Investigating cybercrime

Oerlemans, J.J.

Samenvatting (Summary in Dutch)

Cybercrime onderzoeken

Opsporingsonderzoeken naar cybercrime vereisen het gebruik van nieuwe opsporingsmethoden om bewijs te verzamelen. De juridische basis voor deze opsporingsmethoden in het Nederlands strafprocesrecht is echter niet altijd helder en van voldoende kwaliteit. Deze studie heeft tot doel de vraag te beantwoorden op welke wijze de Nederlandse wetgever digitale opsporingsmethoden adequaat kan reguleren. Daartoe worden drie stappen genomen: (1) het identificeren van de opsporingsmethoden die veelal worden gebruikt in cybercrime-onderzoeken, (2) het nagaan in hoeverre deze opsporingsmethoden adequaat zijn gereguleerd in het Nederlands procesrecht, en (3) het analyseren in hoeverre deze digitale opsporingsmethoden grensoverschrijdend en unilateraal, c.q. zonder toestemming van de betrokken staat of zonder verdragsbasis, kunnen worden toegepast.

Hoofdstuk 1 introduceert het onderwerp van deze studie en zet de probleemstelling, beperkingen aan de reikwijdte van de studie, en onderzoeksmethodologie uiteen. De probleemstelling (PS) luidt als volgt.

PS: *In hoeverre regelt het Nederlands strafprocesrecht op adequate wijze opsporingsmethoden die worden gebruikt in (grensoverschrijdende unilaterale) cybercrime-onderzoeken?*

Onder het 'adequaat regelen van opsporingsmethoden' wordt in deze studie wetgeving verstaan die (1) opsporingsautoriteiten de instrumenten geeft om bewijs te verzamelen in cybercrime-onderzoeken en (2) een minimumniveau van bescherming biedt tegen de willekeurige inmenging van de overheid in het privéleven van burgers. De minimale vereisten voor regelgeving van digitale opsporingsmethoden zijn in deze studie afgeleid van het recht op privacy, zoals bedoeld in art. 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM).

De probleemstelling heeft geleid tot de volgende vijf onderzoeksvragen (OVs).

OV 1: *Welke opsporingsmethoden worden veelal gebruikt in cybercrime-onderzoeken?*

OV 2: *Welke vereisten voor regelgeving voor opsporingsmethoden kunnen uit art. 8 EVRM worden afgeleid?*

OV 3: *Welke kwaliteit van de wetgeving wordt vereist voor de geïdentificeerde digitale opsporingsmethoden?*

OV 4: *Op welke wijze kan het juridisch kader in het Nederlands strafprocesrecht worden verbeterd om de geïdentificeerde opsporingsmethoden afdoende te reguleren?*

OV 5: *In hoeverre is het wenselijk en legitiem om de geïdentificeerde digitale opsporingsmethoden unilateraal en over landsgrenzen heen toe te passen?*

Hoofdstuk 2 beantwoordt de eerste onderzoeksvraag (OV 1). De opsporingsmethoden zijn geïdentificeerd door na te gaan welke bewijsgaringsactiviteiten plaatsvinden in cybercrime-onderzoeken. Deze opsporingsactiviteiten vinden voornamelijk plaats op basis van de digitale sporen van (1) IP-adressen en (2) de online identiteit van mensen. De digitale opsporingsmethoden die worden gebruikt kunnen tevens grensoverschrijdend en op unilaterale wijze worden ingezet. De bewijsvergaringsactiviteiten zullen in de meeste gevallen echter niet soepel verlopen door de uitdagingen van (1) anonimiteit, (2) versleuteling, en (3) de territoriale beperking van handhavingsjurisdictie in cybercrime-onderzoeken. De territoriale beperking van handhavingsjurisdictie schrijft voor dat bewijsgaringsactiviteiten slechts tot de grens mogen worden toegepast, voor zover geen toestemming door de betrokken staat is gegeven en geen verdragsbasis voorhanden is. De studie zet uiteen welke opsporingsmethoden kunnen worden gebruikt om met deze uitdagingen om te gaan. Uit de analyse volgt dat de volgende opsporingmethoden vaak worden gebruikt in cybercrime-onderzoeken:

(1) het vergaren van publiekelijk toegankelijke online informatie;
(2) het vorderen van gegevens van online service providers;
(3) het toepassen van online undercover methoden; en
(4) het uitvoeren van hacken als opsporingsmethode.

Hoofdstuk 3 beantwoordt de tweede onderzoeksvraag (OV 2). In het hoofdstuk wordt de relatie onderzocht tussen het recht op privacy en de regulering van opsporingsmethoden. De belangrijkste voorwaarde uit art. 8 EVRM voor de regulering van opsporingsmethoden is dat de privacyinmenging 'bij de wet is voorzien'. Deze voorwaarde valt uiteen in de volgende drie eisen: (1) beschikbaarheid, (2) voorzienbaarheid, en (3) een zekere kwaliteit van wetgeving. De drie eisen worden 'normatieve vereisten' voor het reguleren van opsporingsmethoden genoemd. De eerste normatieve eis, die van beschikbaarheid, betekent dat er een indicatie moet zijn welke regelgeving van toepassing is voor het gebruik van een opsporingsmethode in een bepaald geval. De tweede normatieve eis, die van voorzienbaarheid, betekent dat het juridisch raamwerk voldoende helder (1) de reikwijdte van de bevoegdheid voor opsporingsautoriteiten aangeeft en (2) de manier waarop de opsporingsmethode wordt uitgevoerd beschrijft. De derde normatieve eis, de kwaliteit van wetgeving, betekent dat regelgeving voor opsporings-

methoden van voldoende kwaliteit moet zijn. Het Europees Hof voor de Rechten van de Mens (EHRM) kan het niveau van wetgeving en de minimale procedurele waarborgen voorschrijven. Deze kwaliteit van wetgeving moet worden geïmplementeerd in regelgeving voor opsporingsmethoden die een inmenging vormen aangaande het recht op privacy. Hoe zwaarder de privacyinbreuk, des te specifieker de wetgeving en meer waarborgen voor de bevoegdheden zijn vereist. Dit mechanisme, dat in de studie de 'schaal van zwaarte voor privacyinmengingen' wordt genoemd, is belangrijk geweest voor het vaststellen van de vereisten voor regelgeving van de geïdentificeerde opsporingsmethoden. De schaal van zwaarte voor privacyinmengingen visualiseert tevens de privacyinmenging en plaatst deze binnen het Nederlands juridisch kader. Het draagt daarmee bij aan het herkennen van de plekken waar het Nederlands juridisch kader niet voldoet aan de gewenste kwaliteit van wetgeving.

Hoofdstuk 4 beantwoordt de derde onderzoeksvraag (OV 3) door na te gaan welke kwaliteit van wetgeving gewenst is voor de regulering van de digitale opsporingsmethoden. Voorts is onderzocht hoe opsporingsmethoden een inmenging vormen aangaande het recht op privacy en welk niveau van wetgeving en waarborgen gewenst zijn om de betrokken individuen afdoende te beschermen. De analyse laat zien dat de toepassing van opsporingsmethoden in een digitale context vaak een zwaardere inmenging met het recht op privacy met zich meebrengen. Dit is zo vanwege de verwerking en opslag van grote hoeveelheden persoonsgegevens.

De vierde onderzoeksvraag (RQ 4) is beantwoord in hoofdstuk 5, 6, 7 en 8. De drie normatieve vereisten van (1) beschikbaarheid, (2) voorzienbaarheid, en (3) de geformuleerde gewenste kwaliteit van wetgeving zijn gebruikt om na te gaan in hoeverre het Nederlands juridisch kader digitale opsporingsmethoden adequaat reguleert. De analyse laat zien dat een juridische basis beschikbaar is, hetgeen kan worden verklaard door het Nederlandse strafvorderlijke legaliteitsbeginsel. Dit legaliteitsbeginsel vereist een juridische basis voor alle opsporingsmethoden die een inmenging vormen op de rechten en vrijheden van de betrokken individuen. De voorzienbaarheid en de kwaliteit van wetgeving voor digitale opsporingsmethoden is echter op veel plekken onvoldoende.

Een helder beeld over de reikwijdte van opsporingsmethoden en de manier waarop opsporingsmethoden worden toegepast, is belangrijk voor de betrokken individuen. Een willekeurige inmenging van opsporingsautoriteiten in het privéleven van personen wordt op deze manier voorkomen, hetgeen een kernelement is van de rechtsstaat. Op dit moment is er onvoldoende duidelijkheid over de reikwijdte van de geselecteerde opsporingsmethoden in de wet zelf, zijn de aangehaalde voorbeelden in de memorie van toelichting vaak achterhaald en er is een gebrek aan jurisprudentie. Dit laat zien hoe omvangrijk de taak is die voor de Nederlandse wetgever en het Openbaar Ministerie is weggelegd. Zij zullen meer helderheid moeten

verschaffen over de juridische basis die van toepassing is op de digitale opsporingsmethoden, de reikwijdte, en de manier waarop de opsporingsmethoden worden toegepast.

Het Nederlands juridisch raamwerk voor opsporingsmethoden zou bovendien aan de wenselijke kwaliteit van wetgeving moeten voldoen. De regels voor opsporingsmethoden zijn oorspronkelijk geschreven voor een offline context. De toepassing van deze opsporingsbevoegdheden in een online context brengt echter een andere privacyinmenging met zich mee. Hier moet het Nederlands juridisch kader op worden aangepast. Vanwege de zwaardere privacyinmenging zijn meer waarborgen vereist in regelgeving binnen het Wetboek van Strafvordering voor het vorderen van gegevens bij online service providers, online undercover opsporingsmethoden en hacken als opsporingsmethode. In de studie wordt verder betoogd dat het vergaren van publiekelijk toegankelijke online informatie beter buiten het Wetboek van Strafvordering kan worden geregeld.

Hoofdstuk 9 beantwoordt de vijfde onderzoeksvraag (OV 5). Rechtshulpverdragen faciliteren bewijsgaringsactiviteiten op buitenlands grondgebied, maar zijn geschreven voor een wereld dat op basis van landsgrenzen is verdeeld. Het probleem is dat internet geen rekening houdt met landsgrenzen en grensoverschrijdende unilaterale bewijsgaring praktisch mogelijk maakt. Ondanks het verbod op deze manier van bewijsgaren, wordt in het hoofdstuk nagegaan in hoeverre het wenselijk is dat de activiteiten toch plaatsvinden. Daartoe worden de negatieve effecten verder onderzocht. De analyse laat zien dat deze opsporingsactiviteiten kunnen leiden tot een inbreuk op de territoriale soevereiniteit van de betrokken Staten en de rechtszekerheid van de betrokken individuen in gevaar kan brengen. De mate waarin deze negatieve effecten zich voordoen verschillen echter per opsporingsmethode. In bepaalde gevallen zou een unilaterale grensoverschrijdende toepassing van digitale opsporingsmethoden tot op zekere hoogte mogelijk moeten zijn. Staten moeten daarnaast erkennen dat digitale bewijsgaringsactiviteiten reeds plaatsvinden en meer bereid moeten zijn deze opsporingsactiviteiten in internationaal verband te reguleren. Voor de Nederlandse wetgever wordt aangegeven waar de beperkingen van unilaterale grensoverschrijdende digitale opsporing mogelijk liggen en op welke plekken verdere regelgeving noodzakelijk is.

In hoofdstuk 10 zijn de uitkomsten van de voorafgaande analyse van het nationaal en internationaal juridisch kader voor het reguleren van digitale opsporingsmethoden geëvalueerd. De evaluatie laat zien dat het "updaten" van het Nederlands juridisch kader voor de regulering van digitale opsporingsmethoden noodzakelijk, maar op zichzelf niet voldoende is. Het bewijs en de verdachten bevinden zich vaak op buitenlands territorium. Om die reden moet ook rekening worden gehouden met het internationaal juridisch kader voor het gebruik van nationale digitale opsporingsmethoden. Tot op heden wordt de noodzaak door Staten onvoldoende onderkend om inter-

nationale verdragen aan te passen en op deze wijze grensoverschrijdende bewijsgaring in opsporingsonderzoeken naar cybercrime te faciliteren.

Hoofdstuk 11 geeft een antwoord op de probleemstelling (PS). Het juridisch raamwerk dat de digitale opsporing regelt, is in veel opzichten verouderd. Het is de hoogste tijd het Nederlands strafprocesrecht te vernieuwen en op die manier digitale opsporingsmethoden adequaat te reguleren. In hoofdstuk 5 tot en met 8 zijn verbeteringen voorgesteld op basis van de normatieve vereisten voor de regulering van opsporingsmethoden op grond van art. 8 EVRM. De grensoverschrijdende aard van cybercrime en de digitale bewijsgaringsactiviteiten in cybercrime-onderzoeken vereisen tevens aanpassing van het internationaal juridisch kader. In hoofdstuk 9 zijn concrete suggesties gedaan welke beperkingen in unilaterale grensoverschrijdende bewijsgaring de Nederlandse wetgever zou kunnen aanbrengen. De studie wordt afgesloten met een overzicht van de voorstellen voor de regulering van digitale opsporingsmethoden op nationaal en internationaal niveau.