

Wet ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en -telecommunicatie.

30 juni 1994
(B.S. 24 januari 1995)

Te onthouden:

De wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en -telecommunicatie (verder: de Afluisterwet) bevat de belangrijkste Belgische reglementering in verband met de bescherming van de vertrouwelijkheid van privé(tele)communicatie.

Twee belangrijke beginselen worden in de wet uitgewerkt:

1. Het afluisteren, kennisnemen en openen van andermans privé(tele)-communicatie zonder de toestemming van alle deelnemers is verboden. Hierbij worden openbare gezagsdragers onderworpen aan een strenger regime dan particulieren.
2. Bij het onderzoeken van welbepaalde bijzonder zwaarwichtige strafbare feiten kan een uitzondering worden gemaakt op dit verbod. Indien afluisteren absoluut nodig is om de ware toedracht van een misdrijf te achterhalen is het toegelaten de privé(tele)communicatie van een verdachte voor een beperkte tijd af te luisteren of op te nemen.

Sleutelbegrippen:

Telecommunicatie – Privacy – Telecommunicatiegeheim – Afluisteren – Strafprocesrecht – Onderzoeksmaatregel

Inhoudsopgave van de bespreking:

- A. [Inleiding](#)
 - Doel van de wet
 - Telecommunicatiegeheim
 - Strafrecht en strafprocesrecht
- B. [Geheim van privécommunicatie en -telecommunicatie](#)
 - Afluisteren, kennisnemen en opnemen
 - Onthullen en verspreiden van de inhoud
 - Opstellen van toestellen
 - Ambtenaren vs. particulieren
- C. [Strafprocesrecht: afluisteren als onderzoeksmaatregel](#)
 - Afluisteren, kennisnemen en opnemen
 - Bij ernstige misdrijven
 - Noodzakelijkheid
- D. [Overige bepalingen](#)
 - Toestellen die afluisteren, kennisnemen en opnemen mogelijk maken

- Aanpassingen aan o.m. de Belgacomwet
- E. [Om meer te weten](#)
- Nuttige links
 - Rechtsleer

Bespreking:

A. Inleiding

Het telecommunicatiegeheim is één van de belangrijkste aspecten van de bescherming van de persoonlijke levenssfeer. Iedereen die gebruik maakt van een communicatiemiddel om een persoonlijke boodschap over te brengen rekent er immers op dat het private karakter van de communicatie door zijn medeburgers zal worden gerespecteerd, ongeacht het gekozen medium (geschreven post, telefoon, e-mail, ...). Het telecommunicatiegeheim wordt overigens niet enkel omwille van deze principiële reden beschermd, maar ook omdat de vertrouwelijkheid van privéberichten wordt beschouwd als een fundamenteel bestanddeel van de democratische rechtsstaat.

België beschikt dan ook al sinds jaar en dag over de nodige wetgeving om het telecommunicatiegeheim te verzekeren. Naast de bescherming van het klassieke briefgeheimⁱ met de bijbehorende strafrechtelijke sanctiëringⁱⁱ werd de privacy van privéberichten aanvankelijk beschermd via de wet van 13 oktober 1930 tot samenordering der verschillende wetsbepalingen op de telegrafie en de telefonie met draadⁱⁱⁱ. Deze wet voerde een verbod in op het registreren en opnemen van telecommunicatie die via een draad werd verspreid (telegrafie, telefonie, telex, fax,...). Draadloze communicatie bleef daarbij evident buiten schot.

De beperkingen van deze wet werden later wat gereduceerd door de wet van 23 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven^{iv} (de zogenaamde 'Belgacomwet'). Naast het statuut van enkele overheidsbedrijven (waaronder Belgacom, vandaar de naam) bevat deze wet ook de meest algemene regels inzake telecommunicatie in België. Hoofdstuk 10bis van titel III van de wet draagt de titel "Geheimhouding van gesprekken en bescherming van de persoonlijke levenssfeer", en nam onder meer het bestaande verbod op de opname en registratie van telecommunicatie over. Ditmaal ging het echter om een iets meer flexibele bepaling, aangezien de wet van toepassing was op alle telecommunicatie, inclusief draadloze vormen (in tegenstelling tot de wet van 1930).

Toch drong een wetswijziging zich al snel op. Het aftappen van telecommunicatie bleek namelijk een van de meest efficiënte manieren te zijn om georganiseerde misdaad te bestrijden. Om die reden besloot de wetgever een gedetailleerde omkadering van deze maatregel op te nemen in het wetboek van strafvordering. Hierin werd vastgelegd voor welke misdrijven afluisteren zou worden toegelaten, onder welke voorwaarden, en welke procedure er moest worden gevolgd.

Van deze gelegenheid werd ook gebruik gemaakt om de bescherming van het telecommunicatiegeheim in het algemeen te herschrijven. Waar vroeger immers één artikel^v het verbod bevatte op de kennisname van de inhoud en het bestaan van bepaalde telecommunicatie, werd er nu een breuk ingevoerd. Voortaan zou het oudere artikel enkel nog betrekking hebben op de kennisname van het *bestaan* van telecommunicatie, echter zonder kennisname van de *inhoud* nog te sanctioneren.

De strafbare kennisname van de inhoud van telecommunicatie werd verplaatst van de Belgacomwet naar het strafwetboek.

Zowel de opsplitsing van het oude beschermingsregime als de invoer van een procedure voor afluisteren in een strafrechtelijk onderzoek gebeurde [via de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennismaken en openen van privé-communicatie en -telecommunicatie](#) (verder: de Afluisterwet). Deze wet zullen we hier kort bespreken.

B. Geheim van privécommunicatie en – telecommunicatie

Zoals in de inleiding al werd aangehaald werd de bescherming van het telecommunicatiegeheim vóór de inwerkingtreding van deze wet in één artikel geregeld, namelijk artikel 109terD van de Belgacomwet. Sinds de inwerkingtreding wordt het kennismaken van de inhoud van andermans telecommunicatie apart gesanctioneerd, en regelt artikel 109terD enkel nog de kennisname van het bestaan van andermans telecommunicatie.

Ook de bescherming van de inhoud van telecommunicatie werd opgesplitst in twee aparte artikelen: enerzijds artikel 259bis Sw., dat van toepassing is op openbare officieren en ambtenaren, en anderzijds 314bis Sw., dat op elke andere persoon van toepassing is. Het voornaamste verschil is dat openbare officieren en ambtenaren strenger worden gestraft. De reden daarvoor is dat zij worden geacht de overheid te vertegenwoordigen, en dat een schending van het telecommunicatiegeheim in hun hoedanigheid van gezagsdragers daarom als een ernstiger inbreuk op het openbaar vertrouwen wordt ervaren.

Beide artikelen bevatten drie categorieën van misdrijven, die hieronder wat verder zullen worden beschreven.

- Afluisteren, kennismaken en opnemen (artikel 259bis §1, 1^o en artikel 314bis §1, 1^o)
Het is verboden opzettelijk en met behulp van een toestel andermans privé-communicatie of -telecommunicatie af te luisteren of te doen afluisteren, er kennis van te nemen of doen van nemen, het op te nemen of doen opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie.

Het gaat om een ruim omschreven misdrijf, waarbij de term 'telecommunicatie' breed wordt geïnterpreteerd. Het artikel is niet alleen van toepassing op telefonie en e-mail, maar ook op fax, teleconferencing, online banking en dergelijke meer. Wanneer deze communicatie privé is (d.w.z. wanneer ze niet bestemd is om door iedereen te worden gehoord) mag men dus op geen enkele manier kennisnemen van de inhoud of deze inhoud opnemen, tenzij men de toestemming heeft van alle deelnemers aan de communicatie.

Ook surfen kan dus worden beschouwd als privécommunicatie, als men bijvoorbeeld via een website persoonlijke gegevens doorgeeft die niet voor het grote publiek bestemd zijn.

Toch zijn er twee grote beperkingen aan het artikel. Op de eerste plaats moet het gaan om andermans communicatie. Het verbod is met andere woorden niet van toepassing op de opname van communicatie waaraan met zelf deelneemt.

Het opnemen van de eigen telefoongesprekken of het bijhouden van tekstbestanden met de eigen chatsessies wordt dus niet gevisieerd door dit artikel.

Daarnaast moet de inbreuk op de privacy plaatsvinden met een technisch hulpmiddel. Kennisname van andermans e-mail door bv. over de schouder van de auteur mee te lezen zal dus niet strafbaar zijn onder deze bepaling.

- Onthullen en verspreiden van de inhoud (artikel 259bis §1, 3° en §2, en artikel 314bis §2)

Het tweede misdrijf is als het ware een voortzetting van het eerste: na de opname van een privé(tele)communicatie is het verboden deze opname te verspreiden onder derden. Dit zou namelijk evenzeer een inbreuk betekenen op het private karakter van de communicatie als het afluisteren zonder de toestemming van alle betrokkenen.

Dit misdrijf wordt opgesplitst in twee hypothesen.

In de eerste hypothese (artikel 314bis §2, 2e lid en 259bis §2) werd de opname op een wettige manier gemaakt, maar werd ze daarna gebruikt met bedrieglijk opzet of met het oogmerk te schaden. Als voorbeeld daarvan zou men kunnen denken aan een chatsessie waaraan men zelf heeft deelgenomen en waarvan men de tekst heeft opgeslagen. Dit is op zich niet verboden. Als men daarna deze tekst op een website zou plaatsen met de bedoeling de reputatie van één van de deelnemers te schaden, dan zou dit wel strafbaar kunnen zijn.

In de tweede hypothese (artikel 314bis §2, 1e lid en 259bis §1, 3°) werd de privé(tele)communicatie op een onwettige manier opgenomen of afgeluisterd, en werd er daarna op eender welke manier gebruik van gemaakt. Een voorbeeld hiervan is het gebruiken van onderschepte e-mail in een poging om de ontrouw van een huwelijkspartner aan te tonen. In deze situatie is er dus geen bedrieglijk opzet of een oogmerk om te schaden vereist: als het oorspronkelijke materiaal op een illegale manier is verkregen, dan is elk later gebruik automatisch verboden. Zelfs het louter bij zich houden van het illegale materiaal is strafbaar.

- Opstellen van toestellen (artikel 314bis §1, 2° en 259bis §1, 2°)
Ten slotte wordt er ook een voorbereidende handeling strafbaar gesteld, namelijk het opstellen of doen opstellen van een toestel om één van de hierboven omschreven misdrijven te plegen. Niet alleen schenden van de privacy kan dus strafbaar zijn, maar ook het voorbereiden hiervan. Een voorbeeld is de installatie van spionagesoftware om e-mails te kunnen onderscheppen.

C. Strafprocesrecht: afluisteren als onderzoeksmaatregel

Het afluisteren van andermans privé(tele)communicatie wordt dus doorgaans als onrechtmatig bestempeld. Toch zijn er enkele hypothesen waarin afluisteren als een aanvaardbare mogelijkheid wordt beschouwd. Dit is met name het geval bij de bestrijding van de georganiseerde misdaad, waar deze maatregel erg efficiënt is gebleken.

Bij de invoering van het nieuwe strafrechtelijke verbod op het afluisteren van privé(tele)communicatie werd hiermee rekening gehouden. In het wetboek van

strafvordering werd er dan ook een nieuwe procedure opgenomen die telefoontaps en gelijkaardige maatregelen in een beperkt aantal gevallen moet toelaten. De procedure werd op een zeer gedetailleerde manier uitgewerkt in de nieuwe artikelen 90ter tot 90decies Sv. Voor de overzichtelijkheid overlopen we hier alleen de krachtlijnen.

De basisregel staat in artikel 90ter § 1: de onderzoeksrechter (die het onderzoek naar zwaarwichtige strafbare feiten leidt) kan in uitzonderlijke gevallen wanneer het onderzoek het vereist privé-communicatie of -telecommunicatie tijdens de overbrenging ervan, afluisteren, er kennis van nemen en opnemen. Wat het internet betreft zou een onderzoeksrechter bijvoorbeeld de mogelijkheid hebben e-mails te onderscheppen of chatsessies mee te volgen.

Dit kan echter enkel als er ernstige aanwijzingen bestaan dat de feiten die hij onderzoekt kunnen worden gekwalificeerd als één van de ernstige misdrijven die in §2 van artikel 90ter staan beschreven, en als andere onderzoeksmiddelen niet zouden kunnen volstaan om de waarheid te achterhalen.

De voorwaarden zijn dus streng: afluisteren kan alleen voor een beperkt aantal ernstige misdrijven, en enkel wanneer de maatregel strikt noodzakelijk is. Deze voorwaarden worden verantwoord door de overweging dat de maatregel een ernstige inbreuk op de privacy van een verdachte betekent.

Paragraaf 2 van het artikel bevat een lange en exhaustieve opsomming van misdrijven die het afluisteren kunnen verantwoorden. In deze lijst treft men onder andere doodslag, moord, (dreigen met) aanslagen, gijzelneming, ontvoering, kinderprostitutie, afpersing en brandstichting. Het is duidelijk dat enkel als zeer ernstig beschouwde misdrijven in aanmerking komen voor deze ingrijpende maatregel. Ook de poging tot het plegen van één van deze misdaden kan de bewakingsmaatregel wettigen (§3). De maatregel kan voor een duur van één maand worden opgelegd, maar kan daarna eventueel nog worden verlengd tot een maximum van zes maanden.

Wat de technische uitvoering van de maatregel betreft heeft de onderzoeksrechter het recht de medewerking van de operator van het relevante communicatienetwerk te eisen, zoals bv. van een internetprovider. Het toezicht zelf kan echter alleen gebeuren door officieren van gerechtelijke politie, die regelmatig verslag uitbrengen bij de onderzoeksrechter. Onder meer een gedetailleerde overschrijving van de opnamen (eventueel vertaald) wordt ter griffie bewaard.

Advocaten en artsen krijgen een beperkte bescherming ten aanzien van de maatregelen, omwille van de vertrouwensrelatie die zij met hun cliënten onderhouden. Afluisteren van hun privé(tele)communicatie is daarom enkel mogelijk wanneer zij zelf (en dus niet hun cliënten) worden verdacht van één van de feiten uit artikel 90ter §2, of wanneer de daders gebruik zouden hebben gemaakt van hun lokalen of telecommunicatie-infrastructuur. Daarbij moet eerst de stafhouder of de vertegenwoordiger van de provinciale orde van geneesheren op de hoogte worden gebracht van de maatregel.

D. Overige bepalingen

De wet sanctioneert dus op de eerste plaats het afluisteren zelf en het plaatsen van toestellen om het afluisteren mogelijk te maken. Artikel 5 laat echter toe nog een stap verder te gaan. De Koning kan namelijk ook de verdeling en productie van afluisterapparatuur reglementeren. Er wordt dus een mogelijkheid voorzien om niet

alleen het gebruik van deze toestellen te reglementeren, maar ook de distributie op zich.

Het is opmerkelijk dat er niet alleen een reglementering kan worden opgesteld voor af luisterapparatuur (omschreven als “toestellen die ontworpen of gemaakt zijn om het af luisteren, kennismaken of opnemen van privé-communicatie of -telecommunicatie, in strijd met de artikelen 259bis en 314bis van het Strafwetboek, mogelijk te maken”), maar ook voor toestellen die als dusdanig worden voorgesteld. Om een reglementering van de distributie van een toestel te kunnen uitvaardigen wordt er dus niet vereist dat het toestel effectief geschikt zou zijn voor af luisteren; het volstaat dat die indruk wordt gecreëerd.

Alle besluiten die worden genomen als uitvoeringsmaatregel van deze wet moeten worden onderworpen aan een voorafgaand advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. Overtredingen van deze reglementeringsbesluiten worden streng bestraft met een boete van 1.000 tot 100.000 Euro. Voor zover bekend werden er echter nog geen uitvoeringsbesluiten op basis van dit artikel genomen, zodat de bestraffing voorlopig niet erg relevant is.

De Af luisterwet bevat ten slotte ook nog een aantal aanpassingsbepalingen waarmee enkele andere wetten een invulling krijgen die overeenstemt met de principes van deze wet. De belangrijkste aanpassingen hebben betrekking op de Belgacomwet, waar artikel 111 (het huidige artikel 109terD) werd aangepast. Zoals hierboven al werd vermeld verbood dit artikel voorheen de wederrechtelijke kennisname van de inhoud of het bestaan van andermans communicatie. Na de aanpassing door deze wet regelt artikel 111 enkel nog de kennisname van het bestaan van andermans communicatie, en wordt de inhoud ervan beschermd via het nieuwe artikel 259bis en 314bis Sw.

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.

ⁱ Huidig artikel 29 G.W.

ⁱⁱ Artikel 460 Sw.

ⁱⁱⁱ 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

^{iv} Wet van 23 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, *B.S.* 27 maart 1991, 6155; verder Belgacomwet genoemd.

^v Namelijk artikel 109terD van de Belgacomwet