

KONINKRIJK BELGIE**ROYAUME DE BELGIQUE****FEDERALE OVERHEIDSDIENST
JUSTITIE****SERVICE PUBLIC FÉDÉRAL
JUSTICE**

ONTWERP VAN KONINKLIJK
BESLUIT HOUDENDE
MODALITEITEN VOOR DE
WETTELIJKE
MEDEWERKINGSPLICHT BIJ
GERECHTELIJKE VORDERINGEN
MET BETREKKING TOT
ELEKTRONISCHE COMMUNICATIE

PROJET D'ARRÊTÉ ROYAL
DETERMINANT LES MODALITÉS DE
L'OBLIGATION DE COLLABORATION
LÉGALE EN CAS DE DEMANDES
JUDICIAIRES CONCERNANT LES
COMMUNICATIONS
ÉLECTRONIQUES

VERSLAG AAN DE KONING**RAPPORT AU ROI**

Sire,

Sire,

Het koninklijk besluit van 9 januari 2003 tot uitvoering van de artikelen 46bis, §2, eerste lid, 88bis, §2, eerste en derde lid, en 90quater, §2, derde lid, van het Wetboek van Strafvordering en van de 109ter, E, §2, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven werd gepubliceerd in het Belgisch Staatsblad van 10 februari 2003. Vijf jaar na datum is er veel veranderd, zowel op juridisch als op technologisch vlak, zodat een aanpassing van dit Koninklijk Besluit zich opdringt.

L'arrêté royal du 9 janvier 2003 portant exécution des articles 46bis, §2, alinéa 1^{er}, 88bis, §2, alinéas 1^{er} et 3, et 90quater, §2, alinéa 3, du Code d'instruction criminelle ainsi que de l'article 109ter, E, §2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques a été publié au Moniteur belge du 10 février 2003. Cinq ans après, la situation a sensiblement changé, tant sur le plan juridique que sur le plan technologique, de sorte qu'une adaptation dudit arrêté royal s'impose.

In de eerste plaats zijn er wetgevend een aantal nieuwe initiatieven genomen die de basisartikelen waarop het Koninklijk Besluit gegrond was, gewijzigd hebben. Artikel 46bis werd grondig gewijzigd, eerst door de wet van 27 december 2004 houdende diverse bepalingen (BS 31 december 2004), later ook door de wet van 23 januari 2007 tot wijziging van artikel 46bis van het Wetboek van Strafvordering (BS 14 maart 2007). Met uitzondering van een kleine technische

Tout d'abord, un certain nombre de nouvelles initiatives ont été prises au niveau législatif, qui ont modifié les articles de base sur lesquels se fonde l'arrêté royal en question. L'article 46bis a été modifié en profondeur, d'abord par la loi du 27 décembre 2004 portant des dispositions diverses (MB du 31 décembre 2004), ensuite par la loi du 23 janvier 2007 modifiant l'article 46bis du Code d'instruction criminelle (MB du 14 mars 2007). À l'exception d'une petite modification d'ordre

wijziging bij de wet van 20 juli 2006 houdende diverse bepalingen (BS 28 juli 2006) bleef artikel 88bis ongewijzigd. Ook artikel 90quater bleef, voor wat betreft de inhoud van dit Koninklijk Besluit, ongewijzigd.

Artikel 109ter van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven werd echter opgeheven door de wet van 13 juni 2005 betreffende de elektronische communicatie, en vervangen door nieuwe bepalingen in deze wet, waardoor de wettelijke basis van het Koninklijk Besluit niet meer bestond. Het zijn de artikelen 125, §2 en 127, §1, eerste lid, 2° en tweede lid van de wet op de elektronische communicatie die nu de wettelijke basis van onderhavig Koninklijk Besluit vormen.

Artikel 125, §2 van de wet van 13 juni 2005 luidt als volgt:

“De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, bij een besluit vastgesteld na overleg in de Ministerraad, de nadere regels en de middelen die moeten worden ingezet om het identificeren, het opsporen, lokaliseren, afluisteren, kennismaken en opnemen van elektronische communicatie mogelijk te maken.”

Artikel 127, §1 van dezelfde wet luidt als volgt:

“De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen die aan de operatoren of aan de eindgebruikers worden opgelegd om:

1° in het kader van een noodoproep de

technique apportée dans le cadre de la loi du 20 juillet 2006 portant des dispositions diverses (MB du 28 juillet 2006), l'article 88bis est demeuré inchangé. De même, l'article 90quater est demeuré inchangé pour ce qui est du contenu de l'arrêté royal.

L'article 109ter de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques a cependant été abrogé par la loi du 13 juin 2005 relative aux communications électroniques et remplacé par de nouvelles dispositions dans cette loi, ce qui a supprimé la base légale de l'arrêté royal. Ce sont les articles 125, §2 et 127, §1, alinéa 1^{er}, 2° et alinéa 2, de la loi relative aux communications électroniques qui constituent désormais la base légale du présent arrêté royal.

L'article 125, §2, de la loi du 13 juin 2005 est libellé comme suit:

« Le Roi fixe, après avis de la Commission de la protection de la vie privée et de l'Institut, par arrêté délibéré en Conseil des ministres, les modalités et les moyens à mettre en œuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques. »

L'article 127, § 1, de la même loi est libellé comme suit :

« Le Roi fixe, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives qui sont imposées aux opérateurs ou aux utilisateurs finals, en vue de permettre :

1° l'identification de la ligne appelante

oproeplijn te kunnen identificeren; 2° de oproeper te kunnen identificeren en het opsporen, lokaliseren, af luisteren, kennismaken en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikelen 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering.”

Zoals hoger gezegd werd artikel 46bis van het Wetboek van Strafvordering grondig gewijzigd door de wet van 23 januari 2007 tot wijziging van artikel 46bis van het Wetboek van Strafvordering. Deze wet had een tweërlei doel: enerzijds diende het artikel aangepast te worden aan de technische evolutie en ook ten gevolge van een welbepaalde rechtspraak die een bepaalde interpretatie gaf aan het artikel die niet strookte met de bedoeling van de wetgever. Wat dat betreft kan nuttig verwezen worden naar de memorie van toelichting bij de wet van 23 januari 2007 waarin deze problematiek toegelicht wordt (Parl. Doc., Senaat, 2005-2006, 3-1824/1).

Het tweede doel van de aanpassing van artikel 46bis was om de CTIF (de Centrale Technische Interceptiefaciliteit van de geïntegreerde politiedienst, gestructureerd op twee niveaus) toe te laten een rechtstreekse toegang tot de klantenbestanden van de operatoren en dienstenverstrekkers te krijgen mits voldoende garanties voor de privacy van de klanten van de operatoren en dienstenverstrekkers. Het voordeel van een directe toegang bestaat erin dat de gerechtskosten voor de identificatie van nummers sterk zullen dalen aangezien de CTIF zelf zal instaan voor de identificatie. Artikel 46bis, §2 bepaalt dat de technische voorwaarden voor deze rechtstreekse toegang bepaald worden bij Koninklijk Besluit.

Naast de juridische vooruitgang is er

dans le cadre d'un appel d'urgence ; 2° l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle. »

Ainsi qu'il a été indiqué ci-dessus, l'article 46bis du Code d'instruction criminelle a été modifié en profondeur par la loi du 23 janvier 2007 modifiant l'article 46bis du Code d'instruction criminelle. Cette loi avait un double objectif: il convenait, d'une part, d'ajuster l'article en question aux évolutions techniques et de l'adapter eu égard à une interprétation spécifique qu'une jurisprudence particulière a donnée à l'article qui ne correspondait pas à l'intention du législateur. À cet égard, il peut être utile de se référer à l'exposé des motifs de la loi du 23 janvier 2007, où cette problématique est commentée (Doc. Parl., Sénat, 2005-2006, 3-1824/1).

Le deuxième objectif de l'adaptation de l'article 46bis était de permettre au CTIF (le système central d'interception technique du service de police intégré, structuré à deux niveaux) d'avoir un accès direct aux fichiers des clients des opérateurs et des fournisseurs de services moyennant des garanties suffisantes quant au respect de la vie privée des clients des opérateurs et des fournisseurs de services. Un accès direct est avantageux en ce qu'il permet de réduire considérablement les frais de justice liés à l'identification des numéros, dès lors que le CTIF assure lui-même l'identification. Article 46bis, §2 prévoit qu'il convient de fixer par arrêté royal les conditions techniques de cet accès direct.

Outre les avancées juridiques, des

ook een technologische vooruitgang die het noodzakelijk maakt het Koninklijk Besluit van 2003 aan te passen. Zoals immers uitgelegd in het Verslag aan de Koning waren de bepalingen van dit Koninklijk Besluit, voor zover zij betrekking hadden op de uitvoering van artikel 90ter en volgende van het Wetboek van Strafvordering, niet van toepassing op de internetsector. De reden hiervoor lag in het feit dat er op dat ogenblik nog geen Europese technische normen bestonden voor de interceptie van internetcommunicatie, en dat de technische mogelijkheden nog te beperkt waren om internetcommunicatie te gaan onderscheppen. Deze situatie is nu wezenlijk veranderd, de technische mogelijkheden zijn uitgebreid en ook Europese technische normen werden uitgevaardigd. Er is dan ook geen enkele reden meer om de internetsector verder uit te sluiten van de medewerkingsmodaliteiten bepaald bij dit Koninklijk Besluit.

Algemene commentaar bij het Koninklijk Besluit

Gezien de hoger beschreven wetswijzigingen dienen de volgende elementen via een Koninklijk Besluit geregeld worden:

- De termijn waarbinnen identificatiegegevens ten gevolge van de maatregel van artikel 46bis Sv. moeten worden meegedeeld (Cf. artikel 46bis, §2, eerste lid);
- De technische voorwaarden voor de toegang tot de in artikel 46bis, §1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst

progrès d'ordre technologique rendent également nécessaire l'adaptation de l'arrêté royal de 2003. En effet, ainsi qu'il est indiqué dans le Rapport au Roi, les dispositions de cet arrêté royal ne s'appliquaient pas, dans la mesure où elles se rapportaient à l'exécution de l'article 90ter et suivants du Code d'instruction criminelle, au secteur Internet. Cela s'expliquait par le fait qu'à l'époque, il n'existait encore aucune norme technique européenne pour l'interception de communications Internet et que les possibilités techniques étaient encore trop limitées pour pouvoir intercepter des communications Internet. La situation est tout autre à l'heure actuelle: les possibilités techniques sont multiples et des normes techniques européennes ont été fixées. Il n'y a dès lors plus aucune raison de continuer à exclure le secteur Internet des modalités de collaboration prévues par cet arrêté royal.

Commentaire général de l'Arrêté royal

Compte tenu des modifications législatives décrites ci-dessus, les éléments suivants doivent être régis par un arrêté royal:

- le délai dans lequel les données d'identification doivent être communiquées à la suite de la mesure visée à l'article 46bis du Code d'instruction criminelle (voir article 46bis, §2, alinéa 1^{er});
- les conditions techniques d'accès aux données visées à l'article 46bis, §1, qui sont disponibles pour le procureur du Roi et le service de police désigné au même paragraphe (voir article

(Cf. artikel 46bis, §2, tweede lid).

46bis, §2, alinéa 2) ;

- De termijn waarbinnen oproepgegevens ten gevolge van de maatregel van artikel 88bis Sv. moeten worden meegedeeld (Cf. artikel 88bis, §2, eerste lid);
- De modaliteiten van de medewerkingsplicht die voor de maatregel van artikel 88bis Sv. gelden voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten (Cf. artikel 88bis, §2, derde lid);
- De modaliteiten van de medewerkingsplicht die voor de maatregel van artikel 90ter e.v. Sv. gelden voor de operatoren van telecommunicatienetwerken en de verstrekkers van telecommunicatiediensten (Cf. artikel 90quater, §2, derde lid);
- De nadere regels en de middelen die moeten worden ingezet om het identificeren, het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van elektronische communicatie mogelijk te maken (Cf. artikel 125, §2 van de wet betreffende de elektronische communicatie);
- de technische en administratieve maatregelen die aan de operatoren of aan de eindgebruikers worden opgelegd om de oproeper te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden
- le délai dans lequel les données d'appel doivent être communiquées à la suite de la mesure visée à l'article 88bis du Code d'instruction criminelle (voir article 88bis, §2, alinéa 1^{er}) ;
- les modalités de l'obligation de collaboration imposées aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications dans le cadre de la mesure visée à l'article 88bis du Code d'instruction criminelle (voir article 88bis, §2, alinéa 3) ;
- les modalités de l'obligation de collaboration imposées aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications dans le cadre de la mesure visée à l'article 90ter et suivants du Code d'instruction criminelle (voir article 90quater, § 2, alinéa 3) ;
- les modalités et les moyens à mettre en œuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques (voir article 125, §2, de la loi relative aux communications électroniques) ;
- les mesures techniques et administratives qui sont imposées aux opérateurs ou aux utilisateurs finals, en vue de permettre l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux

bepaald door de artikel en 46bis, 88bis en 90ter tot 90decies van het Wetboek van Strafvordering (Cf. artikel 127, §1, eerste lid, 2° van de wat betreffende de elektronische communicatie);

- De methode voor de bepaling van de bijdrage in de kosten voor investering, exploitatie en onderhoud van die maatregelen, die ten laste komt van de operatoren van elektronische communicatienetwerken en -diensten, alsook de termijn waarbinnen de operatoren of de abonnees moeten voldoen aan de opgelegde maatregelen (Cf. artikel 127, §1, tweede lid van de wat betreffende de elektronische communicatie).

Het Koninklijk Besluit dat nu aan U wordt voorgelegd is erop gericht als basis te dienen voor de toekomstige werkwijze in de problematiek rond het identificeren, opsporen en intercepteren van telecommunicatie voor gerechtelijke doeleinden.

Wat de internetsector betreft, voorziet het Koninklijk Besluit twee periodes in de uitvoering: in beginsel is het volledige Koninklijk Besluit vanaf zijn inwerkingtreding uitvoerbaar, met uitzondering van de artikelen 6 en 10. Artikel 12, §1 voorziet immers in een overgangstermijn van een jaar waarbinnen de internetsector haar technische middelen en apparatuur kan aanpassen om te kunnen voldoen aan de in de artikelen 6 en 10 vermelde functionele vereisten en de in artikel 6, § 2 vermelde technische specificaties van het European Telecommunications Standards Institute. Gedurende deze overgangstermijn moeten ze wel voldoen aan de minimale vereisten die opgesomd staan in artikel 7.

conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle (voir article 127, §1, alinéa 1^{er}, 2° de la loi relative aux communications électroniques) ;

- la méthode de détermination de la contribution dans les frais d'investissement, d'exploitation et d'entretien de ces mesures qui est à la charge des opérateurs de réseaux et services de communications électroniques, ainsi que le délai dans lequel les opérateurs ou les abonnés doivent donner suite aux mesures imposées (voir article 127, §1, alinéa 2, de la loi relative aux communications électroniques).

L'arrêté royal qui Vous est à présent soumis entend servir de base pour la future façon de procéder dans le cadre de la problématique de l'identification, du repérage et de l'interception de télécommunications à des fins judiciaires.

Pour ce qui est du secteur Internet, l'arrêté royal prévoit deux périodes d'exécution : en principe, l'arrêté royal est intégralement applicable dès son entrée en vigueur, à l'exception des articles 6 et 10. L'article 12, §1 prévoit en effet une période de transition d'un an pendant laquelle le secteur Internet peut adapter ses moyens et équipements techniques afin de pouvoir satisfaire aux exigences fonctionnelles précisées aux articles 6 et 10 ainsi qu'aux spécifications techniques du « European Telecommunications Standards Institute » figurant à l'article 6, §2. Au cours de cette période de transition, ils doivent cependant satisfaire aux exigences minimales énumérées à l'article 7.

Na deze overgangstermijn blijft het gehele Koninklijke Besluit van toepassing op de internetsector, met uitzondering van artikel 7. Op dat moment krijgt artikel 6 volledige uitwerking.

Vanwege de hoge techniciteit, en het feit dat de wettelijke basis voor het Koninklijk Besluit van 9 januari 2003 weggevallen is, wordt ervoor geopteerd een volledig nieuwe tekst aan U voor te leggen en het oude Koninklijk Besluit op te heffen. In het artikelsgewijs commentaar zullen dan ook enkel de verschillen met de vorige tekst uitgelegd worden. Voor de uitleg over de bepalingen die niet wijzigen, kan nuttig verwezen worden naar het Verslag aan de Koning bij het Koninklijk Besluit van 9 januari 2003 (BS 10 februari 2003, p. 6614 en volgende).

Het ontwerp van Koninklijk Besluit werd twee maal voor advies voorgelegd aan de Commissie voor de Bescherming van de Persoonlijke Levenssfeer. In bijlage bij deze memorie werd de nota opgenomen die aan de Commissie werd overgemaakt met de elementen van antwoord op het eerste advies nr. 29/2008.

Artikelsgewijs commentaar

Artikel 1

In het eerste artikel worden de definities gegeven van een aantal begrippen die verder in het Koninklijk Besluit gehanteerd worden.

In vergelijking met het Koninklijk besluit van 2003 worden de definities van de termen “semafoniedienst”, “mobiel satellietgrondstation” en “mobiele persoonlijke satellietcommunicatiedienst” geschrapt. De reden hiervoor is simpel: deze begrippen worden niet meer in het

Après cette période de transition, l'arrêté royal reste intégralement applicable au secteur Internet, à l'exception de l'article 7. À ce moment-là, l'article 6 produira pleinement ses effets.

Eu égard à la haute technicité et au fait que la base légale de l'arrêté royal du 9 janvier 2003 a été supprimée, il a été décidé de Vous soumettre un tout nouveau texte et d'abroger l'ancien arrêté royal. Aussi seules les différences par rapport au texte précédent seront-elles exposées dans le commentaire des articles. Pour ce qui est des explications relatives aux dispositions qui demeurent inchangées, il peut être utile de se référer au Rapport au Roi de l'arrêté royal du 9 janvier 2003 (MB du 10 février 2003, pp. 6614 et suivantes).

Le projet d'arrêté royal a été soumis deux fois pour avis à la Commission de la protection de la vie privée. La note transmise à la Commission et contenant les éléments de réponse au premier avis n° 29/2008, est jointe en annexe de cet exposé des motifs.

Commentaire des articles

Article 1

L'article premier contient les définitions d'un certain nombre de notions utilisées plus loin dans l'arrêté royal.

Par rapport à l'arrêté royal de 2003, les définitions des termes « service de radiomessagerie », « station terrienne mobile de satellite » et « service de communications personnelles mobiles par satellite » ont été supprimées. La raison en est simple : ces notions ne sont plus utilisées dans le nouvel

nieuwe KB gebruikt. Ze werden enkel gehanteerd in artikel 7 van het KB van 2003, dat nu een volledig nieuwe inhoud krijgt. Artikel 7 betreft de vereisten waaraan de internetsector zal moeten voldoen gedurende de bij artikel 12 voorziene overgangstermijn. In het KB van 2003 was dit een gelijkaardig artikel dat voorzag in minimale vereisten waaraan operatoren van telecommunicatienetwerken en verstrekkers van telecommunicatiediensten moesten voldoen gedurende de overgangstermijn die hen geboden werd om het KB te implementeren.

Ook de begrippen “oproepgegevens” en “lokalisatiegegevens” worden niet meer gedefinieerd. Het Koninklijk Besluit hanteert nu immers de termen “verkeersgegevens” en “locatiegegevens”, die gedefinieerd worden in artikel 2, 6° en 7° van de wet van 13 juni 2005 betreffende de elektronische communicatie.

De enige definitie die dus overblijft uit het oude KB is die van “werkelijke tijd”, die ongewijzigd blijft.

Twee nieuwe definities worden ingevoerd: die van dienst NTSU-CTIF, waarmee de centrale Technische Interceptiefaciliteit van de federale politie wordt bedoeld, en die van “internetsector”. De internetsector is het geheel van operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten die aan gebruikers toegang tot het internet aanbieden, die eindgebruikers via een netwerkaansluitpunt elektronische communicatiediensten over het internet aanbieden, die activiteiten op het internet aanbieden, of die faciliteiten hiervoor ter beschikking stellen zoals bijvoorbeeld netwerkdonderdelen,

arrêté royal. Elles n'apparaissaient qu'à l'article 7 de l'arrêté royal de 2003, article dont le contenu est intégralement modifié. L'article 7 porte sur les exigences auxquelles devra répondre le secteur Internet au cours de la période de transition prévue à l'article 12. Dans l'arrêté royal de 2003, il s'agissait d'un article similaire qui prévoyait les exigences minimales auxquelles devaient satisfaire les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications pendant la période de transition qui leur était offerte en vue de mettre en œuvre l'arrêté royal.

Les notions « données d'appel » et « données de localisation » ne sont pas définies non plus. Le présent arrêté royal utilise en effet les termes « données de trafic » et « données de localisation », définies à l'article 2, 6° et 7°, de la loi du 13 juin 2005 relative aux communications électroniques.

Par conséquent, la seule définition qui reste de l'ancien arrêté royal est celle, inchangée, de « temps réel ».

Deux nouvelles définitions ont été introduites : celle du service NTSU-CTIF, qui désigne le système central d'interception technique de la Police fédérale, ainsi que celle de « secteur Internet ». Le secteur Internet désigne l'ensemble des opérateurs de réseaux de communications électroniques et des fournisseurs de services de communications électroniques qui fournissent aux utilisateurs un accès à Internet, qui fournissent à des utilisateurs finals des services de communications électroniques sur Internet via un point de terminaison du réseau, qui fournissent des activités sur Internet, ou qui mettent à disposition des ressources à cet effet

lokalen, eindapparatuur of bijbehorende faciliteiten.

Wat deze definitie betreft dient rekening gehouden te worden met artikel 2 van de wet betreffende de elektronische communicatie, dat de begrippen “netwerkaansluitpunt”, “gebruiker”, “eindgebruiker” en “elektronische communicatiedienst” definieert. Er werd zoveel mogelijk getracht aan te sluiten bij de terminologie van de wet. In principe dienen alle niveaus van de internetsector hieronder begrepen te worden: zowel de operatoren die hun infrastructuur ter beschikking stellen voor het transport van de internetsignalen (fysieke connectie), de internet-toegangsleveranciers die aan de eindgebruiker toegang tot het internet geven, en de internetdienstenleveranciers die over het internet communicatiediensten aanbieden.

Artikel 2

Artikel 2 betreft de Coördinatieceel Justitie en behoudt dus het principe van het KB van 2003. Niettemin worden er enkele noodzakelijk aanvullingen gedaan met het oog op enerzijds de aanpassing van de terminologie aan de wet betreffende de elektronische communicatie, anderzijds de beveiliging van de Coördinatieceel en de gegevens die moeten meegedeeld worden.

Wat dit laatste betreft voorziet het Koninklijk Besluit immers dat de leden van de Coördinatieceel een veiligheidsadvies overeenkomstig artikel 22quinquies van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten, en

telles que, par exemple, des éléments de réseaux, des locaux, de l'équipement terminal ou des installations connexes.

Concernant cette définition, il convient de prendre en considération l'article 2 de la loi relative aux communications électroniques, qui définit les termes « point de terminaison du réseau », « utilisateur », « utilisateur final » et « service de communications électroniques ». L'on a tenté de coller au maximum à la terminologie de la loi. Il convient en principe de comprendre tous les niveaux du secteur Internet : les opérateurs qui mettent à disposition leur infrastructure pour le transport des signaux Internet (connexion physique), les fournisseurs d'accès à Internet, qui fournissent à l'utilisateur final l'accès à Internet, et les fournisseurs de services Internet, qui fournissent des services de communications par Internet.

Article 2

L'article 2 porte sur la Cellule de coordination de la Justice et maintient dès lors le principe prévu dans l'arrêté royal de 2003. Néanmoins, quelques ajouts nécessaires ont été apportés, en vue d'adapter la terminologie à la loi relative aux communications électroniques, d'une part, et d'assurer la protection de la Cellule de coordination et des données qui doivent être transmises, d'autre part.

À propos de ce dernier élément, l'arrêté royal prévoit en effet que les membres de la Cellule de coordination sont tenus d'avoir demandé un avis de sécurité, conformément à l'article 22quinquies de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. En outre, il est conféré au

veiligheidsadviezen aangevraagd moeten hebben. Eveneens wordt aan de Minister van Justitie het recht gegeven om personen die deel uitmaken van de Coördinatiecel, te weigeren. Deze maatregel is er om te voorkomen dat criminele organisaties als tegenmaatregel zouden gaan infiltreren in de Coördinatiecellen Justitie van de operatoren. Het is uitermate belangrijk dat de personeelsleden van de Coördinatiecel betrouwbaar zijn, zij dienen immers om te gaan met gevoelige informatie. Dit is ook van belang gezien de artikelen 46bis, §2, derde lid, 88bis, §2, tweede lid en 90quater, §2, tweede lid van het Wetboek van Strafvordering strafsancities voorzien voor de schending van de geheimhoudingsplicht overeenkomstig artikel 458 van het Strafwetboek.

Het Verslag aan de Koning bij het KB van 2003 maakte duidelijk dat de operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten vrij zijn om op hun manier aan de verplichtingen te voldoen en naar eigen inzicht de werking van de Coördinatiecel Justitie te organiseren. Als voorbeeld werd gegeven de mogelijkheid voor kleinere operatoren of dienstenverstrekkers om gezamenlijk een Coördinatiecel Justitie op te richten. Deze mogelijkheid wordt nu voor alle duidelijkheid expliciet in het Koninklijk Besluit ingeschreven.

Bovendien wordt ook nog ingeschreven dat alle operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten alle maatregelen dienen te nemen om de informatie die door de Coördinatiecel behandeld wordt, te beschermen en te beveiligen.

Ministre de la Justice le droit de refuser des personnes faisant partie de la Cellule de coordination. Cette mesure est prévue afin d'éviter que des organisations criminelles ne s'infiltrent en contre-mesure dans les Cellules de coordination de la Justice des opérateurs. Il est extrêmement important que les membres du personnel de la Cellule de coordination soient fiables. Ils doivent en effet traiter des informations sensibles. C'est important également dès lors que les articles 46bis, §2, alinéa 3, 88bis, §2, alinéa 2 et 90quater, §2, alinéa 2, du Code d'instruction criminelle prévoient des sanctions pénales en cas de violation de l'obligation de secret, conformément à l'article 458 du Code pénal.

Le Rapport au Roi de l'arrêté royal de 2003 indiquait clairement que les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques sont libres de remplir les obligations à leur manière et d'organiser le fonctionnement de la Cellule de coordination de la Justice comme ils l'entendent. Il était mentionné, à titre d'exemple, la possibilité pour les plus petits opérateurs ou fournisseurs de services de créer conjointement une Cellule de coordination de la Justice. Par souci de clarté, cette possibilité est inscrite explicitement dans l'arrêté royal.

Qui plus est, il est également prévu que tous les opérateurs de réseaux de communications électroniques et fournisseurs de services de communications électroniques sont tenus de prendre toutes les mesures en vue de protéger et de sécuriser les informations traitées par la Cellule de

Paragraaf 2 van artikel 2 blijft hetzelfde als in het KB van 2003.

Tenslotte vermeldt paragraaf 3 van artikel 2, in tegenstelling tot het KB van 2003, welke de identificatiegegevens zijn die de Coördinatiecel Justitie moet meedelen aan het Belgisch Instituut voor Postdiensten en Telecommunicatie, die deze dan zal doorgeven aan de Dienst voor het Strafrechtelijk Beleid van de Federale Overheidsdienst Justitie. Deze gegevens worden dit keer dus wel opgesomd in het Koninklijk Besluit zelf, dit om te vermijden dat er zich moeilijkheden voordoen in verband met de permanente beschikbaarheid van de Coördinatiecellen.

Artikel 3

Dit artikel geeft uitvoering aan de bevoegdheid die aan de Koning wordt toegewezen door artikel 46bis, §2, tweede lid van het Wetboek van Strafvordering: de technische voorwaarden voor de toegang tot de in artikel 46bis, §1 bedoelde gegevens, die beschikbaar zijn voor de procureur des Konings en voor de in dezelfde paragraaf aangewezen politiedienst.

Het artikel maakt een onderscheid tussen enerzijds operatoren die nummeringscapaciteit toegewezen gekregen hebben in het nationale nummeringsplan, en anderzijds de andere operatoren. Slechts in het eerste geval dienen de operatoren de dienst NTSU-CTIF toegang te verlenen tot de databanken met het klantenbestand. Dit zal via een beveiligde internettoepassing gebeuren, maar het is aan de dienst NTSU-CTIF om de verdere technische details te bepalen volgens dewelke

coordination.

Le paragraphe 2 de l'article 2 demeure identique par rapport à l'arrêté royal de 2003.

Enfin, contrairement à l'arrêté royal de 2003, le paragraphe 3 de l'article 2 indique quelles sont les données d'identification que la Cellule de coordination de la Justice doit transmettre à l'Institut belge des services postaux et des télécommunications, qui les communiquera ensuite au Service de la Politique criminelle du Service public fédéral Justice. Ces données sont donc bel et bien énumérées dans l'arrêté royal même et ce, afin d'éviter tout problème lié à la disponibilité permanente des Cellules de coordination.

Article 3

Cet article porte exécution de la compétence conférée au Roi par l'article 46bis, §2, alinéa 2, du Code d'instruction criminelle : les conditions techniques d'accès aux données visées à l'article 46bis, §1, qui sont disponibles pour le procureur du Roi et le service de police désigné au même paragraphe.

L'article distingue les opérateurs auxquels a été attribuée une capacité de numérotation dans le plan national de numérotation des autres opérateurs. Seuls les premiers sont tenus de donner accès aux bases de données comprenant le fichier des clients au service NTSU-CTIF. Cet accès sera assuré par une application Internet sécurisée, mais c'est au service NTSU-CTIF qu'il revient de déterminer les détails techniques complémentaires selon lesquelles cette procédure se déroule.

deze procedure verloopt.

Dit wil echter niet zeggen dat de dienst NTSU-CTIF zomaar op gelijk welk tijdstip deze databank zal kunnen consulteren. De regels van het Wetboek van Strafvordering moeten uiteraard gevolgd worden, en het is slechts als een vordering op basis van artikel 46bis door de dienst NTSU-CTIF ontvangen wordt, dat zij de databank kunnen consulteren. De operatoren kunnen overigens zien wanneer deze dienst toegang neemt tot de klantenbestanden, en kan dat dan ook aanklagen als dit niet gebeurt op basis van de procedure beschreven in het Koninklijk besluit: er dient een elektronisch verzoek van de dienst NTSU-CTIF te zijn. De dienst NTSU-CTIF bewaart een log en maakt een journaal op van iedere toegang en consultatie van de databank.

Voor de andere operatoren en dienstverleners verandert het Koninklijk Besluit niets: de gegevens dienen in werkelijke tijd meegedeeld te worden aan de onderzoeksrechter, de procureur des Konings of de officier van gerechtelijke politie.

De kosten van de operatoren om tegemoet te komen aan de vordering, zullen opgenomen worden in een bijlage bij het Koninklijk Besluit.

Artikel 4

Dit artikel geeft uitvoering aan de bevoegdheid die aan de Koning wordt toegewezen door artikel 88bis, §2, eerste lid van het Wetboek van Strafvordering, en wijzigt inhoudelijk niets aan de bepaling in het KB van 2003. Het verandert enkel de terminologie om deze aan te passen aan de wet betreffende de elektronische communicatie.

Cela ne signifie pas pour autant que le service NTSU-CTIF pourra tout simplement consulter à n'importe quel moment cette base de données. Il y a lieu bien entendu d'observer les règles du Code d'instruction criminelle et ce n'est qu'à la réception de la requête visée à l'article 46bis par le service NTSU-CTIF qu'il pourra consulter la base de données. Les opérateurs peuvent par ailleurs voir quand ce service accède aux fichiers des clients et dénoncer l'accès qui ne se produit pas sur la base de la procédure décrite dans l'arrêté royal: une requête électronique du service NTSU-CTIF est requise. Le service NTSU-CTIF conserve un log et fait un journal de chaque accès et consultation de la banque de données.

Quant aux autres opérateurs et fournisseurs de services, l'arrêté royal ne modifie rien: les données doivent être communiquées en temps réel au juge d'instruction, au procureur du Roi et à l'officier de police judiciaire.

Les frais auxquels s'exposent les opérateurs pour répondre à la requête figureront en annexe à l'arrêté royal.

Article 4

Cet article porte exécution de la compétence conférée au Roi par l'article 88bis, §2, alinéa 1^{er}, du Code d'instruction criminelle et ne change rien au contenu de la disposition de l'arrêté royal de 2003. Il modifie uniquement la terminologie en vue de l'adapter à la loi relative aux communications électroniques.

De eerste paragraaf van dit artikel behandelt de zogenaamde retro-opvraging, de tweede paragraaf van artikel 4 behandelt de “real time”-opsporing van telecommunicatie. Er kan verwezen worden naar het Verslag aan de Koning bij het KB van 2003.

Artikel 5

Dit artikel geeft uitvoering aan de bevoegdheid die aan de Koning werd opgedragen door artikel 90quater, §2 van het Wetboek van Strafvordering, en wijzigt inhoudelijk niets aan de bepaling in het KB van 2003.

Artikel 6

Artikel 6 bepaalt de functionele vereisten en technische specificaties voor de uitvoering van de maatregelen voorzien in de artikelen 46bis, 88bis en 90ter e.v. van het Wetboek van Strafvordering. Voor de maatregel van artikel 46bis was dit, bij gebrek aan wettelijke basis, nog niet voorzien in het KB van 2003. Aangezien bij de wet van 23 januari 2007 tot wijziging van artikel 46bis van het Wetboek van Strafvordering deze wettelijke basis voorzien werd, kan dit nu ook omgenomen worden in artikel 6 van het KB.

Ook hier werd de terminologie aangepast in functie van de wet betreffende de elektronische communicatie. Voor de rest zijn de vijf functionele vereisten uit paragraaf 1 die rechtstreeks uit de resolutie van de Raad van Ministers van de Europese Unie van 17 januari 1995 inzake de legale interceptie van telecommunicatieverkeer komen, hetzelfde gebleven.

Op te merken valt dat artikel 12 aan de

Le premier paragraphe de cet article traite de la demande dite rétrospective. Le deuxième paragraphe de l'article 4 traite du repérage de télécommunications effectué « en direct ». Il peut être renvoyé au Rapport au Roi de l'arrêté royal de 2003.

Article 5

Cet article porte exécution de la compétence conférée au Roi par l'article 90quater, §2, du Code d'instruction criminelle et ne change rien au contenu de la disposition de l'arrêté royal de 2003.

Article 6

L'article 6 fixe les exigences fonctionnelles et les spécifications techniques pour l'exécution des mesures prévues aux articles 46bis, 88bis ainsi que 90ter et suivants du Code d'instruction criminelle. À défaut de base légale, l'arrêté royal de 2003 ne les prévoyait pas encore pour la mesure visée à l'article 46bis. Dès lors que cette base légale a été prévue par la loi du 23 janvier 2007 modifiant l'article 46bis du Code d'instruction criminelle, l'article 6 de l'arrêté royal peut désormais le prévoir.

La terminologie a également été adaptée, en l'occurrence, selon la loi relative aux communications électroniques. Pour le reste, les cinq exigences fonctionnelles indiquées au paragraphe 1^{er}, issues directement de la résolution du Conseil des Ministres de l'Union européenne du 17 janvier 1995 relative à l'interception légale des télécommunications, demeurent identiques.

Il est à noter que l'article 12 accorde

internetsector een overgangperiode van een jaar geeft om te voldoen aan deze eisen. Andere operatoren moeten al op basis van het KB van 2003 voldoen aan deze vereisten.

De tweede paragraaf is een herhaling van wat in het KB van 2003 in artikel 7, §2, 5° stond, en is inhoudelijk niet gewijzigd.

De derde paragraaf voorziet tenslotte de technische specificaties van deze functionele eisen, voorzien in de standaarden van het European Telecommunications Standards Institute. Deze werden geactualiseerd en aangevuld met nieuwe normen.

Artikel 7

Dit artikel voorziet de uitvoeringsmodaliteiten van de maatregel omschreven in artikel 90ter e.v. van het Wetboek van Strafvordering voor de internetsector gedurende de bij artikel 10 voorziene overgangstermijn. M.a.w. dit artikel komt eigenlijk te vervallen een jaar na de publicatie van dit besluit. Artikel 7 wordt overigens, zoals eerder al aangegeven, toegepast samen met de andere artikelen van het KB, behalve artikel 6. De antwoordtermijnen van de artikelen 3, 4 en 5 gelden dus ook hier. De eerste paragraaf geeft de algemene bedoeling weer van dit artikel zoals hiervoor beschreven.

Inhoudelijk komt de tekst van artikel 7 overeen met wat in het KB van 2003 in artikel 7, §3 stond voor de andere operatoren.

Artikel 8

Artikel 8 stemt inhoudelijk overeen met artikel 8 van het KB van 2003. Het tweede lid werd echter gewijzigd in die

au secteur Internet une période de transition d'un an afin de répondre à ces exigences. Les autres opérateurs doivent déjà satisfaire à ces exigences sur la base de l'arrêté royal de 2003.

Le deuxième paragraphe est une répétition de ce qui est prévu à l'article 7, §2, 5°, de l'arrêté royal de 2003 et demeure inchangé quant au contenu.

Enfin, le troisième paragraphe précise les spécifications techniques de ces exigences fonctionnelles, prévues dans les standards du « European Telecommunications Standards Institute ». Elles ont été actualisées et complétées par de nouvelles normes.

Article 7

Cet article prévoit les modalités d'exécution de la mesure définie aux articles 90ter et suivants du Code d'instruction criminelle pour le secteur Internet pendant la période de transition visée à l'article 10. En d'autres termes, cet article deviendra en fait caduc un an après la publication du présent arrêté. D'ailleurs, ainsi qu'il a été indiqué plus haut, l'article 7 est applicable conjointement avec les autres articles de l'arrêté royal, à l'exception de l'article 6. Les délais de réponse prévus aux articles 3, 4 et 5 sont donc également valables pour cet article. Le premier paragraphe expose l'objet général de l'article comme exposé ci-avant.

Sur le plan du contenu, le texte de l'article 7 correspond à ce que prévoit l'article 7, §3, de l'arrêté royal de 2003 pour les autres opérateurs.

Article 8

Le contenu de l'article 8 correspond à celui de l'article 8 de l'arrêté royal de 2003. L'alinéa 2 a toutefois été modifié

zin dat de operatoren de klok op hun systemen die gebruikt wordt voor de registratie van de tijdstippen die in het besluit worden vermeld, moeten synchroniseren met het GPS-tijdssignaal.

Artikel 9

Artikel 9 is een herneming van artikel 10 van het KB van 2003.

Artikel 10

Artikel 10 is nieuw, en voorziet dat de Coördinatiecel Justitie de gegevens moet meedelen in een voor de verzoeker gemakkelijk te gebruiken vorm. Het voorziet ook de mogelijkheid dat een ministerieel besluit wordt genomen om een specifiek formaat voor de presentatie van de gegevens op te leggen.

Artikel 11

Ten gevolge van dit nieuwe Koninklijke Besluit, dient het KB van 2003 opgeheven te worden. Onderhavig Koninklijk Besluit vervangt het KB van 2003 volledig.

Artikel 12

Artikel 12 voorziet in twee overgangstermijnen.

De eerste paragraaf bepaalt dat, zoals hoger al omschreven, de internetsector een periode van een jaar heeft om aan de functionele en technische vereisten bepaald in de artikelen 6 en 10, te voldoen.

De tweede paragraaf voorziet in een overgangperiode voor de personen die op dit moment reeds deel uitmaken van de Coördinatiecellen Justitie: zij beschikken over een periode van twee

en ce que les opérateurs doivent synchroniser l'horloge utilisée dans leurs systèmes pour l'enregistrement des heures mentionnées dans l'arrêté avec l'heure GPS.

Article 9

L'article 9 est une répétition de l'article 10 de l'arrêté royal de 2003.

Article 10

L'article 10 est un nouvel article. Il prévoit que la Cellule de la coordination de la Justice doit transmettre les données sous une forme d'utilisation aisée pour le demandeur. Il prévoit en outre la possibilité de prendre un arrêté ministériel en vue d'imposer un format spécifique pour la présentation des données.

Article 11

En raison de ce nouvel arrêté royal, il convient d'abroger l'arrêté royal de 2003. Le présent arrêté royal remplace intégralement l'arrêté royal de 2003.

Article 12

L'article 12 prévoit deux périodes de transition.

Le premier paragraphe dispose que, ainsi qu'il a été indiqué ci-dessus, le secteur Internet dispose d'une période d'un an afin de répondre aux exigences fonctionnelles et techniques visées aux articles 6 et 10.

Le deuxième paragraphe prévoit une période de transition pour les personnes qui font d'ores et déjà partie des Cellules de coordination de la Justice : elles disposent d'une période

maand om een verzoek tot veiligheidsadvies in te dienen bij de minister van Justitie. Slechts de personen die een dergelijk verzoek binnen die twee maanden hebben ingediend zullen mogen verder deel uitmaken van de Coördinatiecel.

Artikel 13

Artikel 13 bepaalt dat de verdere uitvoering van dit Koninklijk Besluit is opgedragen aan de twee bevoegde ministers.

Ik heb de eer te zijn,

Sire,
van Uwe Majesteit,
de zeer eerbiedige
en zeer getrouwe dienaar,

De Minister van Justitie,

de deux mois en vue d'introduire une demande d'avis de sécurité auprès du ministre de la Justice. Seules les personnes qui auront introduit une telle demande dans les deux mois pourront continuer à faire partie de la Cellule de coordination.

Article 13

L'article 13 dispose que la poursuite de l'exécution du présent arrêté royal est confiée aux deux ministres compétents.

J'ai l'honneur d'être,

Sire,
de Votre Majesté,
le très respectueux
et très fidèle serviteur,

Le Ministre de la Justice,

Stefaan DE CLERCK

De Minister voor Ondernemingen en Vereenvoudigen,

Le Ministre pour l'Entreprise et la Simplification,

Vincent VAN QUICKENBORNE

Bijlagen**Annexes**

Ontwerp van Koninklijk Besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie

Antwoord op het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer nr. 29/2008 van 3 september 2008.

Deze nota wenst in te gaan op een aantal opmerkingen in het advies nr. 29/2008 van de Commissie voor de bescherming van de persoonlijke levenssfeer over het ontwerp van koninklijk besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie.

1. Band tussen het ontwerp “medewerking” en het ontwerp “dataretentie” (advies, § 11-14)

Het ontwerp KB “bewaring” bepaalt de categorieën van gegevens die de operatoren moeten bewaren, alsook de bijhorende bewaartermijnen, terwijl het ontwerp KB “medewerking” voor de operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten de te volgen modaliteiten bepaalt bij een gegevensdoorgifte aan de gerechtelijke autoriteiten. De Commissie meent dat, krachtens het voorzienbaarheidsbeginsel en omwille van de klaarheid en transparantie, één enkele gecoördineerde tekst deze materie zou moeten regelen: de operatoren kunnen immers slechts met de gerechtelijke autoriteiten meewerken en deze gegevens doorgeven die ze hebben

Projet d’arrêté royal déterminant les modalités de l’obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques

Réponse à l’avis n° 29/2008 du 3 septembre 2008 de la Commission de la protection de la vie privée.

La présente note a pour objet de répondre à un certain nombre d’observations formulées par la Commission de la protection de la vie privée dans son avis n° 29/2008 relatif au projet d’arrêté royal déterminant les modalités de l’obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

1. Lien entre le projet ‘collaboration’ et le projet ‘conservation’ (avis, points 11-14)

Le projet d’AR ‘conservation’ détermine les catégories de données à conserver par les opérateurs ainsi que les délais de conservation afférents, tandis que le projet d’AR ‘collaboration’ fixe les modalités que les opérateurs de réseaux de communications électroniques et les fournisseurs de services de communications électroniques doivent remplir pour transmettre ces données aux autorités judiciaires. La Commission est d’avis qu’en vertu du principe de prévisibilité et dans un souci de clarté et de transparence, un seul texte coordonné devrait réglementer la matière: les opérateurs ne peuvent en effet collaborer et transmettre aux autorités judiciaires que ce qu’ils ont pu conserver (cf. avis, point 14).

kunnen bewaren (zie advies, §14).

Daar waar de nauwe band tussen beide Koninklijke besluiten duidelijk is, is het toch niet aangewezen om beide materies in één tekst te regelen. Eerst en vooral hebben beide teksten een verschillende wettelijke basis. Het ontwerp KB dataretentie vindt zijn wettelijke basis in artikel 126 van de wet betreffende de elektronische communicatie, terwijl het ontwerp KB medewerkingsplicht zijn wettelijke grondslag vindt in de artikelen 46bis, 88bis, en 90ter van het Wetboek van Strafvordering. Dit op zich is al een gegronde reden om legistiek te voorzien in twee verschillende KB's.

Er moet ook op gewezen worden dat de verplichting tot dataretentie en de medewerkingsplicht elkaar niet noodzakelijk volledig overlappen. In het kader van de dataretentieverplichting dienen de operatoren, gedefinieerd in artikel 2, 11° van de wet van 13 juni 2005 betreffende de elektronische communicatie als “een persoon die een kennisgeving heeft ingediend overeenkomstig artikel 9” bepaalde gegevens te bewaren voor strafrechtelijke doeleinden.

Daarnaast mogen de operatoren ook gegevens bewaren voor bedrijfsredenen, marketingdoeleinden of de levering van diensten met toegevoegde waarde (richtlijn 2002/58/EG).

De artikelen 46bis, 88ter en 90ter van het Wetboek van Strafvordering spreken echter over ‘operatoren van elektronische communicatiediensten en verstrekkers van elektronische communicatiediensten’ die gehouden zijn hun medewerking te verlenen aan justitie, hetgeen inhoudt dat men de bewaarde gegevens waarover men

Bien que le lien étroit entre les deux arrêtés royaux soit évident, il n'est cependant pas indiqué de régler les deux matières dans un seul texte. Tout d'abord, les deux textes reposent sur une base légale différente. Le projet d'AR ‘conservation’ trouve sa base légale dans l'article 126 de la loi relative à la communication électronique, tandis que le projet d'AR ‘collaboration’ trouve son fondement légal dans les articles 46bis, 88bis et 90ter du Code d'Instruction criminelle. Ceci constitue en soi déjà une raison fondée pour, d'un point de vue légistique, rédiger deux AR distincts.

Il convient également de souligner que l'obligation de conservation de données et l'obligation de collaboration ne se recouvrent pas nécessairement entièrement.

Dans le cadre de l'obligation de conservation de données, les opérateurs, définis à l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques comme étant « toute personne ayant introduit une notification conformément à l'article 9 », doivent conserver certaines données à des fins pénales.

Parallèlement, les opérateurs peuvent également conserver des données pour des raisons d'exploitation, à des fins de commercialisation ou pour la fourniture de services à valeur ajoutée (directive 2002/58/CE).

Par contre, les articles 46bis, 88ter et 90ter du Code d'Instruction criminelle disposent que ‘les opérateurs d'un réseau de communication électronique et les fournisseurs de services de communication électronique’ sont tenus de prêter leur concours à la justice, ce qui implique l'obligation de communiquer à la justice les données conservées dont

beschikt (in welk kader ook) dient mee te delen aan justitie indien daarom verzocht wordt.

De medewerkingsplicht is derhalve ruimer (cfr. Ook infra over het toepassingsgebied *ratione personae*).

Daarnaast is de medewerkingsplicht al geregeld in een KB van 2003, dat door huidig ontwerp opgeheven wordt. De regering meent dat het van belang is om beide ontwerpen samen te bestuderen, maar omdat betreffende de dataretentie ook artikel 126 van de wet betreffende de elektronische communicatie gewijzigd dient te worden, en de parlementaire procedure doorlopen moet worden, is het goed mogelijk dat het ontwerp “medewerking” sneller aangenomen wordt dan het ontwerp “dataretentie”.

2. Het toepassingsgebied *ratione personae* (advies, § 15-23)

- *“operatoren van elektronische communicatienetwerken en verstrekkers van elektronische communicatiediensten”:*

De Commissie meent dat deze term moet worden begrepen in de zin van artikel 2, 11°, van de wet betreffende de elektronische communicatie (zie randnummer 16). Dit klopt echter niet.

De gebruikte terminologie in het ontwerp van koninklijk besluit neemt de termen uit het Wetboek van Strafvordering over omdat precies de artikelen 46bis, 88bis en 90quater de wettelijke basis vormen van dit Koninklijk besluit. Desbetreffend dient gewezen op de autonomie van het strafrecht.

De Commissie zegt in randnummer 18 dat de artikelen 46bis, 88bis en 90quater alleen maar kunnen slaan op:

- hetzij de operatoren *sensu strictu*,

ils disposent (dans quelque contexte que ce soit), si la demande leur en est faite.

Par conséquent, l’obligation de collaboration est plus large (voir également ci-après sous ‘le champ d’application *ratione personae*’).

Ensuite, l’obligation de collaboration a déjà été réglée dans un AR de 2003, lequel est abrogé par le présent projet. Le gouvernement estime qu’il importe d’examiner les deux projets conjointement, mais vu que pour la conservation de données, il convient de modifier également l’article 126 de la loi relative aux communications électroniques et que la procédure parlementaire doit être suivie, il est fort possible que le projet ‘collaboration’ soit adopté plus rapidement que le projet ‘conservation’.

2. Le champ d’application *ratione personae* (avis, points 15-23)

- *“les opérateurs d’un réseau de communications électroniques et les fournisseurs d’un service de communication électronique”*

La Commission est d’avis que ces termes doivent être entendus au sens de l’article 2, 11°, de la loi sur les communications électroniques (voir point 16). Ce n’est cependant pas exact.

La terminologie utilisée dans le projet d’arrêté royal reprend les termes du Code d’instruction criminelle, parce que les articles 46bis, 88bis et 90quater constituent précisément la base légale de cet arrêté royal. A cet égard, il convient de souligner l’autonomie du droit pénal.

Au point 18, la Commission affirme que les articles 46bis, 88bis et 90quater ne peuvent viser :

- soit que les opérateurs *sensu*

nl. diegenen die, overeenkomstig artikel 9, §1 WEC een kennisgeving in de vereiste vorm hebben gestuurd aan het BIPT;

- hetzij de operatoren *sensu strictu*, evenals de verstrekkers die in overtreding van artikel 9 WEC geen kennisgeving stuurden aan het BIPT, maar die, *de facto*, deze activiteit uitoefenen.

De artikelen 46bis; 88bis en 90quater van het Wetboek van Strafvordering voorzien in een wettelijke medewerkingsplicht voor operatoren en verstrekkers. Zij zijn in ieder geval verplicht tot medewerking. De modaliteiten van die medewerking dient te worden bepaald bij Koninklijk Besluit, en dat is dan ook het onderwerp van onderhavig KB.

Het probleem ligt voornamelijk in het begrip “*verstrekker*” dat nergens gedefinieerd is. Dit begrip werd in het Wetboek van Strafvordering ingevoerd door de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en –telecommunicatie. De toenmalige regering introduceerde dit begrip bij wijze van amendement en motiveerde als volgt:

“De term « operator van een telecommunicatienetwerk » is in de huidige stand van de wetgeving te beperkt geworden. Het zal immers meer en meer voorkomen dat de vraag om medewerking van het openbaar ministerie of van de onderzoeksrechter gericht zal moeten worden aan een dienstenaanbieder die niet noodzakelijk een operator van een netwerk is (bijvoorbeeld een Internet-toegangsleverancier of de zogenaamde « acces-providers »).”

(cfr. Belgische Senaat, zitting 1997-1998, 1-823/3 en de Belgische Kamer van Volksvertegenwoordigers, gewone zitting 1996-1997, 1075/2 en 9).

stricto, c'es-à-dire ceux qui ont envoyé une notification en bonne et due forme à l'IBPT, conformément à l'article 9, § 1^{er}, LCE ;

- soit les opérateurs *sensu stricto*, ainsi que les fournisseurs qui, en violation de l'article 9 LCE n'ont pas envoyé de notification à l'IBPT, mais qui, *de facto*, exercent cette activité.

Les articles 46bis, 88bis et 90quater du Code d'instruction criminelle prévoient une obligation légale de collaboration pour les opérateurs et les fournisseurs. Ils sont de toute façon obligés de collaborer. Les modalités de cette collaboration doivent être déterminées par arrêté royal, et celles-ci sont donc le sujet du présent arrêté.

Le problème réside principalement au niveau de la notion de « fournisseur », laquelle n'est définie nulle part. Cette notion a été introduite dans le Code d'Instruction criminelle par la loi du 10 juin 1998 modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées. Le gouvernement de l'époque a introduit cette notion sous la forme d'un amendement et a formulé la justification suivante:

« Le terme “opérateur d'un réseau de télécommunication” est devenu trop restreint dans l'état actuel de la législation. En effet, il arrivera de plus en plus que la requête de concours technique du ministère public ou du juge d'instruction devra être adressée à un fournisseur de service qui n'est pas nécessairement un opérateur d'un réseau (par exemple les fournisseurs d'accès à Internet ou ce qu'on appelle les 'access providers'. »

(cf. Sénat, session 1997-1998, 1-823/3 et Chambre des Représentants, session ordinaire 1996-1997, 1075/2 et 9).

Op dat moment was er nog geen wet betreffende de elektronische communicatie, en werd het begrip operator gedefinieerd door de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (de zgn. Belgacomwet). Artikel 68, 23° van deze wet luidde toen als volgt:

“Operatoren” : personen die houder zijn van een individuele vergunning die uitgereikt is krachtens de artikelen 87, 89, §§ 1 en 2, en 92bis van deze wet of die een aangifte hebben gedaan overeenkomstig artikel 88 van deze wet.

M.a.w. het was duidelijk de bedoeling van de wetgever om een toepassingsgebied te creëren dat het begrip operator overstijgt en dat in voorkomend geval de vereiste medewerking aan het openbaar ministerie of de onderzoeksrechter niet beperkt tot het begrip operator zoals gedefinieerd in de Belgacomwet.

Het Koninklijk Besluit van 2003 tot uitvoering van de wet van 1998 werd tweemaal voorgelegd aan de privacycommissie voor advies, die eerst een ongunstig advies uitbracht en daarna een gunstig. De Commissie heeft hierin het bijzonder ruime toepassingsgebied van het KB benadrukt. De term “verstrekker van een telecommunicatiedienst” zoals opgenomen in de tekst slaat volgens de Commissie op elke verstrekker van een toegang, elke inlichtingendienst, certficator of andere entiteit die een dienst in de telecommunicatiesector voorstelt.

Gezien bovenstaande redenering is de medewerkingsplicht dus niet beperkt tot de operatoren *sensu strictu*. Zij geldt ook voor verstrekkers van elektronische communicatiediensten die geen operator zijn in de zin van de wet van 13 juni 2005.

A cette époque, la loi relative à la communication électronique n’existait pas encore et le terme « opérateur » était défini par la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (ladite ‘loi Belgacom’). L’article 68, 23°, de cette loi était à l’époque libelle comme suit :

“opérateurs” : personnes détentrices d’une autorisation individuelle délivrée en vertu des articles 87, 89, §§ 1er et 2, et 92bis de la présente loi ou ayant fait une déclaration en vertu de l’article 88 de la présente loi

En d’autres termes, le législateur avait clairement l’intention de créer un champ d’application plus large que la notion d’opérateur, qui, le cas échéant, ne limite pas la collaboration requise avec le ministère public ou le juge d’instruction à la notion d’opérateur telle que définie dans la ‘loi Belgacom’.

L’arrêté royal de 2003 portant exécution de la loi de 1998 a été soumis deux fois à l’avis de la commission de la protection de la vie privée, laquelle rendit d’abord un avis défavorable et ensuite un avis favorable. Dans son avis, la Commission a souligné le champ d’application particulièrement large de l’AR. La notion de “fournisseurs de services de télécommunication” telle qu’elle figure dans le texte s’applique selon la Commission à tout fournisseur d’accès, service d’information, certificateur ou autre entité proposant un service dans le secteur des télécommunications.

Vu le raisonnement susmentionné, l’obligation de collaboration ne se limite donc pas aux opérateurs *sensu stricto*. Elle s’applique également aux fournisseurs de services de communication électroniques qui ne sont pas des opérateurs au sens de la loi du

13 juin 2005.

Er dient ook opgemerkt dat in het kader van het voorontwerp van wet tot wijziging van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie het begrip “operator” een nieuwe definitie krijgt. Onder “operator” moet voortaan verstaan worden “*een persoon die onder de verplichting valt een kennisgeving te doen overeenkomstig artikel 9*”.

De Commissie heeft overigens wel gelijk wanneer zij zegt dat de “aanbieders en doorverkopers” bedoeld in artikel 9, §§ 5 en 6, van de wet betreffende de elektronische communicatie niet beoogd worden door huidig ontwerp. Artikel 9, §7, tweede lid van de WEC voorziet immers het volgende:

“Bij een besluit vastgesteld na overleg in de Ministerraad, stelt de Koning op voorstel van de minister van Justitie en de minister, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de technische en administratieve maatregelen vast die aan de aanbieders en doorverkopers waarnaar verwezen wordt in paragraaf 5 en 6 worden opgelegd om de oproeper te kunnen identificeren en het opsporen, lokaliseren, afluisteren, kennisnemen en opnemen van privé-communicatie mogelijk te maken onder de voorwaarden bepaald door de artikelen 46bis, 88bis en 90ter tot 90decies van het Wetboek van strafvordering.”

Dit wil overigens niet zeggen dat voor deze categorie geen medewerkingsplicht geldt. Zoals hoger gezegd, zijn zij net als alle operatoren en verstrekkers door de artikelen 46bis, 88bis en 90quater van het Wetboek van Strafvordering tot medewerking met de gerechtelijke autoriteiten gehouden. Alleen zullen de modaliteiten van deze medewerking bij een apart Koninklijk Besluit geregeld worden. Zij zijn dus vrij zelf de modaliteiten van deze medewerking te bepalen, doch de medewerking op zich blijft verplicht.

Il convient également d'observer que, dans le cadre de l'avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques, le terme « opérateur » acquiert une nouvelle définition. Dorénavant, il faut entendre par “opérateur” « toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9 ».

La Commission a par contre raison lorsqu'elle considère que les ‘fournisseurs et revendeurs’ visés à l'article 9, §§ 5 et 6, de la loi sur les communications électroniques ne sont pas visés par le présent projet. En effet, l'article 9, § 7, de la LCE dispose ce qui suit:

“Par arrêté délibéré en Conseil des ministres, le Roi fixe, sur proposition du ministre de la Justice et du ministre, après avis de la Commission pour la protection de la vie privée et de l'Institut, les mesures techniques et administratives imposées aux fournisseurs et revendeurs visés aux §§ 5 et 6, en vue de permettre l'identification de l'appelant, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par les articles 46bis, 88bis et 90ter à 90decies du Code d'instruction criminelle.”

Ceci ne veut d'ailleurs pas dire que l'obligation de collaboration ne s'applique pas à cette catégorie. Comme expliqué ci-dessus, comme tous les opérateurs et fournisseurs ils sont tenu de collaborer avec les autorités judiciaires en vertu des articles 46bis, 88bis et 90quater du Code d'instruction criminelle. Cependant, les modalités de cette collaboration seront réglées par un arrêté royal séparé. Ils sont donc libres de déterminer eux-mêmes les modalités de la collaboration, mais la collaboration comme telle reste obligatoire.

Voor deze aanbieders en doorverkopers zal dus in de toekomst een apart KB worden uitgewerkt waarin de modaliteiten van hun medewerkingsplicht geregeld worden.

- *“de internetsector”*

De Commissie meent dat de definitie van het begrip “internetsector” te breed gedefinieerd is.

Door te verwijzen naar “het geheel van natuurlijke en rechtspersonen” geeft het ontwerp inderdaad de indruk dat méér bedoeld wordt dan het begrip “operatoren van elektronische communicatiediensten en verstrekkers van elektronische communicatiediensten” dat elders in het ontwerp gebruikt wordt. Om deze mogelijk te brede interpretatie uit te sluiten, zal in de definitie van internetsector dezelfde terminologie als in de rest van het ontwerp gebruikt worden.

3. De dienst NTSU-CTIF (Artikel 1 en 3)

- *wettelijke basis – plaats van de dienst binnen de federale politie (advies, § 24-26)*

Op structureel niveau maakt de NTSU deel uit van de speciale eenheden van de federale politie (CGSU). Deze laatste staat rechtstreeks onder auspiciën van de commissaris-generaal. Deze positie is belangrijk in termen van garanties en onafhankelijkheid. Het scheiden van de personen die om telefoontap verzoeken (per definitie de onderzoekers) en de personen die het verzoek technisch uitvoeren (de NTSU) voorkomt dat uiterst intrusieve handelingen worden verricht zonder dat streng wordt gecontroleerd of de vereiste machtigingen aanwezig zijn.

Par conséquent, un AR réglant mes modalités de l’obligation de collaboration sera élaboré ultérieurement pour ces fournisseurs et revendeurs.

- *‘le secteur internet’*

La Commission estime que la définition de la notion de ‘secteur internet’ est trop large.

En évoquant ‘l’ensemble des personnes physiques et des personnes morales’, le projet donne en effet l’impression de viser davantage que la notion ‘opérateurs d’un réseau de communications électroniques et fournisseurs d’un service de communication électronique’ utilisée ailleurs dans le projet. Afin d’exclure cette interprétation potentiellement trop large, les termes de la définition de ‘secteur internet’ seront alignés sur la terminologie utilisée dans le reste du projet.

3. Le service NTSU-CTIF (Articles 1 et 3)

- *base légale – positionnement du service au sein de la police fédérale (avis, points 24-26)*

Sur le plan structurel, le NTSU fait partie des unités spéciales de la police fédérale (CGSU). Cette dernière se trouve directement sous les auspices du commissaire général. Cette position est importante en termes de garanties et d’indépendance. De fait, séparer les demandeurs des écoutes (par définition les enquêteurs), de ceux qui mettent techniquement la demande à exécution (le NTSU) est de nature à empêcher que des actes à caractère hautement intrusifs ne soient exécutés sans qu’un contrôle strict de la présence des autorisations requises ne soit exercé.

De persoon die een verzoek indient, moet daarbij een kopie van de door een bevoegde autoriteit behoorlijk opgestelde machtigingen en vorderingen voegen.

Bovendien kan de verzoeker of zijn meerdere geen “druk” uitoefenen aangezien het CGSU hiërarchisch rechtstreeks afhangt van de directeur-generaal van de federale politie en niet van de lokale of federale onderzoekers. Er is dus een feitelijke scheiding tussen de persoon die een resultaat wil bereiken (het doel) en de persoon die over de instrumenten (de middelen) beschikt om het resultaat te bereiken.

Ten slotte heeft het CGSU geen enkele initiatiefbevoegdheid en werkt het enkel als ondersteuning van verzoekende diensten. Het CGSU neemt dan ook geen initiatief voor onderzoeken, noch voor reactieve of proactieve opsporingen en al zeker niet voor telefoontaps.

Er moet tevens worden gewezen op het gegeven dat de NTSU/CTIF geen toegang heeft tot de inhoud van de afgetapte gegevens, die rechtstreeks en elektronisch aan de verzoeker worden bezorgd. De inhoud van de afgetapte communicatie kan enkel ter kennis worden gebracht van de OGP's/AGP's die met naam vermeld worden in de door de onderzoeksrechter opgestelde vordering. De interceptiefaciliteit is zodanig ontworpen dat de gegevens technisch enkel toegankelijk zijn voor personen van wie de naam vermeld is op de lijst.

De controle van de tenuitvoerlegging van deze wettelijke voorschriften is overigens technisch geïmplementeerd in de NTSU/CTIF-structuur aangezien alle uitgevoerde en aan de gang zijnde handelingen in het systeem worden “bewaard”.

De met het toezicht op de federale politie

De fait, la personne qui introduit une demande doit y annexer une copie des autorisations et réquisitoires dûment établis par une autorité compétente.

De plus, aucune « pression » ne peut être exercée par le demandeur ou son supérieur, puisque, hiérarchiquement, la CGSU dépend directement du Directeur général de la Police fédérale et non des enquêteurs locaux ou fédéraux. Il existe donc une séparation de fait entre celui qui veut obtenir un résultat (la fin) et celui qui dispose des outils (les moyens) pour l'atteindre.

Finale­ment, la CGSU ne dispose d'aucun pouvoir d'initiative et ne travaille qu'en appui des services demandeurs. La CGSU n'initie donc pas d'enquêtes ni de recherches réactives ou proactives et encore moins d'écoutes téléphoniques.

Il faut également rappeler que le NTSU/CTIF n'a pas accès au contenu des données interceptées, celles-ci sont transmises directement et informatiquement vers le demandeur. Le contenu des communications interceptées ne peuvent être portées qu'à la connaissance des OPJ/APJ nommément cités dans la réquisition établie par le juge d'instruction. Le système d'interception est construit de telle sorte que les données ne seront techniquement accessibles qu'aux personnes reprises nommément sur la liste.

Le contrôle de la mise en œuvre de ce prescrit légal est d'ailleurs techniquement implémenté dans la structure NTSU/CTIF puisque toutes les actions réalisées et entreprises sur le système sont « logées et sauvegardées ».

Les services chargés du contrôle de la

belaste diensten (inzonderheid het comité P en de inspectie) hebben ook de mogelijkheid om de toepassing van de procedures van de CTIF (“audit”) op algemene wijze te controleren.

De onderzoeksrechters kunnen – eventueel bijgestaan door het comité P – in het kader van hun dossiers eveneens de door de CTIF genomen maatregelen controleren.

Deze mogelijkheden zijn niet enkel theoretisch aangezien voornoemde instanties reeds meermaals van dit voorrecht gebruik hebben gemaakt.

De leden van de CTIF worden onderworpen aan een veiligheidsonderzoek dat versneld wordt uitgevoerd in het kader van de wet betreffende de veiligheidsmachtigingen.

- *is de CTIF een gegevensverwerker in de zin van de wet betreffende de bescherming van de persoonlijke levenssfeer? (advies, § 27)*

De Commissie meent dat de NTSU-CTIF, voor zover zij persoonsgegevens verwerkt in de zin van artikel 1 van de WVP, daarvan aangifte moet doen bij de Commissie. De federale politie heeft geen aangifte gedaan van zulke verwerking.

De NTSU/CTIF beheert geen gepersonaliseerde gegevensbank: de uitgevoerde identificaties worden rechtstreeks aan de onderzoekers bezorgd zonder dat een kopie ervan wordt bewaard in de NTSU/CTIF.

Zoals hierboven uiteengezet, antwoorden de operatoren rechtstreeks aan de verzoeker.

In het kader van de taps worden enkel statistische gegevens (aantal

police fédérale (notamment le comité P et l'Inspection) ont également la possibilité de contrôler, de manière générale, l'application des procédures prévues au CTIF («audit»).

Dans le cadre de leurs dossiers, les juges d'instruction - éventuellement assistés par le comité P - peuvent également contrôler les mesures qui ont été prises par le CTIF.

Ces possibilités ne sont pas que théoriques puisque ces instances ont, à plusieurs reprises déjà, fait usage de cette prérogative.

Les membres du CTIF sont soumis à une enquête de sécurité. Celle-ci est diligentée dans le cadre de la loi sur les habilitations de sécurité.

- *Le CTIF est-il un prestataire de données au sens de la loi relative à la protection de la vie privée ? (avis, point 27)*

La Commission est d'avis que dans la mesure où il traite des données à caractère personnel au sens de l'article 1^{er} de la LVP, le NTSU-CTIF doit en faire la déclaration à la Commission. La police fédérale n'a fait aucune déclaration de ce traitement.

Le NTSU/CTIF ne gère pas de base de données personnalisée: les identifications réalisées sont directement transmises aux enquêteurs sans qu'une copie n'en soit gardée au NTSU/CTIF.

Comme expliqué ci-dessus, les réponses des opérateurs seront faites directement au demandeur.

Dans le cadre des interceptions, seules des données statistiques (nombre de

maatregelen, duur, enz.) en technische gegevens (LLID, nummer van de vordering, naam van dossiers, enz.) bewaard.

mesures, durées, etc.) et des données techniques (LLID, Nr de réquisitoire, nom de dossiers, etc.) sont sauvegardées.

De andere gegevens worden maar op de servers van de NTSU/CTIF bewaard zolang het dossier wordt behandeld (bovendien zonder dat de NTSU toegang heeft tot de inhoud).

Les autres données ne sont conservées sur les serveurs du NTSU/CTIF que le temps de traitement du dossier (de plus sans que le NTSU ait accès au contenu).

Wanneer de aftapmaatregel is afgehandeld, worden alle gegevens aan de onderzoekers (verzoekers) bezorgd die deze verwerken overeenkomstig het bepaalde in artikel 90ter (vernietiging van de notities, verslag om de vijf dagen, neerlegging ter griffie, enz.).

La mesure d'interception clôturée, toutes les données sont transmises aux enquêteurs (demandeurs) qui les traitent selon le prescrit de l'art 90ter (destruction des notes, rapport de 5 jours, dépôt au greffe, etc.).

De NTSU/CTIF heeft dus geen toegang tot de inhoud van de gegevens, en treedt m.a.w. niet op als verantwoordelijke voor de verwerking. Er dient dus geen aangifte ingediend te worden bij de Commissie.

Le NTSU/CTIF n'a donc pas accès au contenu des données et, en d'autres termes, n'agit pas en tant que responsable du traitement. Aucune déclaration ne doit donc être faite à la Commission.

- *de "permanente toegang" van het CTIF tot de klantenbestanden van operatoren (advies, § 42-48)*

- *'l'accès permanent' du CTIF aux fichiers clients des opérateurs (avis, points 42-48)*

De commissie meent dat een permanente toegang van het CTIF tot de klantenbestanden van operatoren een te verregaande vorm van intrusie in de privacy is en dat dit het proportionaliteitsbeginsel niet eerbiedigt.

La Commission est d'avis qu'un accès permanent du CTIF aux fichiers clients des opérateurs représente une forme d'intrusion excessive dans la vie privée et n'est pas respectueux du principe de proportionnalité.

Daarom dient meer uitleg gegeven te worden over de manier waarop het proces van toegang verloopt. Het woord "permanent" zal in ieder geval vervangen worden door het woord "geautomatiseerd", daar het hier in principe niet om een permanente toegang gaat.

Les modalités du processus d'accès doivent dès lors être précisées. Le mot 'permanent' sera en tout cas remplacé par le mot 'automatisé' car en principe, il ne s'agit en l'occurrence pas d'un accès permanent.

Het ontwerp beoogt de processen die verband houden met de identificatie te

Ce qui est visé par le projet, c'est de faciliter les processus liés à

vergemakkelijken met als gevolg een daling van de kosten en geen ongebreidelde toename van de identificatiemogelijkheden.

Het was de bedoeling dat de NTSU/CTIF gemakkelijker een bestand met de gegevens van de klanten van de operatoren zou kunnen raadplegen, zulks inzonderheid dankzij een door de NTSU/CTIF elektronisch behandeld verzoek (en geen manuele of telefonische raadplegingen meer en evenmin per fax).

De automatisering van de processen verhoogt de snelheid waarmee de informatie ter beschikking wordt gesteld van de verzoekers, vermindert de manuele werklast en de risico's van fouten bij de verwerking (tikfout bijvoorbeeld) en maakt de controle a posteriori mogelijk van alle verzoeken die werden gedaan (in het bijzonder dankzij een logging).

In feite is dit geautomatiseerd proces meer privacyvriendelijk dan de manuele of telefonische raadplegingen of via fax, die bijvoorbeeld niet de controle door middel van loggings toelaten, het risico van verlies van gegevens en eventuele fouten bij de gegevensverwerking.

Belangrijk is ook dat enkel de verzoeken gaan via de NTSU/CTIF en daar worden gecontroleerd. De antwoorden worden daarentegen rechtstreeks aan de oorspronkelijke verzoeker bezorgd zonder opnieuw langs de NTSU/CTIF te gaan.

Dit is eveneens gunstig voor de gegevensbescherming.

- *garanties en veiligheid in verband met de rechtstreekse toegang (advies, §*

l'identification avec par corollaire la diminution des coûts et non l'augmentation effrénée des possibilités d'identification.

L'objectif était de faciliter au NTSU/CTIF l'interrogation d'un fichier reprenant les informations des clients des opérateurs grâce notamment à une requête traitée informatiquement par le NTSU/CTIF (et non plus une interrogation manuelle, téléphonique ou par fax).

L'automatisation des processus augmentera la vitesse de mise à disposition de l'information aux demandeurs, diminuera la charge de travail manuelle ainsi que les risques d'erreurs dans le traitement (erreur de frappe par exemple) et permettra le contrôle, à posteriori, de toutes les demandes qui auront été réalisées (notamment grâce à un logging).

En fait, ce processus automatisé est plus respectueux de la protection de la vie privée que les consultations manuelles, téléphoniques ou par télécopie, qui ne permettent par exemple pas le contrôle à l'aide de loggings et qui comportent un risque de perte de données et potentiellement des erreurs lors du traitement des données.

Il est également important que seules les demandes passent via le NTSU/CTIF et y soient contrôlées. En revanche, les réponses sont directement délivrées au demandeur initial, sans repasser par le NTSU/CTIF.

Ceci contribue également à la protection des données.

- *garanties et sécurité entourant l'accès direct (avis, points 49-52)*

49-52)

De Commissie is van oordeel dat het ontwerp bespaart op de garanties die samengaan met een rechtstreekse toegang (bewaarmaatregelen).

De NTSU neemt twee soorten maatregelen om de gegevens met betrekking tot de maatregelen waarvoor zij verantwoordelijk is te beschermen:

- fysieke maatregelen: beperkte toegang, gecontroleerde toegang met badge, gebouw dat fysiek beschermd wordt, permanente bezetting, camera's, logging van personen die binnenkomen en vertrekken;
- softwarematige maatregelen: verlenen van rechten op grond van specifieke profielen, loggingcontrole van elke op het netwerk verrichte handeling, toegang verleend per dossier (geen algemene toegang) wanneer de naam van de betrokkene specifiek vermeld is op de vordering van de onderzoeksrechter, beveiligde overdracht.

De Commissie voor de Bescherming van de persoonlijke levenssfeer heeft overigens een lijst van referentiemaatregelen opgesteld over de beveiliging van verwerking van persoonsgegevens. Deze lijst is echter bedoeld voor verantwoordelijken voor een verwerking en wil als hulp dienen bij de implementatie van een degelijke beveiliging. Hierboven hebben we echter uitgelegd dat de dienst NTSU-CTIF niet beschouwd kan worden als een verantwoordelijke voor de verwerking en dat zij slechts een rol als doorgeefluik van gegevens heeft. Het is precies in deze rol als doorgeefluik dat de bovenstaande beveiligingsmaatregelen genomen worden. Er wordt ook uitdrukkelijk in artikel 3 van het ontwerp van KB toegevoegd dat een log bewaard

La Commission est d'avis que le projet fait l'économie des garanties entourant un accès direct (mesures de sauvegarde).

Les mesures prises par le NTSU pour protéger les informations relatives aux mesures dont il est responsable sont de deux ordres :

- mesures physiques : accès limité, accès contrôlé et badgé, bâtiment faisant l'objet d'une protection physique, occupation permanente, caméras, login des entrées et sorties ;
- mesures Software : attribution des droits en fonction de profils spécifiques, logging contrôle de chaque action faite sur le réseau, accès donné par dossier (pas d'accès général) lorsque le nom de l'intéressé est spécifiquement et nommément spécifié sur le réquisitoire du juge d'instruction, transmission sécurisée.

La Commission de la Protection de la Vie privée a par ailleurs dressé une liste de mesures de référence sur la sécurisation du traitement de données à caractère personnel. Cette liste s'adresse toutefois aux responsables d'un traitement et se veut être une aide dans le cadre de l'implémentation d'une sécurisation adéquate. Ci-dessus, nous avons cependant expliqué que le service NTSU/CTIF ne peut pas être considéré comme un responsable de traitement de données et qu'il ne sert que d'interface de données. Les mesures de sauvegarde susmentionnées sont précisément prises dans le cadre de ce rôle d'interface. Il est également expressément ajouté à l'article 3 du projet d'arrêté royal qu'un log est conservé et qu'un journal est fait de

wordt en een journaal opgemaakt van iedere consultatie van de databank. Uiteraard dient het veiligheidsbeleid van dag tot dag geëvalueerd te worden door de dienst NTSU-CTIF, en waar nodig de nodige maatregelen genomen te worden voor een betere beveiliging.

4. De Coördinatieceel Justitie (artikel 2) (advies, § 32)

Volgens artikel 2 §1, 4de lid, van het ontwerp heeft de Minister van Justitie het recht om “personen die deel uitmaken van de Coördinatieceel Justitie te weigeren”. De Commissie meent dat dit ministeriële voorrecht slechts kan worden uitgeoefend in overeenstemming met de voormelde wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

Dit is echter niet het geval. Er zijn meerdere hypotheses denkbaar waar de Minister van Justitie het recht moet krijgen om bepaalde personen die deel uitmaken van de coördinatieceel Justitie te weigeren. Denk hierbij in de eerste plaats aan de betrokkenheid van een persoon in een gerechtelijk onderzoek. Of nog wanneer een persoon herhaaldelijk bepaalde nalatigheden heeft begaan, zoals bvb. niet bereikbaar zijn op momenten dat deze persoon van dienst is. Op dat moment moet het mogelijk zijn om te weigeren dat die persoon verder deel uitmaakt van de Coördinatieceel.

Beroepsgeheim (advies, § 33 - 35).

Personeelsleden en aangestelden die de Coördinatieceel Justitie louter bijstaan, mogen geen informatie verwerken en hebben geen toegang tot de informatie

chaque consultation de la banque de données. Il va de soi que la politique en matière de sécurité doit être évaluée au jour le jour par le service NTSU/CTIF, et qu'il convient au besoin de prendre les mesures requises en vue d'une meilleure sécurisation.

4. La Cellule de coordination de la Justice (article 2) (avis, point 32)

Aux termes de l'article 2, § 1^{er}, alinéa 4, du projet, le Ministre de la Justice a le droit de 'refuser des personnes en tant que membres de la Cellule de coordination de la Justice'. La Commission estime que cette prérogative ministérielle ne peut s'exercer que conformément à la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

Ce n'est toutefois pas le cas. Plusieurs hypothèses sont envisageables où le ministre de la Justice doit avoir le droit de refuser certaines personnes en tant que membres de la Cellule de coordination de la Justice. Le premier exemple qui vient à l'esprit est le cas où une personne est impliquée dans une instruction judiciaire. Un autre exemple est le cas où une personne s'est rendue à répétition coupable de certaines négligences, comme par exemple le fait de ne pas être joignable lorsqu'elle est en service. A ce moment-là, il doit être possible de refuser que cette personne continue à faire partie de la Cellule de coordination.

Secret professionnel (avis, points 33-35)

Les agents et préposés qui simplement aident la Cellule de coordination de la Justice ne sont pas habilités à traiter des données et n'ont pas accès aux données

bekomen met toepassing van de artikelen 46bis, 88bis, en 90ter van het Wetboek van Strafvordering. Indien de leden van de Coördinatiecel Justitie aan de personeelsleden en aangestelden die hen bijstaan toch die informatie verstrekken, dan schenden zij het beroepsgeheim opgelegd in de artikelen 46bis, § 2, derde lid, 88bis, § 2, tweede lid en 90quater, tweede lid, en strafbaar gesteld in artikel 458 van het Strafwetboek.

De Commissie meent dat het proportionaliteitsbeginsel niet is nageleefd voor wat betreft de doorgifte van de persoonlijke contactgegevens van de leden van de Coördinatiecel Justitie (advies, § 36-41)

Hier kan akkoord gegaan worden met de Commissie. Wat belangrijk is, is de permanente beschikbaarheid van de Coördinatiecel. Het ontwerp zal daarom voorzien dat er een dienst-gsm beschikbaar dient te zijn waarvan het nummer meegedeeld moet worden aan het BIPT.

5. Meedelen van de inhoud van communicatie (artikel 6) (advies, § 53-55)

De commissie meent dat waar in artikel 6, §1, 2° en 4°, melding gemaakt wordt van het meedelen van de inhoud van communicatie, uitdrukkelijk verwezen moet worden naar artikel 90ter Sv.

Er dient op gewezen te worden dat artikel 6 de functionele vereisten bevat waaraan operatoren en dienstverstrekkers dienen te voldoen bij het meedelen van gegevens.

obtenues en application des articles 46bis, 88bis et 90ter du Code d'Instruction criminelle. Si en dépit de cela, les membres de la Cellule de coordination de la Justice communiquent de telles données aux agents et préposés qui les aident, ils violent le secret professionnel imposé aux articles 46bis, § 2, alinéa 3, 88bis, § 2, alinéa 2, et 90quater, alinéa 2, du Code d'Instruction criminelle et cette violation est punissable aux termes de l'article 458 du Code pénal.

La Commission est d'avis que le principe de proportionnalité n'est pas respecté en ce qui concerne la transmission des coordonnées personnelles des membres de la Cellule de coordination de la Justice (avis, points 36-41).

Sur ce point, nous pouvons nous rallier à l'avis de la Commission. Ce qui importe, c'est que la Cellule de coordination soit disponible en permanence. Le projet prévoira dès lors qu'un gsm de service doit être disponible, dont le numéro devra être communiqué à l'IBPT.

5. Transmission du contenu de la communication (article 6) (avis, points 53-55)

La Commission est d'avis que là où l'article 6, § 1^{er}, 2° et 4°, fait mention de la transmission du contenu de la communication, il y a lieu de référer explicitement à l'article 90ter du Code d'instruction criminelle.

Il convient de souligner que l'article 6 contient les exigences fonctionnelles auxquelles les opérateurs et les fournisseurs de services doivent répondre pour la transmission de données.

Uiteraard kunnen alleen gegevens meegedeeld worden wanneer aan de voorwaarden voldaan is die omschreven zijn in de artikelen van het Wetboek van Strafvordering. Vandaar ook dat in de aanvang van artikel 6 uitdrukkelijk bepaald wordt dat aan de voorwaarden van de artikelen 46bis, 88bis, en 90ter voldaan moet zijn, voor elke van de functionele eisen voorzien in artikel 6. Om dit volledig duidelijk te maken zal ingegaan worden op de suggestie van de Commissie om in artikel 6, § 1, 1°, 2° en 4° aan te geven volgens welke bepaling van het Wetboek van Strafvordering deze gegevens kunnen worden doorgestuurd.

Il va de soi que des données peuvent uniquement être communiquées si les conditions définies dans les articles du Code d'instruction criminelle sont remplies. C'est la raison pour laquelle il est explicitement précisé, au début de l'article 6, que les conditions fixées par les articles 46bis, 88bis et 90ter doivent être remplies pour chacune des exigences fonctionnelles visées à l'article 6. Afin de clarifier totalement ceci, il sera donné suite à la suggestion de la Commission de préciser à l'article 6, § 1^{er}, 1°, 2° et 4°, selon quelle disposition du Code d'Instruction criminelle ces données peuvent être transmises.

6. Overdrachtmodus van gegevens (artikel 10) (advies, § 56-58)

De Commissie is van oordeel dat artikel 10, tweede lid, van het ontwerp van koninklijk besluit zou moeten verduidelijken dat het ministerieel besluit enkel de omvang van de gegevens betreft die worden overgedragen.

Artikel 10, tweede lid, van het ontwerp van koninklijk besluit heeft enkel betrekking op vorm waarin de gegevens moeten worden overgemaakt.

Een uniformering van het formaat en van de overdrachtmodus van de gegevens vergemakkelijkt de verwerking van de gegevens. Deze uniformering hangt af van de beschikbare technische middelen en vereist overleg met de operatoren. Een te strikte modus operandi waarbij de overdrachtmodus in het koninklijk besluit nader wordt omschreven, zou ongeschikt blijken. Vandaar de mogelijkheid om dit bij ministerieel besluit te regelen.

Dit artikel betreft dus alleen de technische modaliteiten en regelt niets

6. Mode de transmission des données (article 10) (avis, points 56-58)

La Commission estime que l'article 10, alinéa 2 du projet d'arrêté royal devrait préciser que l'arrêté ministériel ne porte que sur la taille des données transmises.

L'article 10, alinéa 2, du projet d'arrêté royal porte uniquement sur la forme sous laquelle les données doivent être transmises.

Une uniformisation du format et du mode de transmission des données facilite le traitement des données. Cette uniformisation dépend des moyens techniques disponibles et elle nécessite une concertation avec les opérateurs. Un modus operandi trop rigide, en détaillant le mode de transmission dans l'arrêté royal, se révélerait inadéquat, d'où la possibilité de régler ceci par arrêté ministériel.

Ledit article porte donc uniquement sur les modalités techniques et ne règle en

over de toegang tot de databank van de operatoren, noch over de omvang van de modaliteiten. rien l'accès à la banque de données des opérateurs, ni l'ampleur des modalités.

* * *

* * *

Ontwerp van Koninklijk Besluit houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie

Nota aan de Commissie voor de Bescherming van de Persoonlijke levenssfeer: Organigram NTSU/CTIF – Interceptie binnen de federale politie.

Deze nota is een aanvulling op het antwoord op het advies van de Commissie voor de bescherming van de persoonlijke levenssfeer nr. 29/2008 van 3 september 2008, en betreft de structuur van het NTSU/CTIF en de plaats ervan binnen de federale politie.

Het betreft meer bepaald de artikelen 1 en 3 van het ontwerp van Koninklijk Besluit, en de opmerkingen van de Commissie hieromtrent in haar advies nr. 29/2008 van 3 september 2008, in de paragrafen 24-26 en 42-48.

De volgende organigrammen worden voorzien:

1. Structuur van de federale politie
2. Structuur van de aanvrager van een maatregel (een tapmaatregel bv.)
3. Structuur van de uitvoerder van de gevraagde maatregel: de CGSU/NTSU.

Uit organigram nr. 1 valt af te leiden dat:

- de CGSU deel uitmaakt van de speciale eenheden van de federale politie en rechtstreeks afhangt van de commissaris-generaal, maar de aanvrager (met name één van de 27 FGP's bv.) zich in een andere zuil bevindt;
- er dus geen hiërarchische link is tussen de aanvrager en de uitvoerder. Bovendien staat de uitvoerder hoger in de structuur dan de aanvrager.

Een vraag tot tap kan uitsluitend via een schriftelijke vordering aangevraagd worden die op voorhand doorgefaxt moet worden. Het document wordt overgemaakt aan de CGSU, die de conformiteit en wettelijkheid **ook** controleert, vooraleer tot actie over te gaan.

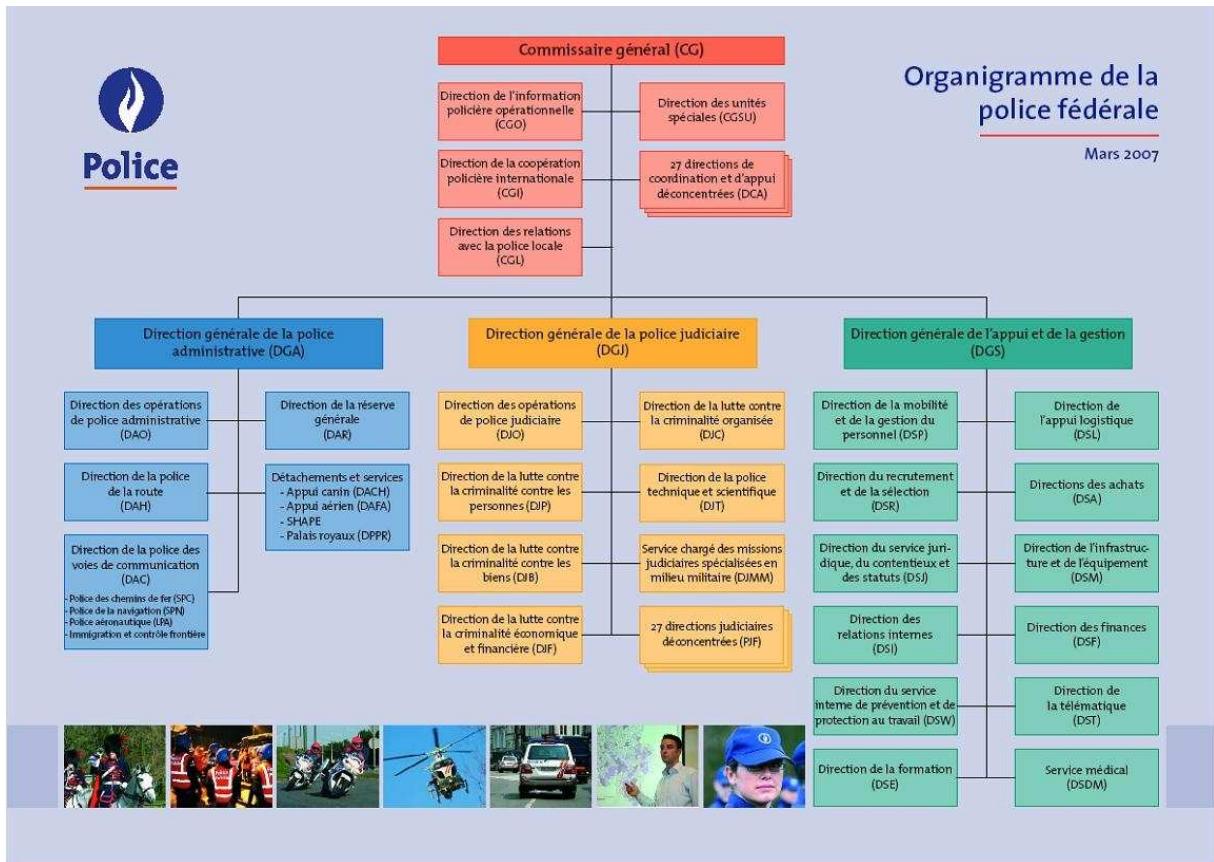
De CGSU kan nooit zelfstandig een tap aanvragen of starten.

De resultaten van de tap worden rechtstreeks overhandigd aan de aanvrager (audio opname) en de CGSU heeft **geen** toegang tot de tap zelf; CGSU/NTSU/CTIF kan dus zelf de tap niet beluisteren.

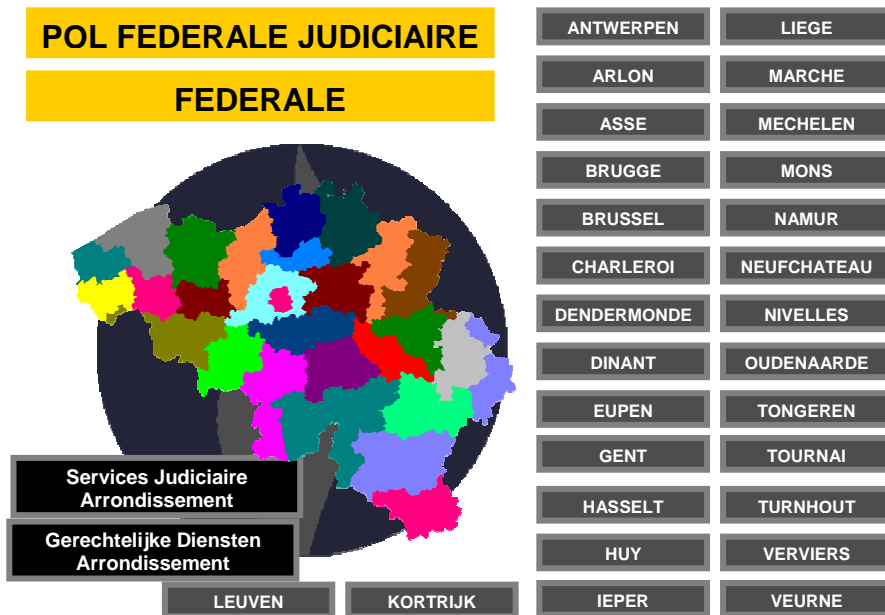
Voordelen: Strikte scheiding – wettelijkheid – onafhankelijkheid – controle.

Bovendien, naast de automatische en systematische controle door het systeem zelf (login, beperkingen van rechten, login controle,...) is de CTIF niet onafhankelijk en staat onder het gezag van het diensthoofd van het NTSU in eerste instantie en die van de CGSU in tweede instantie (zie organigrammen nrs. 3-4-5).

I. Structuur van de federale politie

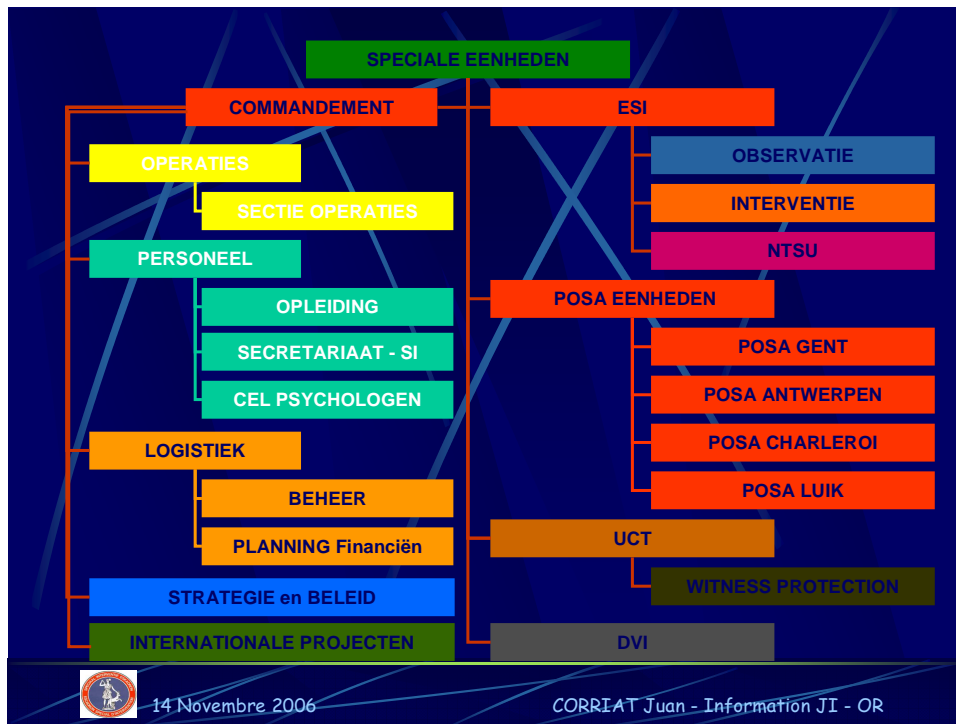


II. Structuur van de aanvrager

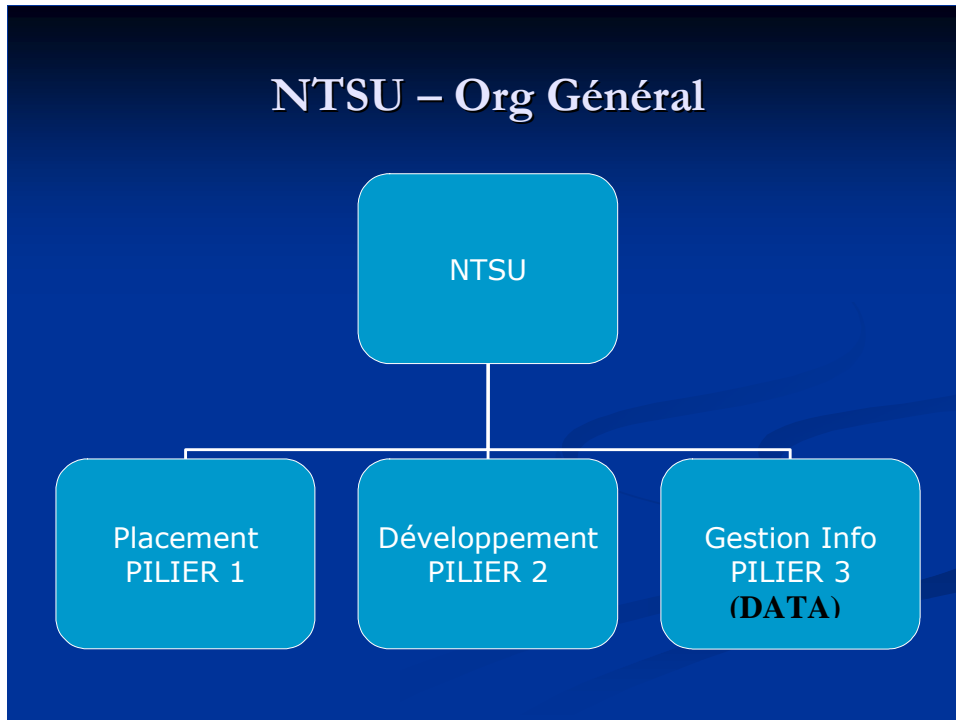


III. Structuur van de uitvoerder van de tap

ORGANIGRAM NR. 3



ORGANIGRAM NR. 4



ORGANIGRAM NR. 5

