UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Geheime surveillance en opsporing

Richtsnoeren voor de inrichting van wetgeving

Eskens, S.J.; van Daalen, O.L.; van Eijk, N.A.N.M.

Publication date
2016

Document Version
Final published version

Link to publication

Citation for published version (APA):
Eskens, S. J., van Daalen, O. L., & van Eijk, N. A. N. M. (2016). *Geheime surveillance en opsporing: Richtsnoeren voor de inrichting van wetgeving*. Instituut voor Informatierecht. http://www.ivir.nl/publicaties/download/Geheime-surveillance-en-opsporing.pdf

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:08 Dec 2021

Geheime surveillance en opsporing

Richtsnoeren voor de inrichting van wetgeving

S.J. Eskens, O.L. van Daalen en N.A.N.M. van Eijk

Instituut voor Informatierecht (IViR, Universiteit van Amsterdam)

November 2016

Inhoud

Voorwoord

Effectief toezicht en transparantie zijn centrale elementen bij het vormgeven en evalueren van de wettelijke waarborgen rond digitale geheime surveillance door nationale inlichtingen- en veiligheidsdiensten. De eerdere IViR-studie 'Ten standards for oversight and transparency of national intelligence services' formuleert tien richtsnoeren die dit verder uitwerken.

Deze *quickscan* behandelt de vraag in hoeverre deze tien richtsnoeren ook van toepassing zijn op geheime surveillance in het kader van de opsporing van strafbare feiten. Het belang van het onderzoek wordt ingegeven door het feit dat in een aantal recente wetsvoorstellen nieuwe bevoegdheden voor het verzamelen en verwerken van persoonsgegevens worden geïntroduceerd. Het wetsvoorstel Computercriminaliteit III is een typisch voorbeeld van deze ontwikkeling en wordt daarom gebruikt om te illustreren hoe de geformuleerde richtsnoeren toegepast kunnen worden.

Dit rapport is mede mogelijk gemaakt door bijdragen van een consortium bestaande uit KPN, Vodafone en Ziggo. Het onderzoek is uitgevoerd in overeenstemming met de Verklaring van wetenschappelijke onafhankelijkheid van de KNAW.

De auteurs danken Prof. mr. Tom Blom, hoogleraar straf(proces)recht aan faculteit der rechtsgeleerdheid (Universiteit van Amsterdam), voor zijn kritische commentaar en suggesties.

Amsterdam, november 2016

1 Inleiding

Bij het gebruik van digitale opsporingsmiddelen door politie en justitie is er toenemende aandacht voor de bescherming van het individuele recht op privacy en de rechtsstaat door middel van toezicht en transparantie. De inzet van digitale opsporingsmiddelen voor geheime surveillance komt tegelijkertijd steeds vaker voor. Twee traditionele barrières voor de inzet van dit soort middelen – technische complexiteit en hoge kosten – zijn weggevallen door technologische ontwikkelingen. Hierdoor is het mogelijk digitale opsporingsmiddelen eenvoudig op grote schaal en tegen lage kosten in te zetten. Het is daarmee de vraag geworden of de van oudsher geldende waarborgen voor de toepassing van opsporingsmiddelen op dat gebied nog daadwerkelijke en effectieve bescherming bieden voor het recht op privacy en de rechtsstaat, of dat deze moeten worden aangescherpt.

Dit onderzoek richt zich op twee soorten waarborgen: waarborgen die verband houden met *toezicht* en waarborgen die verband houden met *transparantie*. Bij toezicht gaat het onder meer om de vraag of de onafhankelijkheid van het toezicht is gewaarborgd. Transparantie draagt ertoe bij dat verantwoording over de ingezette middelen mogelijk en controleerbaar is.

In het rapport 'Ten Standards for oversight and transparency of national intelligence services' heeft het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam) een analyse gemaakt van het geldende juridische kader voor toezicht en transparantie.[1] In dat rapport wordt ingegaan op geheime surveillance door nationale inlichtingen- en veiligheidsdiensten ten behoeve van nationale veiligheid. In deze *quickscan* wordt nagegaan in hoeverre die richtsnoeren ook van toepassing zijn bij geheime surveillance door reguliere politiediensten in het belang van de opsporing van strafbare feiten.

Daartoe wordt in hoofdstuk 2 allereerst het algemene juridische kader geschetst, waarbij wordt onderzocht of er relevante verschillen zijn tussen nationale veiligheid en strafvorderlijke opsporing. Daarna worden de tien richtsnoeren samengevat en toegelicht aan de hand van rechtspraak, waaronder ook relevante recente uitspraken van het Europese Hof voor de Rechten van de Mens (EHRM) zijn meegenomen. In hoofdstuk 3 wordt aan de hand van het wetsvoorstel

---

1 S. Eskens, O.L. van Daalen en N.A.N.M. van Eijk, *Ten standards for oversight and transparancy of national intelligence services*, Amsterdam: IViR 2015, http://www.ivir.nl/publicaties/download/1591.pdf.

Computercriminaliteit III geïllustreerd hoe wetgeving op basis van de richtsnoeren geëvalueerd kan worden.[2] Dit rapport sluit af met een analyse en conclusie in hoofdstuk 4.

Het onderzoek heeft een *quickscan* karakter. Er wordt dus geen volledigheid beoogd: de studie concentreert zich op de belangrijkste ontwikkelingen met betrekking tot transparantie en toezicht. Primair oriëntatiepunt vormt het Europees mensenrechtelijke kader, in het bijzonder artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM) en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie (Handvest), en de interpretatie hiervan door het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de EU (HvJ EU).

Juist omdat een specifiek wetsvoorstel in dit rapport ter illustratie wordt besproken, is het belangrijk het beperkt karakter van deze studie te benadrukken. Deze studie bespreekt slechts de eisen op het gebied van toezicht en transparantie – twee noodzakelijke voorwaarden – en richt zich dus niet op andere aspecten van het mensenrechtelijk kader ten aanzien van digitale opsporingsmiddelen (zoals de geoorloofdheid van de bevoegdheden als zodanig). Het is dan ook niet aangewezen om op basis van dit rapport conclusies te trekken over de verenigbaarheid in algemene zin van dit specifieke wetsvoorstel met mensenrechtelijke eisen.

2 *Kamerstukken II* 2015-16, 34372, 2.

2 Juridisch kader

2.1 Het juridisch kader

Het rapport 'Ten standards for oversight and transparency of national intelligence services' formuleerde tien richtsnoeren waaraan het toezicht op geheime surveillance door nationale inlichtingen- en veiligheidsdiensten moet voldoen. Hierbij wordt 'toezicht' opgevat als de verschillende manieren waarop de inlichtingen- en veiligheidsdiensten gecontroleerd worden en verantwoording afleggen. Dit kan via intern toezicht door de verantwoordelijke minister, via parlementair toezicht, via rechterlijk toezicht, en via extern onafhankelijk toezicht. Toezicht gaat dus niet alleen over concrete gevallen waarin geheime surveillancebevoegdheden jegens een persoon of groep van personen worden toegepast, maar ook over het algehele functioneren van een systeem voor geheime surveillance. De in het rapport geformuleerde eisen rond transparantie zijn met de waarborgen rond toezicht nauw verbonden: het zijn randvoorwaarden om dit toezicht te kunnen uitoefenen en de inzet van opsporingsmiddelen te kunnen verantwoorden.[3]

De tien richtsnoeren voor toezicht en transparantie zijn gebaseerd op een analyse van rechtspraak rond privacy van het EHRM, gelezen in samenhang met jurisprudentie van het HvJ EU en relevante Europese *soft law*-maatregelen.

Artikel 8 EVRM – Recht op eerbiediging van privé-, familie- en gezinsleven

1. Eenieder heeft het recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Artikel 8 EVRM beschermt het recht op privacy en – zo volgt uit de jurisprudentie - op gegevensbescherming. Vormen van surveillance, zoals het aftappen van telefoons, GPS-tracking, of

[3] In de Nederlandse literatuur wordt 'toezicht' meestal omschreven als 'het verzamelen van informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren'; zie F. Mertens, E. Muller, en H. Winter (red.), *Toezicht: Inspecties en autoriteiten in Nederland*, Deventer: Wolters-Kluwer 2015, p. 16.

het onderscheppen van internetverkeersgegevens, vormen een inmenging met het recht op privacy. Het EHRM spreekt over 'secret surveillance' of 'covert surveillance' wanneer het gaat over methoden waarmee overheidsinstanties in het geheim informatie over mensen verzamelen. Dit wijkt af van het Nederlandse gebruik. In de Nederlandse strafrechtelijke terminologie is het meer gebruikelijk om 'surveillance' te onderscheiden van 'opsporing'. Meer algemene verzameling van gegevens door de politie (bijvoorbeeld observatie van de publieke ruimte of internetfora, *zonder* stelselmatig karakter) in het kader van de handhaving van de openbare orde wordt vaak 'surveillance' genoemd, terwijl gerichte strafrechtelijke handhaving door de politie meer ziet op 'opsporing'. In dit rapport wordt met het EHRM voor beide gevallen de term 'geheime surveillance' gebruikt. Dit wordt in paragraaf 2.3 nader uitgewerkt.

Een inmenging door het openbaar gezag met het recht op privacy is alleen gerechtvaardigd voor zover bij wet voorzien (legaliteitsvereiste), en in een democratische samenleving noodzakelijk in het belang van een legitiem doel (noodzakelijkheidsvereiste).[4] De bepaling bevat een limitatieve opsomming van legitieme doelen, waaronder de nationale veiligheid en het voorkomen van wanordelijkheden en strafbare feiten.

Ook het Handvest beschermt het recht op privacy en gegevensbescherming. Artikel 7 Handvest stelt dat eenieder recht heeft op eerbiediging van zijn privacy, en artikel 8 Handvest herhaalt dit voor het recht op bescherming van persoonsgegevens.

Artikel 7 Handvest – Eerbiediging van het privé-leven en het familie- en gezinsleven

Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

Artikel 8 Handvest – Bescherming van persoonsgegevens

1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

[4] In het noodzakelijkheidsvereiste zit ook het in de Nederlandse context vaak gebruikte begrip 'doelmatigheid' verweven.

Artikel 52, eerste paragraaf, Handvest vereist dat beperkingen op de uitoefening van de in het Handvest erkende rechten bij wet zijn gesteld (legaliteitsvereiste), noodzakelijk zijn (noodzakelijkheidsvereiste) en beantwoorden aan een doelstelling van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen. Een verschil tussen het beschermingsmechanisme van het EVRM en het Handvest is dat de laatste ook vereist dat beperkingen de 'wezenlijke inhoud' van de in het Handvest erkende rechten eerbiedigen.

Artikel 52 Handvest – Reikwijdte van de gewaarborgde rechten

1. Beperkingen op de uitoefening van de in dit handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden.

(..)

3. Voorzover dit handvest rechten bevat die corresponderen met rechten die zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend.

De uitleg die het EHRM geeft aan het recht op privacy is relevant voor de interpretatie van het Handvest. Artikel 52, derde paragraaf, Handvest bepaalt namelijk dat de rechten daarin die corresponderen met rechten die zijn gegarandeerd door het EVRM, dezelfde inhoud en reikwijdte hebben. Het HvJ EU geeft dan ook verder invulling aan het recht op privacy aan de hand van EHRM-rechtspraak, bijvoorbeeld in *Digital Rights Ireland*.[5]

Om te komen tot de tien richtsnoeren is in het eerdere rapport gekeken naar de rechtsontwikkeling bij de twee Europese hoven. Dit sluit aan bij het dynamische karakter van het EVRM, en bij het feit dat de rechtspraak van het EHRM de laatste jaren steeds minder casuïstisch wordt.[6] Juist de rechtspraak rond geheime surveillance heeft een abstracter karakter. Dat komt doordat het EHRM bij uitzondering ook klachten over geheime surveillancewetgeving *in abstracto* – een klacht over een wetgevingsinstrument, in plaats van een klacht over de toepassing van een maatregel – accepteert,[7]

5 HvJ EU 8 april 2014, in de gevoegde zaken C-293/12 en C-594/12 (*Digital Rights Ireland*).

6 J. Gerards, 'Rechtsvinding door het Europees Hof voor de Rechten van de Mens', *NJCM-Bulletin* 2006, afl. 1, p. 93-122, 100-101.

7 Zie EHRM 6 september 1978, 5029/71 (*Klass en anderen v. Duitsland*), § 34-38 en 41; EHRM 2 augustus 1984, 8691/79 (*Malone v. Verenigd Koninkrijk*), § 64; EHRM 29 juni 2006, 54934/00 (*Weber en Saravia v. Duitsland*)

en omdat het EHRM bij klachten over de toepassing van geheime surveillance ook uitdrukkelijk abstraheert van de omstandigheden van het geval.[8] Dit betekent dat in de EHRM-rechtspraak over geheime surveillance gaandeweg steeds algemenere principes zijn ontwikkeld, die elke lidstaat in wetgeving en praktijk moet respecteren.

2.2 Nationale veiligheid versus opsporing van strafbare feiten

Het ERHM maakt in zijn overwegingen niet expliciet onderscheid tussen geheime surveillance in het belang van de nationale veiligheid versus geheime surveillance in het belang van het voorkomen van strafbare feiten. Dit is onder meer te verklaren door de manier waarop landen de inlichtingen- en veiligheidsdiensten en de politie organiseren. In Europa zijn er *grosso modo* twee basismodellen voor de organisatie van politie en veiligheidsdiensten: een strikte, principiële scheiding tussen de inlichtingen- en veiligheidsdiensten en de politiediensten (dit is bijvoorbeeld het Engelse, Duitse en Nederlandse model) of juist een meer geïntegreerde organisatie (dit is bijvoorbeeld het Franse, Zweedse en Russische model). Landen die geen strikte scheiding kennen, regelen de taken en bevoegdheden van de diensten meestal ook met een wetgevingsinstrument dat beide domeinen omvat. En wanneer geheime surveillance in zo'n geval aan het EHRM wordt voorgelegd, maakt het bij de toetsing ook geen onderscheid naar autoriteit of het gediende belang: het EHRM analyseert slechts de methoden die worden gebruikt.[9]

(ontvankelijkheidsbeslissing), § 78; EHRM 28 juni 2007, 62540/00 (*Association for European Integration and Human Rights en Ekimdzhiev v. Bulgarije*), § 69; EHRM 1 juli 2008, 58243/00 (*Liberty en anderen v. Verenigd Koninkrijk*), § 56-57; EHRM 10 februari 2009, 25198/02 (*Iordachi en anderen v. Moldavië*), § 30-35; EHRM 18 mei 2010, 26839/05 (*Kennedy v. Verenigd Koninkrijk*), § 119-129; EHRM 4 december 2015, 47143/06 (*Roman Zakharov v. Rusland*), *Computerrecht* 2016/86, m.nt. S.J. Eskens, § 164-179; EHRM 12 januari 2016, 37138/14 (*Szabó en Vissy v. Hongarije*). In de loop van de tijd had het EHRM verschillende methoden ontwikkeld of een *in abstracto* klacht was toegestaan, maar in *Roman Zakharov* harmoniseert het Hof de verschillende methoden.

8 Zie bijv. EHRM 24 april 1990, 11105/84 (*Huvig v. Frankrijk*), § 31: '[the Court] must inevitably assess the relevant French "law" in force at the time in relation to the requirements of the fundamental principle of the rule of law. Such a review necessarily entails some degree of abstraction.'

9 Zie bijvoorbeeld het feitencomplex in de recente zaak van *Roman Zakharov*: de klager klaagde over Russische geheime surveillancewetgeving. De Russische *Operational-Search Activities Act* (OSAA) regelde de interceptie van elektronische communicatie in het kader van strafrechtelijke procedures en daarbuiten. De OSAA bepaalde dat interceptie onder meer kon plaatsvinden in het belang van de opsporing van strafrechtelijke feiten, of om informatie te verzamelen over activiteiten die de nationale veiligheid bedreigen (§ 25-26). Het EHRM vraagt zich in haar beoordeling vervolgens niet af of de beklaagde geheime surveillance in het teken van opsporing of nationale veiligheid stond; ze stelt simpelweg vast dat 'that the surveillance measures permitted by Russian law pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country' (§ 237), en beoordeelt vervolgens of de wetgeving in voldoende waarborgen voorziet. Het EHRM volgt een vergelijkbare aanpak in EHRM 26 maart 1987, 9248/81 *(Leander v. Zweden)* en EHRM 6 juni 2006, 62332/00 *(Segerstedt-Wiber en anderen v. Zweden)*, waar het ging om geheime surveillance door de Zweedse 'veiligheidspolitie'. De Zweedse veiligheidspolitie is onderdeel van de nationale politie, maar voert geheime surveillance uit in het belang van de nationale veiligheid.

In Nederland bestaat in principe een strikte scheiding tussen de AIVD/MIVD en de politie, maar in de praktijk is de scheiding minder strikt.[10] Desalniettemin richt dit rapport zich alleen op opsporing van strafbare feiten, waarmee exclusief ambtenaren van de politie mee belast zijn.[11] Onder 'opsporing' wordt verstaan het onderzoek in verband met strafbare feiten met als doel het nemen van strafvorderlijke beslissingen.[12]

2.3 Het *geheime* karakter van surveillance

Waar het EHRM dus minder aandacht heeft voor de vraag welk openbaar gezag gegevens verzamelt of welk belang dit dient, heeft het des te meer aandacht voor het *geheime* karakter van die verzameling. In de eerste zaak waarin het EHRM zich uitspreekt over geheime surveillance, *Klass v. Duitsland*, besteedt het EHRM hier al veel aandacht aan. Die overwegingen zijn vervolgens het uitgangspunt voor de beoordeling in alle latere zaken over geheime surveillance geweest.

Om te beginnen overweegt het EHRM in *Klass* dat geheime surveillancewetgeving alleen acceptabel is als dit *strikt* noodzakelijk is ter bescherming van de democratie.[13] De toevoeging van 'strikt' aan het noodzakelijkheidsvereiste impliceert een verzwaarde toetsing, want dit staat niet in de verdragsbepalingen. Ook het HvJ EU, in *Digital Rights Ireland* en *Schrems*, onderstreept dat beperkingen op het recht op privacy binnen de grenzen van het strikt noodzakelijke moeten blijven.[14] En in de recente zaak van *Volokhy v. Oekraine* maakt het EHRM expliciet dat deze eis van strikte noodzakelijkheid ook geldt met betrekking tot geheime surveillance in het belang van strafrechtelijke opsporing.[15]

In *Szabó en Vissy v. Hongarije* heeft het EHRM die eis van strikte noodzakelijkheid verder uitgewerkt. Dit gaat volgens het Hof over twee aspecten: een maatregel tot geheime surveillance is alleen in overeenstemming met het EVRM als deze *in het algemeen* strikt noodzakelijk is om de

---

10 Zie daarover uitgebreid T. Vis, *Intelligence, politie en veiligheidsdienst: Verenigbare grootheden?* (diss. Tilburg University), Tilburg 2012, te downloaden via https://pure.uvt.nl

11 Art. 3 Politiewet 2012.

12 Art. 132a Sv.

13 *Klass*, § 42. Zie o.a. ook EHRM 4 mei 2000, 28341/95 (*Rotaru v. Roemenië*), § 47; *Segerstedt-Wiberg*, § 88; EHRM 2 november 2006, 23543/02 (*Volokhy v. Oekraine*), § 43; EHRM 18 mei 2010, 26839/05 (*Kennedy v. Verenigd Koninkrijk*), § 153; EHRM 31 july 2012, 36662/04 (*Drakšas v. Lithouwen*), § 54; EHRM 15 januari 2015, 68955/11 (*Dragojević v. Kroatië*), *JBP* 2015/57, m.nt. J. Lindeman, § 84; *Szabó en Vissy*, § 73.

14 *Digital Rights Ireland*, § 52; HvJ EU 6 oktober 2015, C-362/14 (*Schrems v. Data Protection Commissioner*), § 92.

15 *Volokhy*, § 43.

democratische instituties te beschermen, en als deze *in het concrete geval* strikt noodzakelijk is om inlichtingen te vergaren in een bepaald onderzoek.[16]

Niet alleen legt het Hof in *Klass* een strenge toetsing aan: het formuleert ook een belangrijke maatstaf *voor* die toetsing. In *Klass* benadrukt het EHRM het risico dat geheime surveillance de democratie kan ondermijnen of zelfs ten gronde kan richten, en daarom vereist het EHRM dat het nationale recht voorziet in daadwerkelijke en effectieve bescherming tegen misbruik van geheime surveillancebevoegdheden.[17] Dit risico op misbruik is niet theoretisch: het is volgens het Hof een serieus risico in concrete zaken.[18] Waarborgen moeten daarom duidelijk in de wet worden omschreven, en ook gelden voor het toezicht op de activiteiten van de diensten.[19]

Het is van belang dat het Hof spreekt over 'daadwerkelijke en effectieve bescherming'. Deze toets is voor het EHRM een belangrijk uitgangspunt bij de uitleg van verdragsbepalingen.[20] In de afgelopen jaren heeft het EHRM via dit uitgangspunt het EVRM op een dynamische manier geïnterpreteerd, waarbij zij rekening kan houden met nieuwe ontwikkelingen. De vraag wat nodig is om daadwerkelijke en effectieve bescherming te bieden verandert namelijk met de tijd. Dit is voor de toetsing van geheime surveillance belangrijk, omdat in dat gebied door nieuwe technologische ontwikkelingen de reikwijdte van het EVRM steeds kritisch moet worden onderzocht.

Eén van de zaken waar die technologische ontwikkeling relevant was bij de beoordeling, is *S. en Marper*. Daar overweegt het EHRM dat de behoefte aan passende waarborgen tegen misbruik van persoonlijke gegevens des te groter is 'where the protection of personal data undergoing automatic processing is concerned'.[21] Het Hof vervolgt door te benadrukken dat dit extra zwaar weegt 'when such data are used for police purposes'.

Het EHRM onderstreept verder in *Malone* – een geheime surveillancezaak die kort op *Klass* volgde – dat het risico op willekeur vanzelfsprekend is wanneer bevoegdheden in het geheim worden

16 *Szabó en Vissy*, § 73.

17 *Klass*, § 49-50; Zie o.a. ook *Leander*, § 60; ontvankelijkheidsbeslissing van de Commissie 8 juni 1990, 13564/88 (*L. v. Noorwegen*), § 2; ontvankelijkheidsbeslissing van de Commissie 2 april 1993, 18601/91 (*Esbester v. Verenigd Koninkrijk*); EHRM 24 augustus 1998, 88/1997/872/1084 (*Lambert v. Frankrijk*), § 31; *Weber en Saravia*, § 106; *Ekimdzhiev*, § 77; EHRM 2 oktober 2012, 22491/08 (*Sefilyan v. Armenië*), §127; *Volokhy*, § 52; *Kennedy*, § 153; EHRM 2 september 2010, 35623/05 (*Uzun v. Duitsland*), § 63; *Dragojević*, § 83; *Roman Zakharov*, § 232 en 236; *Szabó en Vissy*, § 57 en 59.

18 *Klass*, § 56. Zie o.a. ook *Kennedy*, § 167; EHRM 22 november 2012, 39315/06 (*Telegraaf Media Nederland Landelijke Media B.V. en anderen v. Nederland*), § 98; *Roman Zakharov*, § 233; *Szabó en Vissy*, § 77.

19 *Volokhy*, § 52.

20 Gerards 2006, p. 111

21 EHRM 4 december 2008, 30562/04 en 30566/04 (*S. en Marper v. Verenigd Koninkrijk*). Zie o.a. ook EHRM 17 december 2009, 16428/05 (*Gardel v. Frankrijk*), § 62; EHRM 18 april 2013, 19522/09 (*M.K. v. Frankrijk*), § 32. Zie ook *Digital Rights Ireland*, § 55.

uitgeoefend.[22] In *Malone* ging het om heimelijk aftappen van telefonie en het verzamelen van verkeersgegevens door de politie. Als gevolg stelt het EHRM allerlei strikte kwaliteitseisen aan regelgeving in dit domein.[23]

Het EHRM stelt tot slot in *Klass* ook dat mededeling aan de betrokkenen in het geval van geheime surveillance belangrijk is in verband met het recht op privacy.[24] Burgers kunnen de rechtmatigheid van geheime surveillance jegens hen namelijk alleen voor de rechter aanvechten als ze achteraf alsnog op de hoogte worden gesteld van het onderzoek. Een mededeling over de surveillance achteraf biedt betrokkenen de gelegenheid hun recht op privacy uit te oefenen en de oordeelsvorming van de rechter te beïnvloeden.

De conclusie is dat de eerder ontwikkelde richtsnoeren voor toezicht en transparantie in de context van geheime surveillance in het belang van de nationale veiligheid onverkort van toepassing zijn binnen het opsporingsdomein. In de volgende paragraaf worden die richtsnoeren beschreven.

2.4 Tien richtsnoeren voor geheime surveillance

2.4.1 Compleet toezicht

Het toezicht op geheime surveillance moet een compleet geheel zijn. Dit is een algemeen uitgangspunt, maar de volgende subparagrafen werken dit idee verder uit. Bij dit eerste punt gaat het om de vraag of de nationale rechtsorde in ieder geval formeel in alle vereiste aspecten van toezicht voorziet. In haar rechtspraak met betrekking tot geheime surveillance heeft het EHRM in het bijzonder aandacht voor drie aspecten van het toezicht: de toezichthoudende instanties, de momenten waarop toezicht plaatsvindt, en het mandaat dat verschillende toezichthoudende instanties hebben. Deze drie elementen kunnen op verschillende manieren worden ingevuld, en vullen elkaar aan.

---

22 *Malone*, § 67. Zie o.a. ook *Huvig*, § 29; *Kruslin*, § 30; EHRM 30 juli 1998, 58/1997/842/1048 (*Valenzuela Contreras v. Spanje*), § 46; EHRM 16 februari 2000, 27798/95 (*Amann v Zwitserland*), § 56; EHRM 4 mei 2000, 28341/95 (*Rotaru v. Roemenië*), § 55; EHRM 12 mei 2000, 35395/97 (*Khan v. Verenigd Koninkrijk*); EHRM 27 april 2004, 50210/99 (*Doerga v. Nederland*), § 50; *Segerstedt-Wiberg*, § 76; *Volokhy*, § 49; *Liberty*, § 62; *Ekimdzhiev*, § 75; *Iordachi*, § 39; *Kennedy*, § 152; EHRM 21 juni 2011, 30194/09 (*Shimovolos v. Rusland*), § 68; *Sefilyan*, § 126; *Telegraaf Media*, § 90; *Dragojević*, § 81; *Roman Zakharov*, § 229; *Szabó en Vissy*, § 62.

23 Deze worden in dit rapport verder niet behandeld, maar zijn wel van groot belang omdat bijvoorbeeld codificatie van bepaalde vereisten de toezichthoudende instanties bevoegd maakt om daadwerkelijk toezicht te houden op die vereisten.

24 *Klass*, § 57. Zie o.a. ook *Weber en Saravia*, § 135; EHRM 26 april 2007, 71525/01 (*Dumitru Popescu v. Roemenië*) (Nr. 2), § 77; *Ekimdzhiev*, § 66 en 90; *Kennedy*, § 167; *Roman Zakharov*, § 234; *Szabó en Vissy*, § 86.

Toezichthoudende instanties

Met betrekking tot de toezichthoudende instanties kijkt het EHRM naar de rol van de uitvoerende macht, de wetgevende macht, de rechterlijke macht, en eventuele gespecialiseerde toezichtcommissies die onafhankelijk en niet-parlementair zijn. Het EHRM neemt in aanmerking welke autoriteit toestemming geeft tot de toepassing van geheime surveillancebevoegdheden, welke autoriteit de surveillance uitvoert, en welke instanties toezicht houden.[25] De vraag of geheime surveillance gerechtvaardigd is in het licht van artikel 8 EVRM hangt mede af van het ingestelde toezicht.

Momenten van toezicht

Aangaande het moment waarop toezicht plaatsvindt, onderscheidt het EHRM voorafgaand toezicht (wanneer bevel en toestemming tot het uitoefenen van de bevoegdheid worden gegeven), toezicht gedurende de uitoefening van bevoegdheden, en toezicht nadat de surveillance is beëindigd.[26] Het is bij de uitoefening van bevoegdheden belangrijk dat er in al deze fases – vooraf, tijdens, en achteraf – toezicht is. In *Szabó en Vissy* benadrukt het EHRM daarbij het belang van onafhankelijk toezicht achteraf op individuele gevallen én op het functioneren van het gehele systeem.[27] De relevantie van doorlopend toezicht (tijdens de uitoefening van bevoegdheden) is gelegen in de complexiteit van wetgeving, en een potentieel zeer ruim toepassingsbereik van geheime surveillancebevoegdheden.[28]

Mandaat van de toezichthoudende instanties

Wat betreft het mandaat van de toezichthoudende instanties, kijkt het EHRM naar de aard en omvang van het toezicht. Het EHRM controleert of de toezichthoudende instanties formeel in staat zijn om zowel de rechtmatigheid en de noodzakelijkheid van de geheime surveillance te beoordelen, en of ze dit in de praktijk ook doen.[29] Vanuit dat perspectief stelt het EHRM ook strenge eisen aan de motivering in de toestemmingsprocedure.[30]

---

25 *Klass*, § 50. Zie o.a. ook de ontvankelijkheidsbeslissing van de Commissie 10 mei 1985, in de gevoegde zaken van 10439/83, 10440/83, 10441/83, 10452/83, 10512/83 en 10513/83 (*Mersch en anderen v. Luxemburg*); *L. v. Noorwegen*; *Ekimdzhiev*, § 77; *Weber and Saravia*, § 106; *Kennedy*, § 153; *Uzun*, § 63; *Shimovolos*, § 68; *Sefilyan*, § 127; *Dragojević*, § 84, *Roman Zakharov*, § 232; *Szabó en Vissy*, § 57.

26 *Klass*, § 50. Zie o.a. ook *Iordachi*, § 42; *Ekimdzhiev*, § 84-85; *Roman Zakharov*, § 233. Met name in *Ekimdzhiev* onderstreept het EHRM het belang van het doorlopende toezicht.

27 *Szabó en Vissy*, § 79. Zie ook *Dumitru Popescu*, § 77.

28 B.-J. Koops, A. Roosendaal, E. Kosta, M. van Lieshout en E. Oldhoff, 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20xx', PI.lab 2016, te downloaden via https://pure.uvt.nl, p. 138. Zij maken deze opmerking in het kader van de voorgestelde Wet op de inlichtingen- en veiligheidsdiensten.

29 Zie o.a. *Klass*, § 53; *Uzun*, § 71; *Drakšas*, § 68; *Roman Zakharov*, § 260-267; *Szabó en Vissy*, § 71-73.

30 Zie o.a. *Dragojević*, § 90-102; *Roman Zakharov*, § 257-267; *Szabó en Vissy*, § 75-77. In deze zaken besteedt het EHRM ook veel aandacht een de drempel die geheime surveillancewetgeving aanlegt, bijvoorbeeld gerede aanleiding, een redelijke verdenking, of een individuele verdenking. Dit rapport gaat hier verder niet op in, maar de betreffende overwegingen van het EHRM roepen wel vragen op over de verschillende noties van verdenking, vermoeden, en

2.4.2 Toezicht op alle fasen van gegevensverwerking

In het kader van geheime surveillance verzamelen, bewaren, selecteren, en analyseren nationale autoriteiten persoonlijke gegevens, en geven ze ruwe data en informatie door aan andere overheidsdiensten. Het EHRM beschouwt ieder van dit soort verwerkingen, zoals het verzamelen en opslaan van persoonlijke gegevens door middel van geheime surveillance, en het verdere gebruik van die gegevens (analyse, doorgifte aan andere autoriteiten, et cetera), als zelfstandige inmengingen met het recht op privacy.[31] Ook een wettelijke verplichting om persoonlijke gegevens te bewaren, en de toegang van nationale autoriteiten tot die gegevens gelden als twee zelfstandige inmengingen, volgens het HvJ EU.[32]

Het EHRM maakt duidelijk dat er voor elke fase van gegevensverwerking passende en adequate waarborgen moeten zijn ter bescherming van de privacyrechten van de betrokkenen.[33] Toezicht is een van die waarborgen, en behoort dus in elke fase aanwezig zijn. Hiermee hangt samen dat de verschillende toezichthoudende instanties ieder afzonderlijk moeten toetsen of het verzamelen en opslaan, en vervolgens het gebruik en het verstrekken van persoonlijke gegevens rechtmatig én noodzakelijk is.[34]

2.4.3 Onafhankelijk toezicht

Naast intern toezicht – waar elke nationale rechtsorde in meer of mindere mate wel in voorziet, en wat in de rechtspraak van het EHRM geen speciale aandacht krijgt – vereist het EHRM *onafhankelijk* toezicht op geheime surveillance (zie richtsnoer 1, par. 2.4.1). In het kader van geheime surveillance

aanwijzingen, in het Nederlandse Wetboek van Strafvordering. Zie daarover o.a. EHRM 4 december 2015, 47143/06 (*Roman Zakharov v. Rusland*), *EHRC* 2016/87, m.nt. M. Hagens, § 6.

31 *Weber en Saravia*, § 79. Zie ook *Leander*, § 48; *Rotaru*, § 46; EHRM 13 november 2012, 24029/07 (*M.M. v. Verenigd Koninkrijk*), § 195 en 200; EHRM 7 december 2006, 29514/05 (*Van der Velden v. Nederland*) (ontvankelijkheidsbeslissing), p. 8 (over het nemen van een DNA-monster, en vervolgens het systematisch opslaan daarvan). NB. Het onderscheiden van deze verschillende fasen staat los van het onderscheiden van toezicht voor, tijdens, en na het onderzoek.

32 *Digital Rights Ireland*, § 34-35.

33 *M.M. v. Verenigd Koninkrijk*, § 195. Zie ook hoe het EHRM in *Weber en Saravia* per fase het toezicht toetst.

34 Zie o.a. *Klass*, § 53, en *Weber en Saravia*, § 116-117 en 122, waarin het EHRM zich goedkeurend uitspreekt over het feit dat verschillende Duitse toezichthoudende instanties telkens opnieuw de rechtmatigheid en de noodzakelijkheid van geheime surveillance beoordeelden. In tegenstelling, zie *Roman Zakharov*, waar de Russische wetgeving weliswaar vereiste dat de noodzakelijkheid van geheime surveillance op meerdere momenten getoetst werd, maar de toezichthoudende instanties dit in de praktijk niet toetsten (§ 262-263). Dit leidde tot het oordeel van het EHRM dat artikel 8 EVRM was geschonden (§ 302-305). Zie hierover ook M.G.J.M. van der Staak, 'Informationele privacy in de strafrechtspleging', *DD* 2006/59 (jrg. 2007), afl. 7, p. 718-736.

en het recht op privacy, betekent dat onafhankelijkheid van de uitvoerende macht en de uitvoerende diensten.[35]

Volgens het EHRM vormt rechterlijk toezicht de beste waarborg voor onafhankelijkheid, onpartijdigheid, en een degelijke procedure.[36] Het EHRM wijst er in *Szabó en Vissy* verder op dat rechterlijk toezicht het vertrouwen van de burger versterkt dat de *rule of law* ook geldt in het domein van geheime surveillance.[37] Met het oog op de enorme hoeveelheid informatie die ter beschikking staat aan de autoriteiten, en de geavanceerde technieken die ze gebruiken, kan de waarde van onafhankelijk toezicht volgens het EHRM niet worden overschat.[38]

Om bovenstaande redenen geeft het EHRM de voorkeur aan *rechterlijk* toezicht op geheime surveillance, waarbij het EHRM stelt dat er in ieder geval als laatste rechtsmiddel rechterlijk toezicht moet zijn. [39] Het instellen van rechterlijk toezicht als zodanig is overigens niet voldoende om geheime surveillance in overeenstemming te brengen met de vereisten van artikel 8 EVRM. Het EHRM controleert ook of het rechterlijk toezicht in de praktijk voldoende waarborgen biedt ter bescherming van het recht op privacy van de betrokkenen.[40]

Naast onafhankelijk toezicht op geheime surveillance door de rechter, hecht het EHRM veel waarde aan onafhankelijk toezicht door een gespecialiseerde, niet-parlementaire toezichtscommissie. In een aantal Europese landen is een deel van het toezicht op de nationale inlichtingen- en veiligheidsdiensten neergelegd bij zo een gespecialiseerde toezichtscommissie (zo houdt In Nederland de CTIVD bijvoorbeeld toezicht op de AIVD en de MIVD). De aanwezigheid van een gespecialiseerde toezichtscommissie kan volgens het EHRM andere zwakke aspecten van het toezichtstelsel compenseren.[41]

---

35 *Klass*, § 21 en 56-60; *Weber en Saravia*, § 117; *Kennedy*, § 166-167; *Segerstedt-Wiberg*, § 62-63; *Dumitru Popescu*, § 70-71. Zie ook Mertens, Muller, en Winter 2015, p. 45-48: onafhankelijkheid van toezichthoudende instanties heeft twee kanten, namelijk onafhankelijkheid van de onder toezicht gestelden, en onafhankelijkheid van het politiek-bestuurlijke leiderschap.

36 *Klass*, § 55; Zie o.a. ook EHRM 5 april 2005, 9940/44 (*Brinks v. Nederland*) (ontvankelijkheidsbeslissing), § 1; *Rotaru*, § 59; *Volokhy*, § 52; *Roman Zakharov*, § 233; *Szabó en Vissy*, § 77.

37 *Szabó en Vissy*, § 79.

38 *Szabó en Vissy*, § 79.

39 Over rechterlijk toezicht, zie: *Klass*, § 55-56. Zie ook *Kennedy*, § 167; *Telegraaf Media Nederland*, § 98; *Roman Zakharov*, § 233 en 259; *Szabó en Vissy*, § 77; over in het bijzonder *als laatste rechtmiddel*, zie: *Klass*, § 55. Zie ook *Rotaru*, § 59; *Brinks*, § 1; *Volokhy*, § 52; *Szabó en Vissy*, § 77.

40 Zie bijvoorbeeld *Roman Zakharov*.

41 Zie bijvoorbeeld *Klass*, § 55-56; *Weber and Saravia*, § 20-25, 55-58, en 115; *Leander*, § 60-67; *Segerstedt-Wiberg*, § 63-64; *Kennedy*, § 165-169; *Ekimdzhiev*, § 87.

2.4.4 Voorafgaand toezicht

Het EHRM vereist *voorafgaand* onafhankelijk toezicht op de toepassing van geheime surveillancebevoegdheden.[42] In beginsel moet dit vorm krijgen in een onafhankelijke instantie die de uitvoerende macht voorafgaand toestemming geeft om een geheime surveillancebevoegdheid in te zetten. Daarbij geeft het EHRM, in lijn met wat hiervoor besproken is, de voorkeur aan voorafgaand toezicht *door de rechter*.[43] De inzet van geheime surveillance vereist dus in beginsel een rechterlijke machtiging.

Het EHRM accepteert in sommige gevallen echter een alternatief voor voorafgaand toezicht door de rechter. Zo'n alternatief is bijvoorbeeld voorafgaande toestemming door de verantwoordelijke minister (een ministeriële last), waarbij de minister verplicht is om een gespecialiseerde toezichtscommissie te raadplegen, en er *achteraf* uitgebreid rechterlijk toezicht is.[44] Een ander alternatief is interne voorafgaande toestemming, met voorafgaand toezicht op dat proces door een rechter of een onafhankelijke, gespecialiseerde toezichtscommissie.[45] In sommige gevallen vindt het EHRM voorafgaand rechterlijk toezicht overigens wél noodzakelijk, en accepteert het geen alternatieve toezichtvormen. Dit speelt bijvoorbeeld bij het geheim surveilleren van journalisten,[46] of het onderscheppen van elektronische communicatie tussen een advocaat en zijn cliënt.[47]

Een ander aspect van het voorafgaande toezicht is de aard en omvang van de voorafgaande toetsing (zie ook richtsnoer 1, par 2.4.1, over het mandaat van de toezichthouder). Zoals hierboven aangegeven, controleert het EHRM of de toezichthoudende instanties formeel in staat zijn om de rechtmatigheid en de noodzakelijkheid van de geheime surveillance te beoordelen, en of ze dit in de praktijk ook (kunnen) doen.[48] In *Dragojevic v. Kroatië* benadrukt het EHRM bovendien het belang van voorafgaande *motivering* – en dus toetsing – van de noodzakelijkheid en proportionaliteit. Het EHRM spreekt in die zaak haar goedkeuring uit voor het feit dat de Kroatische wet voorafgaande rechterlijke toetsing, en een gedetailleerde motivering op de punten van rechtmatigheid, noodzakelijkheid en proportionaliteit vereist.[49] Maar uiteindelijk bleek dat er in Kroatië een praktijk was ontstaan waarbij de rechter-commissaris noodzakelijkheid en proportionaliteit in zijn voorafgaande toestemmingsbesluit niet motiveerde, en de motivering eventueel later in een

---

42 *Klass*, § 55; *Dumitru Popescu (No. 2)*, § 70-73; *Iordachi*, § 40; *Szabó en Vissy*, § 77.

43 *Klass*, § 56. Zie ook *Kennedy*, § 167; *Telegraaf Media Nederland*, § 98; *Roman Zakharov*, § 233 en 259; *Szabó en Viss*y, § 77.

44 Zie bijv. *Klass*, § 51; *Weber en Saravia*, § 115; *Kennedy*, § 31; *Roman Zakharov*, § 258; *Szabó en Vissy*, § 77.

45 *Dumitru Popescu (No. 2)*, § 70-73; *Szabó en Vissy*, § 77.

46 *Telegraaf Media Nederland*, § 101.

47 EHRM 25 maart 1998, 13/1997/797/1000 (*Kopp v. Zwitserland*), § 74.

48 Zie o.a. *Klass*, § 53; *Uzun*, § 71; *Drakšas*, § 68; *Roman Zakharov*, § 260-267; *Szabó en Vissy*, § 71-73.

49 *Dragojević*, § 90-94.

strafrechtelijke procedure werd toegevoegd. Dit leidt tot schending van artikel 8 EVRM.[50] In *Roman Zakharov* staat een gebrekkige informatievoorziening eraan in de weg dat de rechter rechtmatigheid en noodzakelijkheid kan motiveren (zie verder richtsnoer 8).

Uit de rechtspraak van het EHRM komen nog twee aandachtspunten naar voren. Het EHRM onderstreept dat een officier van justitie niet onafhankelijk is van de uitvoerende macht.[51] *Voorafgaand* toezicht door een politiek verantwoordelijk lid van de uitvoerende macht, bijvoorbeeld een minister van justitie, biedt volgens het EHRM daarom niet de vereiste waarborgen.[52]

Daarnaast kan volgens het EHRM de ministeriële verantwoordelijkheid niet het individuele recht op privacy waarborgen. In *Szabó en Vissy* voerde de Hongaarse overheid aan dat hun Minister van Justitie het best gekwalificeerd was om voorafgaand toezicht te houden. De overheid beargumenteerde dat aspecten van binnen- en buitenlands beleid mee moeten wegen bij het nemen van een beslissing tot geheime surveillance in het belang van de nationale veiligheid. Daarom was de Minister van Justitie, die de politieke verantwoordelijkheid droeg voor nationale veiligheid (vergelijkbaar met de Nederlandse figuur van ministeriële verantwoordelijkheid), volgens de overheid beter in staat dan de rechter om zulke beslissingen te nemen.[53] Het EHRM erkende dat hier wat in zit vanuit operationeel perspectief, maar wees het argument toch af.[54] Volgens het EHRM garandeert ministerieel toezicht namelijk niet dat het doel en de middelen van de geheime surveillance getoetst worden in termen van *strikte noodzakelijkheid*. Daarbij merkt het EHRM nog op dat toestemming en toezicht met een politiek karakter het risico op misbruik van bevoegdheden juist vergroot.[55]

2.4.5 Onrechtmatigheden voorkomen, beëindigen, of herstellen

Voorafgaand toezicht, en toezicht tijdens de uitvoering van geheime surveillance, is volgens het EHRM alleen effectief als de toezichthoudende instanties juridisch bindende besluiten kunnen nemen om onrechtmatigheden respectievelijk te voorkomen of te beëindigen.[56] Het EHRM bevestigt dit nogmaals in *Roman Zakharov*, door te stellen dat de bevoegdheden van een toezichthoudende

50 *Dragojević*, § 95-98.
51 *Dumitru Popescu (No. 2)*, § 70-71; *Uzun*, § 72.
52 *Szabó en Vissy*, § 77.
53 *Szabó en Vissy*, § 43.
54 *Szabó en Vissy*, § 76. De Britse overheid maakte een vergelijkbaar argument in *Kennedy*, § 148. In die zaak concludeert het Hof inderdaad niet tot schending van Artikel 8, maar daarbij speelt dat staatsrechtelijke argument van de Britse overheid geen rol.
55 *Szabó en Vissy*, § 77.
56 Zie onder andere *Klass*, § 53; *Weber en Saravia*, § 117; *Kennedy*, § 168.

autoriteit met betrekking tot geconstateerde schendingen belangrijk zijn voor de effectiviteit van het toezicht.[57] In *Klass* en *Weber en Saravia* kwam bijvoorbeeld het Duitse systeem ter sprake. Als de Duitse G10-Kommission, de onafhankelijke toezichtscommissie, concludeert dat de inzet van geheime surveillance onrechtmatig of niet (langer) noodzakelijk is, moet de verantwoordelijke minister de maatregelen onmiddellijk beëindigen.[58] In *Kennedy* spreekt het EHRM haar waardering uit voor het juridische instrumentarium van de Investigatory Powers Tribunal (IPT), de Britse toezichthouder voor geheime surveillance. Wanneer de IPT beslist in het voordeel van de aanvrager, kan het een aftapbevel vernietigen, bevelen tot het vernietigen van verzamelde gegevens, en bevelen tot het betalen van compensatie.[59]

Daarnaast bekijkt het EHRM of een orgaan dat achteraf toezicht houdt, in een juridisch bindende beslissing kan vaststellen dat de geheime surveillance in strijd was met het recht op privacy van de betrokkene, en passende genoegdoening kan toekennen. In *Dragojevic* merkt het EHRM bijvoorbeeld op dat de Kroatische strafrechter zich niet ten gronde kan uitspreken over de vraag of Artikel 8 EVRM is geschonden, en sowieso geen genoegdoening kan toekennen die rechtstreeks een relatie heeft met een geconstateerde schending van het recht op privacy.[60]

In *Dumitru Popescu (No. 2)* keurt het EHRM het toezicht door de Roemeense toezichthouder op deze punten af. Het Roemeense recht verbood de strafrechter om de rechtsgeldigheid van toestemming die het openbaar ministerie had afgegeven te toetsen.[61] En de toezichthoudende parlementaire commissies waren niet bevoegd om in geval van onrechtmatige surveillance een sanctie of rechtsmiddel toe te kennen.[62]

2.4.6 Tegenspraak

Het EHRM erkent dat het bevel en de toestemming (dat wil zeggen, het toezicht op de afgifte van een bevel) tot geheime surveillance gegeven moeten worden zonder dat de betrokkene hiervan op de hoogte is.[63] Dit betekent dat het bevel tot geheime surveillance uitgevoerd zal worden zonder dat de betrokkene de kans heeft om tegenspraak te leveren. Hierin zit een verschil tussen geheime surveillance en andere maatregelen die een inmenging vormen met het fundamentele recht op

57 *Roman Zakharov*, § 282.
58 *Klass*, § 53. Zie ook *Weber en Saravia*, § 117.
59 *Kennedy*, § 80 en 167.
60 *Dragojević*, § 99. Zie hierover ook J. Lindeman, onder EHRM 15 januari 2015, nr. 68955/11 (*Dragojevic v. Kroatië*), *JBP* 2015/57.
61 *Dumitru Popescu (No. 2)*, § 76.
62 *Dumitru Popescu (No. 2)*, § 77.
63 Zie o.a. *Klass*, § 55; *Drakšas* § 67; *Roman Zakharov*, § 233.

privacy van de burger. Bij de tenuitvoerlegging van gewone opsporingsbevoegdheden, waaronder ook dwangbevelen, heeft de verdachte recht op tegenspraak, ondanks het inquisitoire karakter van het opsporingsonderzoek.[64] Bij geheime surveillance, hetzij in het belang van de nationale veiligheid of in het belang van het opsporen van strafbare feiten, is tegenspraak door de betrokkene vóór de tenuitvoerlegging uitgesloten.

Ter vervanging van tegenspraak door de betrokkene zelf, vereist het EHRM dat de procedures rondom geheime surveillance passende en vergelijkbare waarborgen bieden ter bescherming van de rechten van het individu.[65] In het kader van het recht op privacy, is zo een waarborg bijvoorbeeld de mogelijkheid dat individuen die *vermoeden* onderwerp te zijn van geheime surveillance, een klacht kunnen indienen bij de rechter of een onafhankelijke commissie.[66]

Daarnaast leidt het EHRM uit Artikel 8 EVRM – en niet uit Artikel 6 of 13 – af dat, *zelfs als de nationale veiligheid in het geding is*, de democratische rechtsstaat vereist dat maatregelen die fundamentele mensenrechten raken, voorwerp zijn van een procedure op tegenspraak voor een onafhankelijke instantie. Deze onafhankelijke instantie moet in staat zijn om een oordeel te geven over de motivering van het bevel en het bewijs, zo nodig met passende procedurele beperkingen op het gebruik van vertrouwelijke informatie.[67]

Hierbij moet worden aangetekend dat het EHRM bovenstaande voor het eerste bepaalde in een deportatiezaak, en daarna heeft herhaald in andere zaken, van het onvrijwillig toedienen van medicijnen tot het doorzoeken van privéruimtes, maar (nog) niet in geheime surveillancezaken als zodanig. Geheime surveillance, in het belang van de nationale veiligheid of het voorkomen van strafbare feiten, leidt ook niet altijd tot een strafrechtelijke procedure waarin een forum voor tegenspraak geboden kan worden. De overweging van het EHRM is toch relevant voor geheime surveillance, in zoverre dat het EHRM duidelijk onderstreept dat de legitieme doeleinden in Artikel 8, tweede paragraaf, EVRM (zoals nationale veiligheid, en het voorkomen van strafbare feiten)

---

64 Zie bijvoorbeeld art. 23 lid 2 Sv: de verdachte wordt gehoord door de raadskamer, of in ieder geval hiertoe opgeroepen.

65 *Klass*, § 55: 'adequate and equivalent guarantees'. Zie ook *Roman Zakharov*, § 233.

66 Zie bijvoorbeeld de waarborgen in het Duitse systeem, zoals die aan de orde komen in *Klass*, § 23 en 56, en *Weber en Saravia*, § 135. Zie ook *Ekimdzhiev*, § 100, waar het EHRM het voorbeeld van *Klass* aanhaalt (maar nu wel in de context van het recht op een daadwerkelijk rechtsmiddel, niet in de context van het recht op privacy).

67 EHRM 20 juni 2002, 50963/99 (*Al-Nashif v. Bulgarije*), § 123. Zie ook EHRM 3 juli 2012, 34806/04 (*X. v. Finland*), § 220-222 (over het onvrijwillig toedienen van medicijnen); EHRM 28 april 2008, 1365/07 (*C.G., T.H.G. en T.C.G. v. Bulgarije*), § 40-41 en 57 (over uitzetting); EHRM 9 januari 2013, 21722/11 (*Oleksandr Volkov v. Oekraine*), § 184 (over het ontslag van een rechterlijke post); EHRM 5 maart 2015, 28718/09 (*Kotiy v. Oekraine*), § 68-70 (over innemen van reisdocumenten); EHRM 7 juli 2016, 4322/06 (*Zosymov v. Oekraine*), § 60-63 (over de doorzoeking van kantoor, auto, en garage).

weliswaar de *inmenging* met het recht op privacy rechtvaardigen, maar niet rechtvaardigen dat wordt afgezien van fundamentele rechtsstatelijke beginselen – zoals het recht op tegenspraak.

Het idee van tegenspraak zit ook in de overwegingen van het EHRM over mededeling aan de betrokkenen. Het EHRM onderstreept dat betrokkenen misschien niet voorafgaand, en tijdens, maar wel na afloop van het geheime onderzoek een actieve rol kunnen spelen bij het toezicht – met andere woorden, tegenspraak kunnen leveren.[68] Dit vereist natuurlijk dat betrokkenen op de hoogte worden gesteld van geheime surveillance die jegens hen is toegepast (zie verder richtsnoer 8, par 2.4.8).

2.4.7 Voldoende middelen voor effectief toezicht

Toezichthoudende instanties moeten voldoende middelen tot hun beschikking hebben om hun functie effectief te kunnen uitvoeren.[69] In *Szabó en Vissy* herhaalt het EHRM nog eens dat er onafhankelijk toezicht moet zijn op geheime surveillance, en voegt ze daaraan toe dat in beginsel een rechter *met specifieke deskundigheid*, toezicht moet houden.[70] In een zaak over de Duitse gegevensbeschermingsautoriteit overweegt het HvJ EU bovendien dat functionele onafhankelijkheid niet volstaat om een toezichthoudende autoriteit te behoeden voor elke beïnvloeding van buitenaf.[71] Volgens het HvJ EU is het misschien niet nodig dat een toezichthoudende autoriteit zelf over haar begroting kan beschikken, maar mag de budgettaire toekenning van het personeel en de materiële middelen die een dergelijke autoriteit nodig heeft, niet beletten dat de autoriteit haar taken onafhankelijk kan uitvoeren.[72] Het beschikken over deze middelen en deskundigheid draagt ook bij aan de onafhankelijkheid van de betreffende toezichthoudende instantie (zie richtsnoer 3).

2.4.8 Transparantie

In haar geheime surveillancerechtspraak wijst het EHRM in verschillende bewoordingen op het belang van transparantie. De kern is dat transparantie bijdraagt aan effectief toezicht, in de ruime zin van het woord, omdat het toezicht *mogelijk* maakt. Het ideale model dat naar voren komt in de overwegingen van het EHRM voorziet in transparantie naar (i) de betrokkene, door middel van

---

68 *Klass*, § 57; *Weber en Saravia*, § 135.

69 Zie ook Bijlage P, 'Referentiekader publiek toezicht onderzoeksraad', bij: Onderzoeksraad voor Veiligheid, *Explosies MSPO2 Shell Moerdijk*, Den Haag 2015, p. 195: 'Effectief toezicht vereist dat de inspectie beschikt over de kennis en de (personele en financiële) middelen die nodig zijn om het beoogde veiligheidsniveau te waarborgen. De inspectie moet voldoende middelen ter beschikking krijgen om de gestelde taken uit te voeren.'

70 *Szabó en Vissy*, § 77.

71 HvJ EU 16 oktober 2012, C-614/10 (*Commissie v. Oostenrijk*).

72 *Commissie v. Oostenrijk*, § 58.

mededeling achteraf, (ii) de toezichthoudende instanties, door hen toegang te geven tot geclassificeerde informatie en statistische informatie, en (iii) 'civil society' (maatschappelijke organisaties), door het publiek meer inzicht te geven in de omvang van de surveillance. Een dergelijk model verzekert dat betrokkenen hun privacyrechten kunnen uitoefenen, toezichthouders hun taak effectief kunnen uitvoeren, en burgers hun politieke vertegenwoordigers ter verantwoording kunnen roepen.

Transparantie naar de betrokkene

Het EHRM beschouwt het als een onderdeel van het recht op privacy dat geheime surveillance aan de betrokkenen wordt medegedeeld. De algemene regel van het EHRM is dat de autoriteiten – nationale inlichtingen- en veiligheidsdiensten, of politiediensten – mededeling moeten doen aan de betrokkenen, zodra de geheime surveillance is beëindigd en het vrijgeven van deze informatie het belang van het onderzoek niet schaadt.[73] Op die manier kan de betrokkene achteraf alsnog de rechtmatigheid van de geheime surveillance betwisten, en genoegdoening zoeken voor een eventuele inbreuk (dat wil zeggen, een onrechtmatige inmenging) op zijn privacyrecht. Bovendien kan het feit dat persoonlijke gegevens worden verzameld zonder dat de burger hierover wordt ingelicht, betrokkenen het gevoel geven dat hun privéleven constant in de gaten wordt gehouden.[74]

Transparantie naar de toezichthoudende instanties

In *Roman Zakharov v. Rusland* hecht het EHRM veel gewicht aan het feit dat zelfs de rechter die voorafgaand toestemming moest geven tot geheime surveillance, niet over de relevante informatie beschikte. De Russische surveillanceregelgeving sloot namelijk uit dat informatie over geheime agenten, informanten, of de organisatie en tactieken van geheime onderzoeksmethoden aan de rechter wordt gegeven. Door dit gebrek aan relevante informatie, is de rechter niet in staat om te beoordelen of een voldoende feitelijke basis bestaat voor de aanvraag tot de inzet van geheime surveillancebevoegdheden.[75] De omvang van het voorafgaande toezicht is dus beperkt. Uit het feit dat de interceptieaanvragen meestal niet worden voorzien van ondersteunend materiaal, en dat de Russische rechters dit materiaal ook nooit opvragen bij de diensten, leidt het EHRM ook af dat de Russische rechters de noodzakelijkheid- en proportionaliteitstoets niet uitvoeren.[76]

---

73 *Klass*, § 57-58; *Weber en Saravia*, § 135; *Dumitru Popescu (No. 2)*, § 77 ; *Ekimdzhiev*, § 90; *Kennedy*, § 167*; Roman Zakharov*, § 234; *Szabó en Vissy*, § 86. Zie ook paragraaf 2.2 van de Raad van Europa, *Recommendation of the Committee of Ministers to Member States: Regulating the use of personal data in the police sector*, R(87)15, aangenomen op 17 september 1987.

74 *Digital Rights Ireland*, § 37.

75 *Roman Zakharov*, § 261.

76 *Roman Zakharov*, § 263.

De informatievoorziening in Rusland was op andere onderdelen ook gebrekkig. Het EHRM stelde in *Roman Zakharov* vast dat een ministerieel bevel verbood om te loggen, of dossiers aan te maken van uitgevoerde intercepties. Dit verbod maakte het onmogelijk voor de toezichthoudende instanties om vast te stellen of bepaalde geheime surveillanceacties zonder de vereiste rechterlijke toestemming waren uitgevoerd. Het toezicht op onrechtmatige interceptie was hiermee bij voorbaat ineffectief.[77] Tenslotte merkt het EHRM in *Roman Zakharov* nog op dat de officier van justitie geen toegang had tot geclassificeerde stukken met betrekking tot intercepties. Dat leidt bij het EHRM ook tot vragen over de effectiviteit van het toezicht door de officier van justitie.[78]

Transparantie naar het publiek

Daarnaast vindt het EHRM dat het werk van de toezichthoudende organen publiek gecontroleerd ('public scrutiny') moet kunnen worden. Het EHRM formuleert dit in *Roman Zakharov* expliciet als regel, en verwijst daarbij als voorbeeld naar zaken zoals *Kennedy* en *Ekimdzhiev*, waarin respectievelijk wel en geen sprake was van rapportage door de toezichthoudende instanties.[79] In Rusland waren de openbare aanklagers verplicht jaarlijks te rapporteren over hun inspecties, maar deze overzichtsrapporten waren naar het oordeel van het EHRM niet specifiek genoeg. Het EHRM merkt ook op dat de rapportages vertrouwelijk, en op geen enkele manier toegankelijk voor het algemene publiek waren. Het EHRM concludeert in *Roman Zakharov* daarom dat het toezicht door de openbare aanklagers niet voldoende waarborgen biedt tegen misbruik van bevoegdheden.

2.4.9 Opvraagbaarheid van informatie

Nationale regelgeving moet erin voorzien dat toezichthoudende instanties, maatschappelijke organisaties en direct betrokkenen informatie kunnen ontvangen over geheime surveillance. Dit richtsnoer hangt nauw samen met de vorige, en volgt uit het vereiste dat een inmenging met het recht op privacy voorzien bij wet moet zijn. Het EHRM zegt het niet altijd met zo veel woorden, maar in de zaken waar het EHRM *geen* schending van Artikel 8 EVRM concludeert, neemt ze in haar overwegingen mee dat nationale regelgeving in informatieplichten voorziet. In *Klass* en *Weber en Saravia* nam het EHRM in aanmerking dat de verantwoordelijke minister bij wet verplicht was om elk half jaar aan een parlementaire commissie te rapporteren over geheime surveillance in het belang van de nationale veiligheid. De minister was ook verplicht een gespecialiseerde, onafhankelijke

77 *Roman Zakharov*, § 272.
78 *Roman Zakharov*, § 281 en 284.
79 *Roman Zakharov*, § 283.

toezichtscommissie elke maand een overzicht te geven van de uitgevaardigde bevelen tot geheime surveillance.[80]

Tegelijkertijd overwoog het EHRM in *Ekimdzhiev* dat Roemeense surveillancewetgeving niet bepaalde dat de toezichthoudende rechter de resultaten van de geheime surveillance moest krijgen.[81] Daardoor kon de rechter er niet op toe zien dat de diensten zich aan de wet hielden. Het EHRM merkt in die zaak ook op dat de verantwoordelijke minister, of een andere ambtenaar, niet verplicht was om regelmatig te rapporteren (over de toepassing van surveillancebevoegdheden in concrete zaken, of over het functioneren van het systeem als geheel) aan een onafhankelijke toezichtinstantie, of aan het algemene publiek.[82]

Tenslotte besteedt het EHRM in *Szabó en Vissy* aandacht aan het (gebrek) aan transparantie. De Hongaarse minister verantwoordelijk voor de geheime surveillance was weliswaar verplicht om twee keer per jaar een algemeen rapport uit te brengen over het functioneren van de nationale inlichtingen- en veiligheidsdiensten, maar dit rapport was niet publiek beschikbaar. Daarom vond het EHRM dit rapport geen waarborg in termen van 'public scrutiny' bieden.[83] Het EHRM vond het toezicht van een parlementaire commissie die daarvoor was ingesteld ook beperkt, aangezien de commissie niet volledige toegang had tot de relevante documenten.[84]

2.4.10 Informatieverstrekking door derden

De evenknie van verplichte transparantie door overheid, is de mogelijkheid van transparantie van bedrijven en andere instellingen die te maken krijgen met de operationele aspecten van surveillance. In de jurisprudentie zijn er nog geen directe aanknopingspunten voor een recht of plicht van deze derden om over hun medewerking te rapporteren. Het is echter goed denkbaar dat dit volgt uit de 'reflexwerking' van de onder richtsnoer 9 genoemde jurisprudentie over de opvraagbaarheid van informatie, want het door derden leveren van informatie draagt bij aan 'public scrutiny'.

Bovendien raakt dit aan het recht op vrijheid van meningsuiting van bedrijven en anderen instellingen. Een beperking transparant te zijn over de eigen betrokkenheid bij surveillance, dient te

---

80 *Klass*, § 53; *Weber en Saravia*, § 24 en 25. Zie ook *Leander*, § 36-40; *Segerstedt-Wiberg*, § 62; *Kennedy*, § 165-167; *L. v. Norwegen*.

81 *Ekimhzhiev*, § 85. Zie ook *Iordachi*, § 47.

82 *Ekimdzhiev*, § 88.

83 *Szabó en Vissy*, § 82.

84 *Szabó en Vissy*, §82.

voldoen aan de vereisten van artikel 10 EVRM (recht op vrijheid van meningsuiting). In *Stoll v. Zwitserland* refereert het EHRM aan een resolutie van de parlementaire vergadering van de Raad van Europa, waarin wordt gesteld dat het door de staat beschermen van geheimen een voorwendsel kan zijn om de vrije communicatie te onderdrukken.[85] Statistieken over de hoeveelheid taps en intercepties zijn informatie van algemeen belang. Die informatie vormt een belangrijke bron voor 'daadwerkelijk en effectief' toezicht en publiek debat, en daarom zal een beperking van het recht om die informatie te publiceren niet snel toelaatbaar worden geacht.

[85] EHRM 10 december 2007, 69698/01 (*Stoll v. Zwitserland*), § 40.

3 Wetsvoorstel Computercriminaliteit III

Het wetsvoorstel Computercriminaliteit III (Kamerstukken 34372) heeft als doel de bestaande bevoegdheden voor de opsporing en vervolging van computercriminaliteit te versterken. Daartoe brengt het wetsvoorstel wijzingen aan in het Wetboek van Strafvordering en het Wetboek van Strafrecht. Eén van deze wijzigingen is het creëren van een nieuwe bevoegdheid om een geautomatiseerd werk op afstand heimelijk binnen te dringen. Met andere woorden: een bevoegdheid om computers, computernetwerken, mobiele telefoons et cetera te hacken (vanaf hier spreken we voor het gemak over de 'hackbevoegdheid' en 'computers'). Gezien jurisprudentie van de Hoge Raad kan dit ook een gegevensdrager betreffen die met de computer in verbinding staat, bijvoorbeeld een usb-stick, een op afstand te bereiken server (bij clouddiensten), of een externe harde schijf. Kortom: dit is een brede bevoegdheid.

3.1 De hackbevoegdheid

De hackbevoegdheid wordt in het Wetboek van Strafvordering in de titel van de bijzondere opsporingsbevoegdheden geplaatst. 'Bijzonder' betekent met name dat de opsporingsbevoegdheden in het geheim, dus zonder dat de verdachte daar kennis van krijgt, worden uitgeoefend. Andere voorbeelden daarvan zijn stelselmatige observatie, direct afluisteren, aftappen van telefoons en vorderen van gegevens. Door de hackbevoegdheid in deze titel op te nemen, zijn er automatisch ook bepaalde rechtswaarborgen van toepassing, zoals een ruime notificatieplicht (zie hieronder), de voeging van processen-verbaal bij de processtukken, en de vernietiging van gegevens die verschoningsgerechtigden raken.

Drie hackbevoegdheden

Het wetsvoorstel introduceert eigenlijk drie verschillende hackbevoegdheden. Ten eerste creëert het een hackbevoegdheid voor het geval van de klassieke 'verdenking' van een 'ernstig misdrijf'.[86] Het

[86] Art. 126nba (wetsvoorstel) Sv. Dit artikel verwijst naar art. 67 lid 1 Sv, wat regelt in welke gevallen een bevel tot voorlopige hechtenis kan worden gegeven. Zie art. II, onderdeel G, van het wetsvoorstel. Hierbij gaat het om misdrijven waarvoor voorlopige hechtenis is toegelaten. Dit zijn vooral misdrijven waarop een gevangenisstraf van vier jaren of meer is gesteld, bijvoorbeeld doodslag, diefstal, bedrog, plaatsen van een bom, helpen van verdachten van een terroristisch misdrijf, of financiële fraude. Het kan ook gaan om andere misdrijven die speciaal in de wet zijn aangewezen voor

introduceert ook een hackbevoegdheid bij een 'redelijk vermoeden' dat in 'georganiseerd verband ernstige misdrijven beraamd of gepleegd worden'.[87] Ten derde roept het voorstel een hackbevoegdheid in het leven voor 'aanwijzingen' van een 'terroristisch misdrijf'.[88]

Afgezien van de mate van verdenking die wordt vereist, zijn de voorwaarden voor inzet van de drie hackbevoegdheden hetzelfde. Het misdrijf moet ten eerste een *ernstige inbreuk* op de rechtsorde opleveren en het onderzoek moet het hacken *dringend* vorderen.

Daarnaast is vereist dat de hackbevoegdheid wordt ingezet met het oog op het verrichten van een wettelijk omschreven *onderzoekshandeling*. Dit zijn: (a) de vaststelling en vastlegging van bepaalde kenmerken van de computer of de gebruiker, zoals identiteit of locatie; (b) de uitvoering van een bevel tot direct afluisteren, of het aftappen en opnemen van communicatie;[89] of (c) de uitvoering van een bevel tot stelselmatige observatie.[90] Wanneer er sprake is van een ernstig misdrijf waarop een gevangenisstraf van acht jaren of meer is gesteld, of een misdrijf dat bij algemene maatregel van bestuur is aangewezen,[91] kunnen de hackbevoegdheden bovendien worden ingezet met het oog op twee andere wettelijke doeleinden: (d) de vastlegging van gegevens die op de computer zijn opgeslagen of verwerkt (veiligstellen van gegevens);[92] en (e) het ontoegankelijk maken van gegevens.

Tot slot is een *rechterlijke machtiging* vereist voor de inzet van de bevoegdheden.

---

voorlopige hechtenis, zoals het verspreiden van opruiende geschriften, computervredebreuk, DDoS-aanvallen, of het beroepsmatig of in een groep uiten van beledigingen.

87 Art. 126uba (wetsvoorstel) Sv. Dit artikel verwijst naar art. 126o lid 1 Sv, wat de bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband regelt. Zie art. II, onderdeel L, van het wetsvoorstel.

88 Art. 126zpa (wetsvoorstel) Sv. Zie art. II, onderdeel Q, van het wetsvoorstel.

89 De drie voorgestelde artikelen (126nba, 126uba, en 126zpa) verwijzen hiervoor naar respectievelijk art. 126l en 126m Sv.

90 De drie voorgestelde artikelen (126nba, 126uba, en 126zpa) verwijzen hiervoor naar art. 126g Sv.

91 Het kan gaan om de volgende misdrijven. Misdrijven waarop acht jaren of meer is gesteld, zijn delicten zoals deelneming aan een terroristische organisatie, mensenhandel, of moord. De Memorie van Toelichting bij het wetsvoorstel geeft verder aan dat de bij algemene maatregel van bestuur aan te wijzen misdrijven, delicten betreft die met behulp van een computer worden gepleegd en waarbij er een duidelijk maatschappelijk belang is om de situatie te beëindigen en de daders te vervolgen. Bijvoorbeeld het gebruik van een botnet (art. 138ab lid 3 Sr) en het aanbieden van kinderporno (art. 240b Sr). Daarnaast kan met een algemene maatregel van bestuur ook andere ernstige misdrijven kunnen worden aangewezen, als bij het misdrijf een computer wordt gebruikt en 'de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is.' Zie *Kamerstukken II* 2015-16, 34372, 3 (MvT), p. 29.

92 Dit kan betrekking hebben op gegevens die al op de computer zijn opgeslagen, of op gegevens die na het tijdstip van afgifte van het hackbevel op de computer worden opgeslagen.

3.2 De hackbevoegdheid in het licht van de tien richtsnoeren

Compleet toezicht

De volgende paragrafen tonen dat het toezicht op de hackbevoegdheid formeel gezien compleet is, maar dat er bij verschillende aspecten wel kanttekeningen zijn te plaatsen.

Toezichthoudende instanties

Alle relevante partijen zijn betrokken. De wetgevende macht is betrokken bij de totstandkoming van de wettelijke regeling, en via de ministeriële verantwoordelijkheid bij de toepassing van de regeling. De uitvoerende macht is betrokken, want de officier van justitie geeft het bevel tot hacken, aan een daartoe aangewezen opsporingsambtenaar,[93] en het voornemen om de hackbevoegdheid in te zetten moet worden voorgelegd aan de Centrale Toetsingscommissie (CTC).[94] Voor zover bij deze betrokkenheid sprake is van toezicht, is dit echter intern toezicht.

Via het parlement kan in theorie een zekere mate van toezicht uitgeoefend worden via de verantwoordelijke bewindspersonen, al is dat niet ingebed in formele structuren zoals dat voor de inlichtingen- en veiligheidsdiensten gebeurt via de 'Commissie Stiekem'. Er is het voornemen – maar niet de verplichting – van de regering om jaarlijks te rapporteren aan het parlement over de uitoefening van de bevoegdheid.

Belangrijker is dan ook het toezicht door de rechterlijke macht. Onder het wetsvoorstel is vereist dat de rechter-commissaris een schriftelijke machtiging verleent,[95] en de strafrechter houdt vervolgens toezicht als het opsporingsonderzoek leidt tot een onderzoek ter terechtzitting. Dit toezicht is dus vooral gericht op de toepassing de bevoegdheden in specifieke gevallen.

Verder houden de Algemene Rekenkamer,[96] de Inspectie Veiligheid en Justitie,[97] de Nationale ombudsman,[98] en de procureur-generaal bij de Hoge Raad[99] in het algemeen toezicht op de strafrechtketen. Deze toezichthoudende instanties krijgen echter geen speciale rol bij het toezicht op de hackbevoegdheid, met uitzondering van de Inspectie Veiligheid en Justitie.[100] Ook het toezicht

93 Zie art. 126nba lid 1, art. 126uba lid 1, en art. 126zpa lid 1 Sv (wetsvoorstel).
94 Zie MvT, p. 37-38.
95 Zie art. 126nba lid 4, art. 126uba lid 3, en art. 126zpa lid 3 Sv (wetsvoorstel).
96 Art. 82-89 Comptabiliteitswet 2001.
97 Art. 65 Politiewet 2012 en Protocol voor de werkwijze van de Inspectie Veiligheid en Justitie.
98 Art. 1a WNo en art. 9:27 Awb.
99 Art. 122 RO.

door de Inspectie Veiligheid en Justitie is niet onafhankelijk, nu zij valt onder het ministerie van Veiligheid en Justitie (artikel 65, lid 2 Politiewet). Daarnaast zijn er geen waarborgen ten aanzien van de samenstelling van de inspectie. In andere gevallen in het surveillancedomein krijgen sommige van deze instanties wél een speciale, aanvullende toezichtrol. Zo wordt in het wetsvoorstel Aanpassing bewaarplicht telecommunicatiegegevens aangegeven dat de procureur-generaal zijn toezichthoudende bevoegdheid zal inzetten voor zover het betreft de naleving van de voorschriften van het Wetboek van Strafvordering met betrekking tot historische telecommunicatiegegevens door het Openbaar Ministerie. Het toezicht van de procureur-generaal zal gericht zijn op de rechtmatigheid van de toepassing van die voorschriften, en rapportage ervan zal aan de Kamer worden aangeboden.[101]

Er is tot slot geen gespecialiseerde, onafhankelijke toezichtscommissie vergelijkbaar met de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Dit is wel aan te bevelen, omdat de ervaring met de CTIVD leert dat zo een commissie effectief en daadwerkelijk toezicht kan houden op de uitoefening van de hackbevoegdheid in individuele gevallen, en in het algemeen.

Momenten van toezicht

Er is een zekere mate van onafhankelijk toezicht op de drie vereiste momenten. Dit toezicht is in theorie het sterkst op het moment dat een machtiging wordt gevraagd: dan kan de rechter-commissaris dat immers weigeren. Het is tegelijkertijd de vraag in hoeverre dit soort verzoeken ook daadwerkelijk worden geweigerd. Uit de praktijk is gebleken dat de rechter-commissaris bijna nooit weigert een machtiging af te geven, onder andere omdat de rechter-commissaris erop anticipeert dat onrechtmatige of onzorgvuldige inzet van bijzondere bevoegdheden op de zitting aan de orde zal worden gesteld.[102]

Vervolgens houdt de rechter-commissaris in theorie toezicht *tijdens* de uitoefening van de bevoegdheid. De rechter-commissaris is namelijk belast met toezicht op het opsporingsonderzoek,[103] en hij moet een nieuwe machtiging afgeven als de diensten om verlenging, wijziging, of aanvulling van het surveillancebevel vragen.[104] Ook daar kunnen kanttekeningen bij worden geplaatst. Om deze

---

102 A. Beijer, R.J. Bokhorst, M. Boone, C.H. Brants en J.M.W. Lindeman, 'De Wet bijzondere opsporingsbevoegdheden – eindevaluatie', Wetenschappelijk Onderzoek- en Documentatiecentrum 2004, te downloaden via www.wodc.nl, p. 193; N. van Buiten, 'De modernisering van de Wet BOB – Herinneren we ons de IRT-affaire nog?', *DD* 2016/10, afl. 3, p. 130-144, p. 142.

103 Art. 170 lid 2 en 180 lid 2 Sv.

104 Art. 126nba lid 5, 126uba lid 3, en 126zpa lid 3 Sr (wetsvoorstel). Het afgeven van een nieuwe machtiging biedt de gelegenheid tot toezicht. De hackbevoegdheid mag maximaal vier weken worden toegepast, en kan telkens voor een

functie uit te oefenen, kan de rechter-commissaris zich door de officier van justitie laten informeren over het lopende opsporingsonderzoek. Maar in de praktijk is gebleken dat rechter-commissarissen weinig gebruik maken van deze mogelijkheid.[105] Binnen de maximaal vier weken dat een machtiging van de rechter-commissaris geldt, en zo lang de diensten niet om verlenging, wijziging, of aanvulling vragen, is er dus beperkt onafhankelijk toezicht op de voortgang van het onderzoek.

Tot slot zal er in sommige gevallen onafhankelijk toezicht zijn *nadat* de toepassing van de hackbevoegdheid is beëindigd, want als het opsporingsonderzoek leidt tot een onderzoek ter terechtzitting houdt de strafrechter toezicht. Wanneer het opsporingsonderzoek niet leidt tot vervolging, kunnen belanghebbenden die op de hoogte zijn gesteld van de geheime surveillance naar de civiele rechter, of een klacht indienen bij de politie,[106] waarbij uiteindelijk de Nationale ombudsman ingeschakeld kan worden. Ook hier is een kanttekening op zijn plaats. Niet al het opsporingsonderzoek leidt immers tot strafrechtelijke vervolging, en niet in alle gevallen wordt mededeling gedaan aan de betrokkenen. De rechterlijke macht zal dus niet in alle gevallen dat de hackbevoegdheid wordt ingezet achteraf toezicht houden.[107]

Mandaat van de toezichthoudende instanties

De rechterlijke macht heeft belangrijke handvatten gekregen om de uitoefening van de hackbevoegdheid te toetsen. De eis dat de hackbevoegdheid alleen wordt ingezet als het onderzoek dit *dringend* vordert, houdt een noodzakelijkheidstoets in (proportionaliteit en subsidiariteit). Verder dient de rechter-commissaris bij de beoordeling van de vordering van de officier van justitie tot afgifte van een machtiging te toetsen of het bevel aan alle wettelijke eisen voldoet.[108] In een eventuele strafprocedure oefent de strafrechter vervolgens verder toezicht uit op de rechtmatigheid van de inzet van de opsporingsmiddelen. De limitatieve opsomming van de onderzoekshandelingen waarvoor de hackbevoegdheid kan worden ingezet (zie hierboven), maakt dat de noodzaak van de inzet van de bevoegdheden in een concreet geval kan worden beoordeeld.

Ook hierbij kunnen kanttekeningen worden geplaatst. In de praktijk is gebleken dat strafrechters – die achteraf toezicht houden – veel vertrouwen hebben in het voorafgaande toezicht door de rechter-commissaris.[109] Dit betekent dat de zittingsrechter in de praktijk achteraf vooral passief

---

periode van maximaal vier weken worden verlengd; zie MvT, p. 54. Aanvulling van een bevel is bijvoorbeeld nodig als de hackbevoegdheid moet worden toegepast op een ander deel van de computer; zie MvT, p. 53.

105 Beijer et al. 2004, p. 165; Van Buiten 2016, p. 142.

106 Art. 552a Sv.

107 Zie ook Y. Buruma, 'Bijzondere opsporingsmethoden: 12,5 jaar na Van Traa', *DD* 2009/7, afl. 1, p. 58-78.

108 MvT, p. 30.

109 Beijer et al. 2004, p. 265-266.

toezicht lijkt te houden, en de rechtmatigheid van de opsporing niet ambtshalve toetst, tenzij onrechtmatigheden overduidelijk uit het dossier blijken.[110] In dit verband wordt in de Memorie van Toelichting bij het wetsvoorstel nog opgemerkt dat de officier van justitie in beginsel de rechtmatigheid van het opsporingsonderzoek bewaakt, en dat de rechter-commissaris er op mag vertrouwen dat een machtiging om te hacken rechtmatig wordt uitgevoerd.[111]

Toezicht op alle fases van de gegevensverwerking

Hacken is het binnendringen van een computer. Dat alleen al is een inmenging met de privacy van de computergebruiker. De inzet van de bevoegdheid zal in vrijwel alle gevallen echter ook leiden tot verwerking van gegevens *op* die computer. Zo zien twee onderzoekshandelingen direct op het vastleggen van persoonlijke gegevens, namelijk gegevens over de gebruiker van de computer, of gegevens die op de computer zijn opgeslagen. Andere onderzoekshandelingen zien op de uitvoering van een afluister- of aftapbevel, waarbij natuurlijk communicatiegegevens worden verzameld. Daarnaast moet het technische team sowieso proces-verbaal opmaken van het hacken en van hun bevindingen.[112] Hierbij zullen vaak persoonlijke gegevens worden vastgelegd.

Uit het wetsvoorstel en andere regels van strafvordering, volgt dat de rechter-commissaris in alle gevallen dat de hackbevoegdheid wordt ingezet, toezicht houdt op het verzamelen van persoonlijke gegevens. Als het doel van het hacken de vastlegging van gegevens is, dan moet dit worden vermeld in het bevel van de officier van justitie, zodat de rechter-commissaris daarmee rekening kan houden bij de beslissing over het verlenen van de machtiging.[113] Wanneer de hackbevoegdheid wordt ingezet ter uitvoering van een afluister- of aftapbevel, dan is voor het afluisteren of aftappen een afzonderlijke machtiging van de rechter-commissaris vereist.[114]

Het Wetboek van Strafvordering voorziet in een bewaarregeling om achteraf controle mogelijk te maken op de selectie van gegevens in de bulkdata die door bijzondere opsporingsmethoden worden verkregen. Zolang de zaak niet is geëindigd, bewaart de officier van justitie de processen-verbaal met gegevens die zijn verkregen door observatie met behulp van een technisch hulpmiddel, afluisteren, of aftappen, en houdt deze ter beschikking van het onderzoek.[115] Twee maanden nadat

110 Beijer et al. 2004, p. 265-266.
111 MvT, p. 49.
112 Art. 152 Sv.
113 MvT, p. 22.
114 Art. 126l lid 4 en 126m lid 5 Sv.
115 Art. 126cc lid 1 Sv.

de zaak is geëindigd, of wanneer een voorbereidend onderzoek naar redelijke verwachting niet tot een zaak zal leiden, laat de officier van justitie de processen-verbaal en andere voorwerpen in principe vernietigen.[116]

De Wet politiegegevens (Wpg) regelt de verwerking, waaronder het verzamelen, bewaren, gebruiken, en vernietigen, van politiegegevens. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de rechtmatige verwerking van politiegegevens voor zover het daarbij om persoonsgegevens gaat.[117]

Daarmee is er in theorie toezicht op alle fases van gegevensverwerking in het kader van de hackbevoegdheid, namelijk eerst door de rechter-commissaris, en vervolgens door de Autoriteit Persoonsgegevens. Daarbij past wel de kanttekening dat de Autoriteit Persoonsgegevens heeft aangegeven over beperkte capaciteit te beschikken en hoe zich dit verhoudt tot de prioritering met betrekking tot het toezicht op de naleving van de Wpg.

Onafhankelijk toezicht

Er is sprake van onafhankelijk toezicht op de toepassing van de hackbevoegdheid in individuele gevallen, namelijk door de rechter-commissaris als machtigingsrechter en later eventueel door de strafrechter ter terechtzitting. De onafhankelijkheid van de verschillende betrokken rechters wordt onder andere verzekerd door de bepaling dat de rechter die als rechter-commissaris betrokken was bij het vooronderzoek, geen deel mag nemen aan het onderzoek op de terechtzitting.[118]

Tegelijkertijd is er afgezien hiervan geen onafhankelijk toezicht op de uitoefening van deze bevoegdheid, ook niet op de uitoefening in het algemeen. De eventuele betrokkenheid van de Centrale Toetsingscommissie (CTC) of de inspectie Veiligheid en Justitie kan zoals gezegd niet als een vorm van onafhankelijk toezicht worden beschouwd.

116 Art. 126cc lid 2 en 3 Sv. Een uitzondering op de vernietigingsplicht is dat de officier van justitie kan bepalen dat gegevens die zijn verkregen door dergelijke opsporingsmethoden gebruikt worden voor een ander strafrechtelijk onderzoek, of om inzicht te krijgen in de betrokkenheid van personen bij zware criminaliteit; zie art. 126dd Sv.

117 Art. 35 Wet politiegegevens.

118 Art. 268 lid 2 Sv.

Voorafgaand toezicht

De rechter-commissaris houdt voorafgaand toezicht op de toepassing van de hackbevoegdheid, omdat hij een machtiging moet verlenen op vordering van de officier van justitie. Zoals eerder opgemerkt, is gebleken dat de rechter-commissaris bijna nooit weigert een machtiging af te geven.[119] Dit roept de vraag op in hoeverre de rechter-commissaris de noodzakelijkheid en proportionaliteit van de inzet van de hackbevoegdheid voldoende zal toetsen.[120] Het ligt buiten het bereik van dit rapport om verder in te gaan op deze vraag.

Het is van belang dat de rechter-commissaris nader motiveert. Dit is in lijn met andere machtigingen tot de inzet van bijzondere bevoegdheden, die de rechter-commissaris ook met redenen moet omkleden.[121] Onvoldoende verantwoording maakt het voor een rechter-commissaris nog makkelijker om verzoeken zonder al te veel onderzoek goed te keuren (‘rubber stamping’).

Het wetsvoorstel schrijft verder een voorafgaande toetsing door de Centrale Toetsingscommissie voor bij de inzet van de hackbevoegdheid. Dit is een extra waarborg in het kader van de proportionaliteit en de subsidiariteit. Lindeman schrijft dat het CTC naar verluidt in de praktijk behoorlijk streng is, maar geeft daarbij terecht aan dat dit een interne (dus niet onafhankelijke) toetsing blijft.[122]

Onrechtmatigheden voorkomen, beëindigen, of herstellen

De rechter-commissaris bij wie voorafgaand, of gedurende het onderzoek een machtiging wordt gevorderd, kan weigeren om de machtiging af te geven, en daarmee voorkomen dat de hackbevoegdheid wordt ingezet. Daarnaast kan de rechter-commissaris het bevel beëindigen,[123] of de officier van justitie een termijn stellen voor beëindiging van het opsporingsonderzoek.[124] Indien

119 Beijer et al. 2004, p. 193; Van Buiten 2016, p. 142.
120 Zie Lindeman, § 6, onder *Dragojević*. Zie over proportionaliteit en subsidiariteit in de opsporing ook Franken 2009.
121 Zie art. 126g lid 8 en verder.
122 Lindeman, § 7, onder *Dragojević*.
123 Art. 126nba lid 5, art. 126uba lid 3, en art. 126zpa lid 3 Sv (wetsvoorstel).
124 Art. 180 lid 3 Sv.

blijkt dat in het opsporingsonderzoek vormen zijn verzuimd, kan de rechter-commissaris ook bevelen om het verzuim te herstellen.[125]

Bij het toezicht achteraf kan de strafrechter verschillende gevolgen verbinden aan vormverzuimen bij de inzet van de hackbevoegdheid. Hij kan besluiten tot strafvermindering, bewijsuitsluiting, of niet-ontvankelijkheidverklaring van het openbaar ministerie.[126] Hierbij is de kanttekening te plaatsen dat deze vormen van genoegdoening niet rechtstreeks in verband staan met een geconstateerde schending van het fundamentele recht op privacy, maar in het teken staan van het recht op een eerlijk proces.[127] Rechtbanken zijn echter terughoudend om over te gaan tot het uitsluiten van bewijsmateriaal als gevolg van een vormverzuim.[128] Sowieso biedt bewijsuitsluiting bij een privacyschending door de inzet van de hackbevoegdheid waarschijnlijk vaak geen oplossing, omdat door middel van bijzondere opsporingsbevoegdheden meestal alleen startinformatie wordt verkregen, wat niet als bewijs wordt gebruikt.[129] Bovendien is de Nederlandse rechter terughoudend met de toepassing van deze drie herstelmogelijkheden. Volgens sommige auteurs levert dit een leemte in het toezicht op het strafvorderlijke overheidsoptreden, die bovendien niet wordt opgevuld door het toezicht door de overige instanties zoals de Algemene Rekenkamer, de Nationale ombudsman, of de Inspectie Veiligheid en Justitie.[130]

Tegenspraak

De hackbevoegdheid wordt in het geheim uitgevoerd, en de betrokkenen krijgen dus niet de kans om tegenspraak te leveren vóór de daadwerkelijke tenuitvoerlegging. Belanghebbenden kunnen tegenspraak leveren als de inzet van de hackbevoegdheid leidt tot een strafrechtelijke procedure, of als ze achteraf op de hoogte worden gesteld (zie daarover verder richtsnoer 8). Op verschillende punten in dit rapport is al opgemerkt dat niet alle opsporing leidt tot strafvervolging, en dat mededeling aan de betrokkenen soms achterwege blijft. Die vaststelling is ook van belang voor het principe van tegenspraak.

125 Art. 199 Sv.
126 Art. 359a Sv.
127 Zie in deze zin ook Lindeman, § 8, onder *Dragojević*.
128 M. Samadi, § 7, onder EHRM 15 januari 2015, 68955/11 *(Dragojević v. Kroatië), EHRC* 2015/114.
129 Zie hierover ook Van der Staak 2007.
130 Zie o.a. M. Samadi, 'Policing the police: het toezicht op de opsporing', *DD* 2016/37, afl. 6, p. 406-418, met verdere verwijzingen. Zie in dit verband ook T. Blom, Boekbeschouwingen: R. Kuiper, Vormverzuimen. Juridische consequenties van vormverzuimen in strafzaken, *Rechtsgeleerd Magazijn Themis*, 2015, p. 119-120.

In de context van geheime surveillance door inlichtingen- en veiligheidsdiensten wordt gesuggereerd om het ontbreken van tegenspraak door de belanghebbende te compenseren met een 'publieke advocaat' (*public advocate*), die namens de belanghebbende – maar zonder dat de betrokkene daarvan op de hoogte is – tegenspraak kan leveren wanneer een toezichthoudende instantie voorafgaand om toestemming tot de inzet van een geheime surveillancebevoegdheid wordt verzocht. Tegenspraak kan ook meer structureel vorm krijgen door bij de opsporing betrokken derden een mogelijkheid tot bezwaar te bieden en door van hun expertise gebruik te maken (zie ook de volgende subparagraaf).

Voldoende middelen voor effectief toezicht

De rechter-commissaris en de strafrechter, twee belangrijke toezichthoudende instanties in het strafvorderlijke domein, hebben qua middelen in ieder geval toegang tot deskundigheid. Rechters mogen deskundigen benoemen,[131] en in Den Haag is voor rechters speciaal een kenniscentrum computercriminaliteit opgericht, inclusief cursusmogelijkheden.[132] Daarnaast worden de uitvoerende rechercheurs speciaal getraind in hun opleidingstrajecten, en organiseert het openbaar ministerie voor de officiers van justitie bijscholingscursussen op het gebied van computercriminaliteit.[133]

Tegelijkertijd merkt de Memorie van Toelichting bij het wetsvoorstel op dat de officier van justitie en de rechter-commissaris niet bij uitstek deskundig zijn om de technische risico's van het hacken te beoordelen.[134] De Memorie van Toelichting wijst daarom op het belang van de deskundigheid van de opsporingsambtenaren die worden belast met het uitvoeren van de hack. Dit impliceert wel dat onafhankelijk rechterlijk toezicht op de beheersing en beperking van risico's van een hack beperkt zal zijn. De mogelijkheid om tevens op ruimere schaal (aanvullend) gebruik te kunnen maken van externe deskundigheid krijgt weinig aandacht in het wetsvoorstel.

131 Art. 176 en 227 Sv.
132 MvT, p. 39.
133 MvT, p. 39.
134 MvT, p. 33.

Transparantie

De informatieplicht van de officier van justitie voorziet in transparantie jegens de machtigingsrechter. Tijdens de machtigingsprocedure moet de officier van justitie ervoor zorgen dat de rechter-commissaris op tijd alle relevante stukken ontvangt, en moet hij de rechter-commissaris voorzien van de inlichtingen die nodig zijn voor een goede uitoefening van diens toezichthoudende taak.[135] Deze algemene bepaling ziet ook op gevallen waarin de rechter-commissaris toestemming moet geven om bijzondere opsporingsbevoegdheden in te zetten, waaronder de voorgestelde hackbevoegdheid.

De strafrechter die achteraf toezicht houdt, zal met name aangewezen zijn op de logbestanden van het hacken. Het wetsvoorstel bepaalt dat bij of krachtens algemene maatregel van bestuur regels zullen worden gesteld over de geautomatiseerde vastlegging van gegevens over de uitvoering van een hackbevel (= logging).[136] Logging zal verder worden geregeld in het Besluit technische hulpmiddelen strafvordering.[137] Een effectieve controle hierop is onder meer afhankelijk van de manier waarop wordt gelogd, en de manier waarop die logs worden gepresenteerd. En, zoals eerder aangegeven, moet de integriteit van het bewijs worden gewaarborgd. Dat is in het digitale domein een bijzondere uitdaging. Juist omdat deze aspecten zijn gedelegeerd kan niet goed worden beoordeeld of het toezicht voldoet.

In de strafrechtketen wordt gesproken van interne openbaarheid en externe openbaarheid. Interne openbaarheid volgt uit de bepaling dat de officier van justitie de processen-verbaal en andere voorwerpen waaraan gegevens ontleend kunnen worden die zijn verkregen door de uitoefening van opsporingsbevoegdheden bij de processtukken moet voegen.[138] Deze vorm van openbaarheid is gericht op de verdachte, en geeft hem de mogelijkheid de oordeelsvorming van de rechter te beïnvloeden. Wat betreft de hackbevoegdheid is het technische team verplicht een proces-verbaal op te maken van het hacken en hun bevindingen.[139]

Daarnaast voorziet het Wetboek van Strafvordering in een notificatieplicht bij de toepassing van bijzondere opsporingsbevoegdheden.[140] In dit opzicht is het een vooruitgang dat het meest recente wetsvoorstel de hackbevoegdheid in de titel van de bijzondere opsporingsbevoegdheden plaatst.

---

135 Art. 177a Sv.
136 Art. 126nba lid 7 Sv (wetsvoorstel).
137 MvT, p. 39.
138 Art. 126aa Sv.
139 Art. 152 Sv.
140 Art. 126bb Sv.

Hierdoor geldt de notificatieplicht dus ook voor de hackbevoegdheid. Een belangrijke kanttekening is wel dat de notificatieplicht in de praktijk weinig wordt nagekomen,[141] en dat er een wetsvoorstel is om de notificatieplicht in te perken.[142]

Wat betreft externe openbaarheid is in dit kader van belang dat de Minister van Veiligheid en Justitie de inlichtingen dient te verschaffen die door leden van het parlement worden verlangd.[143] De Centrale Toetsingscommissie moet haar interne advies over de toepassing van de hackbevoegdheid voorleggen aan het College van procureurs-generaal. Het College brengt vervolgens periodiek verslag uit aan de staatsecretaris van Veiligheid en Justitie over het aantal ter toetsing en registratie aangeboden (bijzondere) opsporingsbevoegdheden.[144] Verder is er het voornemen jaarlijks aan de Kamer te rapporteren over de inzet van de hackbevoegdheid. Dit betreft het aantal keer dat de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid.[145] Dit voornemen is overigens alleen in de Memorie van Toelichting uitgesproken, maar niet vastgelegd in een wettelijke plicht.

Het wetsvoorstel zelf geeft geen aanvulling op het al bestaande stelsel van transparantie. Daarmee is niet uit te sluiten dat de openbaarheid ten aanzien van het inzetten van nieuwe vormen van geheime surveillance even beperkt en problematisch zal zijn als dat het geval is met bijvoorbeeld de transparantie rond aftappen. Een en ander kan extra problematisch zijn wanneer bij de geheime surveillance methodes gebruikt worden die schade kunnen toebrengen aan derden (disfunctionerende randapparaten; 'zero day'- kwetsbaarheden).

Een onderbelicht punt in het politieke debat is toezicht en transparantie met betrekking tot de technologieën die worden gebruikt bij het uitoefenen van de hackbevoegdheid. Het enkele binnendringen in een computer kan de integriteit van de gegevens op het betreffende systeem aantasten. Daarom is het bijvoorbeeld belangrijk dat de software die wordt gebruikt zoveel mogelijk de integriteit van het te verzamelen bewijs waarborgt. Anders is effectief en daadwerkelijk toezicht op de uitoefening van de hackbevoegdheid sowieso onmogelijk.

Daarnaast bestaat er echter een zaak-overstijgende reden waarom de hackbevoegdheid aan nader toezicht moet worden onderworpen. Bij het hacken wordt namelijk gebruik gemaakt van

141 Beijer et al. 2004, p. 267; T. Spapens, M. Siesling en E. de Feijter, 'Brandstof voor de opsporing: Evaluatie Wet bevoegdheden vorderen gegevens', Wetenschappelijk Onderzoek- en Documentatiecentrum 2011, te downloaden via www.wodc.nl, p. 98-101.

142 *Kamerstukken II* 2013/14, 33747, 1-3.

143 Art. 68 Gw.

144 MvT, p. 37-38.

145 MvT, p. 40.

kwetsbaarheden in systemen. Meestal bevatten niet alleen de computer van de verdachte, maar ook computers van anderen dit soort kwetsbaarheden. De keuze van het openbaar gezag om het bestaan van kwetsbaarheden niet te delen met softwarefabrikanten, betekent dat een zwakkere digitale infrastructuur bewust in stand wordt gehouden. Die maatschappelijke gevolgen pleiten ervoor dat er ook toezicht is op de technologieën die worden ingezet. Het wetsvoorstel legt nu niet vast onder welke voorwaarden zulk toezicht plaatsvindt.

Het wetsvoorstel kan worden aangescherpt door enerzijds transparantie in de wet te verankeren en anderzijds door nader aan te geven ten aanzien van welke aspecten transparantie kan worden geboden. De concrete uitwerking vindt vervolgens plaats via nadere regulering. De informatieverstrekking dient bij voorkeur te geschieden door of onder verantwoordelijkheid van een onafhankelijke toezichthouder.

Opvraagbaarheid van informatie

De voorgaande paragrafen laten zien dat het wetsvoorstel, en met name reeds bestaande structuren binnen de strafrechtketen, voorzien in een zekere transparantie rondom de hackbevoegdheid. Sommige aspecten hiervan, waaronder het loggen, zijn echter gedelegeerd. Andere aspecten, met name de werkwijze van de Centrale Toetsingscommissie en de informatievoorziening aan het parlement, worden niet gereflecteerd in dwingendrechtelijke bepalingen.

Net zoals dat het geval is met de actieve transparantie (vorige paragraaf) mag worden aangenomen dat ten aanzien van verzoeken tot informatie een met het aftappen vergelijkbare terughoudende praktijk zal worden gehanteerd. En net zoals dat het geval is met actieve openbaarheid kan de opvraagbaarheid van informatie daarom nader in de wet worden verankerd.

Informatieverstrekking door derde partijen

De toepassing van de hackbevoegdheid is in de regel niet afhankelijk van een medewerkingsplicht voor derde partijen.[146] Dit maakt de vraag of deze derden over hun betrokkenheid kunnen rapporteren minder relevant (maar versterkt de noodzaak dat de overheid hierover transparant is).

Bij andere vormen van geheime surveillance, zoals bij het aftappen, is er echter wel een grotere betrokkenheid en dient er duidelijkheid te zijn over de wijze waarop over deze betrokkenheid kan worden gerapporteerd ('transparency reporting'). Momenteel is er geen zekerheid over de mate waarin door derden over hun betrokkenheid kan worden gerapporteerd. Dit leidt tot rechtsonzekerheid 'chilling effects'. Dit staat op gespannen voet met het grondrecht op privacy en het grondrecht op vrijheid van meningsuiting.

Om deze onduidelijkheid weg te nemen is het daarom te adviseren 'transparency reporting' een wettelijke basis te geven, met de mogelijkheid van een meer specifieke uitwerking in concrete minimumnormen, die in ieder geval in overleg met alle betrokkenen (bedrijven, civil society) worden opgesteld. Het uitgangspunt daarbij moet zijn dat dit is toegestaan, tenzij in specifieke gevallen dit de opsporing zou verhinderen.

146 Dit moet echter ook niet worden uitgesloten: zo werd bij het hacken van het Bredolab-botnet gebruik gemaakt van de medewerking van Leaseweb. Zie D. Reijerman, "Nationale Recherche haalt Bredolab-botnet uit de lucht, *Tweakers* 25 oktober 2010, https://tweakers.net/nieuws/70424/nationale-recherche-haalt-bredolab-botnet-uit-de-lucht.html.

3.3 Overige wetsvoorstellen

In de voorgaande paragraaf is een eerste analyse gemaakt van hoe de ontwikkelde richtsnoeren voor toezicht en transparantie zich laten toepassen op het Wetsvoorstel Computercriminaliteit III. Dit is echter niet het enige wetsvoorstel waarbij vragen van toezicht en transparantie spelen. Ook voor de wetsvoorstellen voor de bewaarplicht telecommunicatiegegevens,[147] bronbescherming,[148] kentekenplaat-herkenning,[149] en de herziening van artikel 13 Grondwet[150] is deze analyse relevant.

147 Dossiernummer 34 537.
148 Dossiernummer 34 032, 34 027.
149 Dossiernummer 33 542.
150 Dossiernummer 33 989.

4 Conclusies

In deze *quickscan* is nagegaan welke richtsnoeren ten aanzien van toezicht en transparantie van toepassing zijn op geheime surveillance bij de opsporing van strafbare feiten. Daarbij is aangeknoopt bij het eerder verrichte onderzoek naar richtsnoeren op het gebied van toezicht en transparantie in het kader van de activiteiten van inlichtingen- en veiligheidsdiensten. Een voorvraag van deze *quickscan* is dan ook in hoeverre die eerder ontwikkelde richtsnoeren toegepast kunnen worden op het opsporen van strafbare feiten.

De onderliggende bepalingen, meer in het bijzonder artikel 8 van het EVRM en artikelen 7 en 8 van het Handvest, maken geen onderscheid naar de aard van opsporingsactiviteiten of opsporingsorganisaties. Daarbij komt dat er in veel landen geen duidelijk organisatorisch of inhoudelijk onderscheid kan worden gemaakt tussen de activiteiten van inlichtingen- en veiligheidsdiensten en de politie. Het door het EHRM en HvJEU in de afgelopen decennia ontwikkelde raamwerk op het gebied van toezicht en transparantie rond geheime surveillance kent dit onderscheid dan ook niet.

Vanuit dat uitgangspunt zijn de eerder ontwikkelde richtsnoeren vervolgens nader besproken, waar nodig aangevuld door jurisprudentie die sinds de publicatie van de eerdere studie is uitgekomen. Ter illustratie zijn de richtsnoeren toegepast op het Wetsvoorstel Computercriminaliteit III.

Uit deze analyse blijkt dat het rechtsstatelijk kader rond de opsporing van strafbare feiten in Nederland in theorie behoorlijk ontwikkeld is. Het strafvorderlijk systeem kent een zekere mate van toezicht. De waarborgen rond transparantie zijn minder ontwikkeld.

De complexiteit en kosten van geheime surveillance dalen dankzij technologische ontwikkelingen echter. Tegelijkertijd neemt bij geheime surveillance in digitale context het risico toe dat een grote groep burgers hierdoor wordt geraakt, of dat dit vergaande impact heeft op individuen. Bij de inzet van bevoegdheden die niet alleen verdachten raken, maar ook andere betrokkenen of de maatschappij in het algemeen, is een coherent en compleet toezicht- en transparantiekader daarom nog belangrijker. Complexiteit en impact laten onverlet dat de wetgever wanneer hij voornemens op het gebied van toezicht en transparantie formuleert, hij deze ook vastlegt in de wet. Het is onvoldoende als deze slechts in de ontstaansgeschiedenis worden uitgesproken of worden ingevuld via delegatiebevoegdheden.

Er kunnen een aantal conclusies worden getrokken en daarmee samenhangende aanbevelingen worden gedaan.

- Er ontbreekt een instelling vergelijkbaar met de Commissie op de Inlichtingen en Veiligheidsdiensten (CTIVD) die toezicht houdt op geheime surveillance in het belang van het opsporen van strafbare feiten. Er is geen 'systeemtoezicht': er vindt wel enig toezicht plaats in individuele gevallen, maar er is slechts in beperkte mate onafhankelijk toezicht op de uitoefening in algemene zin. Een onafhankelijke toezichtscommissie zou een belangrijke toevoeging zijn aan het systeem van *checks and balances.* Verschillende richtsnoeren zien op de meerwaarde van een dergelijk orgaan.

- Voorafgaande toetsing van in te zetten technologieën zou het toezicht meer compleet maken. Toezicht moet niet beperkt blijven tot de inzet van een middel in een concreet geval. Dit geldt in het bijzonder in het digitale domein, waar de inzet van methoden en technologieën zaak-overstijgende gevolgen kan hebben, bijvoorbeeld doordat kwetsbaarheden niet worden gedeeld en de digitale infrastructuur hierdoor zwakker blijft. Dit pleit in het bijzonder voor een vorm van systeemtoezicht.

- De jurisprudentie is duidelijk wat betreft de inrichting van het toezicht. Dit moet 'daadwerkelijk en effectief' zijn. Dit betekent onder meer dat de rechter-commissaris en zittingsrechter hun bevoegdheden daadwerkelijk uitoefenen. Er kan geen sprake zijn van 'rubber stamping': het voorafgaand verstrekken van lasten en toestemming moet zorgvuldig gebeuren en goed gemotiveerd te worden. Er dient 'real time' toezicht te zijn, dat wil zeggen toezicht gedurende de inzet van de bevoegdheden.[151] De notificatieplicht behoort daadwerkelijk vorm te worden gegeven. En de parlementaire toezichtstaak kan kracht worden bijgezet door de wetgeving te voorzien van 'sunset'-bepalingen op grond waarvan de wetgeving op een bepaalde datum automatisch komt te vervallen. Betrokkenheid van deskundigen in het proces, zeker waar het gaat om nieuwe technologische uitdagingen c.q. toepassingsmogelijkheden, draagt bij aan 'tegenspraak' en tot een meer afgewogen besluitvorming. Er dient bijzondere aandacht te zijn voor een onbalans tussen expertise op het gebied van digitale technologieën bij opsporingsinstanties en de toezichthouders, waaronder de rechter.

151 Buruma 2009 en 2016.

- ‘Public scrutiny’ is belangrijk omdat bij geheime surveillance klassieke waarborgen van openbaarheid ontbreken. Toezichthouders moeten kunnen beschikken over alle relevante informatie, net zoals de burger. Er moet meer aandacht zijn voor de vraag hoe voorzien wordt in transparantie jegens de samenleving. Een manier om hieraan te voldoen is door meer duidelijkheid te scheppen over de voorwaarden waaronder organisaties gegevens mogen publiceren over verzoeken tot medewerking aan de uitoefening van bijzondere bevoegdheden.

5 Literatuur

Kamerstukken II 2013/14, 33747, 1-3.

Kamerstukken II 2015-16, 34372, 1-4.

Kamerstukken II 2015-16, 34537, 1-3.

A. Beijer, R.J. Bokhorst, M. Boone, C.H. Brants en J.M.W. Lindeman, 'De Wet bijzondere opsporingsbevoegdheden – eindevaluatie', Wetenschappelijk Onderzoek- en Documentatiecentrum 2004, www.wodc.nl.

T. Blom, Boekbeschouwingen: R. Kuiper, Vormverzuimen. Juridische consequenties van vormverzuimen in strafzaken, *Rechtsgeleerd Magazijn Themis*, 2015, p. 119-120.

Bijlage P, 'Referentiekader publiek toezicht onderzoeksraad', bij: Onderzoeksraad voor Veiligheid, *Explosies MSPO2 Shell Moerdijk*, Den Haag 2015.

N. van Buiten, 'De modernisering van de Wet BOB – Herinneren we ons de IRT-affaire nog?', *DD* 2016/10, afl. 3, p. 130-144.

Y. Buruma, 'Bijzondere opsporingsmethoden: 12,5 jaar na Van Traa', *DD* 2009/7, afl. 1, p. 58-78.

Y. Buruma, 'De criminele homo digitalis', *NJB* 2016/1073, afl. 22, p. 1534-1541.

S. Eskens, O.L. van Daalen en N.A.N.M. van Eijk, 'Ten standards for oversight and transparency of national intelligence services', Amsterdam: IViR 2015, http://www.ivir.nl/publicaties/download/1591.pdf

J. Gerards, 'Rechtsvinding door het Europees Hof voor de Rechten van de Mens', *NJCM-Bulletin* 2006, afl. 1, p. 93-122.

B.-J. Koops, A. Roosendaal, E. Kosta, M. van Lieshout en E. Oldhoff, 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20xx', PI.lab 2016, https://pure.uvt.nl.

F. Mertens, E. Muller, en H. Winter (red.), *Toezicht: Inspecties en autoriteiten in Nederland*, Deventer: Wolters-Kluwer 2015.

M. Samadi, 'Policing the police: het toezicht op de opsporing', *DD* 2016/37, afl. 6, p. 406-418.

M.G.J.M. van der Staak, 'Informationele privacy in de strafrechtspleging', *DD* 2006/59 (jrg. 2007), afl. 7, p. 718-736.

T. Spapens, M. Siesling en E. de Feijter, 'Brandstof voor de opsporing: Evaluatie Wet bevoegdheden vorderen gegevens', Wetenschappelijk Onderzoek- en Documentatiecentrum 2011, www.wodc.nl.

T. Vis, *Intelligence, politie en veiligheidsdienst: Verenigbare grootheden?* (diss. Tilburg University), Tilburg 2012, https://pure.uvt.nl.

HvJ EU 16 oktober 2012, C-614/10 (*Commissie v. Oostenrijk*).

HvJ EU 8 april 2014, in de gevoegde zaken C-293/12 en C-594/12 (*Digital Rights Ireland*).

HvJ EU 6 oktober 2015, C-362/14 (*Schrems v. Data Protection Commissioner*).

EHRM 6 september 1978, 5029/71 (*Klass en anderen v. Duitsland*).

EHRM 2 augustus 1984, 8691/79 (*Malone v. Verenigd Koninkrijk*).

Ontvankelijkheidsbeslissing van de Commissie 10 mei 1985, 10439/83, 10440/83, 10441/83, 10452/83, 10512/83 en 10513/83 (*Mersch en anderen v. Luxemburg*).

EHRM 26 maart 1987, 9248/81 (*Leander v. Zweden*).

EHRM 24 april 1990, 11105/84 (*Huvig v. Frankrijk*).

EHRM 24 april 1990, 11801/85 (*Kruslin v. Frankrijk*).

Ontvankelijkheidsbeslissing van de Commissie 8 juni 1990, 13564/88 (*L. v. Noorwegen*).

Ontvankelijkheidsbeslissing van de Commissie 2 april 1993, 18601/91 (*Esbester v. Verenigd Koninkrijk*).

EHRM 25 maart 1998, 13/1997/797/1000 (*Kopp v. Zwitserland*).

EHRM 30 juli 1998, 58/1997/842/1048 (*Valenzuela Contreras v. Spanje*).

EHRM 24 augustus 1998, 88/1997/872/1084 (*Lambert v. Frankrijk*).

EHRM 16 februari 2000, 27798/95 (*Amann v Zwitserland*).

EHRM 4 mei 2000, 28341/95 (*Rotaru v. Roemenië*).

EHRM 25 september 2001, 44787/98 (*P.G. en J.H. v. Verenigd Koninkrijk*).

EHRM 20 juni 2002, 50963/99 (*Al-Nashif v. Bulgarije*).

EHRM 27 april 2004, 50210/99 (*Doerga v. Nederland*).

EHRM 25 november 2004, 16269/02 (*Aalmoes & 112 anderen v. Nederland*).

EHRM 5 april 2005, 9940/44 (*Brinks v. Nederland*) (ontvankelijkheidsbeslissing).

EHRM 6 juni 2006, 62332/00 (*Segerstedt-Wiberg en anderen v. Zweden*).

EHRM 29 juni 2006, 54934/00 (*Weber en Saravia v. Duitsland*) (ontvankelijkheidsbeslissing).

EHRM 2 november 2006, 23543/02 (*Volokhy v. Oekraine*).

EHRM 7 december 2006, 29514/05 (*Van der Velden v. Nederland*) (ontvankelijkheidsbeslissing).

EHRM 26 april 2007, 71525/01 (*Dumitru Popescu v. Roemenië*) (Nr. 2).

EHRM 28 juni 2007, 62540/00 (*Association for European Integration and Human Rights en Ekimdzhiev v. Bulgarije*).

EHRM 10 december 2007, 69698/01 (*Stoll v. Zwitserland*).

EHRM 28 april 2008, 1365/07 (*C.G., T.H.G. en T.C.G. v. Bulgarije*).

EHRM 1 juli 2008, 58243/00 (*Liberty en anderen v. Verenigd Koninkrijk*).

EHRM 4 december 2008, 30562/04 en 30566/04 (*S. en Marper v. Verenigd Koninkrijk*).

EHRM 17 december 2009, 16428/05 (*Gardel v. Frankrijk*).

EHRM 10 februari 2009, 25198/02 (*Iordachi en anderen v. Moldavië*).

EHRM 18 mei 2010, 26839/05 (*Kennedy v. Verenigd Koninkrijk*).

EHRM 2 september 2010, 35623/05 (*Uzun v. Duitsland*).

EHRM 21 juni 2011, 30194/09 (*Shimovolos v. Rusland*).

EHRM 3 juli 2012, 34806/04 (*X. v. Finland*).

EHRM 31 july 2012, 36662/04 (*Drakšas v. Lithouwen*).

EHRM 2 oktober 2012, 22491/08 (*Sefilyan v. Armenië*).

EHRM 13 november 2012, 24029/07 (*M.M. v. Verenigd Koninkrijk*).

EHRM 22 november 2012, 39315/06 (*Telegraaf Media Nederland Landelijke Media B.V. en anderen v. Nederland*).

EHRM 9 januari 2013, 21722/11 (*Oleksandr Volkov v. Oekraine*).

EHRM 18 april 2013, 19522/09 (*M.K. v. Frankrijk*).

EHRM 15 januari 2015, 68955/11 (*Dragojević v. Kroatië*), *JBP* 2015/57, m.nt. J. Lindeman.

EHRM 15 januari 2015, 68955/11 (*Dragojević v. Kroatië*), *EHRC* 2015/114, m.nt. M. Samadi.

EHRM 5 maart 2015, 28718/09 (*Kotiy v. Oekraine*).

EHRM 4 december 2015, 47143/06 (*Roman Zakharov v. Rusland*), *Computerrecht* 2016/86, m.nt. S.J. Eskens.

EHRM 4 december 2015, 47143/06 (*Roman Zakharov v. Rusland*), *EHRC* 2016/87, m.nt. M. Hagens.

EHRM 12 januari 2016, 37138/14 (*Szabó en Vissy v. Hongarije*).

EHRM 7 juli 2016, 4322/06 (*Zosymov v. Oekraine*).

6 Over de auteurs

Sarah Johanna Eskens is in maart 2016 gestart als promovenda bij het Instituut voor Informatierecht. Ze doet onderzoek naar de rechten van nieuwsconsumenten (vrijheid van meningsuiting, privacy, gegevensbescherming) wanneer zij nieuws ontvangen dat is afgestemd op hun persoonlijke interesses. Hiervoor volgde zij de Onderzoeksmaster Informatierecht bij het IViR. Als onderdeel van de master deed ze onderzoek naar het toezicht op nationale inlichtingen- en veiligheidsdiensten, studeerde ze een semester aan Cardozo Law School in New York City en liep stage bij het Rathenau Instituut te Den Haag/San Francisco.

http://www.ivir.nl/nl/medewerkerpagina/eskens/

Ot van Daalen is onderzoeker op het gebied van privacy en security. Daarnaast is hij advocaat te Amsterdam, gespecialiseerd in privacy en security. In 2009 richtte hij de digitale burgerrechtenbeweging Bits of Freedom opnieuw op. Daar was hij nauw betrokken bij de totstandkoming van wetgeving op het gebied van privacy en internetvrijheid. Verder is hij bestuurslid van de Europese burgerrechtenorganisatie EDRI en zit hij in de Raad van Advies van Bits of Freedom en het SIDN Fonds. Voordat hij Bits of Freedom oprichtte, werkte hij jarenlang bij advocatenkantoor De Brauw Blackstone Westbroek, onder meer voor de high-tech en de telecomsector.

http://www.ivir.nl/nl/medewerkerpagina/daalen/

Nico van Eijk is parttime hoogleraar Informatierecht, in het bijzonder het Media- en Telecommunicatierecht, aan de Faculteit der Rechtsgeleerdheid van de Universiteit van Amsterdam, en directeur van het Instituut voor Informatierecht. Hij studeerde Rechten aan de Universiteit van Tilburg en promoveerde aan de Universiteit van Amsterdam. Tevens is hij werkzaam als zelfstandig adviseur. Daarnaast is hij onder meer voorzitter van de Vereniging voor Media- en Communicatierecht (VMC), lid van de kenniskring van de CTIVD en lid van de Koninklijke Hollandsche Maatschappij der Wetenschappen (KHMW). Hij vervult bestuurlijke en adviesfuncties bij een aantal bedrijven en instellingen (waaronder het lidmaatschap van de Ziggo Advisory Board (ZAB)).

http://www.ivir.nl/nl/medewerkerpagina/eijk/