Samenvatting

Het onderzoek: aanleiding, onderzoeksvragen en gegevensverzameling

Aanleiding en de onderzoeksvragen

De Wet bewaarplicht telecommunicatiegegevens, is op 1 september 2009 in werking getreden. De centrale gedachte achter de bewaarplicht is dat bepaalde gegevens over telefoon- en internetverkeer van belang kunnen zijn voor de opsporing en vervolging van ernstige misdrijven. Men kan met behulp van die gegevens bijvoorbeeld vaststellen op welk moment en op welke locatie met een bepaalde (mobiele) telefoon is gebeld. Ook is het mogelijk te achterhalen of en wanneer een computer of mobiele telefoon contact heeft gehad met het internet. In geval van een misdrijf waarvoor voorlopige hechtenis is toegestaan, bij een redelijk vermoeden dat misdrijven worden beraamd of gepleegd in georganiseerd verband en bij aanwijzingen van een terroristisch misdrijf, kan een vordering tot verstrekking van verkeersgegevens worden gedaan.
Het feit dat deze gegevens standaard voor een bepaalde periode moeten worden opgeslagen is echter een terugkerend punt van discussie. Zowel in Nederland als op Europees niveau (EU 18620/11) bestaat behoefte aan meer inzicht in het gebruik door politie en justitie van de gegevens die op grond van de Nederlandse Wet bewaarplicht worden opgeslagen.

Het doel van dit onderzoek is inzicht te bieden in de wijze waarop de Wet bewaarplicht uitwerkt in de praktijk. Strikt genomen vormt dit onderzoek geen evaluatie van de Wet bewaarplicht. Het onderzoek reikt verder dan een procesevaluatie (vgl. Wartna, 2005; Nelen et al., 2010), omdat er niet alleen behoefte bestaat aan inzicht in de wijze waarop de Wet bewaarplicht in de praktijk heeft vorm gekregen, maar vooral ook aan inzicht in de wijze waarop de gegevens die op grond van deze wet beschikbaar dienen te worden gehouden voor de opsporing in de praktijk worden gebruikt.
Het is echter niet mogelijk om – zoals het geval is bij een product- of effectevaluatie – vast te stellen wat de effecten zijn van de invoering van de Wet bewaarplicht het gebruik van verkeersgegevens in de opsporingspraktijk. De telecommuncatiegegevens waar het hier om draait waren ook vóórdat de Wet bewaarplicht werd ingevoerd beschikbaar voor de opsporing en werden ook vóór de invoering van de wet bewaarplicht gebruikt in strafrechtelijke onderzoeken naar ernstige misdrijven.
De Wet bewaarplicht heeft weliswaar geleid tot harmonisatie van de bewaartermijnen, maar doordat er in de tussentijd ook andere veranderingen zijn opgetreden zijn de effecten daarvan nauwelijks te meten én te onderscheiden. Veranderingen in de wijze waarop telecommuncatiegegevens in de praktijk worden gebruikt zijn vooral toe te schrijven aan de opkomst van de mobiele telefoon en de smartphone en aan de mogelijkheden om via het internet met elkaar te communiceren. Het is daarom wel mogelijk om te

onderzoeken op welke wijze telecommunicatiegegevens gebruikt worden in de opsporingspraktijk, maar het is niet goed mogelijk deze bevindingen te relateren aan de invoering van de nieuwe wet.
Dit onderzoek richt zich zowel op vragen over de wijze waarop de wet is vormgegeven als op vragen over het gebruik van de opgeslagen gegevens in de praktijk.

Bij het bewaren, beschikbaar houden en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing en vervolging zijn verschillende organisaties en partijen betrokken. De aanbieders dienen de te bewaren gegevens op te slaan, te beveiligen, beschikbaar te stellen voor de opsporing, en tijdig weer te vernietigen. Het Agentschap Telecom ziet toe op dit proces. Het College Bescherming Persoonsgegevens heeft de algemenere taak toe te zien op het gebruik van privacygevoelige gegevens. Politie en Openbaar Ministerie maken gebruik van deze gegevens bij het opsporen en vervolgen van ernstige misdrijven, en de Zittende Magistratuur gebruikt de gegevens in de rechtelijke besluitvorming. In dit rapport wordt relatief veel aandacht besteed aan de wijze waarop de bewaarde gegevens gebruikt worden in de praktijk om daarmee inzicht te bieden in de nut en noodzaak van de bewaarplicht. De wijze waarop de Wet bewaarplicht uitwerkt in de praktijk vormt een ingewikkeld bouwwerk, dat in dit rapport weergegeven wordt door de wijze waarop deze verschillende partijen hun taken uitvoeren te beschrijven. In dit rapport wordt relatief veel aandacht besteed aan de wijze waarop de bewaarde gegevens gebruikt worden in de praktijk. Andere partijen worden belicht, maar vormen niet het zwaartepunt van dit onderzoek.

Gegevensverzameling

Om antwoord te kunnen geven op de onderzoeksvragen zijn verschillende methoden gebruikt. Naast de bestudering van nationale en internationale vakliteratuur, is kwantitatieve en kwalitatieve informatie verzameld over het gebruik van historische verkeersgegevens. Hierover zijn gegevens verzameld bij onder andere de Unit Landelijke Interceptie (ULI) van de landelijke politie eenheid, de politie, de rechterlijke macht (Openbaar Ministerie) en de advocatuur. Tevens is literatuuronderzoek verricht waarbij wetteksten en toelichtingen daarop, lagere regelgeving, Kamerstukken, schriftelijke stukken van uitvoeringsinstanties en wetenschappelijke literatuur zijn bestudeerd.
Voor het onderzoek zijn 17 face-to-face interviews en 16 telefonische interviews afgenomen, waarbij is gesproken met in totaal 41 personen in de periode lopend van juni tot oktober 2012. Daarnaast zijn vonnissen geanalyseerd om te bezien op welke wijze gegevens die op grond van de Wet bewaarplicht beschikbaar worden gehouden voor de opsporing door Nederlandse rechters gebruikt worden in de bewijsvoering van strafzaken.

Communicatie op afstand, ontwikkelingen en gevolg

De mobiele telefoon werd in de afgelopen jaren vervangen door de smartphone, en veel mensen zijn tegenwoordig 24 uur per dag, zeven dagen per week, online. Door het gebruik van smartphones wordt er steeds vaker gecommuniceerd in de vorm van korte berichtjes via apps en e-mail en bellen mensen ook steeds vaker via internet.
Technologische vernieuwingen, de daarmee gepaard gaande versnippering van communicatie en vooral het gebruik van verschillende diensten die op internet worden aangeboden, maken dat het moeilijk is om alle communicatie op afstand van een persoon in kaart te brengen. Bovendien vallen niet alle verkeersgegevens die daarbij worden gegenereerd onder de Nederlandse Wet bewaarplicht. Veel internetgebruikers hebben een e-mailaccount bij webmaildiensten zoals Hotmail, Gmail of Yahoo, waarvan de aanbieder een buitenlands bedrijf is. Dit betekent dat de gegevens niet per definitie beschikbaar worden gehouden voor de Nederlandse opsporing. Ditzelfde geldt vaak voor aanbieders van diensten in de *cloud*. Indien opsporingsdiensten toch willen beschikken over verkeersgegevens van buitenlandse aanbieders zal men een rechtshulpverzoek moeten indienen en moeten afwachten of de gevraagde gegevens nog beschikbaar zijn.

De wetsgeschiedenis en Europese regelgeving inzake de bewaarplicht van verkeersgegevens

Mede aangejaagd door de terroristische aanslagen in Madrid in 2004 en in Londen in 2005, is op 3 mei 2006 de EU-richtlijn in werking getreden die tot doel heeft te waarborgen dat bepaalde telecom- en internetgegevens bewaard blijven zodat deze beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.

Te bewaren data

In artikel 5 van de richtlijn worden de te bewaren categorieën gegevens genoemd die betrekking hebben op bijvoorbeeld de bestemming, de datum, het tijdstip en duur van de communicatie. Er mogen geen gegevens worden bewaard waaruit de inhoud van de communicatie kan worden opgemaakt. De lidstaten dienden de richtlijn vóór 15 september 2007 in wetgeving te hebben omgezet; voor de bewaringsverplichting van internetgegevens was er respijt tot 15 maart 2009. Niet alle lidstaten hebben de richtlijnen inmiddels omgezet in wetgeving. De term ‘ernstige criminaliteit’ is in de richtlijnen niet gedefinieerd. Dit is terug te zien in de verschillende gronden die in de wetgeving van de lidstaten zijn opgenomen die toegang tot de bewaarde gegevens voor strafvorderlijke doeleinden mogelijk maken. Evenals voor de duur

van de bewaartermijn, geldt hier dat de harmonisatie die met de EU-regelgeving is nagestreefd, slechts beperkt is verwezenlijkt.

Privacy

De Wet bewaarplicht raakt aan de privacy van de burgers. Allereerst neemt door het louter opslaan van telecommunicatiegegevens het risico toe dat onbevoegden – zoals hackers – toegang krijgen tot die gegevens. Een tweede en andersoortige inbreuk vindt plaats op het moment dat politie en justitie de beschikking krijgen over bewaarde gegevens in het kader van een onderzoek. Een beperking op het recht op privacy is volgens het Europees Verdrag tot bescherming van de rechten van de mens (EVRM) pas dan toegestaan als deze bij wet is voorzien en noodzakelijk is in een democratische samenleving.
In het Wetboek van Strafvordering (Sv.) is geregeld wie onder welke voorwaarden toegang heeft tot de opgeslagen telecom- en internetgegevens. De officier van justitie kan een vordering doen tot verstrekking van verkeersgegevens (art. 126n en 126u Sv.) ingeval van verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is of bij een redelijk vermoeden dat in georganiseerd verband misdrijven worden beraamd of gepleegd. Een opsporingsambtenaar kan identificerende gegevens vorderen (art. 126na, 126ua Sv.). De gegevens die opgevraagd kunnen worden zijn de zogenaamde gebruikersgegevens (naam, adres, woonplaats, nummer en soort dienst). Ingeval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie verkeersgegevens opvragen (art. 126zh Sv.) en kan een opsporingsambtenaar gebruikersgegevens vorderen (art. 126zi Sv.). Verder kan de officier van justitie bij een verkennend onderzoek naar terroristische misdrijven gegevensbestanden van publieke en particuliere instanties vorderen om de hierin opgenomen gegevens te doen bewerken (art. 126hh Sv.).

Het bewaren en beveiligen van de gegevens in de praktijk

De toezichthouders

Het toezicht op de naleving van de regels ligt in handen van het Agentschap Telecom (AT), dat opereert als een onafhankelijke toezichthouder en toeziet op de naleving van de Wet. Het AT is onderdeel van het ministerie van Economische Zaken, en legt rechtstreeks verantwoording af aan de Minister van Economische Zaken. Daarnaast ziet het College Bescherming Persoonsgegeven (CBP) toe op alle wettelijke regelingen waarin sprake is van het bewaren, gebruiken of verwerken van persoonsgegevens.

De aanbieders

Om te begrijpen hoe de aanbieders omgaan met de verplichtingen die de Wet bewaarplicht met zich meebrengt, is gesproken met vier aanbieders. Voor de invoering van de bewaarplicht liepen de bewaartermijnen tussen bedrijven uiteen. De implementatie van de wet bewaarplicht vormde ondanks de lange aanlooptijd van de wet bij de grote aanbieders een omvangrijk project.
Bij de twee grote aanbieders die zijn geïnterviewd voor dit onderzoek, wordt een database gevuld met gegevens die op grond van de Wet bewaarplicht dienen te worden bewaard. Deze gegevens worden automatisch vernietigd na het verstrijken van de bewaartermijn. Een kleine aanbieder die werd geïnterviewd voor dit onderzoek, is pas recentelijk actief met de bewaartermijnen aan de slag gegaan, omdat de hoeveelheid te beheren gegevens te groot werd. Wanneer een verzoek bij hun binnenkomt worden de gevraagde gegevens door een medewerker handmatig uit het systeem gehaald.
De overheid heeft een overeenkomst afgesloten met de grote Nederlandse aanbieders betreffende de vergoeding van de personele inzet die nodig is om op grond van verschillende wetten en regels opgeslagen gegevens aan de overheid te verstrekken. Kleine aanbieders vallen niet onder deze regeling.
De eigenaren van een vierde geïnterviewde aanbieder herkennen zichzelf wel in de documentatie van het AT als bewaarplichtige van de verkeersgegevens van de e-maildiensten die zij aanbieden, maar geven hieraan vanuit idealistisch standpunt geen gehoor. De onderzoekers hebben de vraag of de diensten die door dit bedrijf worden aangeboden onder de bewaarplicht vallen voorgelegd aan het AT. Volgens het AT is dit niet het geval, maar het AT ziet tegelijkertijd ook dat de wetgeving – als gevolge van technologische vernieuwingen – op bepaalde gebieden onduidelijk is geworden.

Toezichthouder

Op de juiste uitvoering van bedrijfsprocessen wordt toegezien door het AT. Het toezicht is geregeld in een toezichtscyclus, waarbij van de aanbieders gegevens worden opgevraagd over de wijze waarop de te bewaren gegevens worden opgeslagen, beveiligd en vernietigd. Het AT beschikt echter niet over de instrumenten en bevoegdheden om op de inhoud van de bewaarde en geleverde gegevens toe te kunnen zien. In artikel 18.7, tweede lid, van de Telecommunicatiewet (Tw) is uitdrukkelijk bepaald dat de toezichthouder niet bevoegd is verkeers- of locatiegegevens op te vragen die door de aanbieders op grond van artikel 13.2a Tw moet worden bewaard.

Het gebruik van historische verkeersgegevens in de praktijk

In de wet wordt een strikt onderscheid gemaakt tussen telefonie- en internetverkeersgegevens. Voor de duidelijkheid is in dit rapport deze tweedeling gehandhaafd. Echter, in de praktijk is dit onderscheid nagenoeg verdwenen en hanteert de Wet bewaarplicht, volgens experts, een onjuiste tweedeling.

Wat wordt bewaard?

In de bijlage behorende bij artikel 13.2a Tw staat een opsomming van de te bewaren gegevens betreffende telefonie. Het betreft gegevens over onder meer het nummer van oproeper en opgeroepene, tijd, duur van gesprek en locatie. Deze gegevens dienen bewaard te worden voor een periode van 1 jaar. De inhoud van een gesprek of een sms bericht valt niet onder de bewaarplicht. De verkeersgegevens van het verzonden of ontvangen bericht wel. Oproeppogingen waarbij geen contact tot stand is gekomen, vallen wel onder de bewaarplicht.

De inzet

Volgens professionals uit de opsporingspraktijk worden historische verkeersgegevens opgevraagd bij vrijwel alle grotere opsporingsonderzoeken waarbij verdachten of slachtoffers mogelijk gebruik hebben gemaakt van hun telefoon. In het jaar 2012 betrof het aantal vorderingen tot verstrekking van telecommunicatiegegevens 56.825.
Met deze vorderingen wordt informatie opgevraagd over het gebruik van telefoon en eventueel van IP-verkeer, zoals: met welk nummer is er gebeld, wanneer is er gebeld, hoe lang is er gebeld en vanaf welke locatie, en is er contact geweest met het internet? Deze gegevens spelen een belangrijke en zeer gewaardeerde rol in de opsporingspraktijk. Wanneer een opsporingsteam historische verkeersgegevens wil opvragen, dient het team toestemming te hebben van de officier van justitie. Het opsporingsteam moet aangeven welk doel ze met de gevraagde gegevens denken te bereiken en het opvragen van de gegevens dient proportioneel en subsidiair te zijn. De doelstellingen van opsporingsteams voor het opvragen van verkeersgegevens zijn onder te brengen in een aantal algemene categorieën, namelijk: (1) het identificeren van een gebruiker, (2) het achterhalen van contacten, (3) plaatsbepaling, (4) het traceren van een IMEI-nummer, en (5) het maken van een capaciteitsafweging alvorens te gaan tappen.

Relevantie en bewaartermijn telefoniegegevens

Alle geïnterviewde professionals en experts geven aan historische gegevens over telefoonverkeer zeer relevant te vinden. Een aantal geïnterviewde pro-

fessionals uit de opsporingspraktijk geeft aan niet alleen de begin locatie (*first cell*) van een telefoongesprek te willen ontvangen maar ook de eindlocatie (*last cell*). Echter, waar het gesprek eindigt, dus de laatste connectie met een zendmast, staat niet vermeld in de bijlage behorende bij artikel 13.2a Tw.
Tijdens de gesprekken bleek dat het merendeel van de professionals en experts bij de politie van mening is dat de bewaartermijn van een jaar voldoende is voor het werk dat zij doen.

Historische verkeersgegevens Internet

Wat wordt er bewaard?

Historische verkeersgegevens betreffende internet- en e-mail gebruik, kunnen inzicht bieden in onder meer de IP-adressen die door iemand zijn gebruikt, en in de e-mail contacten van zender en ontvanger. De inhoud van gesprekken, berichten of e-mails, zoektermen die zijn intypt in een zoekmachine en IP-adressen van bezochte internetpagina's vallen niet onder de bewaarplicht.

Relatief weinig ingezet

Tijdens de gesprekken die zijn gevoerd voor dit onderzoek werd duidelijk dat de voor dit onderzoek gesproken professionals uit de opsporingspraktijk weinig tot geen kennis hebben over de wijze waarop historische gegevens betreffende het internetverkeer gebruikt zouden kunnen worden in de opsporing. Daarnaast worden werkzaamheden die te maken hebben met aan internet gerelateerde zaken vaak uitgevoerd door experts omdat de digitalisering van de huidige samenleving nog niet behoort niet tot het dagelijkse werkterrein van veel opsporingsambtenaren. Tegelijkertijd constateren we dat de technologische ontwikkelingen heel snel gaan. Zo snel dat het voor de schaarse experts zelf maar met moeite bij te houden is.
Historische gegevens over internetverkeer worden veelal opgevraagd naar aanleiding van een misdrijf of delict dat met behulp van of via het internet is gepleegd zoals bijvoorbeeld het versturen van dreigmails, internetoplichting, mensenhandel of het verspreiden van kinderporno. Het *identificeren van een gebruiker* of van een aansluiting wordt als belangrijkste reden genoemd voor het opvragen van gegevens. Vaste IP-adressen zijn doorgaans langere tijd dezelfde en de gebruiker is eenvoudig te traceren bij de aanbieder of bij het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Echter, het identificeren van een gebruiker van mobiel internet door middel van historische verkeersgegevens verloopt moeizaam en is regelmatig niet mogelijk.

De relevantie en bewaartermijn internetgegevens

Volgens verschillende experts is het merendeel van de gegevens betreffende internet zoals beschreven in de bijlage behorende bij artikel 13.2a Tw is verouderd. De regeling past niet meer bij het huidige internet gebruik en bij de technische ontwikkelingen die zich in dit opzicht hebben voorgedaan sinds de invoering van de wet in 2009. Daarmee is een situatie ontstaan waarin gegevens van burgers worden bewaard die niet of nauwelijks worden gebruikt door opsporingsdiensten. Een zorgvuldige heroverweging van de regeling betreffende IP-verkeer en de te bewaren IP-gegevens lijkt dan ook op zijn plaats.
De voor dit onderzoek geïnterviewde professionals en experts die bekend zijn met internetverkeersgegevens zijn allen van mening dat de bewaartermijn van 6 maanden te kort is; er bestaat een duidelijke behoefte aan IP-verkeersgegevens die verder terug gaan in de tijd in opsporingsonderzoeken naar delicten waarvoor deze gegevens worden opgevraagd.

Het opvragen van zendmastgegevens

Het opvragen van verkeersgegevens op basis van een locatie levert gegevens op van alle mobiele telefoons die in het opgevraagde tijdsbestek zijn gebeld, zelf hebben getelefoneerd of connectie hebben gehad met het internet via de bevraagde mastlocatie. Om zendmastgegevens op te kunnen vragen moet er sprake zijn van een verdenking van een misdrijf zoals omschreven in artikel 67, lid 1 Sv. en het moet het gebruik van de gegevens in het belang zijn van het onderzoek.
Zendmastgegevens worden vooral opgevraagd bij seriematige delicten. In dat geval worden de gegevens van verschillende locaties met elkaar vergeleken, in de hoop een terugkerend nummer te kunnen identificeren. Uiteraard kan deze opsporingsmethode alleen slagen als de verdachte zijn telefoon rond het tijdstip van het misdrijf heeft gebruikt.

Alternatief?

Tegenstanders van de bewaarplicht zien het gericht bevriezen van gegevens als een minder privacy schendende oplossing omdat er in dat geval sprake is van een gerichte dataset die langer bewaard wordt in plaats van het bewaren van alle gegevens van alle klanten van een aanbieder. Geen van de sleutelpersonen die wij spraken vindt het bevriezen van gegevens een vergelijkbaar of gelijkwaardig alternatief voor een algemene bewaarplicht, omdat hiermee geen gegevens kunnen worden opgevraagd die langer geleden zijn vastgelegd. Om gebruik te kunnen maken van deze gegevens moet al van tevoren – op het moment dat de gegevens nog aanwezig zijn en bevroren kunnen worden – bekend zijn welke gegevens later nodig zijn. Aangezien misdrijven

soms pas laat ter kennis van de politie komen, en verdachten soms pas lang nadat een misdrijf heeft plaatsgevonden worden opgespoord, is het noodzakelijk gegevens te bewaren om deze later te kunnen gebruiken in het opsporingsproces.

Gebruik van verkeersgegevens in cijfers

In de Telecommunicatiewet is een regel opgenomen over de verplichting tot publicatie van het jaarlijkse aantal bevragingen door opsporingsdiensten van gegevens over telecommunicatieverkeer (art. 13.4 lid 4 Tw). In het jaar 2012 is er in totaal 56.825 keer een vordering gedaan tot verstrekking van verkeersgegevens. Echter, het door de minister bekend gemaakte aantal vorderingen bevat ook gegevens die niet onder de Wet bewaarplicht telecommunicatiegegevens vallen.
Tevens dient te worden opgemerkt dat het opvragen van telecomgegevens in Nederland wordt geregistreerd per telefoonnummer, IMEI-nummer, IP-adres, of 'paallocatie' waarover gegevens worden opgevraagd. Deze cijfers geven geen inzicht in het aantal personen van wie er jaarlijks telecommunicatiegegevens worden opgevraagd, of van het aantal opsporingsonderzoeken of de aard van de opsporingsonderzoeken waarvoor deze gegevens worden opgevraagd. Ook geven de cijfers geen inzicht in de mate waarin een vordering daadwerkelijk tot een verstrekking van de gegevens heeft geleid.

Rechterlijke vonnissen

In dit rapport bieden we ook inzicht in het gebruik en de waarde van verkeersgegevens in rechterlijke vonnissen. In totaal werden er tussen juli 2012 en februari 2013 74 uitspraken gevonden waarin de term historische verkeersgegevens betreffende telefonie voorkwam. In de vonnissen werden deze gegevens vooral gebruikt om 'contacten tussen verdachten' en 'plaatsbepalingen' aan te tonen.
Bij het zoeken naar zaken waarin gegevens over IP-verkeer waren gebruikt in het vonnis kwam een 26-tal uitspraken naar boven uit de periode januari 2009 - februari 2013. Deze IP-gegevens werden vooral genoemd in vonnissen van opsporingsonderzoeken naar kinderporno. Meer dan de helft van de vonnissen gaat over het downloaden/verspreiden van kinderporno. Bij het opvragen van deze gegevens gaat het niet zozeer om waar de verdachte was en met wie er wordt gecommuniceerd, maar om de vraag of de verdachte te koppelen is aan het gebruikte internetadres of aan andere gebruikersgegevens.