

## BELGISCHE SENAAAT

---

ZITTING 1995-1996

---

11 JUNI 1996

---

**Wetsvoorstel tot opheffing van de artikelen 70*bis* en 95, eerste lid, 5<sup>o</sup>, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven en tot aanvulling van het Wetboek van Strafvordering met bepalingen betreffende de decryptie van berichten**

(Ingediend door de dames Bribosia-Picard en Maximus)

---

### TOELICHTING

---

Cryptografie is een techniek waarmee door middel van een wiskundig algoritme een bericht leesbaar of onleesbaar wordt gemaakt voor ieder die niet over de geheime cryptografische sleutel beschikt. Coderings-systemen bestaan al geruime tijd; ze werden in hoofdzaak voor militaire doeleinden gebruikt. Met de ontwikkeling van Internet en van de informatiemaatschappij hebben ze thans ook bij het groot publiek hun intrede gedaan.

In België verdubbelt het aantal gebruikers van Internet elk jaar. Sedert twee jaar komen er per maand 10 pct. gebruikers bij. Zo berekend zou ons land thans 200 000 regelmatige gebruikers tellen, van wie 20 pct. uit het bedrijfsleven en een groot aantal studenten die op de apparatuur van hun universiteit werken. Gezien het toenemend aantal gebruikers en de vlotte toegankelijkheid van het net, is het belangrijk dat de datatransmissie beveiligd kan worden. Daarvoor kan men een beroep doen op de cryptogra-

## SÉNAT DE BELGIQUE

---

SESSION DE 1995-1996

---

11 JUIN 1996

---

**Proposition de loi abrogeant les articles 70*bis* et 95, alinéa 1<sup>er</sup>, 5<sup>o</sup>, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques et complétant le Code d'instruction criminelle par des dispositions relatives au décryptage des messages**

(Déposée par Mmes Bribosia-Picard et Maximus)

---

### DÉVELOPPEMENTS

---

La cryptographie désigne la technique permettant, à l'aide d'un algorithme mathématique, de rendre un message lisible, illisible pour toute personne ne possédant pas la clé secrète de cryptage. Si les systèmes d'encodage ne sont pas récents et étaient surtout utilisés dans le domaine militaire, ils sont apparus au grand public avec l'émergence d'Internet et de la « société de l'information ».

En Belgique, le nombre d'utilisateurs d'Internet double chaque année, enregistrant une progression mensuelle de 10 p.c. depuis deux ans. Le pays compterait ainsi 200 000 utilisateurs réguliers, dont 20 p.c. issus du monde des entreprises et un grand nombre d'étudiants, ceux-ci bénéficiant des installations mises en place par leurs universités. Vu le nombre croissant d'utilisateurs et l'accessibilité aisée au réseau, il est important que la protection des informations transmises existe. La cryptographie permet cette

fie, die een ruimere toepassing vindt dan op Internet. Zo zijn er thans in België drie bedrijven met wereldfaam die netwerken gebruiken.

Het gebruik van encryptie-apparatuur volledig verbieden zou in de praktijk neerkomen op het afremmen van de ontwikkeling van de informatiemaatschappij. Internet heeft immers geen enkele vorm van vertrouwelijkheid te bieden: wie dat ook maar wil, kan welke boodschap dan ook onderschepen en lezen. Daarom doet men heden ten dage alsmear vaker een beroep op encryptietechnieken, die in talloze gevallen zelfs onmisbaar blijken. Zo kan worden voorkomen dat de eerste de beste in de verstuurd boodschappen neust. Encryptietechnieken zijn voor Internet wat enveloppes voor het postverkeer zijn.

Het gebruik van encryptietechnieken vindt ook toepassing in het elektronisch handelsverkeer, omdat de geadresseerde op die manier de zekerheid heeft dat het bericht afkomstig is van de afzender die geacht wordt het te versturen, en dat niemand het onderweg heeft gewijzigd. Dit is een zeer belangrijk aspect, onder meer bij het elektronisch betaalverkeer en de overdracht van bankinformatie alsook voor het identificeren van de medische hulpverlener en de bescherming van patiëntendossiers. Op al die vlakken moet de veiligheid en de vertrouwelijkheid van de informatie gewaarborgd blijven.

Cryptografie kan dienen om de persoonlijke levenssfeer en de intellectuele eigendom te beschermen, maar men kan ze echter ook aanwenden voor minder oorbare doeleinden zoals bijvoorbeeld het witwassen van de opbrengst van mensen-, drugs- of wapenhandel.

Cryptografie plaatst ons dus voor een dilemma: hoe kan men de ontwikkeling stimuleren van middelen die de veiligheid en de vertrouwelijkheid van de informatie waarborgen en tegelijkertijd de mogelijkheid openhouden dat de gerechtelijke instanties en de inlichtingendiensten controle uitoefenen telkens wanneer de naleving van de rechtsregels en de bescherming van het algemeen belang dat vereisen? Men kan toch niet zonder meer aanvaarden dat het gebruik van nieuwe telecommunicatiesystemen bijdraagt aan toename van misdadige activiteiten. In bepaalde gevallen moet men dus wel voorzien in de mogelijkheid om alle berichten, hoe die ook verstuurd worden, te ontcijferen.

Daar staat dan weer tegenover dat het volstrekt buiten proportie zou staan de gehele bevolking te verbieden encryptietechnieken te gebruiken om in een beperkt aantal gevallen een tap op een lijn te kunnen plaatsen. De verplichting om de encryptiesleutels te deponeren bij een officiële instelling zou niet alleen niet haalbaar en gevaarlijk kunnen blijken, maar ook

protection et, de plus, dépasse la seule dimension d'Internet. Ainsi, trois sociétés de dimension mondiale utilisant des réseaux sont installées en Belgique.

Interdire complètement l'utilisation de dispositifs de cryptage équivaldrait pratiquement à empêcher l'éclosion de la « société de l'information ». En effet, il n'y a aucune confidentialité sur Internet: n'importe qui peut, s'il le veut, intercepter et lire n'importe quel paquet d'information. C'est pourquoi les techniques de cryptage sont aujourd'hui de plus en plus utilisées et même indispensables pour de nombreuses applications. Elles permettent d'éviter que n'importe qui ne puisse voir le contenu des messages transmis. Les techniques de cryptage sont à Internet ce que les enveloppes sont au courrier postal.

La technique de la cryptographie est aussi utilisée dans des applications telles que le commerce électronique, car elle permet au récipiendaire du message d'être sûr qu'il provient bien de celui qui est censé l'émettre et que personne n'y a touché pendant son transport; cet aspect est très important, notamment lors des transactions et transmissions de données bancaires ainsi que pour l'identification du prestataire de soins de santé et la protection des dossiers des patients. Dans tous ces domaines, la sécurité et la confidentialité de l'information doivent être assurées.

La cryptographie peut être utilisée pour protéger la vie privée et la propriété intellectuelle mais elle peut aussi l'être à des fins moins recommandables (par exemple: le blanchiment de l'argent généré par le commerce des êtres humains, de la drogue ou des armes).

La cryptographie pose donc un dilemme: comment permettre le développement de moyens pour protéger la sécurité et la confidentialité de l'information tout en ménageant une possibilité de contrôle des autorités judiciaires et des services de renseignement, dans tous les cas où le respect du droit et de l'intérêt général l'exigent? On ne peut en effet accepter que les nouveaux systèmes de télécommunication facilitent les activités délictueuses. Il faut donc prévoir la possibilité d'accès, dans certains cas, au décryptage de tous les messages, quel que soit leur support.

Cependant, il serait totalement disproportionné d'interdire à toute la population d'utiliser des techniques de cryptage pour permettre un petit nombre « d'écoutes ». Quant à l'obligation de dépôt des clés de cryptage auprès d'un organisme officiel, elle pourrait se révéler non seulement irréalisable et dangereuse, mais aussi inefficace puisque les malfrats, et en parti-

ondoelmatig omdat misdadigers, vooral die onder hen die de elektronische snelweg gebruiken, zeker niet bereid zullen zijn hun codes aan derden te verklappen.

De verplichting om sleutels te deponeren zou er onvermijdelijk toe leiden dat talrijke gebruikers van Internet hun vertrouwen verliezen. Handelsactiviteiten, vooral het elektronisch bankieren, via Internet zouden kunnen slabakken. Immers, valt een dergelijk systeem nog te beheren? Wie kan er waarborgen dat die sleutels nooit in verkeerde handen terecht komen? Kan de Staat een financiële vergoeding waarborgen voor de schade die bijvoorbeeld een bank zou lijden als een codekraker een van haar sleutels «steelt»? Wat moet er gebeuren met systemen van «random»-sleutels? Is het niet gevaarlijk te eisen dat de sleutels uitsluitend in België worden gedeponeerd? De drie bedrijven met wereldfaam die thans in België gevestigd zijn, zouden snel naar gastvrijere oorden trekken. Zelfs een Europees systeem zou niet meer volstaan omdat onze planeet door de informatietechnologie een groot dorp is geworden.

Daar staat tegenover dat een coderingssysteem in bepaalde gevallen gekraakt moet kunnen worden. De artikelen 90ter tot 90novies van boek I van het Wetboek van Strafvordering staan nu reeds het afluisteren van communicaties en de eventuele vertaling ervan toe. Die artikelen zijn ingevoegd bij de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennis nemen en opnemen van privé-communicatie en -telecommunicatie en ons voorstel wil die bepalingen aanvullen door een wettelijke grondslag te geven aan het decoderen van versleutelde berichten in opdracht van de gerechtelijke instanties.

Deze wet van 30 juni 1994 vormt een mijlpaal in de bescherming van de gegevens. De wet van 21 december 1994 houdende sociale en diverse bepalingen bevat evenwel drie wazige artikelen die tot uiteenlopende interpretaties zouden kunnen leiden. Zo zou de verplichting om encryptiesleutels aan derden mee te delen ingevoerd kunnen worden met in Ministerraad overlegde besluiten.

Dat zou erop neerkomen dat die buitenstaander over informatie beschikt waarmee hij niet alleen voor een bepaalde persoon bestemde berichten kan ontcijferen, maar ook de identiteit van die persoon kan nabootsen. Het hoeft geen betoog dat dergelijke informatie een enorme waarde heeft in een maatschappij waar de elektronische identificatie even belangrijk zal worden als de geschreven handtekening thans.

Dit voorstel wil rekening houden met de bedoeling van de wetgever van 1994, nl. een oplossing vinden

culier ceux qui utilisent les autoroutes de l'information, ne sont certainement pas prêts à communiquer leurs codes à un tiers.

Le dépôt obligatoire des clés provoquerait inévitablement une perte de confiance de nombreux utilisateurs d'Internet. Le commerce (notamment «l'électronic banking») qui se fait via ce réseau s'en trouverait diminué. En effet, un tel système serait-il gérable? Pourrait-on garantir que les clés ne soient jamais volées? L'État se porterait-il garant — financièrement — des dommages qu'un voleur pourrait causer, par exemple à une banque, en volant un double des «clés»? Qu'en serait-il des systèmes de clés évolutives? Ne serait-il pas dangereux d'exiger le dépôt uniquement en Belgique? Les trois sociétés mondiales installées en Belgique s'empresseraient d'élire domicile sous des cieux plus cléments. Même au niveau européen, un tel système ne suffirait pas, le monde de l'information ayant fait de notre planète un grand village.

Par contre, il est indispensable dans certains cas de pénétrer dans ce système d'encodage. Les articles 90ter à 90novies, du livre premier du Code d'instruction criminelle permettent déjà les «écoutes» et leur traduction éventuelle. La présente proposition vise à compléter ces dispositions introduites par 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, en donnant un cadre à l'accès par les autorités judiciaires à la compréhension des messages par leur décryptage.

Cette 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, fait déjà un grand pas vers la protection des informations. Cependant, la loi du 21 décembre 1994 portant des dispositions sociales et diverses comporte trois articles peu clairs et pouvant donner lieu à de nombreuses interprétations. Ainsi, ils pourraient permettre, moyennant des arrêtés délibérés en Conseil des ministres, d'obliger de communiquer les clés d'encryptage à un tiers.

Cela signifierait que ce tiers disposerait d'informations lui permettant à la fois de décrypter les messages destinés à une personne donnée, mais également de pouvoir reproduire la signature de cette personne. La valeur d'une telle information, dans une société où les signatures électroniques sont appelés à avoir un rôle aussi important que les signatures manuscrites aujourd'hui, n'est pas à démontrer.

La présente proposition veut rencontrer le souci du législateur de 1994 (solutionner le problème du dé-

voor het probleem van het ontsleutelen van boodschappen en tegelijkertijd de ongewenste gevolgen voorkomen die onvermijdelijk verbonden zijn aan de verplichting om alle coderings- of decoderingssleutels bij een derde instelling te deponeren.

In die overtuiging worden we nog gesterkt door de thans bestaande moeilijkheden om de eigen informatie doelmatig te beschermen. Er wordt immers steeds vaker chantage gepleegd door «cybergangs» (cf. «*Le Soir*» van dinsdag 4 juni 1996): een afperser dringt het computersysteem van een bedrijf binnen, laat daar een slapend virus achter en dreigt het te activeren, tenzij hij geld ontvangt. Daaruit blijkt hoe moeilijk het nu al is om informatie te beschermen, zelfs al blijven de sleutels nog geheim. Dat zal ongetwijfeld nog moeilijker worden wanneer men de sleutels bij een derde instelling moet deponeren zodat het gevaar van diefstal of inzage door derden nog toeneemt.

Aan de grondslag van dit voorstel ligt dus het streven om een alternatief te vinden voor de regeling van de artikelen 70bis en 95 van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de artikelen 202 tot 204 van de wet van 21 december 1994 houdende sociale en diverse bepalingen, zodat het mogelijk wordt versleutelde berichten te ontsleutelen en tegelijkertijd de bescherming van de persoonlijke levenssfeer te waarborgen volgens de wet van 30 juni 1994. Van essentieel belang daarbij is dat dit democratisch beginsel, dat de eerbied voor de persoon en zijn rechten nastreeft, niet met voeten wordt getreden. Dit voorstel wil die twee doelstellingen bereiken en ze met elkaar verzoenen.

### Toelichting bij de artikelen

#### Artikel 1

Dit artikel wijst op de optioneel bicamerale aard van dit wetsvoorstel.

#### Artikelen 2 en 3

De artikelen 202 tot 204 van de wet van 21 december 1994 houdende sociale en diverse bepalingen voegen in de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven een artikel 70bis in, alsook een 5° in artikel 95, eerste lid. Deze twee artikelen zijn vrij wazig opgesteld en zetten de deur open voor een zeer ruime interpretatie. Zo kunnen ze het gebruik van encryptie-apparatuur volledig verbieden of de verplichting opleggen encryptiesleutels bij derden te deponeren, wat de ontwikkeling van de informatiematenschap sterk zal afremmen. Wie kan immers nog een systeem vertrouwen wanneer er geknoeid kan

cryptage des messages) tout en évitant les effets pervers qui accompagneraient inévitablement l'obligation de déposer toutes les clés de cryptage ou de décryptage auprès d'un organisme tiers.

Cette conviction est renforcée par les difficultés existant déjà à l'heure actuelle de protéger son information efficacement. En effet, on assiste de plus en plus au racket organisé par des «cybergang» (voir «*Le Soir*» du mardi 4 juin 1996): un maître chanteur s'introduit dans le système informatique d'une société, y dépose une «bombe informatique» et menace de la faire exploser si aucun versement d'argent n'est effectué. Ceci montre les difficultés existant déjà à l'heure actuelle pour la protection des informations, alors que les clés restent secrètes. Les déposer auprès d'un organisme tiers, en renforçant le danger de vol ou de consultation des clés par un tiers, accroîtrait sans nul doute ces difficultés de protection.

L'esprit qui sous-tend la proposition est donc de trouver une alternative aux articles 70bis et 95 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, insérés par les articles 202 à 204 de la loi du 21 décembre 1994 portant des dispositions sociales et diverses, afin de prévoir l'accès à la compréhension des messages cryptés tout en assurant le respect et la protection de la vie privée, dans l'esprit de la loi du 30 juin 1994. Il est essentiel que ce principe démocratique et visant au respect de l'individu et de ses droits ne soit pas bafoué. La présente proposition veut répondre à ces deux impératifs qu'elle s'efforce de concilier.

### Commentaire des articles

#### Article 1<sup>er</sup>

Indique le caractère bicaméral optionnel de la proposition de loi.

#### Articles 2 et 3

Les articles 202 à 204 de la loi du 21 décembre 1994 portant des dispositions sociales et diverses insèrent un article 70bis et un 5° à l'article 95, alinéa 1<sup>er</sup>, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Ces deux articles assez imprécis laissent une marge d'interprétation considérable. Ainsi, ils pourraient permettre d'interdire complètement l'utilisation de dispositifs de cryptage ou d'obliger à déposer les clés de cryptage auprès d'un tiers, ce qui nuirait fortement au développement de la société de l'information. En effet, qui aurait encore confiance en un système où tout message pourrait être falsifié en ce qui concerne soit son contenu,

worden met de inhoud, de identificatie of gewoon de geheime aard van een boodschap? Voorgesteld wordt bijgevolg die artikelen te doen vervallen.

#### Artikel 4

Dit artikel voegt in het Wetboek van Strafvordering onder een zelfde opschrift een reeks nieuwe artikelen in over het decoderen van boodschappen om de onderzoeksrechter in staat te stellen kennis te nemen van berichten die zijn onderschept volgens artikel 90ter van hetzelfde Wetboek. Het gaat om de volgende artikelen:

*Art. 90undecies.* — Dit artikel geeft een definitie van de in het voorstel gebruikte termen. De definitie van het woord «encryptie» doelt op alle berichten ongeacht de informatiedrager die wordt gebruikt. Alle berichten gaande van de gewone gecodeerde brief tot berichten via multimediatragers komen aldus op een voet van gelijkheid te staan.

*Art. 90duodecies.* — Wanneer de bevoegde rechter (de onderzoeksrechter) informatie wil verkrijgen zoals bepaald in artikel 90ter, §§ 2, 3 en 4, van het Wetboek van Strafvordering of wanneer hij de vertaling wil van een document gevonden bij een huiszoeeking, kan hij ieder die hem bij de ontcijfering kan helpen, verplichten zulks te doen, op voorwaarde dat die hulp nodig is voor het onderzoek. Met het oog op de bescherming van en het respect voor de persoonlijke levenssfeer bepaalt dit artikel dat er ernstige aanwijzingen moeten zijn en legt het nog enkele andere voorwaarden op.

*Art. 90ter decies.* — Dit artikel bepaalt hoe de hulp bij het ontcijferen wordt gevraagd en verkregen.

*Art. 90quater decies.* — Om te voorkomen dat bepaalde personen weigeren de sleutel af te geven of met het gerecht samen te werken, voert dit artikel zware strafsancities in. Iemand die weigert de sleutel af te geven of met het gerecht samen te werken, handelt misschien zo omdat hij er belang bij heeft iets achter te houden. De informatie in de versleutelde berichten zou hem een veroordeling kunnen opleveren. Indien die persoon de sleutel niet wil afgeven, beschikt het gerecht over geen enkel bewijs tegen hem en kan hij vrijuit gaan. Door in een strenge strafsancie te voorzien, wil men de burgers ertoe aanzetten hun medewerking te verlenen. Bij het systeem met «random»-sleutels kan het uiteraard gebeuren dat het bericht niet meer te ontcijferen valt door de persoon die het heeft uitgezonden of ontvangen (de rechter moet zich omringen met deskundigen die dat kunnen zeggen). Dat belet echter niet dat de betrokkene de inhoud van het bericht uit het hoofd kent.

soit son authentification, soit simplement son caractère secret. Il est donc proposé de supprimer ces articles.

#### Article 4

Cet article insère dans le Code d'instruction criminelle une série de nouveaux articles repris sous un même titre, concernant le décryptage de messages, afin que le juge d'instruction puisse prendre connaissance du contenu des messages interceptés dans le cadre de l'article 90ter du même Code. Les articles introduits sont les suivants:

*Art. 90undecies.* — Cet article définit les termes utilisés dans la proposition. Par la définition du terme cryptage telle qu'établie ici, on a voulu viser les messages, quel que soit leur support. Ainsi, on met sur un pied d'égalité les messages, depuis la simple lettre cryptée jusqu'au message transitant par un support multimédia.

*Art. 90duodecies.* — Le juge compétent (le juge d'instruction) désirant obtenir une information comme le prévoit l'article 90ter, §§ 2, 3 et 4, du Code d'instruction criminelle, ou désirant la traduction d'un papier obtenu lors d'une perquisition, peut obliger toute personne susceptible de l'aider au décryptage à le faire, si cette aide est nécessaire pour l'enquête. L'obligation d'indices sérieux et les autres précisions apportées dans cet article visent à la protection et au respect de la vie privée des individus.

*Art. 90ter decies.* — Cet article décrit la procédure selon laquelle l'aide au décryptage est demandée et reçue.

*Art. 90quater decies.* — Afin d'éviter le refus par certains de donner la clé ou de collaborer avec la justice, cet article instaure des peines pénales sévères. En effet, si une personne refuse de donner la clé ou de collaborer avec la justice, c'est qu'elle peut avoir un intérêt à cacher quelque chose. Or, des éléments contenus dans les messages cryptés pourraient lui valoir une condamnation. Si elle ne fournit pas la clé, la justice n'a aucune preuve contre cette personne qui peut ainsi demeurer impunie. L'instauration d'une peine pénale sévère vise à inciter les personnes à collaborer. Bien sûr, il est possible, dans le cas de système à clé variable, que le message soit devenu indécryptable pour la personne même qui l'a envoyé ou reçu (le juge doit s'entourer d'experts pouvant le déterminer), ce qui n'empêche pas la personne d'avoir retenu le contenu du message.

Artikel 56 van het Strafwetboek vindt toepassing bij recidive.

*Art. 90*quinquies decies. — De eerste paragraaf bepaalt hoe lang de rechter een beroep kan doen op hulp bij het ontcijferen. Deze bepaling wil even stringent zijn als die op de telefoontaps omdat hulp bij het ontcijferen in dat kader past.

Paragraaf 2 verplicht de rechter de sleutel te vernietigen die hem is afgegeven om de berichten te ontcijferen, na het verstrijken van de periode van bewaking waarvoor de sleutel werd gevraagd. Nu kan het zijn dat de sleutel alleen nodig is om berichten te ontcijferen die reeds onderschept waren. In dat geval is het normaal dat die berichten zo spoedig mogelijk ontcijferd worden en dat de sleutel onmiddellijk daarna wordt vernietigd.

*Art. 90*sexies decies. — Om lekken zoveel mogelijk uit te sluiten, moet de overschrijving en de bewaring van de met hulp ontcijferde berichten aan dezelfde voorwaarden voldoen als de overschrijving en de bewaring van de opnamen bedoeld in artikel 90septies van het Wetboek van Strafvordering.

*Art. 90*septies decies en octies decies. — Berichten ontvangen of verstuurd door een advocaat of een arts mogen alleen dan worden ontcijferd wanneer deze advocaat of arts er zelf van verdacht wordt een van de in artikel 90ter bedoelde misdrijven te hebben gepleegd of eraan te hebben deelgenomen. Er moeten immers bijzondere maatregelen genomen worden voor die twee beroepen, aangezien daar een beroepsgeheim geldt.

\*  
\* \*

## WETSVOORSTEL

---

### Artikel 1

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

### Art. 2

Artikel 70bis van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de wet van 21 december 1994, wordt opgeheven.

L'article 56 du Code pénal s'applique en cas de récidive.

*Art. 90*quinquies decies. — Le paragraphe premier détermine la période pour laquelle le juge peut faire appel à l'aide au décryptage. La disposition se veut aussi stricte que celle sur les écoutes, l'aide au décryptage s'inscrivant dans ce cadre.

La disposition contenue dans le paragraphe 2 oblige le juge à détruire la clé qui lui a été donnée pour décrypter les messages, dans le cas de l'aide au décryptage, lorsque la période de surveillance pour laquelle la clé a été demandée est terminée. Toutefois, il est possible que la clé ne soit requise que pour décrypter des messages qui avaient déjà été interceptés; dans ce cas, il est logique que ces messages soient décryptés le plus rapidement possible et que s'ensuive la destruction immédiate de la clé.

*Art. 90*sexies decies. — Afin de s'assurer au maximum qu'aucune fuite n'ait lieu, la retranscription et la conservation des messages décryptés grâce à l'aide doit suivre les mêmes conditions que la transcription et la conservation des enregistrements telles que prévues à l'article 90septies du Code d'instruction criminelle.

*Art. 90*septies decies et octies decies. — Le décryptage d'un message reçu par ou transmis par un avocat ou un médecin ne peut avoir lieu que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter ou d'y avoir participé. Il est en effet essentiel de prévoir des dispositions particulières pour ces deux professions, pour lesquelles l'obligation du secret professionnel est requise.

Michèle BRIBOSIA-PICARD

\*  
\* \*

## PROPOSITION DE LOI

---

### Article premier

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

### Art. 2

L'article 70bis de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, inséré par la loi du 21 décembre 1994, est abrogé.

## Art. 3

Artikel 95, eerste lid, 5<sup>o</sup>, van dezelfde wet, ingevoegd bij de wet van 21 december 1994, wordt opgeheven.

## Art. 4

Boek I, hoofdstuk VI, afdeling 2, onderafdeling II, van het Wetboek van Strafvordering wordt aangevuld met een § 7 (nieuw), onder het opschrift «§ 7. — Decryptie van berichten», bestaande uit de artikelen 90*undecies* tot 90*octies decies* en luidende:

«Art. 90*undecies*. — Voor de toepassing van deze paragraaf wordt verstaan onder:

1<sup>o</sup> encryptie: de handeling die bestaat in het vertalen van de klare tekst van een bericht, ongeacht de informatiedrager, door middel van een wiskundige formule of van een algoritme ten einde de vertrouwelijkheid, de integriteit en de identiteit te beveiligen en te voorkomen dat niet-geautoriseerde personen toegang krijgen tot dat bericht of het bericht wijzigen;

2<sup>o</sup> decryptie: de handeling die bestaat in het ontcijferen van een bericht, ongeacht de informatiedrager, door middel van een wiskundige formule of een algoritme;

3<sup>o</sup> gebruiker van de sleutel: ieder die een sleutel vrijwillig aan een andere persoon heeft gegeven of van hem heeft gekregen om berichten tussen die twee personen te kunnen vertalen of ontcijferen;

4<sup>o</sup> encryptiesleutel, ontcijferingssleutel: variabele informatie gebruikt in een wiskundige formule of een algoritme om een bericht te vertalen of te ontcijferen;

5<sup>o</sup> hulp bij decryptie: het verlenen van toegang tot vertaalde begrippen.

Art. 90*duodecies*. — De onderzoeksrechter kan in uitzonderlijke gevallen, wanneer het onderzoek zulks vereist, voor het ontcijferen van een bericht de hulp vorderen van ieder die daartoe in staat is, indien er ernstige aanwijzingen bestaan dat het feit waarvoor hij geacht is, een strafbaar feit is bedoeld in een van de bepalingen opgesomd in artikel 90*ter*, §§ 2, 3 en 4, en indien de overige middelen van onderzoek niet volstaan om de waarheid aan de dag te brengen.

De hulp bij decryptie kan alleen worden bevolen voor berichten verstuurd aan of door personen die op grond van precieze aanwijzingen ervan worden verdacht het strafbaar feit te hebben gepleegd en voor berichten verstuurd aan of door personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met een persoon op wie een verdenking rust.

## Art. 3

L'article 95, alinéa 1<sup>er</sup>, 5<sup>o</sup>, de la même loi, inséré par la loi du 21 décembre 1994, est abrogé.

## Art. 4

Le livre premier, chapitre VI, section 2, distinction II, du Code d'instruction criminelle est complété par un § 7 (nouveau) «§ 7. — Du décryptage des messages», comprenant les articles 90*undecies* à 90*octies decies*, libellés comme suit:

«Art. 90*undecies*. — Pour l'application du présent paragraphe, on entend par:

1<sup>o</sup> cryptage: l'opération qui consiste à transformer le texte clair d'un message, quel que soit le support, par l'utilisation d'une formule mathématique ou d'un algorithme afin de préserver la confidentialité, l'intégrité et l'authenticité et d'empêcher toute personne non autorisée d'avoir accès à ou d'altérer ce message;

2<sup>o</sup> décryptage: l'opération qui consiste à rendre un message à nouveau compréhensible, quel que soit le support, par l'utilisation d'une formule mathématique ou d'un algorithme;

3<sup>o</sup> utilisateur de clé: toute personne qui a volontairement donné ou reçu une clé d'une autre personne, afin de pouvoir crypter ou décrypter tout message entre ces deux personnes;

4<sup>o</sup> clé de cryptage, de décryptage: l'information variable utilisée dans une formule mathématique ou un algorithme utilisée afin de crypter ou de décrypter un message;

5<sup>o</sup> aide au décryptage: la fourniture de l'accès à la compréhension du message.

Art. 90*duodecies*. — Lorsque les nécessités de l'instruction l'exigent, le juge d'instruction peut, à titre exceptionnel, requérir l'aide au décryptage d'un message, de toute personne susceptible de fournir cette aide, s'il existe des indices sérieux que le fait dont il est saisi constitue une infraction visée par l'une des dispositions énumérées à l'article 90*ter*, §§ 2, 3 et 4, et si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité.

L'aide au décryptage ne peut être ordonnée qu'à l'égard des messages envoyés à ou par des personnes soupçonnées, sur la base d'indices précis, d'avoir commis l'infraction, et à l'égard des messages envoyés à ou par des personnes présumées, sur la base de faits précis, être en communication régulière avec un suspect.

*Art. 90ter decies.* — § 1. De onderzoeksrechter doet voor zich de personen dagvaarden die bij decryptie hulp kunnen bieden.

§ 2. De personen die bij decryptie hulp kunnen bieden worden op verzoek van de procureur des Konings gedagvaard door een gerechtsdeurwaarder of door een agent van de openbare macht.

§ 3. Vóór zij worden gehoord, vertonen zij de dagvaarding waarbij zij zijn opgeroepen om bij decryptie hulp te bieden; daarvan wordt melding gemaakt in het proces-verbaal.

§ 4. De informatie verkregen met de hulp bij het ontcijferen van het bericht wordt getekend door de rechter, de griffier en de persoon die bij decryptie hulp geboden heeft, nadat hem daarvan voorlezing is gedaan en nadat hij verklaard heeft daarbij te volharden; indien de persoon die bij decryptie hulp geboden heeft niet wil of niet kan tekenen, wordt daarvan melding gemaakt.

Elke bladzijde van de processen-verbaal van onderzoek wordt getekend door de rechter en door de griffier.

§ 5. Hij die gedagvaard wordt om hulp te bieden bij decryptie, moet verschijnen en moet aan de dagvaarding voldoen; doet hij dat niet, dan kan hij daartoe worden gedwongen door de onderzoeksrechter, die te dien einde op de conclusie van de procureur des Konings, zonder verdere vormen, zonder termijn en zonder hoger beroep, een geldboete van ten hoogste honderd frank uitspreekt en kan bevelen dat de gedaagde lichamelijk zal worden gedwongen hulp te bieden bij decryptie.

§ 6. De persoon die bij decryptie hulp kan bieden en aldus tot geldboete is veroordeeld wegens een eerste niet-verschijning en die na de tweede dagvaarding aan de onderzoeksrechter wettige redenen van verschoning voorlegt, kan op de conclusie van de procureur des Konings van de geldboete worden ontheven.

§ 7. Blijkt uit het getuigschrift van een arts dat de personen die bij decryptie hulp kunnen bieden, zich in de onmogelijkheid bevinden om op de aan hen gedane dagvaarding te verschijnen, dan begeeft de onderzoeksrechter zich in hun woning, als zij in het arrondissement wonen waarvoor de onderzoeksrechter bevoegd is.

§ 8. Indien de personen die bij decryptie hulp kunnen bieden buiten het arrondissement van de onderzoeksrechter wonen, verzoekt deze de onderzoeksrechter van het arrondissement waarin de personen wonen die bij decryptie hulp kunnen bieden, zich bij hen te begeven om hun hulp bij decryptie te krijgen.

*Art. 90 ter decies.* — § 1<sup>er</sup>. Le juge d'instruction fera citer devant lui les personnes susceptibles d'apporter une aide au décryptage.

§ 2. Les personnes susceptibles d'apporter l'aide au décryptage seront citées par un huissier de justice, ou par un agent de la force publique, à la requête du procureur du Roi.

§ 3. Elles représenteront, avant d'être entendues, la citation qui leur aura été donnée pour apporter l'aide au décryptage, et il en sera fait mention dans le procès-verbal.

§ 4. Les informations obtenues grâce à l'aide au décryptage du message seront signées du juge, du greffier et de la personne ayant apporté l'aide au décryptage, après que lecture lui en aura été faite et qu'elle aura déclaré y persister; si ma personne ayant apporté l'aide ne veut ou ne peut signer, il en sera fait mention.

Chaque page du cahier d'information sera signée par le juge et par le greffier.

§ 5. Toute personne citée pour apporter une aide au décryptage, sera tenue de comparaître et de satisfaire à la citation; sinon, elle pourra y être contrainte par le juge d'instruction, qui, à cet effet, sur les conclusions du procureur du Roi, sans autre formalité ni délai, et sans appel, prononcera une amende qui n'excédera pas cent francs, et pourra ordonner que la personne citée soit contrainte par corps à venir apporter son aide au décryptage.

§ 6. La personne susceptible d'apporter une aide au décryptage ainsi condamnée à l'amende sur le premier défaut et qui, sur la seconde citation produira devant le juge d'instruction des excuses légitimes, pourra, sur les conclusions du procureur du Roi, être déchargée de l'amende.

§ 7. Lorsqu'il sera constaté, par le certificat d'un médecin, que les personnes susceptibles d'apporter l'aide au décryptage se trouvent dans l'impossibilité de comparaître sur la citation qui leur aura été donnée, le juge d'instruction se transportera en leur demeure, quand ils habiteront dans l'arrondissement pour lequel le juge d'instruction est compétent.

§ 8. Si les personnes susceptibles d'apporter l'aide au décryptage résident hors de l'arrondissement du juge d'instruction, celui-ci requerra le juge d'instruction de l'arrondissement dans lequel les personnes susceptibles d'apporter l'aide au décryptage sont résidentes, de se transporter auprès d'elles pour recevoir leur aide au décryptage.



§ 9. De rechter die overeenkomstig de §§ 7 en 8 hulp bij decryptie heeft ontvangen, stuurt al de informatie over die hulp gesloten en verzegeld aan de onderzoeksrechter van de rechtbank waarbij de zaak aanhangig is.

*Art. 90quater decies.* — Een ieder die in staat is bij decryptie hulp te verlenen en die weigert zulks te doen, wordt gestraft met gevangenisstraf van een jaar tot vijf jaar en met geldboete van honderd frank tot vijfduizend frank.

*Art. 90quinquies decies.* — § 1. De onderzoeksrechter kan alleen gebruik maken van de hulp bij decryptie:

1° om die berichten te ontcijferen waarvoor de hulp is gevorderd;

2° tijdens de bewakingsperiode waarvoor de hulp is gevraagd en ten hoogste voor één maand.

De onderzoeksrechter kan deze periode evenwel bij met redenen omklede beschikking eenmaal of meermalen verlengen met een termijn die niet langer mag zijn dan één maand. De bewakingsperiode mag niet meer dan zes maanden bedragen onverminderd de beslissing van de onderzoeksrechter om aan de maatregel een einde te maken zodra de omstandigheden die deze gewettigd hebben, verdwenen zijn.

§ 2. Indien de onderzoeksrechter voor de hulp die bij decryptie is verleend, een ontcijferings sleutel in zijn bezit heeft gehad, moet die vernietigd worden onmiddellijk na het ontcijferen van de berichten bedoeld in § 1, 1°, of na het verstrijken van de periode of de verlenging van de periode bedoeld in § 1, 2°.

*Art. 90sexies decies.* — Berichten die zijn ontcijferd via de maatregelen genomen met toepassing van artikel 90duodecies, worden overgeschreven en bewaard overeenkomstig artikel 90septies van dit Wetboek.

*Art. 90septies decies.* — Ontcijferde berichten die onder het beroepsgeheim vallen, worden niet opgetekend in het proces-verbaal.

*Art. 90octies decies.* — Een bericht ontvangen of verstuurd door een advocaat of een arts mag alleen dan ontcijferd worden indien deze er zelf van wordt verdacht een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd of eraan te hebben deelgenomen, of indien precieze feiten doen vermoeden dat derden die een bericht hebben gestuurd, ervan verdacht worden een van de strafbare feiten bedoeld in artikel 90ter te hebben gepleegd.

§ 9. Le juge qui aura reçu l'aide au décryptage, en conséquence des §§ 7 et 8, enverra tous les éléments de cette aide clos et cachetés au juge d'instruction du tribunal saisi de l'affaire.

*Art. 90quater decies.* — Toute personne à même de fournir l'aide au décryptage, et qui refuse de fournir cette aide, est punie d'un emprisonnement d'un an à cinq ans et d'une amende de cent francs à cinq mille francs.

*Art. 90quinquies decies.* — § 1<sup>er</sup>. Le juge d'instruction ne peut faire usage de l'aide au décryptage que:

1° pour procéder au décryptage des messages pour la compréhension desquels l'aide a été requise;

2° pour la période de surveillance pour laquelle l'aide a été demandée et, au plus, pour une durée d'un mois.

Le juge d'instruction peut toutefois prolonger cette période, par ordonnance motivée, pour un ou plusieurs nouveaux termes qui ne peuvent chacun dépasser un mois. La période de surveillance ne peut dépasser un maximum de six mois, sans préjudice de la décision du juge d'instruction de mettre fin à la mesure dès que les circonstances qui l'ont justifiée ont disparu.

§ 2. Si, en vue de l'aide au décryptage, le juge d'instruction a été en possession d'une clé de décryptage, cette clé doit être détruite immédiatement après le décryptage des messages visés au § 1<sup>er</sup>, 1°, ou après l'expiration de la période ou de la prolongation de la période visée au § 1<sup>er</sup>, 2°.

*Art. 90sexies decies.* — Les messages décryptés grâce aux mesures prises en application de l'article 90duodecies sont retranscrits et conservés conformément à l'article 90septies du présent Code.

*Art. 90septies decies.* — Les messages décryptés couverts par le secret professionnel ne sont pas consignés au procès-verbal.

*Art. 90octies decies.* — Le décryptage d'un message reçu par ou transmis par un avocat ou un médecin ne peut avoir lieu que si celui-ci est lui-même soupçonné d'avoir commis une des infractions visées à l'article 90ter ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers ayant communiqué un message sont soupçonnés d'avoir commis une des infractions visées à l'article 90ter.

De maatregel kan niet ten uitvoer worden gelegd zonder dat de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren, naar gelang van het geval, daarvan op de hoogte is gebracht. Aan diezelfde personen wordt door de onderzoeksrechter meegedeeld welke informatie in het ontcijferde bericht onder het beroepsgeheim valt en niet wordt opgetekend in het proces-verbaal.»

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments du message décrypté qu'il estime relever du secret professionnel et qui ne seront pas consignés au procès-verbal.»

Michèle BRIBOSIA-PICARD.  
Lydia MAXIMUS.