

# Wet betreffende de hervorming van sommige economische overheidsbedrijven:

## Hoofdstuk Xbis: Geheimhouding van gesprekken en bescherming van de persoonlijke levenssfeer

21 maart 1991

### Te onthouden:

Deze bespreking concentreert zich op enkele belangrijke bepalingen die het telecommunicatiegeheim beschermen. Het gaat om de regels die werden opgenomen in de Wet van 23 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (de zogenaamde 'Belgacomwet').

De Belgacomwet ontleent haar naam aan het gegeven dat deze wet ook - en zelfs in hoofdzaak - de bedoeling had het statuut van o.a. Belgacom en zijn personeel te regelen. Daarnaast bevat de wet ook de basisregels inzake telecommunicatie, waaronder het gedeelte van de wet dat hier wordt besproken, namelijk het telecommunicatiegeheim. Dit gedeelte maakt maar een klein deel uit van de wet. Het gaat meer bepaald om hoofdstuk 10bis van titel III, met als naam "Geheimhouding van gesprekken en bescherming van de persoonlijke levenssfeer"

Het centrale artikel van dit hoofdstuk is artikel 109terD, dat onder meer de kennisname van het bestaan van andermans communicatie verbiedt zonder de voorafgaande toestemming van alle communicerende partijen.

### Sleutelbegrippen:

Telecommunicatie – Fundamentele vrijheden – Privacy – Telecommunicatiegeheim

### Inhoudsopgave van de bespreking:

- A. [Inleiding](#)
  - Historiek van de Belgacomwet
  - Privacybescherming
  - Grondslag en ratio
  - Afbakening
- B. [Kennisname van het bestaan van andermans telecommunicatie](#)
  - Artikel 109terD, 1°
  - Artikel 109terD, 3°
- C. [Gebruik en vernietiging van andermans telecommunicatiegegevens](#)
  - Artikel 109terD, 2°
  - Artikel 109terD, 4°
- D. [Uitzonderingen](#)
  - Wettelijke toestemming

- Noodzaak
  - Opsporing en lokalisatie
  - Encryptie
- E. [Om meer te weten](#)
- Nuttige links
  - Relevante rechtsleer

## Bespreking:

### A. Inleiding

België heeft een rijke juridische traditie op het gebied van bescherming van de privacy. Al in de eerste versie van de grondwet waren er waarborgen opgenomen die tot doel hadden het privéleven van de burger te af te schermen<sup>i</sup>. Eén van de voornaamste bepalingen was de bescherming van het briefgeheim<sup>ii</sup>, met de bijbehorende strafrechtelijke sanctionering<sup>iii</sup>. Deze regelgeving is noodzakelijk voor het vrijwaren van de fundamentele rechten en vrijheden, en de democratische rechtsstaat in het algemeen.

Het spreekt voor zich dat dergelijke waarborgen moeten mee-evolueren met de stand van de techniek. Het is dan ook logisch dat deze bescherming zich gaandeweg uitbreidde naar telegrafie en telefonie (het zgn. telefoongeheim), en in recentere jaren naar telecommunicatie in het algemeen. Deze bespreking concentreert zich dan ook op enkele belangrijke bepalingen die het telecommunicatiegeheim beschermen, namelijk de regels die werden opgenomen in de Wet van 23 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven<sup>iv</sup> (de zogenaamde 'Belgacomwet').

De Belgacomwet ontleent haar naam aan het gegeven dat deze wet ook – en zelfs in hoofdzaak – de bedoeling had het statuut van o.m. Belgacom en zijn personeel te regelen. Daarnaast bevat de wet echter ook de basisreglementering inzake telecommunicatie, waaronder het gedeelte van de wet dat hier wordt besproken, namelijk de bescherming van de telecommunicatie. Dit gedeelte maakt maar een klein deel uit van de wet. Het gaat meer bepaald om hoofdstuk 10bis van titel III, met als naam “Geheimhouding van gesprekken en bescherming van de persoonlijke levenssfeer”, bestaande uit art. 109terC t/m art. 109terF. Uit de nummering blijkt al dat deze materie in de loop der jaren vaak werd gewijzigd. Op deze ontwikkeling gaan we hieronder wat verder in.

Eén van de eerste wetten<sup>v</sup> over de bescherming van het telecommunicatiegeheim is de Wet van 13 oktober 1930 tot samenordering der verschillende wetsbepalingen op de telegrafie en de telefonie met draad<sup>vi</sup>. Zoals de naam al suggereert kon deze wet niet worden toegepast op draadloze communicatie. Dit hiaat werd later ingevuld door art. 4c van de Wet van 30 juli 1979 betreffende de radioberechtiging<sup>vii</sup> waarin het onder meer verboden werd om radioverbindingen op te vangen die niet voor de ontvanger bestemd waren.

In '91 kwam de eerste versie van de Belgacomwet tot stand, zij het in een geheel andere vorm dan tegenwoordig. Aanvankelijk was de erin opgenomen regelgeving over de telecommunicatie in België niet veel meer dan een rechtstreekse kopie van de bepalingen van de RTT-wet van 1930. Later werden er echter nog een aantal grondige wijzigingen doorgevoerd, waarvan de belangrijkste in 1994<sup>viii</sup> (via de Afluisterwet),

in 1997 (waardoor ze haar huidige nummering kreeg<sup>ix</sup>), in 1999 (voor een aanpassing aan de ISDN-richtlijn<sup>x</sup>), en tenslotte in 2000 (via de Wet op de Informaticacriminaliteit<sup>xi</sup>).

Vanzelfsprekend is het niet de bedoeling al deze aanpassingen in detail te analyseren. Deze bespreking wil vooral de hoofdlijnen van de privacybescherming in de Belgacomwet overlopen, en aangeven op welke manier deze bepalingen van bijzonder belang zijn in de hedendaagse informatiemaatschappij<sup>xii</sup>.

Daarom wordt op de eerste plaats geanalyseerd wat nu precies de inhoud en de draagwijdte is van de belangrijkste bepalingen, met enkele concrete voorbeelden om de ruime toepasbaarheid van deze regels te demonstreren.

## B. Kennisname van het bestaan van andermans telecommunicatie

De basisbetekenis van het telecommunicatiegeheim is het gegeven dat de inhoud en zelfs het bestaan van een specifieke informatie-uitwisseling tussen twee personen geheim moet kunnen worden gehouden. De bescherming van de inhoud is het meest voor de hand liggende aspect: niemand zal het immers erg op prijs stellen wanneer een derde zonder voorafgaande toestemming bijvoorbeeld een telefoongesprek afluistert. Dit aspect wordt echter niet geregeld in de Belgacomwet, maar wordt sinds de invoering van de Afluisterwet<sup>xiii</sup> geregeld via twee specifieke artikelen in het Strafwetboek (artikel 259bis en 314bis Sw.). Hierop gaan we dan ook niet verder in.

De Belgacomwet regelt enkel het tweede aspect, namelijk de ongeoorloofde kennisname van het bestaan van telecommunicatie. Het feit dat deze twee aspecten in twee aparte wetten wordt gesanctioneerd wordt in de rechtsleer vaak bekritiseerd. Het is immers niet mogelijk kennis te nemen van de inhoud van bepaalde communicatie, zonder ook kennis te nemen van het bestaan ervan. Het omgekeerde kan natuurlijk wel. Desondanks zou het bestaan van een eenvoudige regeling in één specifieke wet de duidelijkheid van de wetgeving ten goede komen.

De kennisname van het bestaan van andermans telecommunicatie wordt in twee aparte punten van artikel 109terD geregeld, namelijk in punt 1 en punt 3. Voor beide punten geldt dat de kennisname enkel strafbaar is als ze plaatsvindt zonder de toestemming van alle communicerende partijen<sup>xiv</sup>. Dit is ook niet meer dan logisch, aangezien het de bedoeling van de wetgever was het telecommunicatie-geheim te vrijwaren om de privacy van de deelnemende partijen te waarborgen.

Op beide punten gaan we even wat verder in.

- Artikel 109terD, 1<sup>o</sup>: [het is verboden...] “met bedrieglijk opzet kennis te nemen van het bestaan van met telecommunicatie overgebrachte tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, die herkomstig zijn van en bestemd zijn voor andere personen”

De eerste strafbaarstelling heeft betrekking op de registratie van andermans communicatie, en dus niet op de kennisname van de inhoud, zoals al eerder werd vermeld. Registratie mag dan ook in geen geval verward worden met bv. opname van (de inhoud van) specifieke communicatie.

Het voorwerp van de telecommunicatie waarop deze bepaling toepasbaar is wordt beschreven als ‘overgebrachte tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard’. Hiermee wordt het voorwerp zeer breed omschreven, vooral

via de restcategorie “gegevens van alle aard”. Het is meteen duidelijk dat nagenoeg elke telecommunicatie kan worden geregistreerd.

Ook het begrip “telecommunicatie” moet breed worden geïnterpreteerd, en wordt in art. 68, 4° van de Belgacomwet gedefinieerd als ‘elke overbrenging, uitzending of ontvangst van tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard, per draad, radio-elektriciteit, optische seingeving of een ander elektro-magnetisch systeem.’ Hieronder vallen dus niet alleen de traditionele telefonie en telegrafie, maar ook moderne vormen van telecommunicatie, zoals e-mailen, surfen, chatten, home-shopping, telebanking, *peer-to-peer*-programma's enzovoorts.

Toch gelden hierop twee beperkingen. Op de eerste plaats is het enkel strafbaar telecommunicatie te registreren die herkomstig is van en bestemd voor anderen. Het moet dus gaan over communicatie tussen minstens twee personen, waarbij de registrerende partij geen deelneemt aan de communicatie zelf. Een deelnemer mag dus zelf het bestaan van zijn eigen communicatie op welke wijze ook registreren, en iedereen mag communicatiegegevens registreren die zonder een specifieke bestemming de ether in worden gestuurd.

Een voorbeeld hiervan vindt men in het posten van een bericht in een voor het publiek toegankelijke nieuwsgroep. Een dergelijke boodschap is niet aan een bepaalde gebruiker gericht, en de werkwijze van de ‘uitzender’ geeft al impliciet aan dat hij geen belang hecht aan de vertrouwelijkheid van het bericht. Het is toegankelijk voor iedereen, en registratie door derden is dan ook toegelaten. Om die reden vallen radio- en tv-berichtgeving ook niet onder het toepassingsgebied van deze wet<sup>xv</sup>.

De tweede beperking bevindt zich in het vereiste bedrieglijk opzet van de overtreder. De dader van de registratie moet namelijk de bedoeling hebben gehad door zijn optreden het telecommunicatiegeheim te schenden. Als men door onachtzaamheid kennis neemt van het bestaan van andermans telecommunicatie, dan volstaat dit dus niet.

Een voorbeeld hiervan is de controle van de eigen e-mail op een adres dat door een gezin wordt gedeeld, waarbij men ook de titels en afzenders van de e-mail van de andere leden van het gezin te zien krijgt. Weliswaar neemt men op die wijze kennis van het bestaan van hun telecommunicatie, maar indien dit niet gebeurt met het oogmerk hun privacy te schenden kan er geen strafbaarheid bestaan.

- Artikel 109terD, 3°: [het is verboden...] “met opzet kennis te nemen van gegevens inzake telecommunicatie, die betrekking hebben op een andere persoon, onverminderd de bepalingen van artikel 105nonies, § 5, van deze wet”

De tweede strafbaarstelling lijkt op het eerste zicht sterk op de eerste. Het gaat opnieuw over de kennisname van gegevens inzake telecommunicatie, waarbij telecommunicatie een identieke ruime invulling heeft als in art. 109terD, 1°. Desondanks is er een belangrijk verschil, dat vooral bestaat uit de toepasbaarheid op ‘gegevens inzake telecommunicatie’ (in tegenstelling tot ‘met telecommunicatie overgebrachte tekens, seinen, geschriften, beelden, klanken of gegevens van alle aard’ in 1°).

Er bestaat nogal wat betwisting over de precieze invulling van deze term. De voorbereidende werken geven nochtans een concrete definitie: het gaat over gegevens

“welke betrekking hebben op een persoon die gebruik maakt van diensten voor telecommunicatie. Deze gegevens zijn echter beperkt tot het gedeelte dat tot de telecommunicatie behoort: het telecommunicatieverkeer, de aard en plaats van de inrichtingen voor telecommunicatie, een geheim telefoonnummer, enzovoorts van die persoon, doch niet de algemeen bekende gegevens, zoals de naam, de woonplaats, enzovoorts.”<sup>xvi</sup>

Artikel 109terD, 1° heeft dus betrekking op het kennisnemen van het bestaan van eender welke gegevens die duiden op telecommunicatie, terwijl artikel 109terD, 3° gaat over het kennisnemen van eerder technische gegevens over de telecommunicatie.

Wat betreft het internet kan men dan denken aan het tijdstip waarop men op een bepaald systeem inlogt, de IP-adressen van de communicerende systemen, eventueel bezochte sites, de route die een bepaald gegevenspakketje heeft gevolgd om zijn eindbestemming te bereiken enzovoorts.

Gegevens zoals gebruikersnamen en paswoorden lijken hier niet onder te vallen. Ze bevatten immers geen informatie over het bestaan en gebruik van de telecommunicatie op een bepaald tijdstip<sup>xvii</sup>, maar enkel algemene informatie die indicatief is voor het feit dat tussen twee partijen communicatie mogelijk is. Kennisname van een loginnaam of paswoord is dus op zich geen schending van het telecommunicatiegeheim, net zomin als de kennis van de inhoud van andermans telefoonboek dit is. Beide laten immers enkel toe vast te stellen dat tussen twee personen communicatie mogelijk is<sup>xviii</sup>.

Een weinig transparante regeling, waarmee moeilijk kan worden bepaald wat er precies onder 1° of 3° valt. Nochtans is het onderscheid van groot belang, gezien het verschil in bestanddelen tussen.

Mogelijk het belangrijkste verschil bestaat erin dat artikel 109terD, 3° in tegenstelling tot artikel 109terD, 1° geen bijzonder opzet vereist, maar dat algemeen opzet volstaat. Elke bewuste kennisname van andermans gegevens inzake telecommunicatie is dus strafbaar, ook als men niet de bedoeling heeft de privacy van de ander te schenden.

Een tweede belangrijk verschil tussen is dat het derde lid een uitzondering bevat voor de bepaling van art. 105nonies §5 i.v.m. facturatie door telecomoperatoren. Op deze uitzondering gaan we verder niet in.

#### C. Gebruik en vernietiging van andermans telecommunicatiegegevens

Naast de kennisname van de gegevens worden ook bepaalde vormen van gebruik van deze gegevens verboden. Hierbij is het voornaamste oogmerk de bescherming van de integriteit van de telecommunicatiegegevens, door onder meer de wijziging en de vernietiging ervan te verbieden.

- Artikel 109terD, 2°: [het is verboden...] “met bedrieglijk opzet de in 1° bedoelde informatie met gelijk welk technisch procédé (...) te wijzigen of weg te laten of de andere personen te identificeren;”

De eerste verbodsbepaling is meteen de evidentste: gegevens die het bestaan van specifieke communicatie aantonen mogen niet worden gewijzigd of weggelaten, en de deelnemers aan de communicatie mogen niet worden geïdentificeerd.

Het verbod op de wijziging en de weglating van gegevens zijn maatregelen die er vooral toe strekken de integriteit van deze gegevens te waarborgen, onder meer om

een correcte facturatie mogelijk te maken. Als dusdanig gaat het dan ook niet om een privacybeschermende maatregel.

Het verbod op de identificatie van de personen is dit natuurlijk wel. Men kan zich zelfs de vraag stellen of deze bepaling wel nodig is. De identificatie van een persoon aan de hand van zijn telecommunicatiegegevens zonder zijn voorafgaande toestemming zal meestal immers ook een onrechtmatige verwerking van zijn persoonsgegevens zijn. Ook zonder een aparte bepaling in de Belgacomwet is dit strafbaar<sup>xix</sup>.

Opnieuw wordt er een bedrieglijk opzet vereist, en is er dus enkel sprake van strafbaarheid als de gegevens werden vernietigd of weggelaten met de bedoeling de integriteit ervan aan te tasten, of als de identificatie gebeurde met de bedoeling de privacy te schenden.

Als een netwerkbeheerder bijvoorbeeld zou nagaan wie er een bepaald bestand van zijn website heeft gedownload om hen te waarschuwen voor een virus in dit bestand zou er geen sprake zijn van strafbaarheid onder dit punt van het artikel. De identificatie gebeurt immers niet met het doel andermans privacy te schenden.

Tenslotte geldt het verbod alleen wanneer men gebruik maakt van een “technisch procédé”. Zuiver manuele vernietiging (bijvoorbeeld het kapotscheuren van een papieren factuur) volstaat dus niet.

- Artikel 109terD, 4°: [het is verboden...] “de in 1°, 2° en 3° bedoelde informatie, identificatie en gegevens die met of zonder opzet werden bekomen, kenbaar te maken, er enig gebruik van te maken, deze te wijzigen of ze te vernietigen.”

Het verbod in het vierde lid ten slotte heeft betrekking op de informatie, identificatie en gegevens vermeld in het eerste, tweede of derde lid. Het misdrijf bestaat erin dat deze gegevens op een bepaalde manier worden misbruikt. Het is van belang op te merken dat nergens wordt vereist dat men ook schuldig zou zijn aan één van de hoger vermelde misdrijven; het volstaat dat het voorwerp van het misdrijf beschreven wordt in 1°, 2° of 3°.

Een eerste mogelijke vorm van misbruik bestaat uit het kenbaar maken van deze gegevens. Dit ligt in de lijn van de ratio legis: artikel 109terD heeft als bedoeling de privacy van telecommunicatie te beschermen, en het spreekt voor zich dat het openbaar maken van gegevens over andermans communicatie zonder diens toestemming hier een aantasting van is.

Een tweede misbruik dat men kan maken van deze gegevens bestaat uit het eenvoudige gebruik ervan. Dit is problematisch, omdat er geen verdere voorwaarden worden gesteld: er wordt nergens gespecificeerd dat er een bijzonder oogmerk achter moet schuilen, of dat één van de misdrijven van 1° - 3° daadwerkelijk werd gepleegd. We kunnen dit probleem best schetsen met een eenvoudig voorbeeld.

In de meeste browsers worden er ook na het afsluiten van het programma nog gegevens bewaard over de eerder bezochte websites, zodat de gebruiker deze pagina's snel kan terugvinden.

Stel nu dat er iemand gebruik maakt van een computer die ook door meerdere andere personen wordt gebruikt voor internettoegang, bv. in een bibliotheek, en dat hij via de

'geschiedenis'-functie probeert uit te vinden waar hij eerder is geweest. Onvermijdelijk krijgt hij dan informatie te zien over alle recent bezochte sites, ook degene die door anderen werden bezocht. Onmiskenbaar is dit informatie zoals bedoeld in lid 1 (eender welke gegevens die duiden op telecommunicatie), en waarschijnlijk ook in lid 3 (eerder technische gegevens over de telecommunicatie). Toch werden geen van beide misdrijven gepleegd, vermits ze respectievelijk bijzonder en algemeen opzet vereisen.

Als men in deze hypothese ziet dat iemand anders een website heeft bezocht die interessant zou kunnen zijn voor de eigen interessesfeer, en van die gegevens gebruik maakt (bv. door op de getoonde link te klikken en zo op de door de een ander bezochte website te komen), dan pleegt men wel het misdrijf van 4°. Nochtans is men niet schuldig aan één van de misdrijven van 1°-3°. Hierin ligt het belang van de verwijzing naar 'de in 1°, 2° en 3° bedoelde informatie, identificatie en gegevens', in plaats van 'de informatie, identificatie en gegevens verkregen door een van de misdrijven in 1°, 2° of 3°'. Een belangrijke nuance!

Een derde misbruik tenslotte bestaat uit het wijzigen van de in 1°, 2° en 3° bedoelde informatie, identificatie en gegevens, hierbij inbegrepen de vernietiging ervan.

Om even het voorbeeld van de browser te hernemen: een cachegeheugen met de gegevens van de recentst bezochte sites wordt niet eeuwig bewaard. De meeste browsers laten toe een vast aantal dagen in te stellen, waarna dit geheugen gewist wordt. Men kan deze gegevens echter ook zelf wissen. Als men opzettelijk deze functie gebruikt om andermans telecommunicatiegegevens van het systeem te verwijderen, dan maakt men zich schuldig aan het misdrijf in artikel 109terD, 4°.

#### D. Uitzonderingen

De overtreding van één van de bepalingen van artikel 109terD wordt geregeld in artikel 114 §2:

“Met geldboete van 50 tot 50 000 frank wordt gestraft de persoon die de artikelen (...) 109terD (...) overtreedt.”

Na omrekening naar Euro en vermenigvuldiging met de gerechtelijke opdecimen komt dit neer op €250 tot 250.000<sup>xx</sup>.

Artikel 109terE somt echter een aantal uitzonderingen op de verbodsbepalingen op, die we hier kort overlopen.

- Wettelijke toestemming:  
Artikel 109terE, 1° bevat een evidente uitzondering: er is geen sprake van schending van het telecommunicatiegeheim “wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt”. Dit spreekt voor zich: de Belgacomwet geldt als meest algemene wet, waarop specifiekere wetten uitzonderingen kunnen voorzien<sup>xxi</sup>.
- Noodzaak:  
De tweede uitzondering (artikel 109terE, 2°) heeft betrekking op de hypothese dat de inbreuk noodzakelijk is om “de goede werking van het netwerk na te gaan en de goede uitvoering van een telecommunicatiedienst te garanderen”. Hoewel hierover betwisting heeft bestaan<sup>xxii</sup> blijkt uit de parlementaire voorbereiding dat deze strafuitsluitingsgrond enkel is bestemd voor personen die handelen bij de uitvoering van hun taak “bij het B.I.P.T., bij Belgacom of

bij andere aanbieders van diensten voor telecommunicatie<sup>xxiii</sup>. Een hacker die inbreekt in een computersysteem en daarbij artikel 109terD overtreedt kan zich dus niet beroepen op deze uitzondering door te argumenteren dat hij enkel wilde nagaan of het netwerk afdoende was beveiligd.

De uitzondering van artikel 109terE, 3° heeft een vergelijkbare achtergrond: inbreuken zijn eveneens toegelaten “wanneer de handelingen worden gesteld om de interventie van hulp- en nooddiensten mogelijk te maken die antwoorden op aan hen gerichte verzoeken om hulp”. De noodzakelijkheid van de inbreuk volgt hier uit het dringend karakter van de situatie: wanneer nooddiensten een dringende oproep om hulp krijgen moeten ze snel de oorsprong van de oproep kunnen nagaan, zonder zich zorgen te maken over een risico op eventuele strafbaarheid.

- Opsporing en lokalisatie

Tenslotte is het ook mogelijk in het kader van strafonderzoeken over te gaan tot registratie van verdachte telecommunicatie<sup>xxiv</sup>. Op basis van artikel 109terE, §2 en volgende mag de Koning de precieze modaliteiten van deze registratie vastleggen. Hij kan onder meer de technische middelen bepalen waarmee de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten moeten instaan voor de registratie, evenals voor de vertrouwelijkheid en de integriteit van de hieruit voortvloeiende gegevens.

De telecomoperatoren krijgen ook een algemene verplichting om de oproep- en identificatiegegevens van gebruikers van telecommunicatiediensten te registreren en gedurende een bepaalde termijn te bewaren. De bedoeling van deze verplichting is de vereenvoudiging van de opsporing en vervolging van bepaalde strafbare feiten. De periode van deze verplichting werd nog niet vastgelegd, maar vermits de wet wel bepaalt dat de termijn minimaal 12 maanden moet zijn houden de meeste operatoren zich in de praktijk hieraan.

- Encryptie

Encryptie is de term voor elk procédé dat kan worden gebruikt om de inhoud van een bepaalde boodschap in beginsel onleesbaar te maken. Encryptie wordt – zeker op het internet – beschouwd als een fundamenteel instrument om de privacy te beschermen. In het internetverkeer wordt er overigens frequent gebruik gemaakt van encryptie, hoewel de meeste internauten zich hier vaak niet eens van bewust zijn<sup>xxv</sup>.

Digitaal telecommunicatieverkeer is bij uitstek geschikt voor het gebruik van encryptie. Er zijn dan ook talloze verschillende methodes (zogenaamde algoritmes) om gegevens te versleutelen, met een wisselende complexiteit. Voldoende complexe algoritmes kunnen het ontcijferen van een bericht nagenoeg onmogelijk maken.

Het is om die reden dat vele overheden een limiet opleggen aan het gebruik van encryptie-algoritmes. Sterke algoritmes zouden immers ook kunnen worden gebruikt door criminelen of terroristen om in het geheim<sup>xxvi</sup> hun misdrijven te plannen. Om efficiënte overheidscontrole desondanks mogelijk te maken kan het gebruik van encryptie-algoritmes wettelijk worden beperkt<sup>xxvii</sup>.

De Belgische regeling is op dit vlak flexibel: volgens artikel 109terF van de Belgacomwet is het gebruik van versleuteling vrij<sup>xxviii</sup>.

De Koning kan wel bepaalde versleutelingsdiensten aanduiden die niet aan het publiek mogen worden aangeboden zonder een voorafgaande aangifte bij het B.I.P.T. Tot dusver werd er nog geen gebruik gemaakt van deze mogelijkheid, zodat het gebruik en de verspreiding van encryptie in België voorlopig volledig vrij blijft.

#### E. Om meer te weten

- Nuttige links
  - ∞ [Informatiepagina over encryptie bij PISA \(Providing Information about Internet Security Aspects\)](#)
  - ∞ [De Commissie voor de Bescherming van de Persoonlijke Levenssfeer](#)
  
- Relevante rechtsleer
  - ∞ ARNOU, L., « Het respecteren van het telefoongeheim in België na de af luisterwet van 30 juni 1994 », *Computerr.* 1995/4, 156
  - ∞ BENSOUSSAN, A., *Les télécommunications et le droit*, Paris, Hermès, 1992
  - ∞ DEBBASCH, CH., ISAR, H. en AGOSTINELLI, X., *Droit de la communication*, Paris, Dalloz, 2002
  - ∞ DE SCHUTTER, B., « Het Belgisch Bistel-syndroom », *Computerr.*, 1999/3, p.164
  - ∞ DUMORTIER, J., *Informatica –en telecommunicatierecht*, Leuven, ACCO, 2001
  - ∞ DUMORTIER, J., « Little Brother is watching you : mag de werkgever het internetgebruik van zijn werknemers controleren », in *Liber Amicorum Roger Blanpain*, Brugge, Die Keure, 1998
  - ∞ DUMORTIER, J. en LAMBERT, P., « De wet van 19 december 1997 tot uitvoering van de Europese liberaliseringsrichtlijnen in het Belgisch telecommunicatierecht : een overzicht », *Computerr.* 1998/2, 47-55
  - ∞ DUPONT, L. en VERSTRAETEN, R., *Handboek Belgisch strafrecht*, Leuven, Acco, 1990, nr. 692 jo 695
  - ∞ LAMBERT, P., *Bescherming van (privé-)telecommunicatie*, in *Recente ontwikkelingen in informatica- en telecommunicatierecht*, ICRI, Brugge, Die Keure, 1999, p.183

Bespreking opgesteld door ICRI, gecoördineerd door Hans GRAUX.

---

<sup>i</sup> Men denkt dan bijvoorbeeld aan de onschendbaarheid van de woning (huidig artikel 15 G.W.).

<sup>ii</sup> Huidig artikel 29 G.W.

<sup>iii</sup> Artikel 460 Sw.

<sup>iv</sup> Wet van 23 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.* 27 maart 1991, 6155; verder Belgacomwet genoemd.

<sup>v</sup> Eerdere regelgeving kon men nog terugvinden in de ministeriële omzendbrief van 17 augustus 1923 die onder bepaalde voorwaarden registratie van telecommunicatie mogelijk maakte.

<sup>vi</sup> Artikel 17-20 Wet van 13 oktober 1930 tot samenordering der verschillende wetsbepalingen op de telegrafie en de telefonie met draad, *B.S.* 20 oktober 1930

<sup>vii</sup> Artikel 4c Wet van 30 juli 1979 betreffende de radioberichtgeving, *B.S.* 30 augustus 1979

<sup>viii</sup> Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het af luisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, *B.S.* 24 januari 1995, 1542

---

<sup>ix</sup> Artikel 77 Wet van 19 december 1997 tot wijziging van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven teneinde het reglementaire kader aan te passen aan de verplichtingen die inzake vrije mededinging en harmonisatie op de markt voor telecommunicatie, voortvloeien uit de van kracht zijnde beslissingen van de Europese Unie, *B.S.*, 30 december 1997, 34986.

<sup>x</sup> Richtlijn 97/66/EG (ISDN-richtlijn) van het Europees parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *P.B. L* 024, 30 januari 1998, p.1-8

<sup>xi</sup> Wet van 28 november 2000 inzake informaticacriminaliteit, *B.S.* 3 februari 2001, 2909

<sup>xii</sup> De focus op toepassingen in de informatiemaatschappij is eveneens de reden dat we artikel 109terC links laten liggen in deze bespreking. Dit artikel heeft namelijk betrekking op regels in verband met gegevens in telefoongidsen. Hoewel de intenties van dit artikel zeker ook hun nut zouden kunnen bewijzen in een bredere context, gaat de werkelijke werkingssfeer niet verder dan telefoongidsen..

<sup>xiii</sup> Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennismaken en opnemen van privé-communicatie en –telecommunicatie, *B.S.* 24 januari 1995, 1542

<sup>xiv</sup> Een dergelijke interpretatie vindt ook steun in de Parlementaire Stukken, die aangeven dat er geen strafbaarheid kan zijn als men een persoon die gebruik heeft gemaakt van een bepaalde communicatiedienst heeft geïdentificeerd met diens toestemming. *Parl.St.Kamer*, 1990-91, nr. 1287/1 – 89/90, p.67

<sup>xv</sup> *Parl.St.Kamer*, 1990-91, nr. 1287/1 – 89/90, p. 46

<sup>xvi</sup> *Parl.St.Kamer*, 1990-91, nr. 1287/1 – 89/90, p. 67

<sup>xvii</sup> Zie ook in die zin Kindt, E. en Szafran, E. in hun noot onder [het Redattack-vonnis](#). Corr. Gent, 11 december 2000, *Computerr.* 2001/2, p. 87 e.v.

<sup>xviii</sup> In [het RedAttack-vonnis](#) luidde de eindconclusie nochtans anders. In deze befaamde zaak oordeelde de rechter dat het ontvreemden van gebruikersnamen en paswoorden wel een onrechtmatige kennisname van gegevens inzake telecommunicatie was.

<sup>xix</sup> Voor meer informatie verwijzen we naar [de Wet op de Verwerking van Persoonsgegevens](#).

<sup>xx</sup> Voor de volledigheid kan nog worden opgemerkt dat de omvang van de straf niet onbetwist is. Immers, in art. 114 §7 vinden we de volgende bepalingen terug:

*“Met geldboete van 100 tot 5.000 frank en met een gevangenisstraf van drie maanden tot één jaar of met één van die straffen alleen wordt gestraft de persoon, die zelf of door toedoen van een ander persoon, behoudens toepassing van artikel 109terE, de bepaling van artikel 109terC schendt.”*

Artikel 109terE behandelt echter de uitzonderingen op artikel 109terD, en heeft dus geen uitstaans met artikel 109terC, wat artikel 114 §7 nochtans lijkt te impliceren.

Hiervoor lijkt er maar één voor de hand liggende verklaring te zijn: de wetgever heeft zich vergist in de nummering (een begrijpelijke vergissing, gezien de chaotische manier waarop dit gebeurde), en de straf van artikel 114 §7 is eigenlijk bedoeld voor overtreding van artikel 109terD, en dus niet voor 109terC.

Hoe het ook zij, vanwege het legaliteitsbeginsel is er maar één straf mogelijk, en dat is degene die – mogelijk foutief - bepaald wordt door artikel 114 §2.

<sup>xxi</sup> Overeenkomstig de Latijnse spreuk: *lex specialis derogat legi generali*.

<sup>xxii</sup> Dit argument werd namelijk ingeroepen in [de zaak RedAttack](#), waar een zelfverklaarde hacker zich onder meer verdedigde met het argument dat hij enkel de goede werking van het systeem wilde nagaan.

<sup>xxiii</sup> *Gedr.St.Kamer*, 1990-91, nr. 1287/1 – 89/90, p. 68

<sup>xxiv</sup> Dit kan weliswaar enkel in een klein aantal strikt afgelijnde gevallen, omwille van het indringend karakter van de maatregel. De gevallen waarin registratie van telecommunicatie mogelijk is worden vastgelegd in de artikelen 88bis en 90ter tot 90decies van het Wetboek van Strafvordering. Een bespreking hiervan valt buiten het kader van deze tekst.

<sup>xxv</sup> We verwijzen hiermee voornamelijk naar het gebruik van het SSL-protocol (Secure Socket Layer). Alle gegevens die verzonden worden via een verbinding die door het SSL-protocol wordt beveiligd worden automatisch versleuteld, althans bij gebruik van een browser die het protocol ondersteunt (wat nagenoeg alle moderne browsers doen). Voor meer informatie: zie [deze omschrijving \(Engelstalige link\)](#). Sites die SSL ondersteunen kunnen eenvoudig worden herkend doordat hun adres begint met [https://](#) in plaats van [http://](#). SSL wordt vooral gebruikt bij het verzenden van betalingsgegevens (zoals naam en kredietkaartnummer) op commerciële sites.

<sup>xxvi</sup> Critici merken op dat niets zo snel de aandacht trekt als overdreven sterk geëncrypteerde berichten, en dat het gebruik van dergelijke algoritmes geheimhouding dan ook niet ten goede komt.

<sup>xxvii</sup> Dit is onder meer het geval in de Verenigde Staten, waar encryptie wel wordt toegelaten, maar de export van encryptie-algoritmes streng werd gereguleerd. Daarbij is het officiële beleid momenteel dat het Department of Justice de ontwikkeling van sterke encryptiesystemen aanmoedigt, maar enkel als er een 'recovery system' bestaat waarmee de gerechtelijke instanties de oorspronkelijke inhoud kunnen achterhalen. Voor meer informatie verwijzen we naar [de informatiepagina van het U.S. Department of Justice](#).

<sup>xxviii</sup> Deze flexibele opstelling is een gevolg van de wet van 19 december 1997 die vanaf 1 januari 1998 de levering en het gebruik van cryptografie in België volledig liberaliseerde. (Wet van 19 december 1997 tot

---

wijziging van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven teneinde het reglementaire kader aan te passen aan de verplichtingen die inzake vrije mededinging en harmonisatie op de markt voor telecommunicatie, voortvloeien uit de van kracht zijnde beslissingen van de Europese Unie, *B.S.*, 30 december 1997, 34986). Vóór de inwerkingtreding van deze wet kon de Minister van Telecommunicatie de verspreiding van bepaalde versleutelingsapparatuur verbieden.