juni 1998, worden de volgende wijzigingen aangebracht :

— 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, in de gevallen en gedurende een termijn door de Koning te bepalen, te bewaren, te bepalen bij een in Ministerraad overlegd besluit en op voorstel van de minister van Justitie en de minister van Telecommunicatie en Overheidsbedrijven en Participaties. »;

— 2° artikel 109*ter*, E, wordt als volgt aangevuld :

« § 3. Hij die de verplichtingen door de Koning krachtens de vorige paragrafen bepaald, niet nakomt, wordt gestraft met gevangenisstraf van 3 tot 6 maanden en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met een van die straffen alleen.

Celui qui refuse de fournir la collaboration requise par les alinéas précédents, est puni d'un emprisonnement de six mois à un an et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal. ».

Art. 8

À l'article 90*septies* du même Code, il est inséré entre le quatrième et le dernier alinéa un alinéa nouveau rédigé comme suit :

« Les moyens appropriés peuvent être utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée ou 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 ces moyens et le moment où ces moyens remplacent la conservation sous pli scellé ou le registre spécial prévus aux troisième et quatrième alinéas. ».

Art. 9

À l'article 109*ter*, E, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, inséré par la loi du 21 décembre 1994, renuméroté par la loi du 19 décembre 1997 et modifié par la loi du 10 juin 1998, sont apportées les modifications suivantes :

— 1° le premier alinéa du § 2 est complété comme suit :

« , 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, les données d'appel de moyens de télécommunication et les données d'identification d'utilisateurs de services de télécommunication à déterminer par le Roi, par arrêté délibéré en Conseil des ministres et sur proposition du ministre de la Justice et du ministre des Télécommunications et des Entreprises et Participations publiques. »;

— 2° l'article 109*ter*, E, est complété comme suit :

« § 3. Celui qui ne respecte pas les obligations prévues par le Roi en vertu des paragraphes précédents est puni d'un emprisonnement de trois à six mois et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

§ 4. De Koning bepaalt bij in Ministerraad overlegd besluit en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer de modaliteiten en de middelen om de vertrouwelijkheid en de integriteit van de oproep- en identificatiegegevens bedoeld in § 2 te waarborgen. ».

Gegeven te Brussel, 28 oktober 1999.

ALBERT

VAN KONINGSWEGE :

De minister van Justitie,

M. VERWILGHEN

De minister van Telecommunicatie en Overheidsbedrijven en Participaties,

R. DAEMS

De minister van Economie en Wetenschappelijk Onderzoek,

R. DEMOTTE

§ 4. Le Roi par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée prévoit les modalités et les moyens appropriés pour garantir la confidentialité et l'intégrité des données d'appels et d'identification visées au § 2. ».

Donné à Bruxelles, le 28 octobre 1999.

ALBERT

PAR LE ROI :

Le ministre de la Justice,

M. VERWILGHEN

Le ministre des Télécommunications et des Entreprises et Participations publiques,

R. DAEMS

Le ministre de l'Économie et de la Recherche scientifique,

R. DEMOTTE

BASISTEKST

Artikel 89 van het Wetboek van Strafvordering :

« De bepalingen van de artikelen 35, 35*bis*, 36, 37, 38, en 39, aangaande de inbeslagneming van de voorwerpen die de procureur des Konings in de gevallen van ontdekking op heterdaad mag opsporen, gelden ook voor de onderzoeksrechter. ».

Artikel 90*ter*, § 2, van het Wetboek van Strafvordering :

« § 2. De strafbare feiten die een bewakingsmaatregel kunnen wettigen, zijn die welke bedoeld zijn in :

… »

Artikel 90*septies* van het Wetboek van Strafvordering :

De communicatie of telecommunicatie opgevangen als gevolg van de maatregelen die zijn genomen met toepassing van de artikelen 90*ter*, 90*quater* en 90*quinquies*, wordt opgenomen. Het voorwerp van de maatregel en de dagen en uren waarop deze is uitgevoerd, worden opgenomen bij het begin en op het einde van iedere opname die erop betrekking heeft. Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in het voorgaande lid door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van de overschrijving van de van belang geachte communicaties en telecommunicaties van de opname, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd, wat betreft de niet van belang geachte communicaties en telecommunicaties. De voor de uitvoering van de maatregel aangewezen officier van gerechtelijke politie gaat over tot deze vernietiging en vermeldt dit in een proces-verbaal.

De opnamen worden samen met de overschrijving van de van belang geachte communicaties en telecommunicaties, de eventuele vertaling ervan, de vermelding van de aangehaalde onderwerpen en van de identifi-

BASISTEKST AANGEPAST AAN HET ONTWERP (1)

Artikel 89 van het Wetboek van Strafvordering :

« De bepalingen van de artikelen 35, 35*bis*, 36, 37, 38, 39 *en 39*bis, aangaande de inbeslagneming van de voorwerpen die de procureur des Konings in de gevallen van ontdekking op heterdaad mag opsporen, gelden ook voor de onderzoeksrechter. ».

Artikel 90*ter*, § 2, van het Wetboek van Strafvordering :

« § 2. De strafbare feiten die een bewakingsmaatregel kunnen wettigen, zijn die welke bedoeld zijn in :

*1°*bis. *Artikel 210*bis *van hetzelfde Wetboek;*

*1°*ter. *Artikel 259*bis *van hetzelfde Wetboek;*

*1°*quater. *Artikel 314*bis *van hetzelfde Wetboek;*

*10°*bis. *Artikel 504*quater *van hetzelfde Wetboek;*

*13°*bis. *Artikelen 550*bis *en 550*ter *van hetzelfde Wetboek; ».*

Artikel 90*septies* van het Wetboek van Strafvordering :

De communicatie of telecommunicatie opgevangen als gevolg van de maatregelen die zijn genomen met toepassing van de artikelen 90*ter*, 90*quater* en 90*quinquies*, wordt opgenomen. Het voorwerp van de maatregel en de dagen en uren waarop deze is uitgevoerd, worden opgenomen bij het begin en op het einde van iedere opname die erop betrekking heeft. Iedere aantekening in het kader van de tenuitvoerlegging van de maatregelen bedoeld in het voorgaande lid door de daartoe aangewezen personen, die niet is opgetekend in een proces-verbaal, wordt vernietigd, met uitzondering van de overschrijving van de van belang geachte communicaties en telecommunicaties van de opname, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties. De voor de uitvoering van de maatregel aangewezen officier van gerechtelijke politie gaat over tot deze vernietiging en vermeldt dit in een proces-verbaal.

De opnamen worden samen met de overschrijving van de van belang geachte communicaties en telecommunicaties, de eventuele vertaling ervan, de vermelding van de aangehaalde onderwerpen en van de identifi-

(1) Volledig nieuwe bepalingen werden niet opgenomen.
Wijzigingen in bestaande bepalingen werden opgenomen, in de mate dat dit nodig is om de wijzigingen goed te kunnen verstaan.

TEXTE DE BASE

Article 89 du Code d'Instruction criminelle :

« Les dispositions des articles 35, 35*bis*, 36, 37, 38 et 39, concernant la saisie des objets dont la perquisition peut être faite par le procureur du Roi, dans le cas de flagrant délit, sont communes au juge d'instruction. ».

Article 90*ter*, § 2, du Code d'Instruction criminelle :

« Les infractions pouvant justifier une mesure de surveillance sont celles qui sont visées : … ».

Article 90*septies* du Code d'Instruction criminelle :

Les communications ou télécommunications recueillies grâce aux mesures prises en application des articles 90*ter*, 90*quater* et 90*quinquies*, sont enregistrées. L'objet de la mesure ainsi que les jours et heures auxquels celle-ci a été exécutée sont enregistrés au début et à la fin de chaque enregistrement qui s'y rapporte. À l'exception de la transcription de l'enregistrement des communications et télécommunications estimées pertinentes avec traduction éventuelle et de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, toute note prise dans le cadre de l'exécution des mesures visées à l'alinéa précédent par les personnes commises à cette fin qui n'est pas consignée dans un procès-verbal, est détruite. L'officier de police judiciaire commis pour l'exécution de la mesure procède à cette destruction et en fait mention dans un procès-verbal.

Les enregistrements accompagnés de la transcription des communications et télécommunications estimées pertinentes avec traduction éventuelle, de l'indication des sujets abordés et des données d'identifica-

TEXTE DE BASE ADAPTÉ AU PROJET (1)

Article 89 du Code d'Instruction criminelle :

« Les dispositions des articles 35, 35*bis*, 36, 37, 38, 39 *et 39*bis, concernant la saisie des objets dont la perquisition peut être faite par le procureur du Roi, dans le cas de flagrant délit, sont communes au juge d'instruction. ».

Article 90*ter*, § 2, du Code d'Instruction criminelle :

« Les infractions pouvant justifier une mesure de surveillance sont celles qui sont visées : …
1° bis*. L'article 210*bis *du même Code;*
*1°*ter*. L'article 259*bis *du même Code;*
*1°*quater*. L'article 314*bis *du même Code;*
*10°*bis*. L'article 504*quater *du même Code;*
*13°*bis*. Les articles 550*bis *et 550*ter *du même Code. »*

Article 90*septies* du Code d'Instruction criminelle :

Les communications ou télécommunications recueillies grâce aux mesures prises en application des articles 90*ter*, 90*quater* et 90*quinquies*, sont enregistrées. L'objet de la mesure ainsi que les jours et heures auxquels celle-ci a été exécutée sont enregistrés au début et à la fin de chaque enregistrement qui s'y rapporte. À l'exception de la transcription de l'enregistrement des communications et télécommunications estimées pertinentes avec traduction éventuelle et de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, toute note prise dans le cadre de l'exécution des mesures visées à l'alinéa précédent par les personnes commises à cette fin qui n'est pas consignée dans un procès-verbal, est détruite. L'officier de police judiciaire commis pour l'exécution de la mesure procède à cette destruction et en fait mention dans un procès-verbal.

Les enregistrements accompagnés de la transcription des communications et télécommunications estimées pertinentes avec traduction éventuelle, de l'indication des sujets abordés et des données d'identifica-

---

(1) Les dispositions entièrement nouvelles n'ont pas été reprises.
Des modifications dans des dispositions existentes ont été reprises, dans la mesure où cela est nécessaire pour bien comprendre les modifications.

catiegegevens van de telecommunicatiemiddelen van waaruit en waarnaar opgeroepen werd, wat betreft de niet van belang geachte communicaties en telecommunicaties, en van de afschriften van de processen-verbaal onder verzegelde omslag ter griffie bewaard.

De griffier vermeldt in een per dag bijgehouden bijzonder register :

1° het neerleggen van iedere opname, alsook van de overschrijving van de van belang geachte communicaties en telecommunicaties, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd, wat betreft de niet van belang geachte communicaties en telecommunicaties;

2° het neerleggen van ieder afschrift van proces-verbaal;

3° de dag van de neerlegging ervan;

4° de naam van de onderzoeksrechter die de maatregel heeft bevolen of bevestigd en het voorwerp ervan;

5° de dag waarop de zegels zijn verbroken en in voorkomend geval opnieuw zijn gelegd;

6° de datum van de kennisname van de opname, de overschrijving van de van belang geachte communicaties en telecommunicaties, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd, wat betreft de niet van belang geachte communicaties en telecommunicaties of van de afschriften van de processen-verbaal, alsook de naam van de personen die er kennis van genomen hebben;

7° iedere andere gebeurtenis die erop betrekking heeft.

De rechter spreekt zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman, om het geheel of gedeelten van de ter griffie neergelegde opnamen en overschrijvingen die niet zijn opgetekend in een proces-verbaal, te raadplegen, en over hun verzoek tot overschrijving van bijkomende delen van de opnamen.

Het verzoek dat gericht is tot de onderzoeksrechter, wordt behandeld overeenkomstig artikel 61*quinquies*. De onderzoeksrechter kan dit verzoek bovendien afwij-

catiegegevens van de telecommunicatiemiddelen van waaruit en waarnaar opgeroepen werd, wat betreft de niet van belang geachte communicaties en telecommunicaties, en van de afschriften van de processen-verbaal onder verzegelde omslag ter griffie bewaard.

De griffier vermeldt in een per dag bijgehouden bijzonder register :

1° het neerleggen van iedere opname, alsook van de overschrijving van de van belang geachte communicaties en telecommunicaties, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd, wat betreft de niet van belang geachte communicaties en telecommunicaties;

2° het neerleggen van ieder afschrift van proces-verbaal;

3° de dag van de neerlegging ervan;

4° de naam van de onderzoeksrechter die de maatregel heeft bevolen of bevestigd en het voorwerp ervan;

5° de dag waarop de zegels zijn verbroken en in voorkomend geval opnieuw zijn gelegd;

6° de datum van de kennisname van de opname, de overschrijving van de van belang geachte communicaties en telecommunicaties, de eventuele vertaling ervan en de vermelding van de aangehaalde onderwerpen en van de identificatiegegevens van de telecommunicatiemiddelen van waaruit of waarnaar opgeroepen werd wat betreft de niet van belang geachte communicaties en telecommunicaties of van de afschriften van de processen-verbaal, alsook de naam van de personen die er kennis van genomen hebben;

7° iedere andere gebeurtenis die erop betrekking heeft.

De passende middelen kunnen worden aangewend om de integriteit en de vertrouwelijkheid van de opgenomen communicatie of telecommunicatie te waarborgen of 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 deze middelen en het ogenblik waarop deze middelen de bewaring onder verzegelde omslag of het bijzonder register, bedoeld in het derde en vierde lid, vervangen.

De rechter spreekt zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman, om het geheel of gedeelten van de ter griffie neergelegde opnamen en overschrijvingen die niet zijn opgetekend in een proces-verbaal, te raadplegen, en over hun verzoek tot overschrijving van bijkomende delen van de opnamen.

Het verzoek dat gericht is tot de onderzoeksrechter, wordt behandeld overeenkomstig artikel 61*quinquies*. De onderzoeksrechter kan dit verzoek bovendien afwij-

tion des moyens de télécommunications à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, et des copies des procès-verbaux sont conservés au greffe sous pli scellé.

Le greffier mentionne dans un registre spécial tenu journellement :

1° le dépôt de chaque enregistrement, ainsi que de la transcription des communications et télécommunications estimées pertinentes avec traduction éventuelle et de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes;

2° le dépôt de chaque copie de procès-verbal;

3° le jour de leur dépôt;

4° le nom du juge d'instruction qui a ordonné ou confirmé la mesure et l'objet de celle-ci;

5° le jour où les scellés sont ouverts et éventuellement réapposés;

6° la date de prise de connaissance de l'enregistrement, de la transcription des communications et télécommunications estimées pertinentes avec traduction éventuelle et l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, ou des copies des procès-verbaux, ainsi que le nom des personnes qui en ont pris connaissance;

7° tous les autres événements qui s'y rapportent.

Le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leurs conseils, de consulter la totalité ou des parties des enregistrements et des transcriptions déposés au greffe qui ne sont pas consignées dans un procès-verbal, et sur leur demande de transcrire des parties additionnelles des enregistrements.

La demande qui est adressée au juge d'instruction est traité conformément à l'article 61*quinquies*. Le juge d'instruction peut en outre rejeter cette demande pour

tion des moyens de télécommunications à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, et des copies des procès-verbaux sont conservés au greffe sous pli scellé.

Le greffier mentionne dans un registre spécial tenu journellement :

1° le dépôt de chaque enregistrement, ainsi que de la transcription des communications et télécommunications estimées pertinentes avec traduction éventuelle et de l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes;

2° le dépôt de chaque copie de procès-verbal;

3° le jour de leur dépôt;

4° le nom du juge d'instruction qui a ordonné ou confirmé la mesure et l'objet de celle-ci;

5° le jour où les scellés sont ouverts et éventuellement réapposés;

6° la date de prise de connaissance de l'enregistrement, de la transcription des communications et télécommunications estimées pertinentes avec traduction éventuelle et l'indication des sujets abordés et des données d'identification des moyens de télécommunication à partir desquels ou vers lesquels il a été appelé en ce qui concerne les communications et télécommunications estimées non pertinentes, ou des copies des procès-verbaux, ainsi que le nom des personnes qui en ont pris connaissance;

7° tous les autres événements qui s'y rapportent.

Les moyens appropriés peuvent être utilisés pour garantir l'intégrité et la confidentialité de la communication ou de la télécommunication enregistrée ou 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 ces moyens et le moment où ces moyens remplacent la conservation sous pli scellé ou le registre spécial prévus aux troisième et quatrième alinéas.

Le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leurs conseils, de consulter la totalité ou des parties des enregistrements et des transcriptions déposés au greffe qui ne sont pas consignées dans un procès-verbal, et sur leur demande de transcrire des parties additionnelles des enregistrements.

La demande qui est adressée au juge d'instruction est traité conformément à l'article 61*quinquies*. Le juge d'instruction peut en outre rejeter cette demande pour

zen om redenen die verband houden met de bescherming van andere rechten of belangen van personen.

Onverminderd hetgeen in de vorige leden is bepaald, spreekt de rechter zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman om de gedeelten van de ter griffie neergelegde opnamen van privé-communicatie of -telecommunicatie waaraan de betrokkene heeft deelgenomen en die niet zijn overgeschreven en opgetekend in een proces-verbaal, te raadplegen, en over hun verzoek tot overschrijving van bijkomende delen van deze opnamen.

Artikel 109*ter* E van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven :

« § 1. …

§ 2. De Koning bepaalt, na het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer te hebben ingewonnen, bij een in Ministerraad overlegd besluit, de technische middelen 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 onder de voorwaarden bepaald door de artikelen 88*bis* en 90*ter* tot 90*decies* van het Wetboek van Strafvordering, mogelijk te maken.

Hij bepaalt tevens de grootte van de bijdrage in de investerings-, exploitatie- en onderhoudskosten van deze middelen die ten laste is van de operatoren van telecommunicatienetwerken en van de verstrekkers van telecommunicatiediensten. ».

zen om redenen die verband houden met de bescherming van andere rechten of belangen van personen.

Onverminderd hetgeen in de vorige leden is bepaald, spreekt de rechter zich uit over het verzoek van de inverdenkinggestelde, de beklaagde, de burgerlijke partij of hun raadsman om de gedeelten van de ter griffie neergelegde opnamen van privé-communicatie of -telecommunicatie waaraan de betrokkene heeft deelgenomen en die niet zijn overgeschreven en opgetekend in een proces-verbaal, te raadplegen, en over hun verzoek tot overschrijving van bijkomende delen van deze opnamen.

Artikel 109*ter* E van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven :

« § 1. …

§ 2. De Koning bepaalt, na het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer te hebben ingewonnen, bij een in Ministerraad overlegd besluit, de technische middelen 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 onder de voorwaarden bepaald door de artikelen 88*bis* en 90*ter* tot 90*decies* van het Wetboek van Strafvordering, mogelijk te maken, *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, te bepalen bij een in Ministerraad overlegd besluit en op voorstel van de minister van Justitie en de minister van Telecommunicatie en Overheidsbedrijven en Participaties.*

Hij bepaalt tevens de grootte van de bijdrage in de investerings-, exploitatie- en onderhoudskosten van deze middelen die ten laste is van de operatoren van telecommunicatienetwerken en van de verstrekkers van telecommunicatiediensten.

§ 3. Hij die de verplichtingen door de Koning krachtens de vorige paragrafen bepaald, niet nakomt, wordt gestraft met gevangenisstraf van 3 tot 6 maanden en met geldboete van 26 Belgische frank tot 20 000 Belgische frank of met één van die straffen alleen.

§ 4. De Koning bepaalt bij in Ministerraad overlegd besluit en na advies van de Commissie voor de bescher-

des raisons liées à la protection d'autres droits ou intérêts des personnes.

Sans préjudice des alinéas précédents, le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leurs conseils de consulter les parties des enregistrements déposés au greffe de communications ou de télécommunications privées auxquelles la personne concernée a participé et qui ne sont pas transcrites et consignées dans un procès-verbal, et sur leur demande de transcrire des parties additionnelles de ces enregistrements.

Article 109*ter* E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques :

« § 1. …

§ 2. Le Roi fixe, après avoir recueilli l'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 de télécommunication et les fournisseurs de services de télécommunications doivent permettre, le cas échéant conjointement, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées dans les conditions prévues par les articles 88*bis* et 90*ter* à 90*decies* du Code d'Instruction criminelle.

Il détermine également la mesure de la contribution dans les frais d'investissement, d'exploitation et d'entretien de ces moyens, qui est à la charge des opérateurs de réseaux de télécommunication et des fournisseurs de services de télécommunication. ».

des raisons liées à la protection d'autres droits ou intérêts des personnes.

Sans préjudice des alinéas précédents, le juge se prononce sur la demande de l'inculpé, du prévenu, de la partie civile ou de leurs conseils de consulter les parties des enregistrements déposés au greffe de communications ou de télécommunications privées auxquelles la personne concernée a participé et qui ne sont pas transcrites et consignées dans un procès-verbal, et sur leur demande de transcrire des parties additionnelles de ces enregistrements.

Article 109*ter* E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques :

« § 1er. …

§ 2. Le Roi fixe, après avoir recueilli l'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 de télécommunication et les fournisseurs de services de télécommunications doivent permettre, le cas échéant conjointement, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des télécommunications privées dans les conditions prévues par les articles 88*bis* et 90*ter* à 90*decies* du Code d'Instruction criminelle*, 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, les données d'appel de moyens de télécommunication et les données d'identification d'utilisateurs de services de télécommunication à déterminer par le Roi, par arrêté délibéré en Conseil des ministres et sur proposition du ministre de la Justice et du ministre des Télécommunications et des Entreprises et Participations publiques.*

Il détermine également la mesure de la contribution dans les frais d'investissement, d'exploitation et d'entretien de ces moyens, qui est à la charge des opérateurs de réseaux de télécommunication et des fournisseurs de services de télécommunication.

§ 3. Celui qui ne respecte pas les obligations prévues par le Roi en vertu des paragraphes précédents est puni d'un emprisonnement de trois à six mois et d'une amende de 26 francs belges à 20 000 francs belges ou d'une de ces peines.

§ 4. Le Roi par arrêté délibéré en Conseil des ministres et après avis de la Commission pour la protection

ming van de persoonlijke levenssfeer de modaliteiten en de middelen om de vertrouwelijkheid en de integriteit van de oproep- en identificatiegegevens bedoeld in § 2 te waarborgen. ».

———————

de la vie privée prévoit les modalités et les moyens appropriés pour garantir la confidentialité et l'intégrité des données d'appels et d'identification visées au § 2. ».

Drukkerij-Imprimerie SCHAUBROECK — 9810 NAZARETH