

Standpunt van het Instituut inzake scanners

1. omschrijving van het begrip "scanners"

Scanners zijn ontvangtoestellen die het mogelijk maken om het ganse frequentiespectrum of een gedeelte ervan af te tasten, aan te geven welke frequentie ontvangen wordt en eventueel toe te laten de inhoud van het ontvangen signaal te beluisteren of te demoduleren. In de meeste gevallen is het mogelijk het toestel voor te programmeren met preselecties van voorkeurfrequenties. De mogelijke luisterfrequenties van een scanner zijn bijgevolg niet per se beperkt tot de welbepaalde voorgeprogrammeerde frequenties.

2. voorwaarden voor het houden, gebruiken en commercialiseren van scanners

2.1. In België is de handel in, het bezit en gebruik van scanners, zoals voor alle ontvangtoestellen, in principe vrij, voor zover ze voldoen aan voorwaarden voorzien in de Europese richtlijn 1999/5/EC (de R&TTE richtlijn) zoals omgezet in Belgisch recht.

2.2. Indien een betreffende type scanner echter twee welbepaalde eigenschappen in zich verenigt, kan niet zonder meer aangenomen worden dat het toestel wettelijk toegelaten is. Deze eigenschappen zijn de volgende :

(a) Het ontvangsttoestel is uitgerust met de mogelijkheid om kennis te nemen van de inhoud van het ontvangen signaal. Hierbij wordt bijvoorbeeld het audiosignaal uit een ontvangen signaal gehaald en via een luidspreker beluisterbaar gemaakt. Zo zijn bepaalde meettoestellen (meetontvangers, spectrumanalysers, enz), die ook bepaalde frequentiebanden kunnen afscannen, niet specifiek geconstrueerd om de inhoud van de opgevangen signalen te beluisteren. Zij worden derhalve in deze nota niet geïllustreerd.

(b) Het toestel maakt het mogelijk om buiten de geautoriseerde luisterfrequenties boodschappen op te vangen. De toelating voor het beluisteren van een frequentie kan blijken uit de aard van de betreffende frequenties, in die zin dat het gaat om frequenties die probleemloos en van nature door iedereen beluisterd mogen worden. Bijvoorbeeld citizen band (CB), omroep (broadcast) alsook de frequenties gebruikt door radioamateurs zijn voorbeelden van dergelijke frequenties. De frequenties zijn ofwel volledig (bijvoorbeeld de FM-band en de frequenties voor radioamateurs), ofwel bijna volledig geharmoniseerd (met name de kanalen gebruikt voor CB: alle

Lidstaten hanteren dezelfde 40 basiskanalen, maar in Duitsland en in de UK zijn een aantal extra kanalen voorzien) en geven in de praktijk bijgevolg geen probleem.

2.3. Bepaalde frequenties worden evenwel aangewend voor private communicaties in die zin dat de berichten op die frequenties niet bestemd zijn om door derden beluisterd te worden(1). De toelating om die bepaalde frequenties te beluisteren, kan echter expliciet worden verkregen van degene die de betreffende frequenties gebruikt. Die frequentie wordt dan een geautoriseerde luisterfrequentie voor degene die daartoe de toestemming heeft verkregen (vb: seinwachters bij wielervedstrijden die toelating krijgen om de frequenties van de wedstrijdleiding - wielerbond te beluisteren).

2.4. Wanneer scanners het mogelijk maken om communicaties af te luisteren

- (a) op andere banden dan deze gebruikt voor CB, omroep, radioamateurs of PMR446, en
- (b) zonder dat daarvoor door de betrokkene de toestemming werd gegeven(2)

zal de betreffende scanner onder welbepaalde voorwaarden als een illegaal toestel worden beschouwd.

Deze voorwaarden zijn de volgende :

- 1) een betrapting op heterdaad, hetgeen inhoudt dat :
 - de gebruiker van het toestel op heterdaad betrapt wordt bij het beluisteren van voor hem niet-toegelaten frequenties, of
 - het betreffende toestel wordt ontdekt wanneer het in werking is gesteld en afgestemd is op een verboden frequentie;

of

- 2) in het toestel (of in het apparaat dat de scanner stuurt of

(1) Hiertoe moeten ook o.m. de frequenties gerekend worden die gebruikt worden door de nooddiensten en de politiediensten. Het beluisteren van deze frequenties is zonder de expliciete toestemming van deze diensten, verboden.

(2) De vaak gehoorde redenering als zou het miskennen van de privacy door scannergebruikers, te wijten zijn aan een ondoelmatig beveiligen van de privé-communicaties, is niet correct aangezien deze redenering de verantwoordelijkheid voor het afluisteren niet legt bij degene die afluistert, maar integendeel bij degene die afgeluisterd wordt. Wie geen - kostelijke - encryptietechnieken aanwendt, kan, bij toepassing van die redenering, er niet meer van uitgaan dat zijn communicaties gerespecteerd worden, d.w.z. als vertrouwelijk worden behandeld, maar kan en mag integendeel voortaan afgeluisterd worden. Quod non. Het is immers niet zo dat wat afgeluisterd kan worden, ook afgeluisterd mag worden...

Bovendien mag het recht op onschendbaarheid van de private communicatie, wat een grondrecht is dat verzekerd wordt door o.m. artikel 8 van het Europese Verdrag van de Rechten van de Mens (zie verder), niet uitgehold worden en vervangen worden door de plicht om de private communicaties te crypteren.

superviseert, zoals een PC) zijn niet-toegelaten frequenties voorgeprogrammeerd,

én een van de volgende situaties doet zich voor :

- minstens een van de voorgeprogrammeerde frequenties wordt gebruikt voor draadloze of mobiele analoge telefonie, politie of nooddiensten, luchtvaartdiensten, maritieme diensten;
- getuigenissen bevestigen dat het toestel gebruikt wordt voor het beluisteren van private communicaties;
- wanneer het toestel wordt aangezet, stemt het automatisch af op een verboden frequentie.
- minstens een van de voorgeprogrammeerde frequenties is die van een concurrerende firma;

of

- 3) het toestel laat toe om van de inhoud van (analoge of digitale) geëncrypteerde signalen of van de digitale modulatie op niet-geautoriseerde frequenties (GSM, DCS1800, DECT, TETRA, ...) kennis te nemen;

of

- 4) de gebruiker van het toestel geeft toe dat hij kennis heeft genomen van berichten die niet voor hem bestemd zijn.

2.5. Voor alle duidelijkheid : indien een scanner, of het gebruik dat er van gemaakt wordt, ook maar aan één van de vermelde voorwaarden voldoet, is het Instituut van oordeel dat het betreffende toestel als een illegaal toestel moet worden beschouwd.

Scanners die de mogelijkheid bieden om naar niet-toegelaten banden te luisteren, zonder dat de gebruiker terzake op heterdaad wordt betrapt, en zonder dat er niet-toegelaten banden werden geprogrammeerd, worden door het Instituut getolereerd aangezien scanners immers ook toelaten om op volkomen legale wijze communicaties te beluisteren.

Bijkomende voorwaarde is evenwel dat de scanners geen mogelijkheid bieden om geëncrypteerd verkeer te beluisteren. Scanners die deze laatste mogelijkheid bieden worden door het Instituut steeds beschouwd als illegaal(3), ongeacht het gebruik dat ervan wordt gemaakt en ongeacht de geprogrammeerde frequenties.

3. De juridische basis ter ondersteuning van het standpunt van het Instituut

3.1. Het standpunt van het Instituut inzake scanners volgt uit een toepassing van artikel 33, 1^o, van de wet van 13 juni 2005 betreffende de elektronische communicatie.

(3) Het Instituut is van oordeel dat er mag van uitgegaan worden dat de houder/gebruiker van dergelijk apparaat het kennisnemen van geëncrypteerde signalen minstens op het oog heeft.

3.2. Artikel 33, 1°, van de wet van 13 juni 2005 betreffende de elektronische communicatie bepaalt:

Art. 33. § 1. *Het is verboden de volgende apparatuur te houden, te commercialiseren of te gebruiken :*

1° apparatuur waarvan het gebruik onverenigbaar is met één of meerdere van de volgende bepalingen :

a) de artikelen 41 en 124 ;

b) de artikelen 259bis en 314bis van het Strafwetboek;

(...)

Artikel 41 van de wet van 13 juni 2005 bepaalt :

Art. 41. *Behoudens de officieren van gerechtelijke politie vermeld in artikel 24 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector voor wat betreft punt 2° , mag niemand in het Rijk, noch aan boord van een schip, een luchtvaartuig of enige andere drager onderworpen aan het Belgisch recht :*

1° (...)

2° andere radiocommunicatie dan die bedoeld in artikel 314bis van het Strafwetboek en die niet voor hem bestemd is, opvangen of trachten op te vangen. Indien zulke verbindingen onopzettelijk worden ontvangen, mogen zij noch weergegeven, noch aan derden medegedeeld, noch voor enig ander doeleind worden gebruikt en zelfs aan hun bestaan mag geen bekendheid worden gegeven, behalve in de gevallen door de wet opgelegd of toegestaan.

Artikel 124 van de wet van 13 juni 2005 bepaalt :

Art. 124. *Indien men daartoe geen toestemming heeft gekregen van alle andere, direct of indirect betrokken personen, mag niemand :*

1° met opzet kennis nemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is ;

2° met opzet de personen identificeren die bij de verzending van de informatie en de inhoud ervan betrokken zijn ;

3° onverminderd de toepassing van de artikelen 122 en 123, met opzet kennis nemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon ;

4° de informatie, identificatie of gegevens die met of zonder opzet werden verkregen, wijzigen, schrappen, kenbaar maken, opslaan of er enig gebruik van maken.

Artikel 259bis van het Strafwetboek bepaalt :

Art. 259bis. § 1. Met gevangenisstraf van zes maanden tot twee jaar en met geldboete van vijfhonderd frank tot twintigduizend frank of met een van die straffen alleen wordt gestraft ieder openbaar officier of ambtenaar, drager of agent van de openbare macht die, naar aanleiding van de uitoefening van zijn bediening, buiten de gevallen die de wet bepaalt of zonder inachtneming van de vormen die zij voorschrijft :

1° ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie;

2° ofwel, met het opzet een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen;

(...)

Artikel 314bis van het Strafwetboek(4) bepaalt :

Art. 314bis. §1. Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd frank tot tienduizend frank of met één van die straffen alleen wordt gestraft hij die:

1° ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie;

2° ofwel, met het opzet van een van de hierboven omschreven misdrijven te plegen, enig toestel opstelt of doet opstellen.

(...)

3.3. Overtreding van artikel 33, 1°, van de wet van 13 juni 2, wordt strafbaar gesteld in artikel 145 :

(4) Het Hof van Cassatie stelt hierover in een arrest van 6 juni 1984 :
"Krachtens (...) artikel 4, c), is het strafbaar zonder vergunning een zend- of ontvangtoestel voor radioverbinding te houden en radioverbindingen die niet voor de dader bestemd zijn, op te vangen of trachten op te vangen."

§ 1. Met een geldboete van 50 tot 50.000 frank wordt gestraft de persoon die de artikelen (...) 33 (...) overtreedt.

(...)

§ 4. De verbeurdverklaring van apparaten die niet voldoen aan de voorwaarden van de artikelen (...) 33 (...) wordt altijd uitgesproken.

3.4. Artikel 33, 1°, verbiedt aldus het bestaan(5) in België van o.m. apparatuur die dient om een of meerdere van de geciteerde artikelen te overtreden..

Welnu, wanneer een scannergebruiker op heterdaad wordt betrapt bij het luisteren naar frequenties waarvoor hij geen toestemming heeft, wanneer verboden frequenties in de scanner zijn geprogrammeerd of wanneer de scanner toelaat om digitale mobilofonie te beluisteren, is dit toestel en het gebruik dat ervan gemaakt wordt of kan gemaakt worden, niet verenigbaar met de geciteerde wetsartikelen en met het door deze artikelen beschermde het recht op privacy(6).

3.5. Bijgevolg : indien blijkt dat scanners gebruikt worden om privé-communicaties af te luisteren (zoals bij een betrapting op heterdaad), of wanneer redelijkerwijze aangenomen kan worden dat ze gebruikt werden of worden om privé-communicaties af te luisteren (zoals in geval van geprogrammeerde verboden frequenties of in geval van scanners waarmee digitale mobilofonie kan worden afgeluisterd), hebben we te maken, in de bewoordingen van artikel 33, 1°, met " apparatuur waarvan het gebruik onverenigbaar is met één of meerdere van de volgende bepalingen (...) ".

3.6. Aangezien het plegen van inbreuken op de privacy d.m.v. telecommunicatieapparatuur niet alleen het loutere afluisteren (of een poging daartoe) behelst maar ook andere vormen van het opvangen van communicaties die uitsluitend voor anderen zijn bestemd, wordt artikel 314bis, Sw. aangevuld door artikel 41, 2°, van de wet van 13 juni 2005. Dit artikel is trouwens een zo goed als letterlijke overname van het toenmalige artikel 4, c) , van de wet van 30 juli 1979 betreffende de radioberichtgeving.

(5) Zowel het houden, commercialiseren als gebruiken is immers expliciet verboden.

(6) Het recht op privacy is namelijk een grondrecht, d.w.z. een recht gewaarborgd door artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM), door artikel 17 van het Verdrag inzake Burgerlijke en Politieke rechten (BUPO), alsook door artikelen 22, 23, 3^{de} lid 3°, en 29 van de Belgische Grondwet. Hierbij dient opgemerkt te worden dat het EVRM en BUPO-verdrag allebei rechtstreekse werking hebben in de Belgische rechtsorde.

Het recht op privacy is bovendien, volgens vaste rechtspraak van het Hof van Cassatie, van openbare orde.

4. Wat betreft de verhouding tussen artikel 33 en de R&TTE-richtlijn

4.1. Artikel 33, 1°, van de wet van 13 juni 2005 vindt zijn oorsprong niet in de omzetting van de R&TTE-richtlijn. De bepaling heeft de openbare orde, de veiligheid, bescherming van de privacy, bestrijding van de criminaliteit, ... op het oog en wordt niet beïnvloed door de R&TTE-richtlijn, noch door enige andere richtlijn. Het is een bepaling die door een lidstaat genomen kan worden op grond van artikel 30 van het EEG-verdrag :

Art. 30. De bepalingen van de artikelen 28 en 29 (zijnde het verbod op kwantitatieve beperkingen tussen lidstaten) vormen geen beletsel voor verboden of beperkingen van invoer, uitvoer of doorvoer, welke gerechtvaardigd zijn uit hoofde van bescherming van de openbare zedelijkheid, de openbare orde, de openbare veiligheid, de gezondheid en het leven van personen (...) of uit hoofde van de bescherming van de industriële en commerciële eigendom. (...)"

4.2. Voorgaande houdt in dat wanneer een apparaat onder de toepassing valt van artikel 33, 1°, van de wet van 13 juni 2005 het niet langer relevant is of dit apparaat aan de basisvereisten vermeld in artikel 32 van de wet van 13 juni 2005 voldoet : de voorwaarden voor het houden, commercialiseren en gebruiken van apparatuur zijn ondergeschikt aan de fundamentele voorwaarde die artikel 33, 1°, van de wet van 13 juni 2005 stelt.

5. Conclusie:

Wanneer scanners het mogelijk maken om communicaties af te luisteren

- (a) op andere banden dan deze gebruikt voor CB, omroep, PMR446 of radioamateurs, en
- (b) zonder dat daarvoor door de betrokkene de toestemming werd gegeven

zal de betreffende scanner onder welbepaalde voorwaarden als een illegaal toestel worden beschouwd.

Deze voorwaarden zijn de volgende :

1. een betrapting op heterdaad, hetgeen inhoudt dat :

- de gebruiker van het toestel op heterdaad betrapt wordt bij het beluisteren van voor hem niet-toegelaten frequenties, of
- het betreffende toestel wordt ontdekt wanneer het in werking is gesteld en afgestemd is op een verboden frequentie;

of

2. in het toestel(of in het apparaat dat de scanner stuurt of superviseert, zoals een PC) zijn niet-toegelaten frequenties voorgeprogrammeerd,

én een van de volgende situaties doet zich voor :

- minstens een van de voorgeprogrammeerde frequenties wordt gebruikt voor draadloze of mobiele analoge telefonie, politie of nooddiensten, luchtvaartdiensten, maritieme diensten;
- getuigenissen bevestigen dat het toestel gebruikt wordt voor het beluisteren van private communicaties;
- wanneer het toestel wordt aangezet, blijkt het afgestemd te zijn op een verboden frequentie;
- minstens een van de voorgeprogrammeerde frequenties is die van een concurrerende firma;

of

3. het toestel laat toe om (analoge of digitale)geëncrypteerde gesprekken of van de digitale modulatie op niet-geautoriseerde frequenties (GSM, DCS1800,DECT, TETRA, ...) kennis te nemen;

of

4. de gebruiker van het toestel geeft toe dat hij kennis heeft genomen van berichten die niet voor hem bestemd zijn.