Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

De Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2014-0000622926

Uw kenmerk

Datum 21 november 2014
Betreft Kabinetsstandpunt herziening interceptiestelsel Wiv 2002

1. Inleiding

In het Algemeen Overleg met uw Kamer op 16 april 2014 is toegezegd om na de zomer met het kabinetsstandpunt te komen ter zake van het advies van de Commissie evaluatie Wiv 2002 (commissie Dessens) inzake bijzondere bevoegdheden in de digitale wereld. Dit standpunt treft u hierbij aan.

In haar advies komt de commissie Dessens tot de conclusie dat de techniekafhankelijke interceptiebepalingen van de Wiv 2002 op basis van het onderscheid tussen de ether en de kabel niet meer te rijmen valt met de snel voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie.[1] Aanpassing van de desbetreffende bepalingen in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) (in casu de artikelen 25 tot en met 27) acht de commissie dan ook aangewezen.

Het kabinet heeft in de op 11 maart 2014 aan uw Kamer toegezonden reactie op het rapport van de commissie Dessens aangegeven dat het zou bestuderen hoe bij de grote technische veranderingen sinds de Wiv 2002 een volgens de commissie Dessens niet langer relevant onderscheid (wel- versus niet-kabelgebonden ongerichte interceptie), kan worden vervangen door een relevante norm, waarbij de privacy van Nederlandse burgers blijft gewaarborgd.

Het kabinet is alles afwegende met de commissie van oordeel dat het maken van onderscheid tussen niet-kabelgebonden en kabelgebonden communicatie door de technologische ontwikkelingen op het vlak van communicatie is achterhaald en dat het desbetreffende technologieafhankelijke onderscheid in de Wiv 2002 dient te komen vervallen, mits tegelijkertijd wordt voorzien in een duidelijk normatief kader met toereikende waarborgen.

2. Ontwikkelingen in het digitale domein en de noodzaak van een technologieonafhankelijk interceptiestelsel

In de afgelopen jaren is – mede door de enorme ontwikkeling van het internet –

[1] Een vergelijkbare conclusie had eerder de Adviesraad Internationale Vraagstukken (AIV) ook getrokken in haar advies Digitale oorlogsvoering, no. 77, AIV/No 22, CAVV December 2011

het communicatieverkeer dat via de kabelgebonden infrastructuur verloopt explosief gestegen. In de Wiv 2002, die eind jaren '90 is geformuleerd en in 2002 in werking is getreden, is met deze ontwikkeling geen rekening gehouden. De thans in de wet opgenomen regeling voor ongerichte interceptie van telecommunicatie codificeerde de toenmalige praktijk bij de diensten, met name de toenmalige Militaire Inlichtingendienst (MID), waarbij interceptie van radio- en satellietverkeer centraal stond. Anders dan bij de bijzondere bevoegdheid tot gerichte interceptie (artikel 25 van de wet), die wel technologieonafhankelijk werd geformuleerd, is dat bij de regeling voor ongerichte interceptie achterwege gebleven. De commissie Dessens is dan ook tot de conclusie gekomen dat de regeling van ongerichte interceptie in de Wiv 2002 gedateerd is en geen recht doet aan de heden ten dage noodzakelijke bevoegdheden in het kader van de nationale veiligheid.

Naast een explosieve groei van de hoeveelheid gegevens die in de wereld wordt geproduceerd (en elke twee tot drie jaar verdubbelt) moet worden vastgesteld dat inmiddels ongeveer 90% van alle telecommunicatie via kabelnetwerken verloopt. Heden ten dage vormen alle elektronische communicatienetwerken (ether en kabel) een mondiaal dekkend communicatienetwerk. Deze netwerken bieden in principe elk individu of elke organisatie wereldwijd toegang tot een in aantal en complexiteit groeiende verzameling van applicaties en diensten.

Voor de (inter)nationale veiligheidsbelangen van Nederland en het optreden van de krijgsmacht is een stevige Nederlandse inlichtingenpositie van fundamenteel belang, of het nu gaat om het voorkomen van terrorisme, tegengaan van spionage, beschermen tegen digitale aanvallen, inzicht in bedreigingen voor de internationale rechtsorde, het doorgronden van intenties van een aantal landen, zicht op de capaciteitsontwikkeling van risicolanden of de proliferatie van massavernietigingswapens. De diensten moeten bovendien zicht hebben op de dreigingen waaraan de samenleving en de staat in het digitale domein kunnen worden blootgesteld, om zich daar vervolgens effectief tegen te kunnen wapenen en anderen in staat te stellen maatregelen te treffen. Dit is van groot belang in het kader van de Nationale Cyber Security Strategie en in het licht van het streven van het kabinet naar de digitale overheid. De technische dreigingen en mogelijkheden manifesteren zich zowel op het kabelgebonden als ook op het niet-kabelgebonden deel van het digitale domein. De (potentiële) impact van cyberdreigingen is door uiteenlopende incidenten in de afgelopen jaren steeds duidelijker geworden. Het gaat daarbij niet alleen om dreigingen die onze cyberinfrastructuur kunnen verstoren, maar ook om dreigingen ten aanzien van de integriteit, beschikbaarheid en vertrouwelijkheid van de informatie die we allen digitaal vastleggen, gebruiken en uitwisselen. Om zicht te houden op deze dreigingen zijn de diensten afhankelijk van een adequate toegang tot telecommunicatie.

De diensten moeten daarom beschikken over voldoende inlichtingenmiddelen en -capaciteiten om informatie op het juiste moment in het digitale domein te verwerven, te analyseren en daarover tijdig te rapporteren. Bijzondere bevoegdheden die het mogelijk maken om – onder strikte voorwaarden – te intercepteren in het kabelgebonden domein zijn daarbij onmisbaar.

De uitoefening van deze bijzondere bevoegdheden raakt per definitie aan het recht op bescherming van privacy van de burgers. Gelet op de verantwoordelijkheid en de zorg van de overheid voor de veiligheid van haar burgers is het onontkoombaar

dat de diensten persoonsgegevens verzamelen en verwerken. Dit wil niet zeggen dat veiligheid en privacy tegengestelde belangen zijn. De overheid beoogt met gepaste en doelgerichte uitoefening van deze bevoegdheden bij te dragen aan het realiseren in een veilige samenleving van grondrechten, waaronder ook het recht op privacy. Het doelgerichte karakter van de uitoefening van deze bevoegdheden op basis van de wettelijk vastgelegde taken van de inlichtingendiensten zorgt ervoor dat de 'normale' telecommunicatie van burgers gevrijwaard blijft van ongeoorloofde inmenging door de inlichtingendiensten. Met andere woorden: burgers hoeven niet bevreesd te zijn dat de overheid in willekeurige e-mailconversaties meekijkt of telefoongesprekken meeluistert. Er moet steeds een juiste balans worden gevonden tussen de inzet van de bevoegdheden enerzijds en het kunnen uitoefenen van grondrechten anderzijds. Noodzakelijke inbreuken op het recht op privacy dienen voorzien te zijn van adequate waarborgen. In alle gevallen kan de onafhankelijke toezichthouder (CTIVD) toetsen of voldaan is aan de eisen van proportionaliteit, subsidiariteit en noodzakelijkheid.

3. Uitwerking kabinetsstandpunt: nieuw normatief kader voor interceptie met toereikende waarborgen

3a. Hoofdlijnen nieuw interceptiestelsel

Met de commissie Dessens is het kabinet van oordeel dat er een nieuwe balans gevonden moet worden tussen veiligheid en privacy.

Het kabinet is tot de conclusie gekomen dat een technologie-onafhankelijke en daarmee ook toekomstbestendige herformulering van de bevoegdheden tot interceptie (als bedoeld in de artikelen 26 en 27 van de Wiv 2002) is aangewezen, zij het onder gelijktijdige aanscherping van bestaande en introductie van nieuwe waarborgen. In de huidige wet is reeds limitatief vastgelegd op welke wijze de diensten door gebruikmaking van de aan hen toegekende bevoegdheden op het recht op privacy een inbreuk mogen maken. In alle gevallen moet daarbij worden voldaan aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Deze bevoegdheidsuitoefening is bovendien uitsluitend toegestaan als het belang van de nationale veiligheid, zoals dat nader is uitgewerkt in de taakstelling van de diensten, daartoe noodzaakt.

Van oudsher werd tot voor kort aangenomen dat hoe dichter bij de inhoud van telecommunicatie wordt gekomen, des te groter de inbreuk op grondrechten wordt. Het onderscheid tussen inhoud en niet-inhoud is echter niet het enige bepalende element bij het vaststellen van de ernst van de inbreuk en bij het daarop toe te snijden model van toestemming. Evenzeer is van belang de schaal waarop de gegevens worden verzameld en hoe ingrijpend de gehanteerde methodiek voor (verdere) verwerking van de gegevens is voor de privacy van de burger.

In het licht van het vorenstaande wordt in het nieuwe stelsel voor de interceptie van telecommunicatie ("bulk") op hoofdlijnen een drietal fasen onderscheiden. Deze hoofdlijnen zullen – ter vervanging van de huidige artikelen 26 (verkenning van de communicatie) en 27 (ongerichte interceptie niet-kabelgebonden telecommunicatie) – in het voor te bereiden wetsvoorstel nader worden uitgewerkt en toegelicht.

De onderscheiden fasen zijn:

1) doelgericht verwerven van telecommunicatie,
2) voorbewerken van de geïntercepteerde telecommunicatie, en
3) (verder) verwerken van de telecommunicatie.

Ter verduidelijking zijn de hiervoor genoemde fasen in het interceptiestelsel in een diagram, die als bijlage bij deze brief is gevoegd, weergegeven[2]. Daarbij is in het kort aangeduid welke activiteiten de onderscheiden fasen omvatten alsmede de waarborgen die ter zake in het nieuwe wettelijk stelsel zullen worden neergelegd.

Ter toelichting daarop kan nog het volgende worden opgemerkt. Elke fase heeft een duidelijk omschreven doel. In de eerste fase – het verwerven – worden op grond van een door de verantwoordelijke minister verleende last ten aanzien van de daarin zo nauwkeurig mogelijk omschreven onderzoeksopdracht doelgericht relevante gegevens geïntercepteerd en interpreteerbaar gemaakt (bijvoorbeeld door ontsleuteling). Ook voorbereidende, technische activiteiten die de doelgerichte verwerving en ontsluiting van gegevens mogelijk maken, kunnen binnen deze fase vallen. Personen of organisaties worden in deze fase nog niet onderzocht, waardoor de inbreuk op de persoonlijke levenssfeer in deze fase gering is. De tweede fase – het voorbewerken - heeft tot doel in het kader van lopende, goedgekeurde onderzoeksopdrachten aan de hand van de verworven data het interceptieproces in brede zin te optimaliseren. Omdat voor deze optimalisatie metadata-analyse of een korte kennisneming van de inhoud van de telecommunicatie nodig kunnen zijn, gaat de inbreuk op de persoonlijke levenssfeer in deze fase verder dan in de eerste fase. In de derde fase - het verwerken – vindt de selectie van relevante telecommunicatie plaats en worden de geselecteerde gegevens gebruikt om inzicht te verwerven in de intenties, de capaciteiten en de gedragingen van personen en organisaties die onderwerp zijn van onderzoek. In deze fase vindt subjectgericht onderzoek plaats, waarbij de inhoud van telecommunicatie en metadata wordt geanalyseerd om personen of organisaties te identificeren en zicht te krijgen op patronen.

Van fase tot fase wordt derhalve in oplopende mate inzicht verkregen in de persoonlijke levenssfeer. De waarborgen die in de wet zullen worden opgenomen, worden zwaarder naarmate de persoonlijke levenssfeer van individuen indringender in beeld komt.

In alle fasen zullen in de Wiv waarborgen worden ingebouwd, die zowel het gebruik van de interceptiebevoegdheid (verwerving) als de verdere verwerking van de geïntercepteerde gegevens voor daarbij te onderscheiden doeleinden afhankelijk maakt van (a) voorafgaande en in tijd begrensde ministeriële toestemming (een “last”, inclusief een toets op noodzaak, proportionaliteit en subsidiariteit), (b) doelgerichte inzet[3], (c) bewaar- en vernietigingstermijnen met betrekking tot de desbetreffende gegevens en (d) een (gecombineerd) stelsel van functie- en taakscheiding c.q. compartimentering waar het gaat om de toegang tot de gegevens in de verschillende fasen en buiten het interceptieproces. Deze waarborgen gaan niet alleen gelden waar het gaat om interceptie van kabelgebonden telecommunicatie, maar ook voor de interceptie van niet-kabelgebonden telecommunicatie als bedoeld in artikel 27, eerste lid, Wiv 2002.

[2] Het diagram is een vereenvoudigde weergave en betreft geen volledige uitwerking van het interceptieproces.

[3] Het begrip doelgerichte inzet zal gerelateerd aan de desbetreffende fase invulling krijgen. In de verwervingsfase zal bijvoorbeeld kunnen worden verwezen naar onderzoeksopdrachten zoals opgenomen in bijvoorbeeld het Aanwijzingsbesluit Buitenland of de Inlichtingen- en Veiligheidsbehoefte Defensie. Hoe verder in het proces wordt gekomen zal het doel steeds concreter dienen te worden geformuleerd.

Voor dit laatste is thans geen toestemming vereist.

Naast de hiervoor bedoelde waarborgen zal zowel voor interne controledoeleinden als voor het toezicht door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), verslaglegging plaatsvinden.

Door dit stelsel van maatregelen met de doelgerichte inzet en de weging van proportionaliteit, subsidiariteit en noodzakelijkheid in de lastgeving vooraf, wordt de privacy van Nederlandse burgers gewaarborgd.

3b. Medewerking netwerkaanbieders

Voor de uitoefening van de bevoegdheid tot intercepteren van kabelgebonden telecommunicatie als hier bedoeld zal in de praktijk de medewerking vereist zijn van de desbetreffende netwerkaanbieder. Deze vorm van interceptie is altijd aan een bepaald onderzoeksdoel van de diensten verbonden. De ministeriële toestemming tot interceptie (“last”) geldt daarbij als een wettelijke opdracht aan een netwerkaanbieder om medewerking te verlenen aan de interceptie. Een belangrijke en in de wet op te nemen voorwaarde hierbij is de plicht tot overleg tussen de diensten en de netwerkaanbieder, voorafgaand aan de uitvoering van de door de minister verleende interceptielast. Van een onbeperkte en zelfstandige toegang van de diensten tot de Nederlandse telecommunicatie-infrastructuur is derhalve geen sprake. De medewerkingsplicht zal worden ondersteund door een informatieplicht voor aanbieders om desgevraagd relevante informatie te verkrijgen.

3c. Metadata-analyse

Waar het gaat om het gebruik van de aldus geïntercepteerde telecommunicatie voor het inlichtingenproces kan dat betrekking hebben op zowel gebruik van geïntercepteerde metadata als op de inhoud van de telecommunicatie. Alleen voor dit laatste is op dit moment in artikel 27 van de Wiv 2002 het vereiste van ministeriële toestemming gesteld. De onderschepte metadata kan worden onderworpen aan een louter technische metadata-analyse en een meer vergaande analyse, waarbij wordt beoogd subjecten te identificeren en zicht te krijgen op patronen[4]. Beide vormen van metadata-analyse vinden thans hun wettelijke grondslag in artikel 12 e.v. van de Wiv 2002 en daarvoor is geen toestemming vereist. De vorm van metadata-analyse waarbij wordt beoogd subjecten te identificeren en zicht te krijgen op patronen zal in het nieuwe stelsel worden onderworpen aan de wettelijk vast te leggen eis van ministeriële toestemming. Ook hier zullen de eisen van doelgerichte inzet, noodzakelijkheid, subsidiariteit en proportionaliteit van toepassing zijn. Voorts zal er een bewaar- en vernietigingstermijn in de wet worden opgenomen.

3d. Verscherpt toezichtsregime

De ministeriële toestemmingen die in het nieuwe stelsel in de opeenvolgende fasen benodigd zijn, zullen voorts onderworpen zijn aan het in het Algemeen Overleg van 16 april 2014 geschetste heroverwegingsstelsel. Dat houdt in dat indien de CTIVD in het kader van haar rechtmatigheidstoezicht tot de conclusie

[4] Bijvoorbeeld door het koppelen van geïntercepteerde metadata aan andersoortige gegevensbestanden, zoals NAW-gegevens (gegevens betreffende naam, adres en woonplaats).

komt dat een verleende toestemming onrechtmatig is, de minister verplicht is deze te heroverwegen. Indien de minister persisteert in de verleende toestemming dient de CTIVD en de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) onverwijld daarvan op de hoogte te worden gesteld. De CIVD kan desgewenst de minister ter verantwoording roepen.

4. De uitwisseling van gegevens met buitenlandse collega-diensten

Het kabinet heeft eerder aangegeven dat de uitwisseling van grote hoeveelheden ruwe gegevens ("bulkdata") door de AIVD en MIVD met buitenlandse collega-diensten zal worden onderworpen aan ministeriële toestemming. Overeenkomstig dit standpunt zal de Wiv 2002 daarop worden aangepast. Aangezien in het kader van de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten ook andere soorten gegevens worden uitgewisseld, zal deze regeling zich niet alleen tot telecommunicatiegegevens uitstrekken maar algemener van opzet zijn.

De uitwisseling van dit soort gegevens zal met de volgende daarbij passende waarborgen worden omgeven:

a. Vanzelfsprekend kunnen alleen data worden gedeeld die rechtmatig zijn vergaard, waarbij is voldaan aan de *gestelde* criteria.

b. Bij elke (voorgenomen) samenwerking zal een toets plaats dienen te vinden aan de wettelijk vast te leggen criteria voor samenwerking met buitenlandse diensten. Deze criteria zijn de democratische inbedding van de dienst, het mensenrechtenbeleid in het desbetreffende land en de professionaliteit en betrouwbaarheid van de dienst. De uitkomst van dit proces bepaalt mede of en, zo ja, welke vorm van samenwerking,zoals de uitwisseling van gegevens, toelaatbaar wordt geacht. Voor het aangaan van een samenwerkingsrelatie met een buitenlandse dienst waarbij de toets aan deze criteria leidt tot de conclusie dat deze risico's opleveren, geldt dat de minister daarvoor toestemming dient te geven.

c. Bij de verstrekking wordt altijd de voorwaarde gesteld dat degene aan wie de gegevens worden verstrekt, deze gegevens niet aan anderen mag verstrekken.

d. Voor verstrekking van "bulkdata" (grote hoeveelheden ruwe gegevens) dient ministeriële toestemming te worden verleend.

5. Slotopmerking

Het kabinet heeft in het voorgaande op hoofdlijnen het beoogde nieuwe interceptiestelsel toegelicht en de daarbij te introduceren (extra) waarborgen geschetst. Bij de verdere uitwerking worden ook relevante aanbieders van communicatienetwerken betrokken. De uitwerking ervan wordt neergelegd in wetgeving en wordt thans voorbereid. Het is evident dat bij die uitwerking acht wordt geslagen op de eisen die niet alleen vanuit onze Grondwet (artikel 10 en 13) maar ook uit relevante mensenrechtelijke verdragen, in het bijzonder het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) en de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM), ter zake van met name de interceptie van telecommunicatie en de verwerking van de diverse soorten telecommunicatiegegevens voortvloeien. Gecombineerd met een versterkt stelsel

van toezicht en klachtbehandeling, zoals eerder door het kabinet is aangekondigd, komt naar het oordeel van het kabinet aldus een wettelijke regeling tot stand die voldoet aan de rechtsstatelijke eisen die hieraan gesteld worden.

Datum
21 november 2014

Kenmerk
2014-0000622926

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

De Minister van Defensie,

J.A. Hennis-Plasschaert

Bijlage: diagram interceptiestelsel