KONINKRIJK BELGIE

1000 Brussel,
Postadres : Ministerie van Justitie
Waterloolaan 115
Kantoren : Regentschapsstraat 61
Tel. : 02 / 542.72.00
Fax : 02 / 542.72.12

COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

ADVIES Nr 17 / 97 van 9 juli 1997

O. ref. : 10 / A / 97 / 009

BETREFT : Toepassing van de artikelen 202 en 203 van de wet van 21 december 1994 houdende sociale bepalingen (technische medewerking van de operatoren met oog op uitvoering van gerechtelijke maatregelen van afluisteren e.d.)

De Commissie voor de bescherming van de persoonlijke levenssfeer,

Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, inzonderheid op artikel 29;

Gelet op de mondelinge aanvraag van de heer adjunct-kabinetschef van de heer Minister van Justitie, ontvangen op 2 april 1997;

Gelet op het verslag van de heer B. DE SCHUTTER,

Brengt op 9 juli 1997 het volgende advies uit :

I. VOORWERP VAN DE ADVIESAANVRAAG

---

1. Door de Minister van Justitie is aan de Commissie een advies gevraagd over de wijze waarop uitvoering gegeven zou kunnen worden aan de artikelen 70bis en 95, 5°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij de wet van 21 december 1994 houdende sociale en diverse bepalingen.

De adviesaanvraag blijkt mede geïnspireerd te zijn door een schriftelijke vraag die de heer volksvertegenwoordiger Decroly i.v.m. de interpretatie van de voornoemde artikelen op 24 januari 1997 aan de Minister gesteld heeft ([1]).

II. DE BEPALINGEN DIE HET VOORWERP VAN HET ADVIES VORMEN

---

2. Artikel 70bis van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, ingevoegd bij artikel 202 van de wet van 21 december 1994, luidt als volgt :

> "De Koning bepaalt, bij een in Ministerraad overlegd besluit, de technische middelen waarmee Belgacom en de door Hem aangewezen uitbaters van de niet-gereserveerde diensten, in voorkomend geval, eventueel gezamenlijk, moeten instaan om het opsporen, afluisteren, kennisnemen en opnemen van privé-telecommunicaties onder de voorwaarden bepaald door de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en - telecommunicatie, mogelijk te maken".

Artikel 95 van de wet van 21 maart 1991 bepaalt dat de Minister bevoegd voor de aangelegenheden die de telecommunicatie betreffen, op voorstel van het Belgische Instituut voor Postdiensten en Telecommunicatie, in een aantal gevallen de goedkeuring van een eindapparaat kan intrekken of een verbod kan opleggen om op de openbare telecommunicatie-infrastructuur aangesloten te blijven. Aan de lijst van gevallen is bij artikel 203 van de wet van 21 december 1994 een vijfde geval (art. 95, 5°) toegevoegd. Voortaan zijn de bedoelde intrekking en het bedoelde verbod ook mogelijk "wanneer blijkt dat : ... 5° het eindapparaat de middelen ondoeltreffend maakt die het opsporen, afluisteren, kennisnemen en opnemen van privé-telecommunicatie onder de voorwaarden bepaald door de artikelen 88 bis en 90 ter tot 90 decies van het Wetboek van Strafvordering mogelijk maken".

---

[1] Vraag nr. 474, Parl. Vr. en Antw., Kamer, 1996-97, 9634.

3. Beide genoemde bepalingen strekken ertoe de uitvoerbaarheid te waarborgen van de artikelen 88bis en 90ter tot 90decies van het Wetboek van Strafvordering, ingevoegd bij de wet van 30 juni 1994. Die laatste bepalingen verlenen aan de onderzoeksrechter de bevoegdheid om, onder bepaalde voorwaarden, de nummers op te sporen van binnenkomende en uitgaande oproepen (art. 88 bis) of om privé-communicatie en telecommunicatie af te luisteren, ervan kennis te nemen en ze op te nemen (artt. 90 ter tot 90 decies). Met artikel 70 bis van de wet van 21 maart 1991 wordt beoogd de operatoren tot medewerking te verplichten, opdat zij de "afluisterbaarheid" van hun infrastructuur, toestellen en diensten zouden waarborgen ([2]). Artikel 95, 5° van de wet van 21 maart 1991 is bedoeld om te vermijden dat vercijferingsmateriaal, dat op de markt beschikbaar is, de tenuitvoerlegging van een door de onderzoeksrechter bevolen onderzoeksmaatregel onmogelijk zou maken ([3]).

Zoals o.m. uit de schriftelijke vraag van de heer Decroly blijkt, rijst de vraag of het met toepassing van de genoemde wetsbepalingen mogelijk of wenselijk is om het gebruik van vercijferingssystemen (cryptografie) volledig te verbieden, dan wel om met andere middelen de uitvoerbaarheid van een afluistermaatregel te verzekeren ([4]).

Die kwestie vormt het ontwerp van het voorliggende advies.

III. ALGEMENE BESCHOUWINGEN INZAKE CRYPTOGRAFIE

A. Begrippen

4. Encryptie is de procedure waarbij klare, leesbare gegevens (tekst, data, figuren), ongeacht de informatiedrager, door middel van een wiskundige berekening worden versleuteld in gecodeerde gegevens. Decryptie is deze procedure in omgekeerde richting. Encryptie en decryptie geschieden door middel van bepaalde sleutels en algoritmes, d.i. nauwkeurig gedefinieerde wiskundige regels om een gesteld resultaat te verkrijgen uit een eindig aantal bewerkingen.

5. In het algemeen worden drie soorten cryptosystemen (naam gegeven aan de combinatie van algoritme en sleutel) onderscheiden. Deze worden hierna kort vermeld.

5.1. het symmetrische (secret key) cryptosysteem

Hier wordt dezelfde sleutel gebruikt voor en- en decryptie. Deze sleutel moet bijgevolg geheim blijven. Deze systemen zijn snel maar functioneren, door de unieke sleutel, enkel in een gesloten systeem waarin partijen elkaar kennen en vertrouwen.

Voorbeelden van algemeen bekende algoritmen zijn IDEA en DES.

---

[2] Memorie van toelichting bij het ontwerp dat geleid heeft tot de wet van 21 december 1994, Parl. St., Senaat, 1994-95, nr. 1218-1, p. 88.

[3] Zelfde memorie van toelichting, p. 89.

[4] Zie, benevens de vraag van de heer Decroly, ook de mondelinge vraag van mevrouw Bribosia-Picard en het antwoord van de heer De Clerck, Minister van Justitie, Parl. Hand., Senaat, 9 mei 1996, pp. 1032-1033 (infra, nr. 17).

5.2. het asymmetrische (public key) systeem.

Hier gebruikt men verschillende sleutels voor encryptie en voor decryptie, een private en een publieke sleutel. Deze methode staat toe dat de publieke sleutel bekendgemaakt wordt, zodat iedereen een bericht gesleuteld kan versturen (met de publieke sleutel van de bestemmeling) maar alleen de bestemmeling (met zijn private sleutel) het kan ontcijferen. Deze methode kan, door de strikte geheimhouding van de private sleutel, in een open netwerk gehanteerd worden, het systeem werkt echter langzamer dan een symmetrisch systeem, en het is ook duurder.

Deze methode wordt aangewend voor het genereren van digitale handtekeningen, wat de authentificatie van boodschap en verzender toelaat. In dit geval wordt de informatie versleuteld met behulp van de private sleutel en ontcijferd met behulp van de publieke.

Een voorbeeld van een asymmetrisch cryptosysteem is RSA (het Rivest-Shamir-Adelman publieke sleutel algoritme).

5.3. de hybride systemen

De voor-en nadelen van beide genoemde systemen maken dat ze in de praktijk vaak complementair gebruikt worden in systemen die de voordelen van beide in zich dragen.

Een illustratie hiervan is het softwarepakket PGP (Pretty Good Privacy) van Phil Zimmerman, verkrijgbaar en gebruikt op het Internet.

6. Van belang is ook dat cryptosystemen zowel op het niveau van hardware als software te verkrijgen zijn - sommige zijn zelfs een combinatie van beide - en dat men wat sleutelsystemen betreft nog verdere onderverdelingen kan maken: zo zijn er o.m. systemen die gebruik maken van" random keys", wat inhoudt dat zij om de paar seconden van sleutel veranderen, of van "session keys", wat inhoudt dat de (symmetrische) sleutel na iedere communicatiesessie veranderd wordt.

B. Functies van cryptografie

7. Dit advies beperkt zich tot de mogelijkheden van de cryptografie om de vertrouwelijkheid van een boodschap te garanderen. Voor het debat rond vercijfering is het primordiaal zich bewust te zijn van de andere functies die de cryptografie in de informatiemaatschappij kan vervullen. Deze zijn met name :

- het waarborgen de integriteit van het bericht, d.i. ervoor zorgen dat het aangekomen bericht identiek is aan het verstuurde;
- het waarborgen van de identificatie en de authenticiteit van het bericht en de verzender ervan : het verschaffen van zekerheid omtrent de identiteit van de afzender en omtrent het feit dat het wel degelijk hij is die het bericht verstuurd heeft; in dit kader speelt de digitale handtekening een grote rol;
- het zorgen voor de “niet-verwerping” (non-repudiation) van het bericht : in juridisch opzicht belangrijk omdat men t.a.v. derden een aantal hoedanigheden van het bericht kan bewijzen.

De evolutie gaat dan ook in de richting van de zgn. “dual-use keys”, die zowel voor integriteit-authenticiteit-identificatie als voor confidentialiteit gebruikt zullen worden.

Bij het onderzoek naar de vraag omtrent de wijze waarop kan vermeden worden dat encryptie ertoe leidt dat de overheidsopdracht ter bestrijding van de criminaliteit wordt bemoeilijkt of onmogelijk gemaakt, dient dus niet alleen aandacht te worden besteed aan het spanningsveld met de beveiliging van de informatie en bescherming van de persoonlijke levenssfeer, waarover in dit advies essentieel wordt gehandeld. Zoals zonet aangegeven, worden asymetrische encryptiesystemen ook steeds meer gebruikt voor het genereren van elektornische handtekeningen waardoor de zekerheid wordt verkregen omtrent het feit dat een welbepaalde persoon een bericht heeft verstuurd. Indien de algoritmen en sleutels voor het genereren van deze elektronsiche handtekeningen gekend kunnen worden door andere personen dan diegenen waartoe de elektronische handtekening behoort, kunnen deze personen zich aldus voordoen en rechtshandelingen stellen in naam van de titularis van de elektronische handtekening. Dit kan ertoe leiden dat in het rechtsverkeer heel wat onzekerheden ontstaan.

Om al deze redenen is het gebruik van encryptie een essentieel element geworden in het gegevensverkeer, ter vrijwaring tegen ongeoorloofde toegang tot de gegevens. Zulke vrijwaring kan o.m. ingegeven zijn door de bescherming van de persoonlijke levenssfeer. De encryptie komt echter voor in alle sectoren van gegevensverwerking, zoals bijv. het electronisch handelsverkeer, de internationale transacties of het hele Internetgebeuren.

8. De waarborg van vertrouwelijkheid door encryptie geboden - en zodoende haar deugdelijkheid om het privé-leven van de burger te beschermen - komt echter lijnrecht te staan tegenover de onmacht van de overheid om in bepaalde omstandigheden bruikbare - d.i. leesbare - informatie te bekomen in het raam van de uitoefening van haar opdrachten, in het bijzonder bij de bestrijding van ernstige vormen van criminaliteit, vooral in een grensoverschrijdend kader. Ook de georganiseerde criminaliteit (drughandel, witwasactiviteiten, ...) hanteert immers encoderingsmethoden om transacties te doen of boodschappen over te zenden.
De vraag is dus hoe een evenwicht gevonden kan worden tussen, enerzijds, het recht op eerbiediging van het privé-leven, en anderzijds, de noodzaak van een inmenging van het openbaar gezag, in een democratische samenleving, in het belang van de openbare veiligheid, de openbare orde en het voorkomen van strafbare feiten.

IV. NORMATIEF KADER

A. Grondrecht op eerbiediging van het privé-leven.

9. Het recht op eerbiediging van het privé-leven wordt gewaarborgd bij artikel 17 van het Internationaal Verdrag inzake burgerlijke en politieke rechten, artikel 8 van het Europees Verdrag over de rechten van de mens en artikel 22 van de Grondwet.

Vooral artikel 8 van het Europees Verdrag, met inbegrip van de jurisprudentie die daarover ontwikkeld is door het Europees Hof voor de Rechten van de Mens, o.m. inzake afluisteractiviteiten, verschaft een aantal toetsstenen bij het zoeken naar het hiervóór genoemde evenwicht tussen het recht van het individu op de bescherming van zijn persoonlijke levenssfeer en het belang van een democratische samenleving bij een efficiënte misdaadbestrijding.

10. Opdat een inmenging in het recht op eerbiediging van het privé-leven geoorloofd zou zijn, dient zij aan een aantal voorwaarden te beantwoorden.

10.1. De inmenging dient in de eerste plaats "bij de wet voorzien" te zijn. Met betrekking tot afluistermaatregelen betekent zulks dat de wet de volgende bepalingen moet bevatten :

1°- aanwijzing van de categorieën personen wier telefoon kan worden afgeluisterd evenals van de misdrijven waarvoor zulks is toegestaan;
2°- beperking in de tijd van de toelating tot telefoontap;
3°- regels inzake het opstellen van processen-verbaal van afgeluisterde gesprekken;
4°- het voorzien in de integrale en ongeschonden terbeschikkingstelling van de afgeluisterde gesprekken aan rechter en verdediging;
5°- de nodige controlemaatregelen en rechtsmiddelen tegen de onderzoeksmaatregel;
6°- bepaling van de taak en de verantwoordelijkheid van de rechter die de maatregel beveelt;
7°- verbod van trucage, misleidingen en provocaties door middel van taps;
8°- eerbiediging van het vertrouwelijk verkeer tussen een verdachte en zijn raadsman (advocaat, arts);

10.2 De inmenging moet voorts gericht zijn op een of meer van de oogmerken die in artikel 8, lid 2, opgesomd zijn.

In verband met de misdaadbestrijding dient in het bijzonder melding gemaakt te worden van de bescherming van de openbare orde en het voorkomen van strafbare feiten.

10.3 Ten slotte moet de inmenging "nodig" zijn, in een democratische samenleving, om een van de hiervoor bedoelde wettige oogmerken te bereiken.

Volgens het Europees Hof betekent zulks dat de beperking van het recht op eerbiediging van het privé-leven moet beantwoorden aan een dwingende maatschappelijke behoefte. Bovendien dient die beperking te beantwoorden aan de evenredigheidsvereiste : er dient, zoals gezegd, een billijk evenwicht te bestaan tussen de rechten van het individu en de belangen van de samenleving ([5]).

B. Artikelen 90 ter tot 90 decies van het Wetboek van Strafvordering

11. De mogelijkheid om privé-communicatie en telecommunicatie af te luisteren en op te nemen (art. 90 ter tot 90 decies Sv.) is, zoals gezegd, ingevoerd bij de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en telecommunicatie.

De voornoemde wetsbepalingen expliciteren en verstreken het verbod op het afluisteren van telefoongesprekken. Tezelfdertijd bepalen zij dat afwijkingen van dit verbod mogelijk zijn, en stellen zij de voorwaarden daartoe vast.

---

[5] Zie, o.m., E.H.R.M., 19 februari 1997, Laskey, Jaggard en Brown, § 42 te verschijnen in Rec, 1997.

Aan de bij artikel 8, lid 2, EVRM gestelde vereisten voor de kwaliteit van een wet die rechtsgrond biedt voor de inmenging in het privé-leven, lijkt voldaan te zijn. De genoemde wetsbepalingen voorzien immers in een aantal waarborgen voor de persoon die het voorwerp is van een gerechtelijke afluistermaatregel :

- wat de specificiteit betreft : de persoon, het communicatie-of telecommunicatiemiddel of de plaats die het voorwerp is van de bewaking moet aangegeven zijn in de beschikking van de onderzoeksrechter (art. 90 quater, § 1, tweede lid, 3°) en de maatregel kan maar bevolen worden t.a.v. een limitatieve lijst misdrijven (art. 90 ter, § 2);
- wat de tijdsbeperking betreft : de bewakingsmaatregel kan slechts uitwerking hebben gedurende één maand te rekenen van de beslissing waarbij de maatregel wordt bevolen (art. 90 quater, § 1, tweede lid, 4°), zij het dat die maatregel telkens verlengd kan worden (art. 90 quinquies);
- wat de notulering betreft : gegevens door de maatregel verkregen worden enkel in een proces-verbaal vermeld voor zover zij van belang zijn voor het onderzoek (art. 90 sexies);
- wat de terbeschikkingstelling betreft : de opnames, zelfs die passages uit de afgeluisterde conversatie die geen relevantie hebben voor het gevoerde onderzoek, dienen overgeschreven te worden;
- de integrale overschrijving en eventuele vertaling worden onder verzegelde omslag ter griffie bewaard, en daarvan wordt melding gemaakt in een register (art. 90 septies) ([6]);
- wat de controle betreft : de door de onderzoeksrechter verleende machtiging moet met redenen omkleed zijn en dient, op straffe van nietigheid, een aantal vermeldingen te bevatten (art. 90 quater, § 1), hetgeen een rechtelijke toetsing mogelijk maakt; voorts is een parlemtaire controle mogelijk doordat de Minister van Justitie elk jaar aan het Parlement verslag uitbrengt over de toepassing van de betrokken bepalingen (art. 90 decies);
- wat de taak van de rechter betreft : aan de onderzoeksrechter wordt een centrale rol toebedeeld;
- wat het correct karakter van de opname betreft : de partijen kunnen de juistheid van de opname eventueel betwisten aan de hand van de opname zelf en de overschrijving ervan (art. 90 septies);
- wat de confidentialiteit betreft : behoudens uitzonderingen kan de maatregel niet worden toegepast op artsen en advocaten (art. 90 octies), en worden gegevens gedekt door het beroepsgeheim niet opgetekend in het proces-verbaal (art. 90 sexies).

12. Relevant voor de beoordeling van de verscheidene beleidsopties inzake cryptografie is dat de hele structuur en de hele opzet van de Belgische afluisterwetgeving het "verkennend" afluisteren verbieden. Dit blijkt uit het gegeven dat de onderzoeksrechter slechts tot deze maatregel kan besluiten nádat hij met een gerechtelijk onderzoek belast werd en de betrokken personen ervan verdacht worden feiten gepleegd te hebben die omschreven kunnen worden als een van de specifiek genoemde misdrijven (art. 90 ter, §§ 1 en 2).

---

[6] Het vereiste van volledige overschrijving van de afgeluisterde gesprekken zou in de toekomst afgeschaft worden (zie de artikelen 8 en 9 van het wetsontwerp tot wijziging van de wet van 30 juni 1994 , Parl. St., Kamer, 1996-97, nr. 1075-1). In haar advies nr. 09/97 van 20 maart 1997 over het betrokken wetsontwerp zag de Commissie geen bezwaar tegen die vereenvoudiging.

C. Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

13. De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens is pertinent, zelfs na het uitvaardigen van de wet van 30 juni 1994.

Artikel 16, § 3, van de wet van 8 december 1992 luidt immers als volgt :

> "Om de veiligheid van de persoonsgegevens te waarborgen, moet de houder van het bestand, of in voorkomend geval zijn vertegenwoordiger in België, de gepaste technische en organisatorische maatregelen treffen, die nodig zijn voor de bescherming van de bestanden tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking van persoonsgegevens.
> Deze maatregelen moeten een passend beveiligingsniveau verzekeren, rekening houdend, enerzijds, met de stand van de techniek terzake en de kosten voor het toepassen van de maatregelen en, anderzijds, met de aard van de te beveiligen gegevens en de potentiële risico's.
> Op advies van de Commissie voor de bescherming van de persoonlijke levenssfeer kan de Koning voor alle of voor bepaalde categorieën van verwerkingen aangepaste normen inzake informaticaveiligheid uitvaardigen".

In de verplichting om passende bevestigingsmaatregelen te nemen wordt overigens ook voorzien bij artikel 7 van het Europees Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens en bij artikel 17 (“Beveiliging van de verwerking”) van de richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Die bepalingen, gaan ook uit van het ""BATNEEC"-principe" ("Best available technology not entailing excessive costs").

V. UITVOERING VAN DE ARTIKELEN 70BIS EN 95, 5° VAN DE WET VAN 21 MAART 1991

A. Onduidelijke bepalingen

14. Artikel 70bis van de wet van 21 maart 1991 moet gelezen worden in samenhang met artikel 90 quater, §2, eerste lid, van het Wetboek van Strafvordering. Die laatste bepaling luidt als volgt : "Indien de (afluister)maatregel een bewerking op een communicatienetwerk inhoudt, is de operator van dit netwerk ertoe gehouden zijn technische medewerking te verlenen, wanneer de onderzoeksrechter hierom verzoekt." Uit de gezamenlijke lezing van beide artikelen kan de verplichting voor de operatoren afgeleid worden om te zorgen dat hun infrastructuur, hun toestellen en hun diensten afluisterbaar zijn.

Op dit ogenblik is echter nog geen koninklijk besluit ter uitvoering van artikel 70bis genomen. De operatoren blijven dus in het ongewisse omtrent de technische kenmerken die hun toestellen moeten bezitten om afluisterbaar te zijn.
Bovendien worden in de wet de omvang van de verplichtingen van Belgacom en de uitbaters van de niet-gereserveerde diensten niet nader gepreciseerd. Dit brengt mee dat de nakoming van de wettelijk opgelegde verplichtingen moeilijk afgedwongen kan worden.

15. Ook artikel 95,5°, van de wet van 21 maart 1991 geeft aanleiding tot heelwat discussies.

Ten eerste is er de beperking van de bepalingen tot "eindapparaten", terwijl encryptie niet enkel als hardware, maar ook als software aangeboden kan worden. Zo is het gekende PGP een softwarepakket.
Een tweede probleem is zoals bij artikel 70bis, dat er geen precisering is van de technische normen die nodig zijn om een apparaat afluisterbaar te maken.([7])
De loutere bepaling dat een eindapparaat de afluistermiddelen niet "ondoeltreffend" mag maken, is niet erg duidelijk.
Ten eerste kan men stellen dat encryptie de middelen niet ondoeltreffend maakt indien men een opgenomen communicatie nadien kan decrypteren, zulks naar analogie met een communicatie in een vreemde taal waarvoor de afluisterwet ook geen specifiek regime uitwerkt maar enkel bepaalt dat de opname vertaald moet worden. Bovendien schept de uitdrukking "ondoeltreffend maken" dezelfde moeilijkheden t.a.v. andere telecomprotocols (EDIFACT, samendrukking) waarbij men, naargelang de invalshoek, al dan niet kan besluiten dat ze de middelen ondoeltreffend maken.

16. Artikel 70bis van de wet van 21 maart 1991, gelezen in samenhang met artikel 90 quater, §2, van het Wetboek van Strafvordering, verplicht Belgacom en de aanbieders van de niet-gereserveerde diensten hun infrastructuur, toestellen en diensten afluisterbaar te houden. Vertaald naar de cryptografie betekent dit dat Belgacom en de aanbieders van de niet-gereserveerde diensten aan hun klanten dus enkel cryptografie kunnen aanbieden die te allen tijde gedecrypteerd kan worden. Artikel 95,5° van de wet van 21 maart 1991 maakt het voorts mogelijk om het aanbieden van cryptografie in eindapparaten aan banden te leggen.
De Belgische wetgeving laat aldus een belangrijke vraag onbeantwoord: wat met de gebruiker die zich - bijvoorbeeld via Internet - encryptiesoftware (bijvoorbeeld Pretty Good Privacy) aanschaft en zijn signaal vervolgens zelf geëncrypteerd bij Belgacom of een andere aanbieder aanlevert ? Kan men stellen, uitgaande van een zeer ruime interpretatie van artikel 70bis, dat Belgacom en de andere aanbieders in een dergelijk geval aan het signaal de toegang tot hun netwerk moeten ontzeggen?
Dit zou natuurlijk op een gedeeltelijk verbod van cryptografie in België neerkomen en het probleem inzake de compatibiliteit van artikel 70bis met artikel 8.2 EVRM scherp stellen. Cryptografiewetgeving moet immers, net als de afluisterwetgeving zelf, aan de criteria van artikel 8.2 EVRM voldoen. Indien men daarentegen aanneemt dat de operatoren in het bedoelde geval de toegang tot hun netwerk niet moeten verbieden, komt men tot de vaststelling dat er een moeilijk te verantwoorden verschil in behandeling zou zijn tussen de gebruiker die zich, via de traditionele weg of via het Internet, een software encryptiepakket heeft aangeschaft, en die ongemoeid wordt gelaten, en de gebruiker die zijn encryptiefaciliteiten via zijn telecomoperator heeft verkregen, en die ermee rekening dient te houden dat deze operator de middelen tot decryptie steeds ter beschikking van de gerechtelijke overheid moet houden.

---

[7] De Commissie merkt op dat de Minister die bevoegd is voor de telecommunicatie op grond van artikel 94, §2, van de wet van 21 maart 1991 de technische specificaties zou kunnen vaststellen waaraan eindapparaten moeten beantwoorden. Wanneer dan zou blijken dat een eindapparaat niet meer beantwoordt aan zulke specificaties, zou de goedkeuring ervan op grond van artikel 95,2°, ingetrokken kunnen worden. In dat geval zou de intrekking niet moeten steunen op de vage bepaling van artikel 95,5°.

B. Standpunt van de regering ten aanzien van de uitvoering van de artikelen 70bis en 95,5°

17. Ten tijde van de parlementaire voorbereiding van de wet van 21 december 1994, waarbij de artikelen 70bis en 95, 5°, in de wet van 21 maart 1991 zijn ingevoegd, gaf de Minister van Verkeerswezen toe dat het op dat ogenblik nog niet duidelijk was op welke wijze ervoor gezorgd moest worden dat de telefoongesprekken afluisterbaar zouden zijn.[8]

In antwoord op een mondelinge vraag van senator Bribosia-Picard gaf de Minister van Justitie op 9 mei 1996 wel een aantal aanwijzingen i.v.m. mogelijke middelen, zonder evenwel duidelijk voor een of andere mogelijkheid te opteren. Uit het antwoord van de Minister blijkt dat hij geen voorstander is van een algemeen verbod van cryptografie, en evenmin van het systematisch deponeren van de sleutels bij een daartoe aangewezen instantie (het Belgisch Instituut voor Postdiensten en Telecommunicatie). Volgens de Minister zou bij voorkeur gestreefd moeten worden "naar een maximale toegankelijkheid van de netwerken in samenwerking met de sleutelbeheerders, de zogenaamde trusted third party, een derde die de verbinding kan vormen en de toegang kan creëren tot het netwerk, de operator, de netwerkbeheerder". Ook de "samenwerking met de operatoren van de telecommunicatie-infrastructuur" wordt in het vooruitzicht gesteld.[9]

C. Bespreking van een aantal mogelijke beleidsopties, inzonderheid vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer.

a. Verbod van cryptografie.

18. Een verbod van cryptografie -dat wat gestrengheid betreft, ook nog gradaties kan kennen ([10]) - is om diverse redenen moeilijk houdbaar.

Ten eerste zou het verbod zeer moeilijk te handhaven zijn gezien de enorme (en steeds groeiende) hoeveelheid communicatie die plaatsvindt, gezien het steeds groeiend aandeel van de internationale communicatie hierin en gezien de beschikbaarheid van cryptografie via kanalen die, zoals het Internet, (voorlopig?) aan de controle van de overheid ontsnappen. In landen waar een totaal verbod op cryptografie geldt (zoals Saoedi-Arabië), of zelfs maar een gedeeltelijk verbod, (zoals Zuid-Afrika : verbod om te encrypteren op het publieke telefoonnetwerk), wordt dit verbod trouwens op grote schaal genegeerd. Het lijkt uitgesloten voor een land om op dit gebied "cavalier seul" te spelen.

Door zulk een verbod zou men de ontwikkeling van de informatiemaatschappij, gezien de belangrijke rol van cryptografie hierin bovendien, in aanzienlijke mate afremmen. Niet alleen het garanderen van de vertrouwelijkheid van berichten zou bemoeilijkt worden; met een verbod van cryptografie zouden het publiek en de bedrijfswereld ook nog andere toepassingen van de cryptografie - waaronder de authentificatie ontzegd worden.
Een verbod zou concurrentienadelen voor de bedrijven creëren. Het zou ook problemen van privaatrechtelijke aard scheppen daar het gebrek aan voldoende veiligheid in geval van schade als een onzorgvuldig handelen of een nalatigheid (onrechtmatige daad) beschouwd kan worden en aanleiding kan geven tot een aansprakelijkheidseis. Dit zou uiteindelijk ook de

---

[8]Verslag van mevrouw Cahay-Andre, Parl. St., Senaat, 1994-95, nr. 1218-9, p. 5; verklaring van de heer Di Rupo, Minister van Verkeerswegen, Parl. Hand., Senaat, 1 december 1994, p. 442.

[9]Verklaring van de heer De Clerck, Minister van Justitie, Parl. Hand., Senaat, 9 mei 1996, p. 1032.

[10]Men kan onderscheiden : verbod op het voorhanden hebben of in voorraad hebben van cryptografie; verbod op het ter verspreiding voorhanden hebben of het ter verspreiding aanbieden van cryptografie; verbod op het openbaar maken of het publiek aanbieden van cryptografie.

aansprakelijkheid van de overheid in het gedrang kunnen brengen.

Verder zou een dergelijk verbod noch de toetsing aan het pertinentiecriterium, zoals ontwikkeld door het Europees Hof van de Rechten van de Mens op basis van artikel 8.2 EVRM, noch de toetsing aan het door hetzelfde Hof op basis van hetzelfde artikel ontwikkelde evenredigheidscriterium doorstaan. Een geïsoleerd verbod op cryptografie is immers niet pertinent, daar het inefficiënt zou zijn (zie supra), het is ook volkomen disproportioneel, zelfs waar het uitsluitend een verbod op "confidentialiteitscryptografie" zou betreffen, daar men een gigantisch aantal potentiële gebruikers het middel om de vertrouwelijkheid van hun communicatie te garanderen zou ontzeggen, om in een beperkt aantal gevallen de communicatie te kunnen afluisteren.

Specifiek voor België valt een verbod op cryptografie zeer moeilijk te rijmen met de verplichtingen voor de houder van een bestand zoals bepaald in artikel 16, §3, van de wet van 8 december 1992. De Commissie meent ten slotte de aandacht te moeten vestigen op het feit dat een Nederlands voorlopig voorontwerp tot verbod van cryptografie, na massaal protest door de regering is ingetrokken.

b. Verbod van bepaalde sterke vormen van cryptografie.

19. Tegen een beperkt verbod pleiten grosso modo dezelfde argumenten als tegen een totaal verbod.

Bovendien loopt men hier nog meer het risico de georganiseerde misdaad in de kaart te spelen i.p.v. ze te beteugelen : criminelen zullen dit verbod negeren en hun communicatie door onbreekbare crypto beschermd zien, terwijl het tegelijkertijd voor hen makkelijker zal zijn om toegang te hebben tot informatie van bedrijven (en particulieren) die als goede "(corporate) citizens" hun informatie slechts met de zwakkere encryptietoepassingen (mogen) versleutelen.

Een aanpak gesteund op een beperkt verbod zou bovendien een constante monitoring vergen van de evoluties op het terrein, en zou een soepele procedure vereisen om de normen daaraan aan te passen.

c. Sleuteldepot.

20. Het sleuteldepot, in het Engels ook wel “recovery” of “key escrow” genoemd, houdt in dat men de decryptiesleutels hetzij bij de overheid deponeert (zie o.m. het Amerikaanse Clipper Chip I voorstel), hetzij een derde (een Trusted Third Party, zie o.m. de huidige Franse wet en het Amerikaanse Clipper Chip II) hetzij zelf bijhoudt, maar dan wel totaal onafhankelijk van de gebruikers in het bedrijf ("self-escrow", zie o.m. Clipper Chip III).
De technische problemen en kosten die zulk systeem met zich zou meebrengen zijn enorm. De ultima ratio van ieder sleuteldepotsysteem moet immers een wereldwijde toepassing ervan zijn. Bovendien worden de grootste sleutelbeheerproblemen juist gecrëerd door die systemen die de kleinste inmenging in de privacy inhouden, met name de systemen met wisselende en/of sessiesleutels, die het immers mogelijk kunnen maken om de decryptering te beperken tot één bepaalde communicatie of zelfs tot een bepaald onderdeel ervan.

21. In een recent rapport van 27 mei 1997, getiteld "The Risks of Key Recovery, Key Escrow and Trusted Third-party Encryption"[11], formuleren een aantal specialisten (professoren en onderzoekers van MIT en Cambridge en specialisten van Sun, Microsoft en AT&T) het zo: "Key recovery as envisioned by law enforcement will require the deployment of secure infrastructures involving thousands of companies, recovery agents, regulatory bodies, and law enforcement agencies worldwide interacting and cooperating on an unprecedented scale" en verder : "The commercial and academic world simply does not have the tools to properly analyse or design the complex systems that arise from key recovery".
Tevens kan men denken aan de kosten die het runnen van "recovery agents" met zich zal brengen; dezen zullen immers de klok rond, zeven dagen op zeven, bemand moeten zijn om de responstijd te halen die nu in de verscheidene voorstellen vooropgesteld wordt - in het Amerikaanse voorstel moeten de sleutels bekomen kunnen worden binnen de twee uur, in het Britse zelfs binnen het uur.
Dat bovendien deze recovery-agents zelf het slachtoffer van aanvallen zullen worden, is niet moeilijk in te beelden.

Het argument dat deze "recovery agents" in het kader van gerechtelijke procedures ook voor de bedrijven van nut kunnen zijn, snijdt volgens de auteurs van het rapport geen hout.
Voorstanders hadden geopperd dat ook de bedrijven nood hebben aan “key-recovery” faciliteiten, bijvoorbeeld bij verlies of diefstal van een sleutel of bij de weigering van een ex-werknemer om zijn sleutels vrij te geven. De auteurs onderkennen deze nood, maar zeggen dat de "law enforcement key recovery" hieraan niet kan bijdragen omdat de behoeften van bedrijven en overheid in dit opzicht totaal verschillend zijn en de systemen dus maar weinig gemeen zouden hebben.

Zo stellen zij :

a) dat de bedrijfswereld alleen maar baat heeft bij het recupereren van sleutels voor opgeslagen data, terwijl "law enforcement" voordeel heeft bij de recuperatiemogelijkheid van alle sleutels, in het bijzonder deze gebruikt om communicatiesessies te versleutelen;
b) dat het bedrijfsleven geen enkele baat heeft bij de recupereerbaarheid van authentificatie of digitale handtekening sleutels en dat dit zelfs bepaalde concepten, zoals de niet-verwerping, in gevaar kan brengen, terwijl het zeer moeilijk is om dit soort sleutels uit te sluiten uit een "key recovery" systeem, gezien het bestaan van "dual-use keys";
c) dat de bedrijfswereld voor de "electronic commerce" behoefte heeft aan certificatie-autoriteiten die instaan voor de identiteit van de encryptiegebruiker en niet aan "key-recovery agents". ([12])

22. Op juridisch gebied roepen deze systemen eveneens een aantal problemen op. Ook hier is het verre van zeker of zij zouden voldoen aan de voorwaarden van artikel 8.2 EVRM. Een nationaal systeem zou, bij gebrek aan efficiëntie, als niet pertinent beschouwd kunnen worden, en in het algemeen zouden alle systemen als disproportioneel aanzien kunnen worden. Men geeft immers de ordediensten van tevoren de mogelijkheden de communicaties van alle gebruikers te onderscheppen, ook al mag dit maar gebeuren ten behoeve van strikt afgebakende gevallen. Waar de sleutels niet voldoende "ver" van de afluisterende diensten gedeponeerd worden, creëert men "incentives" tot verkennend (pro-actief) afluisteren, iets

[11]http://www.crypto.com/key_study/report.shtml

[12]Certificatie-autoriteiten kennen, in tegenstelling tot "key-recovery agents", de geheime sleutels van de gebruikers niet en dienen deze niet te kennen. Sommige voorstellen (bijv. Clipper Chip III) pogen beide systemen te verenigen, maar dit is gevaarlijk daar men zo het risico loopt dat, bij "law enforcement" de ordediensten ook de toegang krijgen tot digitale handtekeningen(sleutels).

wat met name de Belgische wetgever ten strengste heeft willen verbieden.

Een ander probleem zijn de systemen met lage "key-granularity". Dit betekent dat er slechts weinig types sleutels te recupereren vallen en dat de bij de "recovery agent" te bekomen data slechts zeer breed gedefinieerd kunnen worden (bijvoorbeeld alle data m.b.t. een bepaalde gebruiker). Vraag is natuurlijk of dit soort systemen aan het proportionaliteitsvereiste van artikel 8.2. EVRM voldoet.

Een probleem specifiek voor België is ook hier weer hoe een sleuteldepotsysteem te rijmen valt met de middelenverbintenis van de houder van een bestand om de veiligheid van zijn verwerkingen te garanderen, zoals bedoeld in de wet van 8 december 1992.

De Commissie moet anderzijds erkennen dat er ook voordelen aan deze techniek verbonden zijn in zoverre een vergunningensysteem voor sleuteldepotcryptografie opgezet zou worden. Het gebruik van niet-vergunde cryptografie zou dan een aanwijzing kunnen zijn voor het bestaan van criminele activiteiten.

23. Aangezien een sleuteldepotsysteem per definitie grensoverschrijdend moet kunnen werken, zou een meer internationale aanpak verkieselijk zijn.
Op dit ogenblik echter ontbreekt het aan duidelijke stelregels in deze materie.
De Europese Commissie werkt aan een richtlijn ([13]), de Raad van Europa laat in haar aanbeveling " Recommendation No R (95) 13 of the Committee of Ministers to Members States concerning problems of criminal procedure law connected with information technology" ([14]) een ingrijpen in strafrechtsaangelegenheden mogelijk, terwijl de OESO in haar aanbeveling " Recommendation of the Council concerning guidelines for cryptography policy" ([15]) zich beperkt tot: " National Cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.
(...) This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access".

24. Rekening houdend met alle elementen is de Commissie van mening dat de weg van het sleuteldepot te veel organisatorische problemen met zich brengt en dat zij in de afweging van het recht op beveiliging van persoonsgegevens en het belang van de misdaadbestrijding, aan laatstgenomen belang een disproportioneel gewicht toekent.

d. Standaardisering.

25. In de Verenigde Staten, waar de groei van cryptografie het sterkst is, zijn een aantal initiatieven genomen om het gebruik van cryptografie binnen de eigen landsgrenzen te reguleren. Tot op heden zijn er een drietal belangrijke initiatieven geweest.

1. Clipper Chip I.

26. Toen de Amerikaanse overheid besefte dat zij mislukt was in haar poging om het gebruik van een onder haar auspiciën ontwikkelde standaard te beperken tot het gebruik binnen de administratie, trachtte zij deze standaard tevens ingang te doen vinden buiten het overheidsdomein, dit naar analogie met de Internetstandaard TCP/IP die nu wereldwijd gebruikt wordt.

---

[13] COM (94), 128 def, COD 288 en COM (97) 94 def - COD 288)

[14] http://www.privacy.or...e/info-tech-1995.html

[15] http://www.oecd.org/dsti/iccp/crypto-e.html

Zij probeerde haar doel te bereiken d.m.v. het Clipper Chip initiatief: de Clipper Chip, een nieuwe cryptografiestandaard (EES of Escrowed Encryption Standard), zou in de
worden bij de overheid.
Het
wilde haar positie als belangrijkste klant voor cryptografie wel maximaal benutten om de Chip aldus tot norm te verheffen : zij zou immers zelf enkel van de Clipper Chip aldus voorziene hardware afnemen.
initiatief kreeg een storm van protest te verwerken en niet in het minst om de keuze van overheidsdiensten als sleuteldepots.

Clipper Chip II.

27.
Chip I. Het Clipper Chip II initiatief verbreedde de keuze van sleuteldepots tot onafhankelijke

De vrees bleef nochtans bestaan dat de overheid, eens een voldoende marktaandeel toch nog “escrowed encryption” wettelijk zou verplichten. Een ander pijnpunt bij dit initiatief was dat het algoritme "Skipjack" geheim gehouden werd, zodat men het niet op zijn

Voor Europa was er de onaantrekkelijke gedachte dat op de Europese markt toestellen zouden worden, waarvoor de Amerikaanse overheid steeds over de mogelijkheid tot decrypteren zou beschikken.

zou ook het Clipper Chip II-initiatief door de Amerikaanse overheid verlaten worden.

28. Volgens een nieuw initiatief, Clipper Chip III, wil de overheid geen standaard De aandacht is verlegd naar een systeem van sleutelmanagement; de deelneming aan dit systeem gebeurt op vrijwillige basis en de keuze van het algoritme is vrij.

worden aangemoedigd om aan het systeem deel te nemen doordat de deelname aan
zouden private en publieke, binnen- en buitenlandse certificatie-autoriteiten (CA) en private publieke “Key Recovery Agents (KRA)” geregistreerd worden. Een geregistreerde CA mag aan
volwaardige deelname aan de electronische handel - slechts afleveren als deze gebruiker aan
access” mogelijk te maken. Gezien de tegenkantingen van de experts aangaande het met verbinden van de concepten CA en KRA, valt het sterk te betwijfelen of dit initiatief, dat gepaard gaat met een massale ondersteuning van “key recovery encryption” op

De grote les te trekken uit de Amerikaanse initiatieven is waarschijnlijk, dat iedere poging tot om enige kans op slagen te hebben, in nauwe samenwerking met de bedrijfswereld moet worden uitgewerkt. Maar het is tevens duidelijk dat deze laatste weinig

e. Machtiging voorafgaand aan het gebruik van cryptografie

29. In een systeem van voorafgaande machtiging wordt de nadruk gelegd op de voorafgaande informatieverstrekking aan de overheid over het gebruik van versleuteling, waarbij als hoofdelement een verantwoording voor dit gebruik gegeven moet worden.
Ook hier is de vraag of een dergelijke oplossing werkbaar kan zijn. Vanuit de bedrijfswereld zal de weerstand blijven bestaan tegen wat als een log administratief systeem ervaren kan worden. Toch biedt deze oplossing de voordelen van een geïnformeerde overheid enerzijds en van een beschermde gebruiker anderzijds, aangezien er geen afgifte van de sleutel moet gebeuren. Alleen is het uitkijken naar de criteria die de overheid zal hanteren om de machtiging te verlenen of te weigeren.

Een eenvoudiger alternatief zou erin kunnen bestaan de machtiging te vervangen door een verplichting tot aangifte, zonder meer.

f. Medewerkingsverplichting.

30. De verplichting voor telecomoperatoren om met de overheid mee te werken in het kader van afluistermaatregelen is waarschijnlijk het enige gemeenschappelijke element van alle West-Europese cryptografiewetgevingen. In België worden deze verplichtingen geconcretiseerd in artikel 70bis van de wet van 21 maart 1991 en artikel 90 quater, §2, van het Wetboek van Strafvorderingen.

Deze verplichting kan echter moeilijk nagekomen worden als het initiatief tot encryptie uitgaat van de gebruiker en de encryptie dus niet voorgesteld wordt door de operator, m.a.w. als het de gebruiker is die het signaal geëncrypteerd aan zijn operator aanlevert (zie supra, nr. 16).

Aan dit probleem zou een veel ruimer gestelde medewerkingsverplichting (ten dele) kunnen remediëren.
In België vormt zulke ruime verplichting de kern van een wetsvoorstel van 11 juni 1996 van de dames Bribosia-Picard en Maximus.([16]) Dit voorstel wil de artikelen 70bis en 95,5° van de wet van 21 maart 1991 opheffen, en de bestaande regeling vervangen door een algemene medewerkingsverplichting. Het sleutelartikel is het voorgestelde artikel 90 duodecies van het Wetboek van Strafvordering, waarvan het eerste lid luidt als volgt : "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 geadieerd is, een strafbaar feit is bedoeld in één 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."

[16]Wetsvoorstel tot opheffing van de artikelen 70bis en 95, eerste lid, 5°, van de wet van 21 maart 1991 betreffende de hervorming van sommige overheidsbedrijven en tot aanvulling van het Wetboek van Strafvordering met bepalingen betreffende de decryptie van berichten, Parl.St., Senaat,1995-1996, nr., 1-352/1.

VI.

31.
en de noodzakelijke overheidstaak om zware inbreuken te bestrijden, zal wellicht alleen via ingrijpen gerealiseerd kunnen worden. Een regeling inzake vercijfering reikt verder
asymmetrische sleutelsystemen, is essentieel bij de erkenning van de electronische en slaat op alle rechtsgevolgen eraan verbonden, zowel wat het bericht als wat de persoon zelf betreft.
Commissie meent dat een oplossing in de zin van een algemene verplichting tot medewerking,
artikelen 90ter tot 90 decies van het Wetboek van Strafvordering, op dit ogenblik de meest

32. Het voorliggend advies is noodzakelijk van algemene aard. De Commissie behoudt dan ook het recht voor om haar zienswijze te preciseren en eventueel aan te passen naar aanleiding van een concreet ontwerp of voorstel dat haar voorgelegd zou worden.

De voorzitter,

(get.) J. PAUL.
P. THOMAS.