ROYAUME DE BELGIQUE

KONINKRIJK BELGIE

AVIS DU CONSEIL D'ETAT

ADVIES VAN DE RAAD VAN STATE

Le CONSEIL D'ETAT, 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 :

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 :

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.
>
> A 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 210bis en projet), "la fraude informatique" (article 504quater en projet) ainsi que "les 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" (articles 550bis et 550ter en projet).

Quant au Code d'instruction criminelle, il s'agit d'organiser "la saisie de données" au cours de l'instruction (article 39bis en projet), d'adapter la perquisition aux exigences de la criminalité informatique (article 88ter 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 88quater 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 90ter 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 109ter 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 télécommunica-

tion (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".

Observations générales

I. Les aspects internationaux de la criminalité informatique

Dans une étude adoptée le 2 juillet 1998, l'assemblée générale du Conseil d'Etat 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 Etats 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 Etats 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).

---

(1) Voir à ce propos l'étude adoptée par l'assemblée générale du Conseil d'Etat de France le 2 juillet 1998 et publiée in "Internet et les réseaux numériques", La Documentation française, 1998, p. 200.

Il est utile de méditer ce texte qui révèle sans illusion la nécessité autant que les limites de ce que chaque Etat 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 Etats 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 Etats 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 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'Etat exerce l'autorité étatique sur son propre territoire, et le fait seul, à l'exclusion de tout autre Etat. Il en découle qu'en temps de paix, il est absolument interdit à un Etat de procéder à une fonction de contrainte sur le territoire d'un autre Etat. Ceci concerne notamment tous les actes de la fonction exécutive, liés ou non à la justice. Un Etat 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'Etat dont elle relève, d'investiguer sur des données situées à l'étranger.

Il semble bien que la plupart des Etats 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 Etat 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 Etat étranger.

---

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

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

On peut y lire qu'à l'égard des "données stockées dans un autre pays ... la plupart des Etats membres tendent 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 88ter 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 88ter, § 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'Etat 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 88ter, 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 88ter fait une allusion, sans doute métaphorique, n'y suffit pas davantage.

La règle du projet s'inspire assurément de certains voeux formulés par la Recommandation précitée. Il faut 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 Etat, 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 Etat 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 Etats 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 Etat 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 Etats. 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 Etats 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 Etats européens : la Convention européenne d'entraide judiciaire en matière pénale faite à Strasbourg le 20 avril 1959 et approuvée 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 Etats 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'autorisa-

tion lorsque les autorités policières d'un Etat 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'Etat 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'Etat (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 telles écoutes pouvaient être prises en considération par le juge si elles avaient été recueillies conformément à la loi étrangère du pays où l'écoute avait eu lieu, si du moins cette loi était elle-même conforme à l'article 8, § 1er, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

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" (2).

---

(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.

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

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 (1).

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

---

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

tenu secret par son placement dans une salle forte, un coffre-fort, voire une simple enveloppe." (1).

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." (2).

a) Ainsi, l'article 550bis, § 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.

---

(1) 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.

(2) Ibidem.

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 550bis, § 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 oeuvre.

Il ressort du Rapport du Comité européen pour les problèmes criminels (1) 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 Etats 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.

---

(1) Voir les pages 54 à 56.

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

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 210bis 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 504quater 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 550ter 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’Etat 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’Etat 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 550bis en projet.

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'Etat 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 550bis 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'Etat s'interroge également sur la cohérence interne de l'article 90quater 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 90quater 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 à dix mille francs".

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 90quater 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 à vingt mille francs.

Le Conseil d'Etat 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 210bis en projet appelle une objection au regard du principe de la légalité des incriminations.

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 550bis 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.

---

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

(2) Voir p. 59 du rapport.

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.

c) L'article 39bis 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 Etats membres à organiser ce type d'information et ce dans le respect des impératifs de l'enquête (2).

---

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

(2) Voir p. 35 du rapport.

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

A 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 88quater 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 90quater en projet.

e) L'article 90septies 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 109ter, 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 commentaire 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 90ter, 90 quater, 90sexies et 90 septies du Code d'instruction criminelle" (2), la section de législation du Conseil d'Etat 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.

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

---

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

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

Onderwerp van het ontwerp

Zoals in de memorie van toelichting aangegeven is, 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 210bis), het "informaticabedrog" (lees : de computerfraude (ontworpen artikel 504quater) en de "misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen" (ontworpen artikelen 550bis en 550ter).

In het Wetboek van Strafvordering moet de "inbeslagneming van gegevens" tijdens het onderzoek (ontworpen artikel 39bis) worden geregeld, de opsporing worden aangepast aan de eisen inzake computercriminaliteit (ontworpen artikel 88ter) 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 88quater).

De lijst van strafbare feiten waarvoor interceptiemaatregelen kunnen worden uitgevaardigd, wordt verruimd tot strafbare feiten ter zake 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 90ter).

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 109ter 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".

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 Etats 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 Etats 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 gepleegd is, als een van de bestanddelen ervan of van de bezwarende omstandigheden waarin het gepleegd is, er gelokaliseerd is. 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 beperkt is; de bestanddelen van een strafbaar

---

(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.

feit en de bezwarende omstandigheden waarin het gepleegd wordt, kunnen dus gemakkelijk tegelijkertijd op het grondgebied van verschillende staten gelokaliseerd zijn. Er mag dan ook van uitgegaan worden 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 gesteld wordt, het aan de rechter overgelaten wordt om alleen en in de grootste 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 vastgesteld wordt, 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 dank zij de informatica, gegevens in het buitenland kan navorsen zonder daarom het grondgebied van de staat waaronder ze ressorteert, in stoffelijke zin te verlaten.

---

(1) Paul Reuter, "Droit international public", blz. 165.

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 Lid-Staten.

Daarin staat te lezen dat wat betreft de "gegevens die in een ander land opgeslagen zijn ..., de meeste Lid-Staten 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 88ter 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 88ter, § 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 88ter, 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 88ter verwezen wordt, is evenmin toereikend.

In de bepaling van het ontwerp wordt stellig uitgegaan van bepaalde, in de voormelde Aanbeveling geuite wensen. Er dient evenwel te worden opgemerkt dat in het ontwerp geen sprake is van het expliciete onderscheid dat in die Aanbeveling gemaakt is 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 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 bezien worden 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 verloren worden 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 gebracht zijn, die gegevens niettemin regelmatig verkregen moeten zijn 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

---

(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 e.v. en de opmerkingen van D. Garabedian.

gegevens verkregen door het afluisteren van telefoongesprekken door de rechter in aanmerking mochten worden genomen indien ze verkregen waren overeenkomstig de buitenlandse wet van het land waar afgeluisterd was, 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 gepleegd worden - 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 gepleegd worden, waar het namelijk gaat om klas-

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

sieke strafbare feiten, die reeds buiten de context van de informatica bestaan (1).

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 bestraft wordt, terwijl datzelfde gedrag misschien niet bestraft zou zijn zonder het gebruik van de computer.

Het volgende mag niet uit het oog verloren worden :

> "... les données confidentielles intégrées sur un support informatique n'ont, en soi, pas plus de valeur que les données figurant sur tout support quelconque enu secret par son placement dans une salle forte, un coffre-fort, voire une simple enveloppe." (2).

P. 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

---

(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", blz. 169.

(2) P. Glineur, "Droit et éthique de l'informatique", gepolykopieerde syllabus van het licentiaat informatica (cursus 1ste licentiaat faculteit wetenschappen) en van het licentiaat informatica en menswetenschappen (cursus 2de licentiaat - faculteit sociale, politieke en economische wetenschappen) van de "Université libre de Bruxelles", 1999, blz. 186.

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 550bis, § 1, van het Strafwetboek degene die, zonder daartoe gerechtigd te zijn, zich toegang verschaft heeft tot een computersysteem, of bij vergissing in dat systeem binnengedrongen is, 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 toegebracht wordt.

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

---

(1) Ibidem.

De formulering van het ontworpen artikel 550bis, § 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 (1) 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.

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.

---

(1) Zie de bladzijden 54 tot 56.

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

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 504quater), en anderzijds datamanipulatie met het specifieke doel schade te berokkenen geviseerd wordt door de bepalingen inzake informatica- en datasabotage (... ontworpen artikel 550ter)".

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 gepleegd heeft.

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 gemaakt worden.

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

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 loutere ongeoorloofde

binnendringen in een computersysteem reeds een strafbaar feit oplevert overeenkomstig paragraaf 1, eerste lid, van het ontworpen artikel 550bis.

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 90quater 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 90quater 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 frank tot tienduizend frank".

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

Paragraaf 4 van het ontworpen artikel 90quater 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, gestraft worden met gevangenisstraf van zes maanden tot één 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 gestraft worden.

De steller van het ontwerp dient die keuze te rechtvaardigen.

B. <u>Het beginsel van de wettelijkheid van de strafbaarstellingen</u>

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

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 550bis 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 nr. 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 nr. 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 nr. R(89)9.

(2) Zie blz. 59 van het rapport.

c) Het ontworpen artikel 39bis 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 gedefinieerd moeten worden.

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 Lid-Staten in de voormelde Aanbeveling nr. R(95)13 verzocht dit verstrekken van inlichtingen te regelen met oog voor de noden van het onderzoek (2).

---

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

(2) Zie blz. 35 van het rapport.

Dat vereiste is van belang, aangezien eenieder die zich door een opsporingshandeling of een onderzoekshandeling met betrekking tot zijn goederen geschaad acht, krachtens de artikelen 28sexies en 61quater 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 88quater 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 90quater.

e) Het ontworpen artikel 90septies 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 109ter, E, betreft, gaat het voor de operatoren van telecommunicatienetwerken en verstrekkers van telecommunicatiediensten om het registreren en bewaren van "oproepgegevens". Volgens 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 geregistreerd en bewaard moeten worden.

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 geregistreerd en bewaard moeten worden 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 90ter, 90quater, 90sexies en 90septies 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.

---

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

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

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 gehouden moeten worden dat de Nederlandse tekst van verscheidene bepalingen van het ontwerp 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 550bis, § 1, tweede lid, "bedraagt de gevangenisstraf zes maanden ..." in plaats van "is de gevangenisstraf van 6 maanden ...", in artikel 5, het ontworpen artikel 39bis, § 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 gecopieerd, 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 herzien moeten worden.

La chambre était composée de		De kamer was samengesteld uit
Messieurs de Heren	Y. KREINS,	conseiller d'Etat, président, staatsraad, voorzitter,
	P. LIENARDY, P. QUERTAINMONT,	conseillers d'Etat, staatsraden,
	P. GOTHOT, J. van COMPERNOLLE,	assesseurs de la section de législation, assessoren van de afdeling wetgeving,
Madame Mevrouw	J. GIELISSEN,	greffier assumé, toegevoegd griffier.

Le rapport a été présenté par Mme P. VANDERNACHT, auditeur. La note du Bureau de coordination a été rédigée et exposée par M. P. BROUWERS, référendaire.

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

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de M. P. LIENARDY.

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

LE GREFFIER - DE GRIFFIER,

LE PRESIDENT - DE VOORZITTER,

J. GIELISSEN

Y. KREINS