

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 betrapping op heterdaad, hetgeen inhoudt dat :

- de gebruiker van het toestel op heterdaad betrappt 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.

Avis de l'Institut concernant les scanners

1. description de la notion de "scanners"

Les scanners sont des appareils récepteurs permettant de balayer l'intégralité ou une partie du spectre des fréquences, d'indiquer quelle fréquence est reçue et d'éventuellement écouter et/ou démoduler le contenu du signal reçu. Dans la plupart des cas, il est possible de préprogrammer l'appareil avec des présélections de fréquences préférées. Par conséquent, les fréquences d'écoute possibles d'un scanner ne sont pas nécessairement limitées à des fréquences préprogrammées bien définies.

2. conditions de détention, d'utilisation et de commercialisation des scanners

2.1. En Belgique, le commerce, la possession et l'utilisation de scanners sont, comme pour tous les appareils récepteurs, en principe libres, pour autant qu'ils remplissent les conditions prévues dans la directive européenne 1999/5/CE (la directive R&TTE) telles que transposées en droit belge.

2.2. Toutefois, si un type de scanner donné combine deux caractéristiques précises, l'on ne peut pas automatiquement supposer que l'appareil est légalement autorisé. Ces caractéristiques sont les suivantes :

(a) L'équipement de l'appareil récepteur permet de prendre connaissance du contenu du signal reçu.

Dans ce cadre, le signal audio par exemple est issu d'un signal reçu et peut être écouté par le biais d'un haut-parleur. Ainsi, certains appareils de mesure (récepteurs de mesure, analyseurs de spectre, etc.) pouvant également scanner certaines bandes de fréquences, ne sont pas spécifiquement conçus pour écouter le contenu des signaux reçus. Ils ne sont donc pas visés par la présente note.

(b) L'appareil permet de recevoir des messages en dehors des fréquences d'écoute autorisées.

L'autorisation d'écoute d'une fréquence peut être établie par le type des fréquences en question, en ce sens qu'il s'agit de fréquences qui de par leur nature peuvent être écoutées par tout le monde sans aucun problème. De telles fréquences sont par exemple la bande 'citizen band', la radiodiffusion (broadcast) ainsi que les fréquences utilisées par les radioamateurs. Les fréquences sont soit complètement harmonisées (par exemple bande FM et les fréquences pour les radioamateurs), soit presque complètement harmonisées (à savoir les canaux utilisés par Cb : tous les Etats Membres utilisent les mêmes 40 canaux de base, mais en Allemagne et au Royaume Uni, un certain nombre de canaux supplémentaires sont prévus) et ne posent par conséquent aucun problème dans la pratique.

2.3. Certaines fréquences sont néanmoins utilisées pour des communications privées en ce sens que les messages sur ces fréquences ne sont pas destinés à être écoutés par des tiers (1). L'autorisation d'écouter ces fréquences spécifiques peut toutefois être explicitement obtenue par la personne qui utilise les fréquences en question. Cette fréquence devient alors une fréquence d'écoute autorisée pour celui qui en a reçu l'autorisation (ex. : les signaleurs qui lors des courses cyclistes ont reçu l'autorisation d'écouter les fréquences de la direction de la course – de la fédération cycliste).

2.4. Lorsque les scanners permettent d'écouter les communications

(a) sur d'autres bandes que celles utilisées pour CB, la radiodiffusion, les radioamateurs ou PMR446, et

(b) sans que l'intéressé(e) ait donné son autorisation à cet effet(2)

le scanner en question sera considéré comme un appareil illégal dans des conditions spécifiques.

Ces conditions sont les suivantes :

1) être pris sur le fait, ce qui implique que :

- l'utilisateur de l'appareil est pris sur le fait lors de l'écoute de fréquences dont l'accès lui est interdit, ou
- l'appareil en question est découvert alors qu'il est en marche et est réglé sur une fréquence interdite ;

ou

2) des fréquences non autorisées sont préprogrammées dans l'appareil ou dans tout système contrôlant l'appareil, tel qu'un PC,

et une des situations suivantes se produit :

- au moins une des fréquences préprogrammées est utilisée pour la téléphonie analogique sans fil ou mobile, pour la police ou les services de secours, pour les services de navigation aérienne, pour les services maritimes ;
 - des témoignages confirment que l'appareil est utilisé pour écouter des communications privées ;
 - lorsque l'appareil est allumé, il se règle automatiquement sur une fréquence interdite.
- au moins une des fréquences préprogrammées est celle d'une firme concurrente;

(1) A cet effet, il faut également inclure entre autres les fréquences qui sont utilisées par les services de secours et les services de police. L'écoute de ces fréquences sans l'autorisation expresse de ces services est interdite.

(2) Le raisonnement souvent entendu selon lequel la méconnaissance du respect de la vie privée par les utilisateurs de scanners, serait due à une protection inefficace des communications privées, n'est pas correcte, puisque ce raisonnement ne rend pas responsable de l'écoute celui qui écoute, mais bien celui qui est écouté. Celui qui utilise des techniques de codage – coûteux -, peut, si l'on applique ce raisonnement, ne plus considérer que ses communications sont respectées, c.-à-d. qu'elles sont traitées de manière confidentielle, mais a la possibilité et peut au contraire être écouté. Quod non. En effet, ce n'est pas parce qu'il est possible d'écouter quelque chose, que c'est également autorisé. D'autre part, le droit d'inviolabilité des communications privées, soit un droit fondamental notamment garanti par l'article 8 de la Convention européenne sur les Droits de l'Homme (voir plus loin), ne peut pas être vidé de son sens et être remplacé par l'obligation de crypter les communications privées.

ou

3) l'appareil permet de prendre connaissance du contenu des signaux cryptés (analogues ou digitales) ou de modulation digitale sur des fréquences interdites (GSM, DCS1800, DECT, TETRA, ...);

ou

4) l'utilisateur de l'appareil reconnaît avoir pris connaissance de communications qui ne lui sont pas destinées.

2.5. Dans un souci de clarté : si un scanner, ou si l'utilisation qui est en faite, remplit déjà une des conditions citées, l'Institut estime que l'appareil en question doit être considéré comme un appareil illégal.

Les scanners permettant d'écouter des bandes non autorisées, sans que l'utilisateur ne soit pris sur le fait à ce sujet, et sans que des bandes non autorisées n'aient été programmées, sont tolérés par l'Institut étant donné que les scanners permettent en effet d'également écouter des communications de manière tout à fait légale. Une condition supplémentaire est toutefois que les scanners n'offrent pas la possibilité d'écouter le trafic crypté. Les scanners offrant cette dernière possibilité sont toujours considérés par l'Institut comme illégaux (3), quel que soit l'usage qui en est fait et quelles que soient les fréquences programmées.

3) La base juridique appuyant l'avis de l'Institut

3.1. Le point de vue de l'Institut en ce qui concerne les scanners découle d'une application de l'article 33, 1°, de la loi du 13 juin 2005 relative aux communications électroniques.

3.2. L'article 33, 1°, de la loi du 13 juin 2005 relative aux communications électroniques stipule :

Art. 33. § 1er. *Il est interdit de détenir, de commercialiser ou d'utiliser les équipements suivants :*

1° les équipements dont l'utilisation est inconciliable avec une ou plusieurs des dispositions suivantes :

a) les articles 41 et 124 ;

b) les articles 259bis et 314bis du Code pénal ;

(...)

(3) L'Institut estime que l'on peut partir du principe que le titulaire/ l'utilisateur de tels équipements vise au moins à prendre connaissance des signaux cryptés.

Article 41 de la loi du 13 juin 2005 prévoit :

Art. 41. *A l'exception des officiers de police judiciaire cités à l'article 24 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges pour ce qui concerne le point 2°, nul ne peut, dans le Royaume ou à bord d'un bateau, d'un aéronef ou de tout autre support soumis au droit belge :*

1° (..)

2° *capter ou tenter de capter des radiocommunications autres que celles visées à l'article 314bis du Code pénal et qui ne lui sont pas destinées. Si de telles communications sont involontairement reçues, elles ne peuvent être reproduites, ni communiquées à des tiers, ni utilisées à une fin quelconque et leur existence même ne peut être révélée sauf dans les cas imposés ou autorisés par la loi.*

Article 124 de la loi du 13 juin 2005 prévoit :

Art. 124. *S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :*

1° *prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ;*

2° *identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ;*

3° *sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ;*

4° *modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non.*

Article 259 bis du Code pénal prévoit :

Art. 259bis. § 1. *Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents francs à vingt mille francs ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit :*

1° *soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des*

télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;

2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque;

3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.

(...)

Article 314 bis du Code pénal (4) prévoit :

Art. 314bis. § 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque :

1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications;

2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.

3.3. Une infraction de l'article 33, 1°, de la loi du 13 juin 2005 est punissable par l'article 145 :

Art. 145. § 1er. Est punie d'une amende de 50 à 50.000 EUR, la personne qui enfreint les articles (...), 33, (...)

(...)

§ 4. La confiscation d'appareils ne satisfaisant pas aux conditions prévues aux articles 32, (...) est toujours prononcée.

(4) La Cour de Cassation stipule à cet égard dans un arrêt du 6 juin 1984 : "En vertu de (...) l'article 4, c), capter ou tenter de capter un appareil émetteur ou récepteur de radiocommunications non destiné à l'auteur est punissable.

(5) Tant la détention, la commercialisation que l'utilisation sont en effet explicitement interdits.

(6) Le droit à la protection de la vie privée est en effet un droit fondamental, c.-à-d. un droit garanti par l'article 8 de la Convention européenne des Droits de l'Homme (CEDH), par l'article 17 du Pacte relatif aux droits civils et politiques, ainsi que par les articles 22, 23, alinéa 3 3°, et 29 de la Constitution belge. A cet égard, il convient de souligner que la convention CEDH et le pacte relatif aux droits civils et politiques trouvent tous deux une application immédiate dans l'ordre juridique belge.

3.4. Article 33, 1°, interdit donc l'existence(5) en Belgique entre autres des équipements qui servent à enfreindre la loi ou portent atteinte à l'ordre public.

Lorsqu'un utilisateur de scanner est pris en flagrant délit d'écoute d'une ou de fréquences sans en avoir l'autorisation, lorsque des fréquences interdites sont programmées dans le scanner ou lorsque le scanner permet d'écouter une mobilophonie digitale, cet appareil et l'utilisation qui est en faite ou peut en être faite, n'est pas compatible avec les articles cités de la loi et la protection de la vie privée(6) protégée par ces articles.

3.5. En conséquence : s'il devait s'avérer que des scanners sont utilisés pour écouter des communications privées (comme lors d'une prise en flagrant délit), ou lorsqu'on peut raisonnablement supposer qu'ils étaient ou sont utilisés pour écouter des communications privées (comme en cas de fréquences programmées interdites ou en cas de scanners permettant d'écouter la mobilophonie digitale), nous avons affaire à, selon les termes de l'article 33, 1°, "*des équipements dont l'utilisation est inconciliable avec une ou plusieurs des dispositions suivantes (...)*"

3.6. Etant donné que les atteintes à la vie privée au moyen d'équipements de télécommunications ne comprennent pas seulement l'écoute (ou une tentative d'écoute) mais également toutes les autres formes d'interception de communications qui sont destinées exclusivement à d'autres, l'article 314bis est complété par l'article 41, 2° de la loi du 13 juin 2005. Cet article est une reprise presque littéral de l'ancien article 4, c) de la loi du 30.7.1979 relative aux radiocommunications.

4. Concernant le rapport entre l'article 33 et la directive R&TTE-

4.1. L'article 33, 1°, de la loi du 13 juin 2005 ne trouve pas son origine dans la transposition de la directive R&TTE. La disposition vise l'ordre public, la sécurité, la protection de la vie privée, la lutte contre la criminalité, ... et n'est pas influencée par la directive R&TTE, ni par aucune autre directive. Il s'agit d'une disposition pouvant être prise par un Etat membre sur la base d'un article 30 du traité CEE :

Article 30 : *Les dispositions des articles 28 et 29 (à savoir l'interdiction des limitations quantitatives entre les Etats membres) ne font pas obstacle aux interdictions ou restrictions d'importation, d'exportation ou de transit, justifiées par des raisons de moralité publique, d'ordre public, de sécurité publique, de protection de la santé et de la vie des personnes (...) ou de protection de la propriété industrielle et commerciale. (...)*"

4.2. Ce qui précède implique que lorsqu'un appareil tombe sous le champ d'application de l'article 33, 1°, de la loi du 13 juin 2005, il n'est plus important de savoir si cet appareil satisfait aux conditions de base mentionnées à l'article 32 de la loi du 13 juin 2005 : les conditions de détention, de commercialisation et d'utilisation de l'équipement sont soumises à la condition fondamentale posée à l'article 33, 1°, de la loi du 13 juin 2005.

5. Conclusion:

Lorsque les scanners permettent d'écouter les communications

- (a) sur d'autres bandes que celles utilisées pour CB, la radiodiffusion, les radioamateurs ou PMR446, et
 - (b) sans que l'intéressé(e) ait donné son autorisation à cet effet
- le scanner en question sera considéré comme un appareil illégal dans des conditions spécifiques.

Ces conditions sont les suivantes :

1. être pris sur le fait, ce qui implique que :

- l'utilisateur de l'appareil est pris sur le fait lors de l'écoute de fréquences dont l'accès lui est interdit, ou
- l'appareil en question est découvert lorsqu'il est mis en marche et est réglé sur une fréquence interdite ;

ou

2. des fréquences non autorisées sont préprogrammées dans l'appareil ou dans tout système contrôlant l'appareil, tel qu'un PC,

et une des situations suivantes se produit :

- au moins une des fréquences préprogrammées est utilisée pour la téléphonie analogique sans fil ou mobile, pour la police ou les services de secours, pour les services de navigation aérienne, pour les services maritimes ;
 - des témoignages confirment que l'appareil est utilisé pour écouter des communications privées ;
 - lorsque l'appareil est allumé, il se règle automatiquement sur une fréquence interdite.
- au moins une des fréquences préprogrammées est celle d'une firme concurrente ;

ou

3. l'appareil permet d'écouter des conversations cryptées (analogues ou digitales) ou de modulation digitale sur des fréquences interdites (GSM, DCS1800, DECT, TETRA, ...);

ou

4. l'utilisateur de l'appareil reconnaît avoir pris connaissance de communications qui ne lui sont pas destinées.