462 - 1 (1988-1989)

SENAT DE BELGIQUE

SESSION DE 1988-1989

26 OCTOBRE 1988

Proposition de loi complétant le Code pénal en vue de réprimer les abus en matière d'informatique et l'écoute de conversations

(Déposée par M. Verhaegen)

DEVELOPPEMENTS

Les développements récents et ceux qui sont en cours dans le secteur de la technologie informatique ont nécessairement une incidence sur le droit.

A preuve, en premier lieu, l'inquiétude qui se manifeste au sujet de la protection de la vie privée dans le cadre du traitement automatique des données personnelles. Une réglementation en la matière à déjà été insérée dans plusieurs législations étrangères. Pour combler la lacune que présente la législation belge dans ce domaine, nous avons déposé une proposition de loi relative à la protection de la vie privée dans le domaine de l'informatique. Le droit pénal n'y joue qu'un rôle marginal. Elle met l'accent sur les droits des personnes au sujet desquelles des données sont enregistrées, les règles relatives au fonctionnement des banques de données et la création d'un Office pour la protection de la vie privée dans le domaine de l'informatique.

La technologie informatique soulève toutefois d'autres problèmes que celui de la protection de la vie privée.

Depuis peu, le phénomène de la « criminalité informatique » est devenu à son tour un sujet brûlant.

R. A 14550

BELGISCHE SENAAT

ZITTING 1988-1989

26 OKTOBER 1988

Voorstel van wet tot aanvulling van het Strafwetboek ter bestraffing van computermisbruik en het afluisteren van gesprekken

(Ingediend door de heer Verhaegen)

TOELICHTING

De recente en aan de gang zijnde ontwikkelingen op het vlak van de informatietechnologie hebben noodzakelijkerwijze ook hun weerslag op het recht.

Dit komt vooreerst tot uitdrukking in de ongerustheid over de bescherming van de privacy bij de geautomatiseerde verwerking van persoonsgegevens. In verschillende buitenlandse wetgevingen werd daaromtrent reeds een regeling tot stand gebracht. Teneinde de leemte in Belgische wetgeving ter zake op te vangen, hebben wij een wetsvoorstel ingediend « betreffende de bescherming van de persoonlijke levenssfeer inzake de informatica ». In dit wetsvoorstel speelt het strafrecht slechts een marginale rol. De nadruk ligt in dit laatste wetsvoorstel op de rechten van de geregistreerden, de regels inzake de werking van databanken en de oprichting van de « Dienst tot bescherming van de persoonlijke levenssfeer in verband met de informatica ».

De informatietechnologie stelt evenwel niet alleen het probleem van de bescherming van de privacy.

De jongste tijd staat ook het verschijnsel van de « computercriminaliteit » volop in de actualiteit.

R. A 14550

Par abus informatique, il faut entendre tout comportement dommageable au niveau du stockage, du traitement ou de l'échange de données au moyen d'appareils automatisés (*cf.* le rapport de la *Nederlandse Commissie Computercriminaliteit, Informatietechniek en Strafrecht,* Imprimerie nationale, Ministère de la Justice, La Haye, 1987; et H.W.K. Kaspersen, *Computermisbruik,* in : *Computermisdaad en strafrecht,* Kluwer rechtswetenschappen, Anvers-Deventer, 1986).

La question cruciale est celle de savoir si le droit pénal, tel qu'il s'applique actuellement, peut remplir valablement sa fonction face aux comportements dommageables dans l'usage des systèmes de traitement de données.

Les abus informatiques continueront à se multiplier à la faveur de l'évolution en cours, qui se traduit par :

1° une facilité d'utilisation sans cesse croissante des matériels et logiciels informatiques et un analphabétisme informatique décroissant;

2° une utilisation croissante de l'électronique pour les paiements;

3° la combinaison des techniques de la télécommunication et de l'informatique dans la « télématique » (*cf.* G.P.V. Vandenberghe, *Computermisbruik, beveiliging en strafrecht,* in : *Computermisdaad en strafrecht,* Kluwer rechtswetenschappen, Anvers-Deventer, 1986).

La lutte contre cette forme nouvelle de criminalité est devenue une priorité dans tous les pays industrialisés. Dans le cadre de l'O.C.D.E., un groupe de travail a présenté un rapport sous le titre « La fraude liée à l'informatique : analyse des politiques juridiques » (Paris, 1986). Le rapport de l'O.C.D.E. recommande que les Etats membres criminalisent au moins cinq comportements :

a) l'entrée, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques effectués sciemment dans l'intention de commettre un transfert illégal de fonds ou d'une autre « chose de valeur »;

b) l'entrée, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques effectués sciemment dans l'intention de commettre un faux;

c) l'entrée, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques effectués sciemment dans l'intention d'entraver le fonctionnement du système informatique et/ou de télécommunications;

d) la violation du droit exclusif du détenteur d'un programme informatique protégé avec l'intention de

Onder computermisbruik dient te worden verstaan : schadelijk gedrag met betrekking tot de opslag, verwerking of uitwisseling van gegevens door geautomatiseerde apparatuur (*cf.* het rapport van de Nederlandse Commissie Computercriminaliteit, Informatietechniek en Strafrecht, Staatsuitgeverij, Ministerie van Justitie, 's Gravenhage, 1987; en H.W.K. Kaspersen, Computermisbruik, in : *Computermisdaad en strafrecht*, Kluwer rechtswetenschappen, Antwerpen-Deventer, 1986).

De cruciale vraag is of het strafrecht, zoals het nu geldt, zijn functie zinvol kan vervullen t.a.v. schadelijke gedragingen waarbij gegevensverwerkende systemen betrokken zijn.

De volgende ontwikkelingen zullen nog een toename van het computermisbruik tot gevolg hebben :

1° de steeds grotere gebruiksvriendelijkheid van computer-hardware en -software enerzijds, de daling in het computer-analfabetisme anderzijds;

2° het toenemend gebruik van elektronisch geld;

3° het samengaan van de telecommunicatie en de informatica in de « telematica » (*cf.* G.P.V. Vandenberghe, Computermisbruik, beveiliging en strafrecht, in : *Computermisdaad en strafrecht*, Kluwer rechtswetenschappen, Antwerpen-Deventer, 1986).

In alle geïndustrialiseerde landen treedt de vraag naar de aanpak van deze nieuwe vorm van criminaliteit op de voorgrond. Binnen de O.E.S.O. heeft een werkgroep een rapport uitgebracht onder de titel « Computer-related crime : analysis of legal policy » (Parijs, 1986). Het rapport van de O.E.S.O. stelt dat in iedere lid-staat er tenminste vijf gedragingen strafbaar moeten zijn :

a) het opzettelijk inbrengen, wijzigen, wissen of uit functie plaatsen van computergegevens of -programma's met het oogmerk om een onrechtmatige overdracht van gelden of van een andere zaak van waarde te bewerkstelligen;

b) het opzettelijk inbrengen, wijzigen, wissen of uit functie plaatsen van computergegevens of -programma's met het oogmerk om te vervalsen;

c) het opzettelijk inbrengen, wijzigen, wissen of uit functie plaatsen van computergegevens of -programma's met het oogmerk om het functioneren van een computer- of telecommunicatiesysteem te belemmeren;

d) de inbreuk op het exclusieve recht van de houder van een beschermd computerprogramma met

l'exploiter commercialement et de le mettre sur le marché;

e) l'accès dans un système informatique et/ou de télécommunications ou l'interception d'un tel système fait sciemment en violant les règles de sécurité ou dans une autre intention malhonnête ou nuisible.

Certains pays ont déjà mis en place une nouvelle législation relative aux abus informatiques.

Quelques-uns jugent que la législation (classique) existante est suffisante. Beaucoup sont en train de mettre au point des initiatives législatives.

L'on peut considérer qu'il y a deux types d'attitudes face à la « criminalité informatique ».

La première consiste à considérer la criminalité informatique comme une forme de criminalité dont la répression ne requiert pas de législation nouvelle, la législation existante étant jugée suffisante. C'est ce que l'on fait en Islande et au Japon.

La seconde consiste à penser que des mesures législatives sont nécessaires pour que l'on puisse réprimer la criminalité informatique. Elle est favorable à l'élaboration de nouvelles lois ou à la modification des lois existantes en vue de combattre cette nouvelle forme de criminalité. Tel est le point de vue de la plupart des pays industrialisés.

Législation nouvelle dans le domaine de la criminalité informatique

Il nous a paru utile d'examiner comment une législation relative à la criminalité informatique a déjà vu le jour dans un certain nombre de pays.

— *Suède*

Dès 1973, la Suède a adopté la « Data Lag », qui vise principalement à assurer la protection de la vie privée. L'on trouve toutefois dans cette loi un article particulier (art. 21), qui règle la répression des intrusions (non autorisées) dans les systèmes informatiques et du sabotage informatique.

— *Angleterre et pays de Galles*

En 1981 fut adopté, en Angleterre et au pays de Galles, le « Forgery and Counterfeiting Act ». Cette loi étend l'application de la législation sur les faux en écriture (« forgery ») en élargissant le sens du terme « instrument ».

— *Canada*

En 1985, le Canada a adopté le « Criminal Law Amendment Act », qui modifia la loi pénale existante,

het oogmerk dat programma commercieel te exploiteren en op de markt te brengen;

e) het zich opzettelijk verschaffen van toegang tot of het opzettelijk onderscheppen van functies van een computer- of telecommunicatiesysteem, hetzij door inbreuk te maken op beveiligingsmaatregelen, hetzij met andere oneerlijke of schadelijke bedoelingen.

Sommige landen hebben reeds een nieuwe wetgeving op het gebied van computermisbruik tot stand gebracht.

Enkele landen achten de bestaande (klassieke) wetgeving toereikend. Vele landen zijn nog bezig met het ontwikkelen van wetgevende initiatieven.

De benadering van « computercriminaliteit » in de verschillende landen kan in twee categorieën ingedeeld worden.

Volgens het eerste type van benadering wordt computercriminaliteit beschouwd als een vorm van criminaliteit die niet met behulp van nieuwe wetgeving bestreden hoeft te worden, omdat de bestaande wetgeving toereikend is. IJsland en Japan volgen deze benadering.

Volgens de tweede benadering zijn wetgevende maatregelen vereist om computercriminaliteit te kunnen bestrijden. Men bepleit totstandkoming van nieuwe wetten of wijziging van de bestaande wetten om deze nieuwe vorm van criminaliteit tegen te gaan. Deze benadering wordt aangetroffen in de meeste geïndustrialiseerde landen.

Nieuwe wetgeving op het gebied van computercriminaliteit

Het lijkt ons nuttig na te gaan hoe in een aantal landen reeds wetgeving op het gebied van computercriminaliteit tot stand is gebracht.

— *Zweden*

Reeds in 1973 is in Zweden de « Data Lag » aangenomen, die hoofdzakelijk betrekking heeft op de bescherming van privacy. De wet kent echter een speciaal artikel (art. 21), waarin de strafbaarstelling van onbevoegde toegangsverschaffing en computersabotage geregeld wordt.

— *Engeland en Wales*

In 1981 is in Engeland en Wales de « Forgery and Counterfeiting Act » aangenomen. In deze wet is sprake van een uitbreiding van de toepasbaarheid van valsheid in geschrifte (« forgery ») via een uitbreiding van de term « instrument ».

— *Canada*

In 1985 werd in Canada de « Criminal Law Amendment Act » aangenomen, die de bestaande

en vue de combattre la criminalité informatique. Cette loi réprime le sabotage informatique, l'intrusion dans les systèmes informatiques, et l'usage non autorisé d'ordinateurs. Elle définit, en outre, toute une série de notions informatiques.

— *Danemark*

En 1985 le Danemark a adopté une loi sur la « Datakriminalitet », qui adapte les définitions des délits visés par la loi pénale danoise.

Cette loi règle la répression de l'intrusion, de la fraude informatique et des actes de nature à perturber ou à empêcher la communication de données.

— *Etats-Unis d'Amérique*

Pour les Etats-Unis, il y a lieu de faire une distinction entre la législation fédérale et les législations des Etats fédérés.

Au niveau fédéral fut adopté, en 1984, le « Counterfeit Access Device and Computer Fraud and Abuse Act », qui réprime, sous certaines conditions, l'intrusion (non autorisée) dans des systèmes informatiques. Cette loi ne s'applique toutefois qu'aux systèmes informatiques utilisés par les autorités fédérales, les banques ou les bureaux d'information en matière de crédit.

En 1984 fut également adopté le « Small Business Computer Security and Education Act ». Cette loi crée un Conseil chargé de conseiller et d'informer les petites et moyennes entreprises sur les possibilités de prévention de la fraude informatique par l'application de mesures de protection.

En 1986 fut adoptée une loi fédérale qui réprime notamment l'intrusion (non autorisée) dans des ordinateurs présentant un « intérêt fédéral » et le sabotage de ceux-ci.

Elle vise non seulement les ordinateurs utilisés par les autorités fédérales, les banques ou les bureaux d'information en matière de crédit, mais aussi les ordinateurs qui interviennent dans les communications entre Etats et qui sont utilisés par des agents de change enregistrés.

Une législation sur la criminalité informatique a été mise en place, depuis 1978, au niveau des Etats fédérés. En effet, une quarantaine d'Etats américains ont adopté une législation spécifique sur les abus informatiques ou modifié la législation existante.

— *République fédérale d'Allemagne*

En mai 1986, la R.F.A. a adopté « das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität ». Cette loi règle la répression de l'espionnage relatif aux données, de la fraude informatique, de l'altération de données, du sabotage informatique et

strafwet met het oog op de computercriminaliteit wijzigt. In deze wet worden computersabotage, onbevoegde toegangsverschaffing en onbevoegd gebruik van een computer strafbaar gesteld. Bovendien geeft de wet een aantal definities van computerbegrippen.

— *Denemarken*

In 1985 werd in Denemarken een wet inzake « Datakriminalitet » aangenomen, die de bestaande delictsomschrijvingen in de Deense strafwet aanpast.

De wet regelt de strafbaarstelling voor toegangsverschaffing, computerfraude en het storen of verhinderen van datacommunicatie.

— *Verenigde Staten van Amerika*

De Verenigde Staten kennen een onderscheid tussen wetgeving op federaal niveau en wetgeving op het niveau van de deelstaten.

Op federaal niveau werd in 1984 de « Counterfeit Access Device and Computer Fraud and Abuse Act » aangenomen, die onder bepaalde voorwaarden de onbevoegde toegangsverschaffing strafbaar stelt. Deze wet is evenwel slechts van toepassing op computersystemen die door de federale overheid, banken of kredietinformatiebureaus gebruikt worden.

Eveneens in 1984 werd de « Small Business Computer Security and Education Act » aangenomen. Deze wet stelt een Raad in, teneinde het midden- en kleinbedrijf te adviseren en te onderrichten omtrent het voorkomen van computerfraude via beveiligingsmaatregelen.

In 1986 werd een federale wet aangenomen, waarin onder andere onbevoegde toegangsverschaffing en computersabotage ten aanzien van computers met een « federal interest » strafbaar worden gesteld.

Daaronder vallen volgens deze wet niet alleen computers die door de federale overheid, banken of kredietinformatiebureaus gebruikt worden, maar ook computers die een rol spelen in het interstatelijk verkeer en die gebruikt worden door geregistreerde effectenmakelaars.

Op statelijk niveau bestaat vanaf 1978 een wetgeving ten aanzien van computercriminaliteit. Ongeveer veertig Amerikaanse Staten hebben namelijk óf specifieke computermisbruikwetgeving aangenomen óf de bestaande wetgeving gewijzigd.

— *Duitse Bondsrepubliek*

In mei 1986 is in de D.B.R. « das zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität » aangenomen. Deze wet regelt de strafbaarstelling van spionage van gegevens, computerfraude, verandering van gegevens, computersabotage en de vervalsing

de la falsification prouvée de données. Elle permet, en outre, de mieux protéger les secrets commerciaux et industriels.

Nous estimons qu'il y a lieu, pour ce qui est de la Belgique, de compléter le Code pénal de manière à faire tomber plus explicitement, sous le coup de la législation répressive, certains comportements au niveau du stockage, du traitement et de l'échange de données à l'aide d'appareillages spécialement conçus à cet effet.

C'est dans cette optique que nous avons inscrit dans la présente proposition de loi une série de dispositions complétant le Code pénal. Nous avons conscience du fait que leur adoption modifiera le droit pénal dans une mesure importante. Cette modification se justifie, à notre avis, compte tenu des changements sociaux que l'usage des techniques informatiques modernes entraîne et entraînera encore.

Les intérêts mis en jeu lors de l'utilisation des techniques informatiques concernent la disponibilité, l'intégrité et l'exclusivité tant des moyens que des données (*cf.* le rapport de la *Nederlandse Commissie Computercriminaliteit, Informatietechniek en Strafrecht,* Imprimerie nationale, Ministère de la Justice, La Haye, 1987).

L'article 2 de la présente proposition de loi vise à assurer la protection des moyens de stockage, de traitement ou de transfert automatiques de données.

Il est très important, pour la continuité de nombreuses entreprises et institutions, qu'elles puissent toujours disposer sans restriction de leurs moyens de traitement, de stockage et/ou de transfert de données.

Nous utilisons l'expression « système automatisé de stockage ou de traitement de données, ou de télécommunication ». Cette définition générale couvre toutes sortes de types de supports de données. Cette approche fonctionnelle permettra aussi d'éviter que des problèmes ne surgissent lorsque s'estomperont encore davantage les limites entre le traitement et le transfert de données par les télécommunications.

L'article 2 de notre proposition de loi réprime quant à lui la « violation de la paix informatique », c'est-à-dire l'intrusion (illicite) dans des parties protégées de systèmes automatiques de traitement de données.

L'article 3 de notre proposition de loi concerne la protection des données.

Cet article réprime non seulement la mise hors d'usage, l'effacement ou la mise hors d'accès de

van gegevens met bewijskracht. Bovendien biedt de wet de mogelijkheid om tot een ruimere bescherming van handels- en industriële geheimen te komen.

Wij zijn van oordeel dat het in België wenselijk is om door aanvulling van het Strafwetboek bepaalde gedragingen op het gebied van de opslag, verwerking en uitwisseling van gegevens met behulp van daartoe vervaardigde apparatuur, duidelijker binnen het bereik van de Belgische strafwetgeving te brengen.

Dit wetsvoorstel bevat dan ook een aantal voorstellen tot aanvulling van het Strafwetboek. Wij zijn er ons van bewust dat de aanvaarding ervan tot een belangrijke aanpassing van het strafrecht zal leiden. Dit is naar ons oordeel aanvaardbaar gezien de maatschappelijke veranderingen die zijn en worden veroorzaakt door het gebruik van moderne informatietechnieken.

De belangen die in het geding zijn bij het gebruik van informatietechnieken hebben betrekking op de beschikbaarheid, de integriteit en de exclusiviteit van zowel de middelen als van de gegevens (*cf.* het rapport van de Nederlandse Commissie Computercriminaliteit, Informatietechniek en Strafrecht, Staatsuitgeverij, Ministerie van Justitie, 's Gravenhage, 1987).

Het tweede artikel van dit wetsvoorstel beoogt de bescherming van de middelen bedoeld voor geautomatiseerde opslag, verwerking of overdracht van gegevens.

Voor de continuïteit van veel bedrijven en instellingen is het van groot belang dat geen afbreuk wordt gedaan aan de beschikbaarheid van hun middelen van gegevensverwerking, -opslag en/of -overdracht.

Wij gebruiken de term « geautomatiseerd werk voor opslag of werking van gegevens of voor telecommunicatie ». Deze algemene omschrijving omvat allerlei typen van gegevensdragende middelen. Bovendien zijn door deze functionele benadering geen problemen te verwachten bij een verdere vervaging van de grenzen tussen gegevensverwerking en gegevensoverdracht door middel van telecommunicatie.

Door het tweede artikel van ons wetsvoorstel wordt ook de zgn. « computervredebreuk » strafbaar gesteld, nl. het zich wederrechtelijk toegang verschaffen tot beveiligde delen van geautomatiseerde gegevensverwerkende systemen.

Het derde artikel van ons wetsvoorstel heeft betrekking op de bescherming van gegevens.

Door dit artikel wordt niet alleen het onbruikbaar maken, wissen of ontoegankelijk maken van

données, mais aussi la « manipulation de données », c'est-à-dire leur élimination et leur altération ainsi que l'ajout de données nouvelles.

Par « données », nous entendons des reproductions, selon des modalités convenues, de faits, de notions ou d'instructions, reproductions pouvant se prêter à des transferts, des interprétations et des traitements par des personnes ou par des systèmes automatiques. Cette définition s'applique notamment aux programmes informatiques. Elle englobe aussi les annotations, les images et les conversations en langage naturel qui sont suffisamment formalisées pour pouvoir être transférées, traitées ou stockées, avec ou sans l'aide d'appareillages conçus à cet effet.

Nous proposons également d'adopter un certain nombre de dispositions légales pour protéger le caractère exclusif ou confidentiel de certaines données.

Comme ces matières sont étroitement imbriquées, nous traiterons tout d'abord, dans les articles qui les concernent, de l'interdiction d'écouter des conversations. Nous étendrons ensuite cette interdiction à l'écoute ou à l'enregistrement de télécommunications et de transferts de données par la voie de systèmes automatiques.

⁂

PROPOSITION DE LOI

ARTICLE UNIQUE

Au Titre IX du Livre II du Code pénal, il est inséré un Chapitre IV, intitulé « Des abus informatiques et de l'écoute de conversations » et comprenant les six articles suivants :

« *Article 550*bis. — Toute personne qui sciemment détruit, endommage ou rend inutilisable un système automatisé de stockage ou de traitement de données ou de télécommunication, perturbe le fonctionnement d'un tel système ou déjoue une mesure de sécurité prise à l'égard d'un tel système, sera punie d'un emprisonnement de huit jours à deux ans et d'une amende de 1 000 francs à 100 000 francs ou d'une de ces peines seulement :

— si elle empêche ou entrave ainsi le stockage ou le traitement de données ou d'éléments de télécommunication d'utilité publique;

— ou si elle met ainsi en danger des biens ou compromet la dispensation de services. »

gegevens strafbaar gesteld. Ook de zgn. « gegevensmanipulatie » wordt strafbaar gesteld : het verwijderen en het veranderen van gegevens en het toevoegen van andere gegevens.

Onder « gegevens » wordt in ons wetsvoorstel verstaan : een weergave van feiten, begrippen of instructies op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of automatische systemen. Computerprogramma's vallen onder deze omschrijving. Ook aantekeningen, beelden en gesprekken in natuurlijke taal vallen eronder als zijnde voldoende geformaliseerd voor overdracht, verwerking of opslag, al dan niet met behulp van daartoe vervaardigde apparatuur.

Wij stellen ook voor wettelijke bepalingen in te voeren die betrekking hebben op de bescherming van de exclusieve of vertrouwelijke aard van gegevens.

Gezien de onderlinge verwevenheid van de materies behandelen wij in de desbetreffende artikelen vooreerst het verbod tot het afluisteren van gesprekken. Vervolgens breiden wij dit verbod uit tot het afluisteren of het opnemen van telecommunicatie en gegevensoverdracht door geautomatiseerde werken.

G. VERHAEGEN.

⁂

VOORSTEL VAN WET

ENIG ARTIKEL

In Boek II, Titel IX, van het Strafwetboek wordt een Hoofdstuk IV ingevoegd onder het opschrift « Computermisbruik en het afluisteren van gesprekken », met de zes volgende artikelen :

« *Artikel 550*bis. — Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, storing in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verbreekt, wordt gestraft met gevangenisstraf van acht dagen tot twee jaar en met geldboete van 1 000 frank tot 100 000 frank of met een van die straffen alleen, indien :

— daardoor verhindering of bemoeilijking van opslag of verwerking van data of van gegevens van telecommunicatie ten algemenen nutte ontstaat;

— of daardoor gevaar voor goederen of verlening van diensten ontstaat.

Article 550ter. — Sera punie d'un emprisonnement de huit jours à deux ans et d'une amende de 1 000 francs à 100 000 francs, ou d'une de ces peines seulement, toute personne qui rend inutilisables ou inaccessibles, détruit ou modifie sciemment et illicitement des données qui ont été stockées ou qui sont traitées ou transmises au moyen d'un système automatisé, ou qui y ajoute des données nouvelles.

Artikel 550ter. — Wordt gestraft met gevangenisstraf van acht dagen tot twee jaar en met geldboete van 1 000 frank tot 100 000 frank, of met een van die straffen alleen, hij die opzettelijk en wederrechtelijk gegevens, die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen , onbruikbaar maakt, ontoegankelijk maakt of vernietigt, verandert of andere gegevens daaraan toevoegt.

Article 550quater. — Sera punie d'un emprisonnement de huit jours à deux ans et d'une amende de 1 000 francs à 100 000 francs, ou d'une de ces peines seulement :

1° toute personne qui écoute, fait écouter, enregistre ou fait enregistrer une conversation privée ou une communication privée par un moyen technique quelconque, sans l'accord de tous ceux qui participent à cette conversation ou sont concernés par cette communication;

2° toute personne qui enregistre ou fait enregistrer, à l'aide d'un moyen technique quelconque, des télécommunications ou des données transmises au moyen d'un système automatisé,

— sans en avoir été chargée par une personne prenant part à ce type de transmission;

— ou sans y prendre part elle-même.

Artikel 550quater. — Met gevangenisstraf van acht dagen tot twee jaar en met geldboete van 1 000 frank tot 100 000 frank, of met een van die straffen alleen, wordt gestraft :

1° hij die een particulier gesprek of een particuliere mededeling met behulp van enig technisch hulpmiddel afluistert, doet afluisteren, opneemt of doet opnemen zonder de toestemming van allen die aan dat gesprek deelnemen of bij die mededeling zijn betrokken;

2° hij die met een technisch hulpmiddel telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk opneemt of doet opnemen

— zonder daartoe opdracht te hebben gekregen van en deelnemer aan deze vormen van overdracht;

— of zonder deelnemer te zijn aan deze vormen van overdracht.

Article 550quinquies. — Sera punie d'un emprisonnement de huit jours à deux ans et d'une amende de 1 000 francs à 100 000 francs, ou d'une de ces peines seulement :

1° toute personne qui, en vue de l'écoute ou de l'enregistrement illicite d'une conversation, d'une télécommunication ou de données transmises par un système automatisé, veille à ce qu'un moyen technique adéquat soit présent à un endroit déterminé;

2° toute personne qui dispose d'un objet auquel peuvent être soustraites, selon ce qu'elle sait ou présume raisonnablement, des données obtenues par l'écoute ou l'enregistrement illicites d'une conversation, d'une télécommunication ou de données transmises par un système automatisé ou qui met un tel objet à la disposition d'autrui.

Artikel 550quinquies. — Met gevangenisstraf van acht dagen tot twee jaar en met geldboete van 1 000 frank tot 100 000 frank, of met een van die straffen alleen, wordt gestraft :

1° hij die, met het oogmerk dat daardoor een gesprek, telecommunicatie of gegevensoverdracht door een geautomatiseerd werk, wederrechtelijk wordt afgeluisterd of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn;

2° hij die de beschikking heeft over een voorwerp waaraan, naar hij weet of redelijkerwijze moet vermoeden, gegevens kunnen worden ontleend die door wederrechtelijk afluisteren of opnemen van een gesprek, telecommunicatie of gegevensoverdracht door een geautomatiseerd werk zijn verkregen, of zulk een voorwerp ter beschikking stelt van een ander.

Article 550sexies. — Sera punie d'un emprisonnement de huit jours à deux ans et d'une amende de 1 000 francs à 100 000 francs, ou d'une de ces peines seulement, la personne qui aura communiqué intentionnellement à autrui des données obtenues par l'écoute ou l'enregistrement illicites d'une conversation, d'une télécommunication ou de données transmises par un système automatisé.

Artikel 550sexies. — Met gevangenisstraf van acht dagen tot twee jaar en met geldboete van 1 000 frank tot 100 000 frank, of met een van die straffen alleen, wordt gestraft hij die gegevens die door wederrechtelijk afluisteren of opnemen van een gesprek, telecommunicatie of gegevensoverdracht door een geautomatiseerd werk verkregen zijn, opzettelijk aan een ander bekend maakt.

Article 550septies. — Toute condamnation emportera la confiscation des moyens techniques ou

Artikel 550septies. — In geval van veroordeling wordt de verbeurdverklaring uitgesproken van de

objets ayant servi à commettre l'une des infractions visées aux articles 550*quater* à 550*sexies*, ainsi que des enregistrements réalisés illicitement et des données obtenues illicitement. »

technische hulpmiddelen of de voorwerpen die tot het plegen van een misdrijf als bedoeld in de artikelen 550*quater* tot en met 550*sexies* hebben gediend, alsook van de wederrechtelijk verkregen opnamen en gegevens. »

G. VERHAEGEN.

41.859 — E. Guyot, s. a., Bruxelles