STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 10277
26 februari 2019

Aanwijzing voor de internationale aspecten van de inzet van de bevoegdheid ex art. 126nba sv

Rechtskarakter: Aanwijzing i.d.z.v. art. 130, lid 6 Wet RO
Van: College van procureurs-generaal
Aan: Hoofden van de OM-onderdelen
Registratienummer 2019A001
Datum inwerkingtreding: 01-03-2019
Publicatie in Stcrt.: PM
Vervallen: –
Relevante beleidsregels: Aanwijzing opsporingsbevoegdheden (2014A009); Aanwijzing inzake de informatie-uitwisseling in het kader van de wederzijdse rechtshulp in strafzaken (552i Sv) (2008A024); Aanwijzing internationale gemeenschappelijke onderzoeksteams (2008A007)
Wetsbepalingen: artt. 126nba, eerste lid, 126uba, eerste lid, 126zpa, eerste lid, en 539a Sv

SAMENVATTING

Deze aanwijzing geeft regels voor de toepassing van de bevoegdheid tot het op afstand en heimelijk binnendringen van een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen (artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid Sv). Omdat het internet niet gebonden is aan landsgrenzen zullen bij de uitvoering van de bevoegdheid gegevens en geautomatiseerde werken kunnen worden benaderd die zich in het buitenland bevinden. Deze aanwijzing geeft regels voor het handelen in deze internationale context.

1. UITGANGSPUNTEN

1.1. Soevereiniteit en het internet

Met behulp van het internet kunnen gegevens eenvoudig en vliegensvlug over grote afstanden worden verzonden. De technische architectuur van het internet volgt de traditionele landsgrenzen niet. De infrastructuur van het internet, in het bijzonder de opslag van consumenten- en bedrijfsgegevens in de 'cloud', is daarnaast in eigendom van talloze internationale bedrijven. Deze bedrijven gebruiken in toenemende mate kunstmatige intelligentie om het beheer en de verwerking van klantgegevens in een onophoudelijk proces te optimaliseren. De locatie van de door hen opgeslagen gegevens is daardoor zeer vluchtig en steeds vaker ook voor het bedrijf onbekend. Om computercriminaliteit en gedigitaliseerde criminaliteit toch te kunnen blijven opsporen is het noodzakelijk dat er zorgvuldig wordt gehandeld in gevallen waar de locatie van gegevens niet op voorhand vastgesteld is of onbekend blijft.

1.2. Rechtshulp algemeen

Op grond van de wet en de jurisprudentie bestaat er voor politie en OM ruimte om buiten de grenzen van het Nederlandse grondgebied op te treden.[1] Artikel 539a Sv voorziet in een wettelijke basis om opsporingshandelingen te verrichten buiten Nederland. Een rechtshulpverzoek is daarbij het uitgangspunt. De aangezochte staat wordt verzocht aan dit rechtshulpverzoek uitvoering te geven en vervolgens de gevraagde informatie of gegevens te vorderen, te verkrijgen en te leveren. De aangezochte staat is ook zelf bevoegd om op te treden tegen inbreuken op de rechtsorde die op of vanuit het eigen grondgebied worden beraamd of gepleegd. Een verzoek om rechtshulp kan, afhankelijk van de rechtshulprelatie met het desbetreffende land, mondeling of schriftelijk worden gedaan. Als er meerdere staten rechtsmacht kunnen claimen ligt onderling overleg voor de hand.

1.3. Locatie van de gegevens is bekend

Indien bekend is dat gegevens waarvoor de bevoegdheid wordt ingezet zich op het grondgebied van een specifieke andere staat bevinden, doet de officier van justitie een verzoek tot rechtshulp aan de bevoegde autoriteiten van die staat. In het rechtshulpverzoek wordt gevraagd de gezochte gegevens te vorderen en/of (zelfstandig) veilig te stellen op basis van de daarvoor in dat land geldende wettelijke

[1] Kamerstukken II 2015/16, 34 327, 3, p. 49.

grondslagen. De officier van justitie kan ook toestemming vragen om de gezochte gegevens zelf veilig te stellen.

Diverse landen hebben als uitvloeisel van het Cybercrimeverdrag ten behoeve van de snelle afhandeling van rechtshulp in cybercrimezaken een 24/7 contactpunt ingericht[2]. Deze 24/7 contactpunten kunnen steeds vaker ook worden bevraagd in zaken waarbij snel digitaal bewijs moet worden veiliggesteld, doch waarbij het geen cybercrime betreft.

Indien op het moment waarop aan de rechter-commissaris machtiging voor de inzet van de bevoegdheid van artikel 126nba Sv[3] gevraagd wordt, bekend is dat de gegevens niet in Nederland zijn opgeslagen[4], wordt dat in de aanvraag vermeld. Hiermee is in een dergelijke situatie verzekerd dat het aspect van de inbreuk op de soevereiniteit van een andere staat onderwerp vormt van een expliciete afweging door de officier van justitie en de rechter-commissaris.

1.4. Locatie van de gegevens is niet bekend

Een kenmerk van geautomatiseerd verwerkte gegevens is dat de locatie waar zij zijn opgeslagen, steeds vaker niet op voorhand duidelijk is. In deze situatie is er onvoldoende informatie om een rechtshulpverzoek te doen, en kan bovendien niet worden uitgesloten dat de gegevens in Nederland staan. In een dergelijke situatie wordt onderzocht of met een redelijke inspanning (zie § 2.2. hierna) een locatie in een specifiek buitenland kan worden vastgesteld. Als dat niet het geval is wordt gehandeld alsof de gegevens in Nederland zijn opgeslagen.

1.5. Locatie van de gegevens wordt bekend tijdens de onderzoekshandelingen

Als tijdens de onderzoekshandelingen blijkt dat deze gericht zijn op gegevens die zich op het territorium van een specifieke andere staat bevinden, wordt zo snel mogelijk alsnog een rechtshulpverzoek gedaan aan de desbetreffende staat voor het gebruik van deze gegevens en het onderzoek (zie § 2.2. hierna) of besloten de onderzoekshandelingen te stoppen.

2. UITZONDERINGEN

2.1. Algemeen

Er kunnen zich situaties voordoen waarbij de hierboven omschreven uitgangspunten uitzondering moeten lijden. In deze gevallen zal het belang van het onderzoek zorgvuldig moeten worden afgewogen tegen de mogelijke schending van de soevereiniteit van die andere staat of staten. Dat brengt mee dat de officier van justitie in alle gevallen aan de rechter-commissaris meldt wat bekend is over de locatie van de gegevens. Dat geldt dus ook in het geval dat er niets bekend is over de locatie van de gegevens. Hiermee is geborgd dat het risico op een inbreuk op de soevereiniteit van een andere staat expliciet wordt afgewogen door de officier van justitie en aan de rechter-commissaris wordt medegedeeld.

2.2. Scenario's waarin mogelijk zonder voorafgaande toestemming wordt opgetreden

a) De locatie van de gegevens is bekend, er is een rechtshulp verzoek gedaan, maar er kan niet (langer) worden gewacht op een reactie of er is geen reactie van het land te verwachten (zie § 2.4. hierna)
b) De locatie van de gegevens is nog niet bekend op het moment dat de bevoegdheid wordt uitgeoefend en er onderzoekshandelingen worden uitgevoerd. Tijdens het onderzoek wordt de locatie echter wel bekend.
   In een dergelijk geval kan besloten worden (zie § 2.4. hierna) om:
   – *een rechtshulpverzoek te doen en de inzet te staken in afwachting van de reactie op het rechtshulpverzoek of*
   – *zo snel mogelijk een rechtshulpverzoek te doen en in afwachting van de reactie op het rechtshulpverzoek de inzet van de bevoegdheid te voltooien.*
c) Als de locatie van de gegevens met een redelijke inspanning niet kan worden vastgesteld.
   In een dergelijk situatie wordt ervan uitgegaan dat de gegevens in Nederland staan en worden de Nederlandse rechtsregels toegepast.
   De ***redelijkheid*** is sterk afhankelijk van het concrete geval. In gevallen waarbij onverwijld optreden

[2] Artikel 35 Cybercrimeverdrag.
[3] De bevoegdheid ex artt. 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid Sv wordt verder aangeduid met een verwijzing naar alleen art. 126nba Sv.
[4] Artikel 126nba, tweede lid, onderdeel b, Sv.

noodzakelijk is, denk bijvoorbeeld aan grootschalige aanvallen op de Nederlandse infrastructuur of in het geval van levensbedreigende situaties, kan er mede gelet op de omstandigheden van het geval (bijvoorbeeld het gebruik van anonimiseringssoftware of opslag in de cloud) redelijkerwijs geen mogelijkheid zijn om de exacte locatie van de gegevens of het geautomatiseerd werk vast te stellen.
Bij een ***redelijke inspanning*** staan de tijd en moeite voor het vaststellen van een specifieke geografische locatie in een reële verhouding tot de noodzakelijkheid van onverwijld optreden[5], de tijdsdruk en de doorlooptijd van het onderzoek[6].

2.3. Procedure

In de scenario's a) en b) bespreekt de zaaksofficier van justitie de context van de aanvaarde soevereiniteitsschending met de landelijk officier van justitie bij het Landelijk Parket, die is aangewezen voor de voorbereiding en concrete inzet van de bevoegdheid ex art. 126nba Sv. De zaaksofficier van justitie legt vervolgens een met redenen omkleed besluit ter instemming voor aan de rechercheofficier van justitie van zijn of haar arrondissementsparket.

2.4. Afwegingscriteria

Bij de afweging om in concrete gevallen a) en b) zonder voorafgaande toestemming te handelen zijn de volgende elementen van belang:
- Ernst of onmiddellijkheid van de gevolgen van de aanval of dreiging
- Aard en ernst van het strafbare feit
- Vluchtigheid van de gegevens of informatie die wordt gezocht, en of die moet worden veiliggesteld, danwel ontoegankelijk moet worden gemaakt
- Mate van betrokkenheid van de Nederlandse rechtsorde en de gevolgen daarvoor (inclusief slachtofferbelangen)
- De aard van de te verrichten opsporingshandelingen:
  - Afhankelijk van de mate van ingrijpendheid
  - Mate van inbreuk op de privacy van de verdachte
  - Mate van inbreuk op privacy van slachtoffers die middels het geautomatiseerde werk wordt gemaakt
- Risico's voor het geautomatiseerde werk:
  - Technische risico's
  - Inschatting van de mogelijke schade voor derden

OVERGANGSRECHT

De beleidsregels in deze aanwijzing hebben onmiddellijke gelding vanaf de datum van inwerkingtreding.

[5] In de Memorie van Toelichting bij de wet Computercriminaliteit III wordt het concrete voorbeeld gegeven van een DDoS-aanval op een overheidsdienst of een financiële instelling in Nederland waardoor de online dienstverlening gedurende langere tijd wordt onderbroken (Kamerstukken II 2015/16, 34 327, 3, p. 47.).

[6] Bij concrete inspanningen kan bijvoorbeeld worden gedacht aan het raadplegen van de WHOIS informatie van ICANN, het zo mogelijk vorderen van gegevens bij Nederlandse internetdienstaanbieders waar de verdachte mogelijk gebruik van maakt of het analyseren van in het onderzoek beschikbaar internetverkeer (netflow en/of traceroutes).