

Vergaderjaar 2000–2001

**27 591**

## **Grootschalig af luisteren van moderne telecommunicatiesystemen**

**Nr. 1**

### **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

's-Gravenhage, 19 januari 2001

#### **Inleiding**

Hierbij bieden wij u, mede namens de minister van Justitie, een notitie aan over de technische en de juridische aspecten van het grootschalig af luisteren van moderne telecommunicatiesystemen. Deze notitie is het resultaat van een onderzoek van de regering. Hierbij is onder meer gebruik gemaakt van rapporten van het Franse, Belgische en Europese parlement en andere beschikbare open bronnen.

De maatschappelijke en politieke belangstelling voor dit onderwerp is de afgelopen jaren sterk toegenomen. Mede door aanhoudende berichten over het «Echelon»-netwerk is de discussie in een stroomversnelling geraakt.

In dit verband verklaarden de EU-ministers van Justitie en Binnenlandse Zaken in hun officiële verklaring van de 2266ste EU-Raadsvergadering van 29 mei 2000 dat «de interceptie van telecommunicatie een belangrijk middel kan zijn bij het bestrijden van criminaliteit en het verdedigen van de nationale veiligheid, echter in geen geval kan worden benut voor het behalen van commercieel voordeel».

Hierover heeft het Tweede kamerlid Van Oven schriftelijke vragen gesteld aan de Minister van Justitie. In zijn antwoord hierop verwees de Minister van Justitie naar eerdere antwoorden op de Kamervragen betreffende het onderwerp «Echelon» (Aanhangsel Handelingen II 1999/00, nrs. 1112 en 1308). Daarnaast heeft de regering in relatie met dit onderwerp in de periode 1995–2000 kamervragen beantwoord van de Tweede Kamerleden De Graaf (D66), Korthals (VVD), Roethof (D66), Bakker (D66), Halsema (GroenLinks), Van Oven (PvdA) en Wagenaar (PvdA). Bovengenoemde ontwikkelingen leidden ertoe dat de Tweede Kamer een rondetafelgesprek over deze onderwerpen heeft georganiseerd.

Met het oog op deze ontwikkelingen is bijgevoegde notitie opgesteld over het grootschalig af luisteren van moderne telecommunicatiesystemen. Hieronder volgen de belangrijkste bevindingen van de notitie.

### **Technische aspecten: kwetsbaarheid van telecommunicatiesystemen**

Moderne telecommunicatiesystemen – openbare en niet-openbare, nationale en internationale – zijn technisch kwetsbaar voor af luisterpraktijken. Deze kwetsbaarheid is groot bij systemen die geheel of gedeeltelijk gebruikmaken van de ether. Daarom moet rekening worden gehouden met de mogelijkheid dat deze systemen ongemerkt en op afstand worden afgeluisterd, zowel door (satelliet)grondstations als door satellieten. De leesbaarheid van de afgetapte informatie is afhankelijk van de manier waarop deze is vercijferd.

Op grond van de Nederlandse Telecommunicatiewet zijn aanbieders van netwerken en diensten in Nederland gehouden technische en organisatorische maatregelen te treffen ter beveiliging en bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers. Er bestaat thans onvoldoende grond voor de veronderstelling dat aanbieders niet aan deze criteria kunnen voldoen. Voor overheidsdoeleinden is het gebruikelijke beschermingsniveau echter niet in alle gevallen toereikend. Dit niveau kan desgewenst op relatief eenvoudige wijze worden verhoogd met behulp van cryptografie. In Nederland kunnen ook burgers zonder enige restrictie, als additionele bescherming tegen af luisteren, cryptografische beschermingsmaatregelen toepassen. Geen enkel niveau van beveiliging biedt echter absolute garanties tegen af luisteren. Het beschermingsniveau van de beschikbare cryptografie kan bijvoorbeeld door overheden zijn beïnvloed.

Voor de beveiliging van bijzondere informatie van de overheid zijn gerichte, voor overheidsgebruik ontwikkelde beschermingsmaatregelen noodzakelijk.

### **Situatie in Nederland: wettelijk kader**

De feitelijke uitvoering van de interceptie en selectie van niet-kabelgebonden telecommunicatie ten behoeve van de Militaire Inlichtingendienst en de Binnenlandse Veiligheidsdienst gebeurt bij de Afdeling Verbindings-inlichtingen van de MID. Opsporingsinstanties en de BVD zijn binnen de daartoe door de wet gestelde grenzen bevoegd tot het aftappen van kabelgebonden telecommunicatie. Het stelsel van wetgeving bestaande uit het Wetboek van Strafvordering, het wetsvoorstel op de inlichtingen- en veiligheidsdiensten (Wiv) en de aftapbepalingen in de Telecommunicatiewet maakt het, ook in de toekomst, de diensten mogelijk hun wettelijke taken uit te voeren, maar schept naar het oordeel van de regering tevens voldoende waarborgen tegen onbevoegde inbreuken op de privacy van de burger. Zo worden in het wetsvoorstel Wiv de bevoegdheden van de BVD en de MID op dit terrein expliciet genoemd en worden ten aanzien van de inzet van deze bevoegdheden een aantal grenzen gesteld (onder meer lastgeving vooraf, toetsing op proportionaliteit en subsidiariteit).

### **Juridische aspecten: rechtsmacht en rechtsbescherming**

Bij het grootschalig af luisteren van met name internationaal telecommunicatieverkeer speelt de vraag naar de toepassing van nationale rechtsmacht versus internationaal recht. Bij de beantwoording van deze vraag bestaat er op dit moment voor Nederland een voorkeur voor

de opvatting dat het internationaal recht geen beperkingen kan opleggen aan de uitoefening van rechtsmacht over handelingen verricht op eigen territoir of op een plaats waar andere landen geen rechtsmacht bezitten, bijvoorbeeld op een schip op volle zee of een satelliet in de ruimte. Er is in Nederland geen wetgeving die mogelijkheden biedt om het afluisteren van telecommunicatie in dit verband tegen te gaan. Het staat vrijwel vast dat dergelijke wetgeving ook niet handhaafbaar zou zijn. De bescherming van het telecommunicatiegeheim van de burgers zou onder meer moeten worden gezocht in het maken van afspraken in internationaal verband, die er op gericht dienen te zijn dat burgers zich moeten kunnen verweren tegen onbevoegd afluisteren en intercepteren.

De juridische consequenties van bovengenoemde stellingnamen dienen nog nader te worden bediscussieerd. Separaat aan deze notitie zal een regeringsstandpunt met betrekking tot deze aspecten worden ontwikkeld.

### **Europese ontwikkelingen**

Zoals in de inleiding al is aangegeven is de problematiek van het groot-schalig aftappen van telecommunicatiesystemen ook in het Europees Parlement aan de orde gesteld. Het «Committee on Civil Liberties and Civil Affairs» heeft aan het «Scientific and Technological Options Assessment (STOA)» verzocht een studie naar dit onderwerp te verrichten. Dit heeft geresulteerd in een serie van vijf onderzoeksrapporten getiteld: «Development of surveillance technology and risks of abuse of economic information», die in oktober 1999 zijn verschenen. Dit was voor het Europees Parlement aanleiding op 5 juli 2000 een Tijdelijk Comité op te richten dat tot taak heeft het bestaan van het «Echelon»-systeem te verifiëren en vast te stellen hoe dit zich verhoudt met het Gemeenschapsrecht, in bijzonder artikel 286 van het EGverdrag en de directieven 95/46/EC en 97/66/EC, en het artikel 6(2) van het EU-verdrag. Tevens heeft het comité tot taak vast te stellen of de Europese Industrie wordt bedreigd door het aftappen van telecommunicatiesystemen op mondiale schaal, en dient het comité, indien mogelijk, voorstellen te ontwikkelen voor politieke en wettelijke initiatieven.

### **Afluisterpraktijken: bestaat «Echelon»?**

De maatschappelijke en politieke belangstelling voor het zogenaamde «Echelon»-netwerk is groot. Over «Echelon» bestaat echter vooralsof veel onduidelijkheid en veel beschouwingen zijn dan ook speculatief. Mede daarom hebben de parlementen van Frankrijk en België en het Europees parlement inmiddels onderzoek laten verrichten naar het bestaan, de aard en de activiteiten van dit netwerk. Het Franse en het Belgische onderzoeksrapport, verschenen in oktober 2000, concluderen beide op grond van informatie uit open bronnen dat «Echelon» bestaat. De Tijdelijk Comité van het Europees parlement is nog niet klaar, maar wetenschappelijke voorstudies concluderen eveneens dat «Echelon» bestaat. De regering beschikt niet over eigen, door de in verband met Echelon genoemde regeringen bevestigde informatie over het bestaan van «Echelon», maar acht dit op grond van de thans beschikbare informatie, onderzoeken en openbare bronnen aannemelijk. Hierbij kan tevens worden opgemerkt dat niet slechts overheden maar ook burgers, bedrijfsleven en criminele organisaties dergelijke activiteiten kunnen plegen. Tevens gaat de regering er op basis van bovenstaande informatie vanuit dat er ook andere systemen bestaan die de aan «Echelon» toegeschreven mogelijkheden bezitten. Op grond hiervan concludeert de regering dat het grootschalig afluisteren van moderne telecommunicatiesystemen niet slechts is voorbehouden aan de met «Echelon» in verband gebrachte

landen maar een activiteit is van opsporings-, veiligheids-, en inlichtingen-  
diensten van vele overheden van landen met uiteenlopende politieke  
kleur.

De Minister van Defensie,  
F. H. G. de Grave