Telecomgegevens voor opsporing

Bijdragen aan de rechtshandhaving en veiligheid in Nederland

In Nederland wordt voor en achter de schermen gewerkt aan de veiligheid van burgers en ons land. (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten zijn actief om criminele of terroristische activiteiten te voorkomen en personen op te sporen die verdacht worden van een misdrijf. Soms hebben zij bij dit onderzoek informatie nodig van aanbieders van telecommunicatie en internetdiensten.

Telecom- en internetaanbieders zijn wettelijk verplicht om telecom- en internetinformatie van hun klanten beschikbaar te stellen in het kader van onderzoek. Dat is vastgelegd in het Besluit verstrekking gegevens telecommunicatie. Het gaat om persoonlijke informatie: adresgegevens behorende bij telefoonnummers, IP-adressen en e-mailadressen.

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) draagt zorg voor zorgvuldige opslag en gebruik van deze gegevens, volgens wettelijke kaders. Het CIOT beheert het geautomatiseerde CIOT-InformatieSysteem (CIS), waarin het vraag- en antwoordverkeer snel, soepel en zorgvuldig wordt afgehandeld. Het CIOT fungeert dus als een 'doorgeefluik' tussen diensten die informatie nodig hebben en de telecom- en internetaanbieders die deze informatie kunnen bieden. Daarmee leveren de aanbieders via het CIOT hun bijdrage aan een rechtvaardige en veilige samenleving.

Het Centraal Informatiepunt Onderzoek Telecommunicatie

Het CIOT voert het Besluit verstrekking gegevens telecommunicatie uit. Aanbieders van telecommunicatie- en internetdiensten moeten het CIOT bedrijfsvoeringgegevens leveren over de gebruikers van hun diensten. Het volledig geautomatiseerde CIOT-informatiesysteem stroomlijnt het vragen van informatie en de beantwoording daarvan.
Het CIOT heeft zelf geen inzage in de gegevens, maar beheert het CIS en draagt zo bij aan zorgvuldige opslag en gebruik van de informatie. Het CIOT rapporteert jaarlijks aan de minister van Veiligheid en Justitie over het gebruik van het systeem.

Het is de missie van het CIOT om een bijdrage te leveren aan een rechtvaardige en veilige samenleving. Het informatiepunt wil een (pro)actieve rol spelen in het bedrijfsproces van de (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten door de aangeleverde gegevens op een efficiënte, veilige en gestructureerde manier beschikbaar te maken. Het CIOT houdt zich hierbij aan de regels en grenzen die zijn vastgelegd in de wet.

Rechtshandhaving en nationale veiligheid

Het CIOT is opgericht om de informatieverzoeken van (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten en de beantwoording daarvan door telecom- en internetaanbieders eenvoudiger, volumeonafhankelijk en veiliger te maken. Door de marktwerking in de telecommunicatie- en internetsector komen er steeds meer aanbieders van deze diensten. Om te voorkomen dat de bevoegde autoriteiten contact moeten houden met alle aanbieders, is het CIOT-informatiesysteem ontwikkeld als een centrale voorziening, die al het vraag- en antwoordverkeer automatisch regelt.

Het belang van telecom- en internetinformatie in onderzoek neemt toe, waardoor het CIOT-informatiesysteem steeds vaker wordt geraadpleegd door de bevoegde autoriteiten. Zij houden zich immers intensief bezig met de aanpak van criminele activiteiten en de bescherming van de nationale veiligheid. Tijdens zo'n onderzoek is het erg belangrijk om de identiteit van een verdachte persoon te kunnen vaststellen. Zo worden naam-, adres- en woonplaatsgegevens gevonden bij een telefoonnummer van een mobiele telefoon, dat bij een telecomaanbieder geregistreerd staat.

De volgende diensten zijn bevoegd om het CIOT-informatiesysteem te bevragen; de politiekorpsen, de Rijksrecherche, de Sociale Inlichtingen- en Opsporingsdienst, de Koninklijke Marechaussee, de Inlichtingen- en Opsporingsdienst VROM, de Fiscale Inlichtingen- en Opsporingsdienst, de Algemene Inspectiedienst LNV en het Openbaar Ministerie. Deze diensten ontlenen hun bevoegdheid aan het Wetboek van strafvordering. De artikelen 126zi, 126zh, 126ua, 126u, 126na, 126n en 126ii zijn van toepassing.

Naast deze diensten hebben ook de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst toegang tot de gegevens in het CIOT-informatiesysteem. Deze bevoegdheid is hun toegekend op grond van de artikelen 28 en 29 van de Wet op de inlichtingen- en veiligheidsdiensten. Beheerders van een alarmnummer (112) kunnen op basis van artikel 11.10 van de Telecommunicatiewet namen en adresgegevens behorende bij telefoonnummers opvragen.

Werken volgens de wet

Het CIOT moet haar werk uitvoeren volgens een aantal wetten en besluiten, net zoals de aanbieders van de telefonie- en internetinformatie en de diensten die de informatie opvragen. Het Besluit verstrekking gegevens telecommunicatie is de basis voor de werkzaamheden van het CIOT. Dit besluit is een nadere uitwerking van artikel 13.4 van de Telecommunicatiewet. Het schrijft voor dat aanbieders van telecommunicatie- en internetdiensten in bepaalde situaties informatie over hun klanten moeten leveren.

Het besluit regelt verder dat de gegevens via een centraal informatiepunt (het CIOT) op geautomatiseerde wijze aan de (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten worden verstrekt. Alleen bevoegde autoriteiten mogen de informatie opvragen. Het CIOT mag zelf geen bestanden opslaan voor andere doeleinden dan haar wettelijke taken, maar moet wel gegevens over het gebruik van het systeem bewaren ten behoeve van een jaarlijkse audit en rapportages aan de minister van Veiligheid en Justitie.

De (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten mogen alleen informatie bij het CIOT opvragen ten behoeve van strafvordering, inlichtingenverzameling of hulpverlening in noodsituaties. Dit is vastgelegd in het Nederlandse wetboek van Strafvordering, de Nederlandse wet op de Inlichtingen- en Veiligheidsdiensten in Nederland en de Telecommunicatiewet.

Op de gegevens die via het CIOT-informatiesysteem worden opgevraagd, is de Wet bescherming persoonsgegevens van toepassing. Omdat deze wet zo belangrijk is – het gaat immers om privacygevoelige informatie – voert het CIOT regelmatig overleg met het College Bescherming Persoonsgegevens om de werking van het CIS af te stemmen.

Zorgvuldige controles

De werkzaamheden van het CIOT en het gebruik van het CIOT-informatiesysteem worden regelmatig gecontroleerd. Ook dit is vastgelegd in het Besluit verstrekking gegevens telecommunicatie. Er moet jaarlijks een audit plaatsvinden bij het CIOT, aanbieders en aanvragers. Daarbij wordt nagegaan of de werkzaamheden volgens de wet zijn uitgevoerd en of de aanbieders de juiste informatie aanleveren bij het CIOT. De opdracht tot de audits wordt gegeven door het Ministerie van Veiligheid en Justitie en besproken in de Commissie van Advies CIOT, waarin de betrokken ministeries, de aanbieders en aanvragers van informatie en andere belangrijke stakeholders zijn vertegenwoordigd.

Het CIOT rapporteert in een jaarverslag aan de minister van Veiligheid en Justitie over het aantal keren dat de bevoegde autoriteiten via het CIOT informatie hebben ontvangen in het kader van de opsporing van strafbare feiten. In het verslag staat hoe vaak informatie is verstrekt door tussenkomst van het CIOT, wat de rechtsgrondslag was van elk verzoek en welke (Bijzondere) Opsporingsdienst het verzoek heeft gedaan.

Organisatie van het CIOT

Het CIOT is een onderdeel van de Justitiële Informatiedienst en valt onder het ministerie van Veiligheid en Justitie van het Directoraat-generaal Rechtspleging en Rechtshandhaving. In 1999 werd het CIOT opgericht.

Verplichte informatielevering door telefonie- en internetaanbieders

Aanbieders van openbare telecommunicatienetwerken en/of -diensten zijn sinds 1 september 2004 wettelijk verplicht om de bedrijfsvoeringgegevens van hun klanten beschikbaar te stellen aan het CIOT. Voor aanbieders van openbare internetnetwerken en/of -diensten geldt die verplichting sinds 1 september 2006.

Het CIOT zorgt ervoor dat aanbieders worden aangesloten op het CIOT-informatiesysteem.

Daarna moet elke aanbieder elke 24 uur een actueel digitaal bestand leveren. Zij krijgen hiervoor een vergoeding van de overheid.

In het bestand staat de volgende informatie over de personen die gebruik maken van het netwerk/de dienst van de aanbieder:

Telecommunicatieaanbieders	Internetaanbieders
Naam, adres, postcode, woonplaats	Naam, adres, postcode, woonplaats
De telecommunicatiedienst die de gebruiker afneemt (vast, mobiel, abonnement, prepaid, etc.)	De internetdienst die de gebruiker afneemt (inbellen, kabel, ADSL, e-mail, account, etc.)
Telefoonnummer(s) van de gebruiker	Identificatienummers van randapparaten van de gebruiker, IP-nummers, e-mailadres(sen) van de gebruiker, gebruikersnaam of inlognaam
Naam van de telecommunicatie-aanbieder	Naam van de internetaanbieder

Overeenkomsten

Aanbieders moeten voldoen aan een aantal technische, juridische en administratieve voorwaarden zoals de verplichte registratie bij de autoriteit Consument & Markt. Daarmee is onder andere de beveiliging van de gegevens en het waarborgen van de privacy geregeld. Op haar beurt sluit het CIOT met elke aanbieder drie overeenkomsten af. De bewerkerovereenkomst gaat over de verantwoordelijkheid voor het bewerken van de informatie, in het kader van de Wet bescherming persoonsgegevens. Zo regelt het CIOT onder andere dat de gegevens van de aanbieder in een aparte, beveiligde omgeving worden bewaard en dat ze alleen worden gebruikt voor het rechtmatig verstrekken van informatie. De auditovereenkomst bevat afspraken over de jaarlijkse controle op het rechtmatige gebruik van het informatiesysteem en de controle op de juistheid van de aangeleverde gegevens. Verder sluit het CIOT met elke aanbieder een Service Level Agreement af, zodat duidelijk is wat de aanbieder van het CIOT mag verwachten en hoe dit is georganiseerd.

Volledig geautomatiseerd van vraag naar antwoord

Het CIOT zorgt ervoor dat aanbieders van telecom- en internetdiensten en de autoriteiten die de informatie kunnen opvragen, worden aangesloten op het CIOT-informatiesysteem. Daarna start een eenvoudig, transparant proces van vraag naar antwoord, dat volautomatisch per computer – en daarmee efficiënt en kostenbesparend – verloopt.

Voor elk aanbiederbestand is ruimte gereserveerd in één van de black boxen: een beveiligde omgeving waarin de aanbieder eenmaal per 24 uur een bestand opslaat met de wettelijk vastgestelde klantgegevens. Omdat de black box een afgeschermde omgeving is, kunnen de verschillende aanbieders elkaars bestanden niet benaderen.

De aanvragers hebben 24 uur per dag, zeven dagen per week rechtstreeks toegang tot het informatiesysteem via een eigen cliënt. Alleen bevoegde autoriteiten mogen informatieverzoeken doen. De minister van Veiligheid en Justitie heeft zo'n autorisatie verleend aan de ruim 40 (Bijzondere) Opsporings-, Inlichtingen- en Veiligheidsdiensten. Zij krijgen daarvoor een speciale toegangscode en mogen vervolgens alleen gerichte vragen stellen in het kader van onderzoek.

De aanvrager voert zijn informatieverzoek in op de cliënt, die het doorstuurt naar de server bij het CIOT. Op de server wordt het verzoek anoniem gemaakt. Het verzoek gaat naar alle black boxen waar automatisch wordt gekeken of de gezochte informatie aanwezig is. De aanbieder kan niet nagaan van welke aanvrager het verzoek komt en met welk specifiek doel welke vraag gesteld wordt. Het antwoord gaat terug naar de server, die het doorstuurt naar de cliënt van de aanvrager. Om alles veilig te laten gebeuren, wordt gebruik gemaakt van onder andere een gesloten netwerk en versleuteling door middel van een Public Key Infrastructuur (PKI). De doorlooptijd van het proces is maximaal tien seconden. Een hele verbetering ten opzichte van de vroegere bevragingen per fax. Niet alleen in snelheid maar ook uit een oogpunt van veiligheid.

Rechtmatig gebruik

Het technische beheer van de infrastructuur, het onderhoud en de ontwikkeling van het systeem worden uitgevoerd door het CIOT. Zij slaat ook procesinformatie op waarmee het rechtmatige gebruik van het systeem kan worden getoetst. Dit is informatie waaruit blijkt door welke aanbieder, aan welke autoriteit en op welke rechtsgrondslag informatie is verstrekt. Het CIOT is volgens het Besluit verstrekking gegevens telecommunicatie verplicht deze procesinformatie te verzamelen ten behoeve van de jaarlijkse audits en de rapportages aan de minister van Veiligheid en Justitie. Het gaat dus beslist niet om de inhoudelijke informatie. Die gegevens zijn uitsluitend zichtbaar voor de aanvrager zelf. Het CIOT bezit geen centrale database, maar meerdere black boxen, waaruit de gegevens alleen worden verstrekt door middel van het vraag- en antwoordproces. Het CIOT ziet niet van wie informatie beschikbaar is in het CIOT-informatiesysteem. De in het CIOT-informatiesysteem opgeslagen informatie blijft onder de verantwoordelijkheid van de aanbieders van telecommunicatiediensten vallen. Wil een burger weten of van hem of haar informatie is opgeslagen in het CIOT-informatiesysteem, dan kan hij of zij zich wenden tot de aanbieder van wie hij of zij telecommunicatiediensten afneemt.

Samenwerking en afstemming

Het CIOT is een zo onafhankelijk mogelijke organisatie, die nauw samenwerkt met de betrokken ministeries en daarbij behorende organisaties. Naast het ministerie van Veiligheid en Justitie, het Openbaar Ministerie en de rechterlijke macht, zijn dat het ministerie van Economische Zaken (EZ) en het Agentschap Telecom, het ministerie van Binnenlandse Zaken en Koninkrijkszaken (BZK), het ministerie van Defensie, het ministerie van Landbouw, Natuur en Voedselkwaliteit (LNV), het ministerie van VROM, het ministerie van Financiën, het ministerie van Sociale Zaken en Werkgelegenheid (SZW) en het College Bescherming Persoonsgegevens.

De ministeries van Justitie, EZ en BZK zijn, samen met de aanbieders en aanvragers en andere belangrijke stakeholders, vertegenwoordigd in de Commissie van Advies CIOT. De commissie geeft opdracht tot de jaarlijkse audit, evalueert het functioneren van het CIOT en geeft daar advies over.

Verder adviseert de commissie over verbetering van het informatiesysteem en het ontwikkelen van aanvullende functionaliteiten.

De aanbieders en bevoegde autoriteiten die informatie aanvragen, hebben meegewerkt aan de ontwikkeling van het CIOT-informatiesysteem. Zij worden ook geraadpleegd bij het onderhoud van het systeem. Bijvoorbeeld tijdens de landelijke gebruikersdag, die het CIOT jaarlijks organiseert voor de aanvragers, of tijdens de informatiebijeenkomsten die worden georganiseerd met de aanbieders.

Uit de praktijk

Telefonie- en internetinformatie is een belangrijk hulpmiddel bij het oplossen van misdrijven. Het CIOT informatiesysteem wordt daarom veelvuldig bevraagd. Vooral bij vastgelopen onderzoeken kan het aantal opgevraagde gegevens oplopen. Bijvoorbeeld bij
een onderzoek naar een moord, waarin alle aanknopingspunten waren onderzocht zonder nieuwe informatie op te leveren. De bevoegde autoriteit besloot toen om de verkeersgegevens op te vragen van de zendmasten voor mobiele telefonie in de buurt van het plaats delict op de dag van de moord. Dat leverde ruim 30.000 telefoonnummers op, die via het CIOT werden bevraagd bij telecommunicatieaanbieders. Analyse van de aldus verkregen informatie leverde nieuwe inzichten op en leidde uiteindelijk tot de aanhouding van de verdachte van de moord.

Hebt u vragen of wilt u meer informatie, neem dan contact op met:

Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)
Turfmarkt 147
2511 DP Den Haag
Postbus 484
2501 CL Den Haag
Tel: (070) 370 33 10
E-mail: ciot@ciot.justid.nl
www.justid.nl