De gespannen relatie tussen privacy en cybercrime

Schermer, B.W.

Prof.mr.dr. B.W. Schermer

De gespannen relatie tussen privacy en cybercrime

Universiteit Leiden

De gespannen relatie tussen privacy en cybercrime

Oratie uitgesproken door

Prof.mr.dr. Bart W. Schermer

bij de aanvaarding van het ambt van Hoogleraar

Privacy en Cybercrime

aan de Universiteit Leiden

op maandag 7 november 2022.

Universiteit
Leiden

1 Inleiding

Mevrouw de rector magnificus, geacht faculteitsbestuur, zeer gewaardeerde toehoorders,

In april 2020 werden 20 miljoen berichten en afbeeldingen buitgemaakt bij telecommunicatieaanbieder EncroChat.[1] Het betrof de privécommunicatie van zo'n 60.000 gebruikers.

In april van dit jaar werden één miljoen bestanden van de gemeente Buren op het *dark web* geplaatst.[2] Het ging om 130 gigabyte aan bestanden, een fractie van de 5 terabyte aan data die in totaal waren buitgemaakt.[3] De bestanden bevatten gevoelige informatie van inwoners, zoals burgerservicenummers en kopieën van identiteitsbewijzen.

Wat hebben deze twee zaken met elkaar gemeen? Zowel de gemeente Buren als telecommunicatieaanbieder EncroChat werden het slachtoffer van een hack. Wat deze twee zaken ook gemeen hebben is dat de privacy van de betrokkenen (de inwoners van de gemeente Buren en de gebruikers van EncroChat) door de hack ernstig werd geschaad.

Waarin deze twee zaken van elkaar verschillen is degene die de hack pleegde: bij de gemeente Buren waren het cybercriminelen en spreken we in juridische termen van computervredebreuk. In het geval van EncroChat was het de politie en spreken we van digitaal binnentreden (artikel 126nba Sv). Een legitieme opsporingsmethode die door de politie mag worden gebruikt.

Hoewel de handeling gelijk is, is de juridische duiding volledig anders.

Wat deze twee zaken illustreren is dat zowel cybercriminaliteit als de bestrijding ervan op gespannen voet kunnen staan met het recht op privacy. In de komende 45 minuten wil ik met u de gespannen relatie tussen privacy en cybercrime verkennen. Daarbij richt ik mij in het bijzonder op de bescherming van het recht op privacy in de context van de opsporing en bestrijding van cybercriminaliteit en cyber-gefaciliteerde criminaliteit.

De opbouw van deze oratie is als volgt. Allereerst beschrijf ik de rol die technologie speelt in de ontwikkeling van cybercriminaliteit en de manier waarop digitale technologieën criminelen faciliteren in hun 'werk' (hoofdstukken 2 en 3). Ik laat zien welke barrières digitale technologieën opwerpen voor de opsporing (hoofdstuk 4 en 5), maar ook welke kansen zij bieden (hoofdstuk 6). Vervolgens ga ik in op de vraag hoe het recht een balans tracht te vinden tussen het belang van de opsporing en de rechten van de verdachten (hoofdstuk 7 tot en met 9). Aan de hand van drie voorbeelden laat ik vervolgens zien hoe nieuwe, innovatieve opsporingsmethoden het huidige strafvorderlijk kader uitdagen (hoofdstuk 10). Vervolgens bekijk ik of het huidige en aankomende strafvorderlijk kader toekomstbestendig zijn (hoofdstuk 11).[4] Ik rond af met een korte beschouwing over hoe de wetgever een nieuwe 'crisis in de opsporing' kan voorkomen (hoofdstuk 12 en 13). Uiteraard sluit ik deze oratie af met enige woorden van dank (hoofdstuk 14).

2 De technologie als katalysator voor nieuwe criminele gedragingen

Nieuwe technologieën bieden nieuwe kansen voor onze maatschappij, maar maken ook nieuwe schadelijke en ongewenste gedragingen mogelijk. De ontwikkeling van informatie- en communicatietechnologieën (ICT) ging gepaard met de opkomst van nieuwe vormen van criminaliteit zoals hacking en dDos aanvallen. Met nieuwe technologische ontwikkelingen zoals de *Metaverse* en kunstmatige intelligentie komen daar delicten zoals diefstal van virtuele goederen en de verspreiding van *deep nudes* bij.[5] De technologie is een katalysator voor nieuwe criminele gedragingen.

Hoewel de criminaliteitscijfers al jaren dalen, laat cybercriminaliteit een tegenovergestelde trend zien: het is één van

de weinige categorieën criminaliteit die jaar op jaar stijgt.[6] Deze opwaartse trend kan op verschillende manieren worden verklaard.[7] Ik geef hier twee verklaringen. Allereerst is er het toenemende gebruik van digitale technologieën en onze afhankelijkheid ervan. Onze samenleving digitaliseert en de criminaliteit dus ook. Een tweede verklaring ligt in de positieve *business case* voor cybercriminaliteit. De opbrengsten van cybercriminaliteit zijn hoog, terwijl de risico's relatief laag zijn. Een hack in het voorjaar van dit jaar bij game ontwikkelaar Ronin, de aanbieder van het populaire spel Axie Infinity, leverde de daders maar liefst 600 miljoen dollar in cryptovaluta op.[8] Tegenover deze hoge opbrengsten staat een relatief lage pakkans. Zeker wanneer dader en slachtoffer zich in verschillende jurisdicties bevinden is de pakkans laag.

3 Cybercrime gecategoriseerd

Met het oog op het duiden van de relatie tussen privacy en cybercrime is het nuttig om een zekere ordening aan te brengen in het brede begrip cybercriminaliteit.

Het Cybercrime Verdrag van de Raad van Europa maakt een onderscheid tussen: (1) delicten gericht tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computers en gegevens, en (2) computer-gerelateerde delicten.[9]

Bij de eerste categorie zijn computers en de daarin opgeslagen gegevens specifiek het doelwit.[10] Er wordt in dit kader ook wel gesproken over *target cybercrimes* of *cybercrime in enge zin.*[11] Denk hierbij aan het hacken van computers (strafbaar gesteld als computervredebreuk in 138ab Sr), het aftappen van gegevens (strafbaar gesteld in artikel 139c Sr) en het vernielen van geautomatiseerde werken (strafbaar gesteld in artikel 350 Sr).

Bij de tweede categorie, de *computer-gerelateerde delicten* of *tool cybercrimes*, gaat het om commune delicten die regelmatig met behulp van computers worden gepleegd.[12] Denk bijvoorbeeld aan internetoplichting en andere vormen van digitale fraude. Bij deze gedragingen vormt de computer een belangrijk onderdeel van de *modus operandi.*[13]

In beide categorieën staat de computer in meer of mindere mate centraal, hetzij als doel, hetzij als middel. Daar waar digitale technologieën slechts een zijdelingse rol spelen bij het voorbereiden of plegen van een delict wordt veelal gesproken over *computers incidental to crime.*[14] Denk hierbij bijvoorbeeld aan een moordenaar die een computer gebruikt om informatie over een geschikt wapen te googlen. De computer draagt wel bij aan het delict, maar speelt geen onderscheidende rol van betekenis.

Tussen de 'echte' cybercriminaliteit en de delicten waarin computers slechts een zijdelingse rol spelen is de laatste jaren een nieuwe (derde) categorie ontstaan die ik *cyber-gefaciliteerde criminalitei*t noem.[15] Bij deze categorie spelen digitale technologieën een prominente rol in de voorbereiding en het plegen van het delict als middel om de identiteit, communicatie en/of het handelen van criminelen te verhullen. Het 'cyber' component zit hem hier dus in het aanwenden van digitale technologieën om het plegen van delicten zoals moord, drugshandel of terrorisme te faciliteren.[16]

Over deze nieuwe categorie straks meer.

4 Digitale technologieën als barrière voor de opsporing

Digitale technologieën maken ons leven makkelijker. Datzelfde geldt helaas ook voor het leven van criminelen. Digitale technologieën maken het plegen van misdrijven eenvoudiger. Daarnaast bemoeilijken de kenmerken en het gebruik van digitale technologieën de opsporing.

Oerlemans beschrijft in zijn proefschrift *Investigating Cybercrime* drie cruciale obstakels die digitale technologieën opwerpen voor de opsporing te weten: jurisdictie, anonimiteit en encryptie.[17]

urisdictie
Het eerste obstakel is jurisdictie. Daar waar er in de fysieke wereld doorgaans weinig afstand tussen dader en slachtoffer is, is dit in de digitale wereld meestal anders. Niet zelden bevinden dader en slachtoffer zich zelfs in verschillende jurisdicties. Het ontbreken van handhavingsjurisdictie maakt het voor opsporingsinstanties moeilijk om snel en effectief onderzoek te doen. De politie kan gebruik maken van rechtshulp, maar dat is een relatief traag en omslachtig proces. Daar komt nog bij dat wanneer de cybercrimineel zich in een jurisdictie bevindt waarmee Nederland geen uitleveringsverdrag heeft, de kans zeer klein is dat deze ooit voor de Nederlandse rechter verschijnt.

Anonimiteit
Een tweede obstakel voor de opsporing is de eenvoud waarmee cybercriminelen hun identiteit kunnen verhullen. Omdat het Internet een open systeem is dat zonder identificatie en autorisatie van gebruikers werkt, is de ware identiteit van een internetgebruiker niet eenvoudig te achterhalen. Via een IP-adres kan een netwerkapparaat worden geïdentificeerd, maar daarna moet dit apparaat nog worden gekoppeld aan de gebruiker. Daarbij is het niet gezegd dat de gebruiker van het apparaat, ook de pleger van het delict is. Het kan goed zijn dat de crimineel de computer van iemand anders heeft overgenomen en via die weg een aanval uitvoert.

Encryptie
Een derde obstakel is encryptie. Encryptie is van essentieel belang voor cyberveiligheid. Door het versleutelen van bestanden (*encryption at rest*) en het versleutelen van communicatie (*encryption in transit*) voorkomen we dat derden ongewenst toegang krijgen tot onze gegevens. Maar tegelijkertijd stelt encryptie criminelen óók in staat om hun criminele gedragingen af te schermen voor de opsporing. In dit kader spreekt de opsporing daarom ook wel van het *going dark* probleem.[18]

5 Cyber-gefaciliteerde criminaliteit als extra barrière

Bij cyber-gefaciliteerde criminaliteit spelen met name de obstakels anonimiteit en encryptie een rol. Met behulp van cryptofoons kunnen cybercriminelen vrij en veilig communiceren, ondergrondse marktplaatsen brengen criminele vraag en aanbod eenvoudig samen en beveiligde fora bieden een vrijplaats voor pedoseksuelen.

Met behulp van 'grijze infrastructuren' zijn criminelen in staat om hun criminele handelingen af te schermen voor de opsporing. Grijze infrastructuren zijn ICT-infrastructuren en -diensten die specifiek gericht zijn op het ondersteunen van criminelen, of gezien hun kenmerken daar bijzonder geschikt voor zijn.[19] Grijze infrastructuren faciliteren criminelen in hun werk door hun identiteit, locatie, gedragingen en/of communicatie te verhullen. Voorbeelden van grijze infrastructuren zijn *bulletproof hosting* en cryptocommunicatie.

Omdat grijze infrastructuren het werk van criminelen makkelijker en veiliger maken, is het niet verwonderlijk dat zij steeds populairder worden onder criminelen. Europol signaleert dan ook een toenemend gebruik van grijze infrastructuren.[20]

Overigens verbergen criminelen niet alleen hun activiteiten via grijze infrastructuren. Legitieme digitale infrastructuren kunnen het werk van de opsporing ook bemoeilijken. Met name het gebruik van *end-to-end* versleutelde communicatiediensten zoals Signal, Telegram en WhatsApp wordt door de politie als een potentiële bedreiging gezien, omdat deze diensten in theorie niet afluisterbaar zijn.[21]

6 Kansen voor de opsporing

Digitale technologieën in het algemeen en grijze infrastructuren in het bijzonder werpen nieuwe barrières op voor de opsporing, maar tegelijkertijd bieden zij ook nieuwe kansen voor

de opsporing. Deze kansen hebben net als de bedreigingen hun oorsprong in de kenmerken van digitale technologieën.

In de digitale wereld worden onze handelingen en interacties doorgaans geobserveerd en geregistreerd. Denk bijvoorbeeld aan het vastleggen van verkeersgegevens of het bijhouden van logbestanden. Deze en andere digitale gegevens vormen waardevolle informatiebronnen voor de opsporing. Verder wordt ons gedrag in de fysieke wereld vastgelegd door de apparaten die wij bij ons dragen of in onze omgeving aanwezig zijn. Een mobieltje dat een zendmast aanstraalt, een slimme deurbel die ons filmt en een smartwatch die onze stappen telt: het zijn alle waardevolle informatiebronnen voor de opsporing. Met de ophanden zijnde komst van immersieve technologieën zoals *augmented reality* wordt de kans dat een volledig digitaal beeld van ons wordt vastgelegd nog vele malen groter.[22] De politie kan toegang krijgen tot onze 'digitale schaduw' door de inzet van opsporingsbevoegdheden en dwangmiddelen zoals inbeslagname van gegevensdragers, het vorderen van gegevens en het digitaal binnentreden.

Ook de eerdergenoemde grijze infrastructuren bieden kansen voor de politie. Omdat criminelen zich bij het gebruik van deze diensten doorgaans veilig wanen, zijn zij weinig terughoudend in hun communicatie. Een schokkend voorbeeld daarvan is de communicatie rondom de moord op journalist Peter R. de Vries. De verdachten communiceerden vrijelijk over de gruwelijke manier waarop het slachtoffer aan zijn einde kwam.[23] Wanneer de opsporing in staat is om de grijze infrastructuren te kraken, geeft dat een ongekend inzicht in het criminele gedrag en biedt het sleutelbewijs in vele rechtszaken. Het oprollen van cryptocommunicatie aanbieders als Ennetcom, Sky-ECC en EncroChat alsmede de overname van *darknet markets* als Hansamarket en Alphabay tonen aan dat criminelen ook niet veilig zijn op grijze infrastructuren.[24]

7 Nieuwe kansen, nieuwe bevoegdheden?

De politie maakt dankbaar gebruik van de nieuwe kansen die digitale technologieën bieden voor de opsporing. Tegelijkertijd worden criminelen zich steeds bewuster van de digitale sporen die zij achterlaten en proberen deze te verhullen. Om toegang te krijgen tot relevante bronnen moet de politie steeds creatiever worden in haar aanpak. Het gevolg is een wedloop tussen de criminelen die zich bedienen van steeds geavanceerdere technologieën om hun identiteit en gedrag te verhullen en de politie die met behulp van nieuwe opsporingsmethoden weer zicht probeert te krijgen op de criminelen.

Deze methoden kunnen op gespannen voet staan met het recht op privacy.

8 Het grondrecht op privacy

De twee belangrijkste doelstellingen van het strafproces zijn: (1) het achterhalen van de (materiële) waarheid en (2) het bieden van bescherming aan de (verdachte) burger.[25] Deze bescherming ziet onder andere op het waarborgen van fundamentele rechten zoals het recht op privacy. De opsporingsmethoden die de politie inzet kunnen in meer of mindere mate ingrijpen in het recht op privacy.

Het recht op privacy is vastgelegd in internationale mensenrechtenverdragen zoals artikel 17 van het Internationaal Verdrag inzake burgerlijke en politieke rechten (IVBPR), artikel 8 van het 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). Op nationaal niveau is het recht op privacy en gegevensbescherming vastgelegd in de artikelen 10 tot en met 13 Grondwet.

Maar wat het recht op privacy precies omvat is niet eenduidig te zeggen. De reden hiervoor is dat privacy afhankelijk is van tal van contextuele, historische en culturele factoren.[26]

Artikel 8 EVRM spreekt van 'privé- en familieleven'. Wat onder het privé- en familieleven valt en daarmee een onderdeel vormt van onze persoonlijke levenssfeer is volgens de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) ruim. Zo gaat het onder andere om de privacy van het menselijk lichaam, de woning, communicatie, relaties en informatie over onze persoon. Zelfs activiteiten die zich in het publieke leven afspelen kunnen onder de reikwijdte van het begrip privé- en familieleven vallen.[27]

Met name het recht op informationele privacy heeft de laatste dertig jaar sterk aan belang en belangstelling gewonnen door de vergaande digitalisering. Bij de Grondwetswijziging van 1983 is het recht op gegevensbescherming zelfs als een zelfstandig recht opgenomen.[28] Ook in het Handvest van de Grondrechten van de Europese Unie is het recht op gegevensbescherming als een apart recht benoemd (artikel 8 Handvest). In de context van de opsporing en bestrijding van cybercriminaliteit en cyber-gefaciliteerde criminaliteit kunnen met name de informationele privacy en het communicatiegeheim in het gedrang komen.

9 Privacy en opsporing

Privacy is geconceptualiseerd als een negatief recht: de staat heeft zich te onthouden van inmenging in de persoonlijke levenssfeer van de burger.[29] Het recht op privacy is echter niet absoluut. Artikel 8 lid 2 EVRM geeft de gronden en voorwaarden voor de beperking van het recht op privacy. Ook de artikelen 10 tot en met 13 van onze Grondwet bieden ruimte voor beperkingen op het recht op privacy bij of krachtens de wet.

De handhaving van de openbare orde en het voorkomen en opsporen van strafbare feiten zijn zwaarwegende belangen die de overheid ertoe kunnen nopen om inbreuken te maken op de persoonlijke levenssfeer. In de belangenafweging tussen het recht op privacy en het voorkomen en opsporen van strafbare feiten vormt artikel 8 EVRM een belangrijke toetssteen.

9.1 Het toetsingsschema van artikel 8 EVRM

Om de legitimiteit van de inzet van een opsporingsbevoegdheid te kunnen beoordelen moeten we het 'toetsingsschema' van artikel 8 EVRM doorlopen. Gewapend met dit schema kunnen wij de legitimiteit van nieuwe innovatieve opsporingsmethoden beoordelen. Het schema is als volgt opgebouwd.

1) Is er sprake van een inbreuk op privé-, familie- en gezinsleven?

2) Wordt daarmee één van de in artikel 8 lid 2 EVRM genoemde legitieme doelen nagestreefd?

3) Is de inbreuk noodzakelijk in een democratische samenleving?

4) Is de inbreuk bij de wet voorzien?

Ad 1) Is er sprake van een inbreuk op het privé-, familie en gezinsleven?

Er moet allereerst sprake zijn van een inbreuk op het privé- of familieleven (de persoonlijke levenssfeer). Wanneer de persoonlijke levenssfeer niet, of maar in zeer geringe mate wordt geraakt door de opsporing, dan is het recht op privé- en familieleven niet in het geding. In veel gevallen zullen opsporingsmethoden die worden ingezet in het kader van de bestrijding van cybercriminaliteit en cyber-gefaciliteerde criminaliteit echter wel degelijk een inbreuk op de persoonlijke levenssfeer maken.

Ad 2) Wordt een legitiem doel nagestreefd?

Als er sprake is van een inbreuk op de persoonlijke levenssfeer moet worden vastgesteld of deze inbreuk wordt gemaakt met het oog op het dienen van één van de legitieme doelen genoemd in artikel 8 EVRM. De in artikel 8 lid 2 EVRM genoemde doelen zijn: de nationale veiligheid, de openbare vei-

ligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden en de bescherming van de rechten en vrijheden van anderen.

Ad 3) Is de inbreuk noodzakelijk in een democratische samenleving?
De inbreuk moet noodzakelijk zijn in een democratische samenleving. Wil een inbreuk noodzakelijk zijn in een democratische samenleving dan moet er allereerst sprake zijn van een dringende maatschappelijke behoefte (*a pressing social need*).[30] De inmenging in de persoonlijke levenssfeer moet vervolgens noodzakelijk zijn om invulling te geven aan deze behoefte. De noodzakelijkheidseis in artikel 8 EVRM staat niet gelijk aan absoluut noodzakelijk (*strictly required*), maar is sterker dan het in de artikelen 5 en 6 EVRM gehanteerde begrip 'redelijk'.[31] Het is uiteindelijk aan de verdragspartijen om *in concreto* deze afweging te maken. Het Hof kent de verdragspartijen hierbij een ruime beoordelingsruimte toe (*margin of appreciation*).

Bij de beoordeling van de noodzakelijkheid spelen de begrippen proportionaliteit en subsidiariteit een centrale rol. De inmenging moet in verhouding staan tot het beoogde doel (proportionaliteit) en er mag geen minder ingrijpend middel zijn dat gebruikt kan worden om hetzelfde resultaat te bereiken (subsidiariteit).

Ad 4) Is de inbreuk bij de wet voorzien?
Tenslotte moet elke inbreuk bij de wet voorzien zijn. Dit criterium kent vijf uitgangspunten:

1) er moet een basis zijn in het nationale recht;

2) de wettelijke bepaling moet toegankelijk zijn (*accessible*);

3) de wet moet een dusdanige kwaliteit hebben dat de inbreuk voorzienbaar is (*foreseeability*);

4) de wet moet geen ruimte laten voor willekeur; en

5) de wet moet toereikende procedurele waarborgen bieden.[32]

Deze uitgangspunten zoals geformuleerd door het EHRM hebben tot doel om de rechtszekerheid voor burgers te garanderen.[33]

In de context van deze oratie wil ik in het bijzonder in gaan op de laatste drie uitgangspunten: voorzienbaarheid, afwezigheid van willekeur, en toereikende procedurele waarborgen.

9.2 De regeling van opsporingsbevoegdheden
In zijn algemeenheid kunnen we stellen dat naarmate de inbreuk op de grondrechten van burgers (potentieel) groter is, er een meer robuuste wettelijke regeling noodzakelijk is. In de Nederlandse context betekent dit dat voor opsporingsmethoden met een beperkte impact op de persoonlijke levenssfeer de algemene taakstellende bevoegdheid van de politie (artikel 3 Politiewet) volstaat, terwijl voor zwaardere inbreuken een meer specifieke bevoegdheid moet zijn omschreven, zoals een bijzondere opsporingsbevoegdheid.

Het EHRM beoordeelt de kwaliteit van een wet die het gebruik van bepaalde opsporingsmethoden legitimeert aan de hand van diverse criteria, waaronder:

- de aard, de omvang en de duur van de maatregel;
- de gronden op basis waarvan de maatregel gevorderd kan worden;
- de autoriteiten die bevoegd zijn om de maatregel toe te staan, uit te voeren en te toetsen; en
- de effectiviteit van de beschikbare rechtsmiddelen.[34]

Deze algemene criteria worden in een specifiek geval nader ingekleurd. De hierboven genoemde criteria leiden ertoe dat een nationale regeling heldere kaders moet bevatten voor het toepassen van een (bijzondere) opsporingsbevoegdheid.

9.3 Consequenties van een inbreuk op het grondrecht op privacy
Wanneer een privacyschending niet bij de is wet voorzien, of niet plaats heeft op de wijze bij de wet voorzien (een vormverzuim), dan kan dit consequenties hebben voor het recht op een eerlijk proces zoals beschermd door artikel 6 EVRM.

Wanneer door de rechter onherstelbare vormverzuimen zijn geconstateerd in het voorbereidend onderzoek, dan kunnen daar ingevolge artikel 359a Wetboek van Strafvordering strafvorderlijke consequenties aan worden verbonden.[35] Bij zeer ernstige vormverzuimen kan zelfs bewijsuitsluiting volgen of de niet ontvankelijkheid van het Openbaar Ministerie in de vervolging worden uitgesproken.

Wel lijkt het erop dat rechters in het algemeen terughoudend zijn met het verbinden van dergelijke zware consequenties aan geconstateerde vormverzuimen.[36] Dit hangt in belangrijke mate samen met het feit dat het belang van de materiële waarheidsvinding veelal zwaarder weegt dan het sanctioneren van het optreden van de politie. Het idee dat een verdachte vrijuit kan gaan omdat de rechter de opsporing tot orde roept is een weinig aantrekkelijke gedachte. In dit kader waarschuwen auteurs als Kuiper, Nan en Samadi voor de relatieve 'straffeloosheid' van het begaan van vormfouten en de mogelijke gevolgen die dit heeft voor de houding van de opsporing ten aanzien van de regels.[37]

Overigens betekent een schending van artikel 8 EVRM niet onmiddellijk dat de beginselen van een goede procesorde zijn geschaad.[38] Wanneer een schending van artikel 8 EVRM niet van wezenlijke invloed is op het verloop van het proces, dan hoeven daar van de Hoge Raad geen rechtsgevolgen aan te worden verbonden.[39] Goos constateert in dit kader dat schendingen van het recht op privacy in beginsel hooguit tot strafvermindering leiden.[40] Ook kan het blijven bij een enkele constatering van het verzuim door de rechter, zonder dat daar gevolgen aan worden verbonden.

10 Spanning tussen privacy en digitale opsporing

Wat de opsporing van cybercriminaliteit en cyber-gefaciliteerde criminaliteit in het licht van artikel 8 EVRM problematisch maakt, is dat nieuwe opsporingsmethoden veelal niet of nauwelijks genormeerd zijn. Daar waar er geen specifieke regeling is voor de toepassing van een opsporingsmethode moeten politie en OM op de handen blijven zitten totdat de wetgever (vaak na enkele jaren) de opsporingsmethode heeft genormeerd, of de toepassing van de methode in bestaande bevoegdheden lezen. Een voorbeeld van dit laatste is de stelselmatige observatie: hoewel deze bevoegdheid oorspronkelijk met name bedoeld was om het werk van fysieke observatieteams in goede banen te leiden, wordt zij nu ook gehanteerd om het volgen van online gedrag te normeren.

Maar dergelijke analoge en extensieve interpretaties van opsporingsbevoegdheden hebben natuurlijk hun grenzen, omdat ze op gespannen voet staan met het strafvorderlijk legaliteitsbeginsel en de hierboven uiteengezette vereisten zoals geformuleerd door het EHRM.

Bij de aanpak van cybercriminaliteit en cyber-gefaciliteerde criminaliteit kunnen de bestaande strafvorderlijke kaders dus knellen.

Ik zal onderstaand aan de hand van drie praktijkvoorbeelden de moeizame verhouding tussen cybercrime, privacy en opsporing illustreren. Het gaat om: (1) het overnemen van grijze infrastructuren, (2) bulkverzameling en -analyse van gegevens, en (3) de inzet van opsporingsbevoegdheden voor intelligence- en verstoringsdoeleinden.

10.1 Het overnemen van grijze infrastructuren
Om criminele activiteiten te stoppen en om waardevolle opsporingsinformatie te verzamelen is de politie er veel aan gelegen om toegang te krijgen tot grijze infrastructuren. In recente jaren hebben er daarom diverse acties plaatsgevonden tegen aanbieders van criminele marktplaatsen en versleutelde communicatiediensten. Zo kreeg de politie in 2016 toegang tot de versleutelde berichten van cryptoaanbieder Ennetcom[41], nam ze in 2017 de *darknet market* Hansamarket over[42] en wist zij in 2020 de aanbieders EncroChat en SkyECC te kraken en alle communicatie af te luisteren.[43] In 2021 heeft de Nederlandse politie zelfs meegedaan met een operatie waarbij een eigen cryptocommunicatiedienst werd opgericht om criminelen te misleiden.[44]

Deze acties, waarmee gevoelige slagen zijn toegebracht aan de georganiseerde criminaliteit, roepen wel vragen op met betrekking tot de rechtmatigheid van de toepassing van de gehanteerde opsporingsmethoden. Met name het overnemen en tijdelijk 'runnen' van grijze infrastructuren om zo meer zicht te krijgen op de criminele activiteiten op het platform, vormt een grote inbreuk op de persoonlijke levenssfeer van de gebruikers.[45]

Er bestaat geen specifieke opsporingsbevoegdheid voor het binnendringen en overnemen van grijze infrastructuren. De acties gericht tegen grijze infrastructuren worden daarom gebaseerd op een verscheidenheid aan opsporingsbevoegdheden. Het kan gaan om een stapeling aan bevoegdheden zoals het binnendringen van een geautomatiseerd werk, pseudokoop en -dienstverlening, het stelselmatig inwinnen van informatie, infiltratie, het afluisteren van communicatie, het vastleggen van gegevens *et cetera*.[46] De vraag is of de waarborgen die deze opsporingsbevoegdheden individueel bieden voldoende zijn om de totale inbreuk te 'dekken'. Bij het combineren van bevoegdheden kan de som meer zijn dan de delen: de bevoegdheden kunnen immers in hun onderlinge samenhang een zeer indringend beeld opleveren van de persoonlijke levenssfeer van de betrokkenen. In de Amerikaanse rechtspraak is in dit kader de zogenaamde 'mozaïek theorie' ontwikkeld.[47] Deze theorie stelt dat opsporingshandelingen die zelfstandig geen inbreuk op het Vierde Amendement (het recht op privacy) opleveren, dit in gezamenlijkheid wel kunnen doen. Vertaald naar de Nederlandse context: wanneer de afzonderlijke steentjes (de opsporingshandelingen) samen een volledig beeld (het mozaiek) schetsen, moet indachtig dit beeld worden geoordeeld over rechtmatigheid en toepasselijke waarborgen, niét op basis van de individuele bevoegdheden.

Naast het recht op privacy moeten we bij acties tegen grijze infrastructuren ook rekening houden met andere aspecten. Zo kunnen bij het overnemen en runnen van grijze infrastructuren vragen ontstaan over onder andere het recht op een eerlijk proces (denk aan het instigatieverbod) en de integriteit en de beheersbaarheid van de opsporing. De politie runt immers tijdelijk een infrastructuur via welke criminele handelingen plaatsvinden, of neemt zelfs het initiatief om een dergelijke criminele infrastructuur op te richten.[48]

Met het oog op de bescherming van de persoonlijke levenssfeer, het recht op een eerlijk proces en de integriteit en beheersbaarheid van de opsporing is het daarom van groot belang dat de officier van justitie, maar belangrijker nog de rechter-commissaris, bij de beoordeling van de toepassing van deze bevoegdheden het geheel kan blijven overzien en beoordelen.

Bij de beoordeling van de rechtmatigheid van acties tegen grijze infrastructuren moet tenslotte nog worden opgemerkt dat strafrechtelijke onderzoeken naar grijze infrastructuren doorgaans (ook) het verzamelen van belastende informatie tegen de gebruikers van de dienst tot doel hebben. Informatie uit onderzoeken naar grijze infrastructuren worden gedeeld met talloze onderzoeken naar gebruikers van deze diensten.[49] Dat deze aanpak bijzonder succesvol is blijkt uit de belangrijke rol die de informatie speelt in vele strafzaken. Met de ontmanteling van grijze infrastructuren heeft de politie de georganiseerde crimi-

naliteit in Nederland zware slagen toegebracht. Maar hiermee hangt er in strafvorderlijke zin wel heel veel af van het originele onderzoek naar de grijze infrastructuur. Wanneer er namelijk in dat onderzoek onherstelbare vormverzuimen zijn begaan die van bepalende invloed zijn geweest op het verloop van andere zaken, dan kunnen daar door de rechter strafvorderlijke consequenties aan worden verbonden, waaronder de uitsluiting van het materiaal dat is verkregen uit het originele onderzoek.[50] Deze observatie kan in de afweging tussen het belang van de waarheidsvinding en de rechtmatigheid van het verkregen bewijs een rol spelen. Het is ernstig de vraag of de rechter bewijsuitsluiting aandurft om de opsporing tot de orde te roepen, als dat betekent dat vele andere zaken 'stuk' kunnen gaan.

Hetgeen ons brengt bij het tweede voorbeeld.

10.2 Bulkverzameling en -analyse van gegevens
De politie krijgt via inbeslagname van gegevensdragers, vorderingen bij ICT-dienstverleners en ontmantelde grijze infrastructuren de beschikking over grote hoeveelheden gegevens. Deze 'bulkgegevens' zijn bijzonder waardevol voor de opsporing en vormen cruciaal bewijs in talloze strafzaken. Maar bulkverzameling en -analyse van gegevens kan een grote privacyinbreuk opleveren en moet daarom aan zeer strenge wettelijke vereisten voldoen.[51]

Hoewel het voorbereidend onderzoek waarin gegevens worden verzameld en geanalyseerd één geheel is, wordt de regulering ervan verdeeld over twee regelingen: het Wetboek van Strafvordering en de Wet politiegegevens (Wpg). Het Wetboek van Strafvordering normeert het *verzamelen* van de gegevens, de Wpg normeert het *gebruik* van deze gegevens.[52] In de Ontwerp Memorie van toelichting bij het nieuwe Boek 2 van het Wetboek van Strafvordering benadrukt de wetgever nogmaals dat er een 'harde knip' bestaat tussen deze twee systemen.[53]

Auteurs als Stevens, Galič, Hirsch Ballin, Oerlemans en ook ikzelf hebben kanttekeningen geplaatst bij de houdbaarheid van deze scheiding.[54] Het probleem is dat door het kunstmatige onderscheid tussen deze twee systemen de rechtsbescherming als het ware tussen wal en schip belandt. De sterke waarborgen uit het Wetboek van Strafvordering zijn enkel op de verzamelfase van toepassing, niet op het daaropvolgende gebruik van de gegevens. Op het gebruik van de gegevens (denk aan het verrijken van gegevens, het analyseren van gegevens en het doorgeven van gegevens) is de Wpg van toepassing. De Wpg kent echter minder sterke waarborgen dan het Wetboek van Strafvordering.[55]

De Wpg stelt weliswaar eisen aan een zorgvuldige verwerking van de gegevens, maar het toezicht op de naleving van deze eisen is grotendeels intern van aard. De enige vorm van onafhankelijk, extern toezicht is dat door de Autoriteit Persoonsgegevens (de AP). De AP richt zich op de naleving van de vereisten uit de wet in het algemeen (denk bijvoorbeeld aan de beveiliging van de gegevens), maar toetst niet de legitimiteit van een analyse in een individueel geval. Zelfs al zou de AP willen optreden in concrete gevallen, dan ontbreekt het haar aan effectieve middelen om onrechtmatig optreden van de politie te sanctioneren. Zo kan de AP geen strafvorderlijke consequenties (bewijsuitsluiting, niet-ontvankelijkheid) verbinden aan niet-naleving van de Wpg. Het ontbreken van een effectief systeem van waarborgen waaronder *ex ante* en *ex post* toetsing door een onafhankelijke autoriteit is zorgelijk, omdat volgens de Europese rechter nu juist de grootste impact op de persoonlijke levenssfeer kan worden gemaakt in de analyse fase.[56]

10.3 Intelligence en verstoring
Ook in ons derde voorbeeld speelt de verwerking van gegevens een belangrijke rol.

Cybercrime is niet langer het domein van slimme eenlingen. Tegenwoordig gaat het steeds vaker om criminele organisaties en is er ook in toenemende mate sprake van directe of indirecte inmenging door statelijke actoren. Cybersecurity dreigingen worden daarmee steeds ernstiger.[57]

Het beeld dat wij hebben van cybersecurity dreigingen is echter gefragmenteerd en onvolledig. Dit is in belangrijke mate toe te schrijven aan het versnipperde institutionele landschap voor cybersecurity. Defensie moet de digitale landsgrenzen bewaken, de inlichtingen- en veiligheidsdiensten moeten de nationale veiligheid waarborgen en het Nationaal Cybersecurity Centrum moet de cyberweerbaarheid van de overheid vergroten. Daarnaast zijn er nog tal van private partijen waaronder cybersecuritybedrijven die zicht hebben op een deel van het probleem.

De politie is één van de belangrijkste spelers in het cybersecurity ecosysteem. Niet alleen is zij vaak de eerste partij die wordt gebeld bij een cyberincident, ze beschikt ook over een uitgebreid arsenaal aan bevoegdheden om informatie te verzamelen. Deze informatie (*intelligence*) is waardevol voor de andere partijen in het cybersecurity ecosysteem. Europol pleit er daarom voor om de opsporing te integreren in het cybersecurity ecosysteem en de informatie-uitwisseling te verbeteren.[58]

Naast het verbeteren van de informatiepositie binnen het cybersecurity ecosysteem is de politie ook goed gepositioneerd om cybercriminele activiteiten te verstoren. De politie heeft als één van de weinige actoren in het cybersecurity ecosysteem wettelijke bevoegdheden om cybercriminele activiteiten effectief te verstoren. Denk bijvoorbeeld aan de inbeslagname van servers of het binnendringen van computersystemen. Omdat de pakkans van met name buitenlandse cybercriminelen bijzonder laag is, wordt verstoring als een alternatief voor de opsporing gezien.[59]

Het doel van het opsporingsonderzoek, het nemen van strafvorderlijke beslissingen, staat centraal bij de vraag of er sprake is van opsporing. Dit geldt zowel voor het huidige opsporingsbegrip uit artikel 132a Sv als voor het nieuwe opsporingsbegrip uit artikel 1.1.6 van het voorstel voor een nieuw Wetboek van Strafvordering. De wetgever geeft aan dat het doel strafvorderlijke beslissingen te nemen (mede) kan inhouden dat strafbare feiten worden gestopt.[60] Zo bevatten het huidige en het nieuwe wetboek bijvoorbeeld bevoegdheden om gegevens ontoegankelijk te maken voor zover dat noodzakelijk is om een strafbaar feit te beëindigen of om nieuwe strafbare feiten te voorkomen.[61] Naar mijn mening betekent dit echter niet dat alle bevoegdheden ingezet zouden moeten kunnen worden met als primaire doel het verstoren van criminele gedragingen.

Met de inzet van opsporingsbevoegdheden voor intelligence- en verstoringsdoeleinden drijft het gebruik ervan namelijk steeds verder af van haar oorspronkelijke doel: de opsporing. Dit is problematisch omdat de naleving van de waarborgen in het Wetboek van Strafvordering in belangrijke mate *ex post* getoetst worden. Tijdens het onderzoek op de terechtzitting wordt het handelen van de politie beoordeeld en kunnen strafvorderlijke sancties worden verbonden aan onzorgvuldig of onrechtmatig handelen. Wanneer bevoegdheden worden ingezet voor intelligence- en verstoringsdoeleinden, dan is het niet langer een vaststaand gegeven dat het komt tot een daadwerkelijke vervolging en daarmee een onderzoek op de terechtzitting. Hiermee verdwijnt de belangrijke strafvorderlijke waarborg van het *ex post* toezicht door de rechter uit beeld.[62]

11 De grenzen van het strafvorderlijk kader bereikt?

De bovenstaande drie voorbeelden laten zien dat de opsporing en bestrijding van cybercriminaliteit en cyber-gefaciliteerde criminaliteit zich deels in een juridisch grijs gebied afspelen. Op sommige plekken is het juridisch kader onduidelijk, op andere plaatsen kunnen we al concluderen dat het strafvorderlijk kader tekortschiet. Deze conclusie is overigens niet nieuw. De Commissie Koops signaleerde al in 2018 in algemene zin een aantal van de juridische knelpunten die voortvloeien uit de hierboven beschreven praktijkvoorbeelden.[63] Het moderniseringstraject voor het Wetboek van Strafvordering zou de gesignaleerde vraagstukken kunnen adresseren, maar het is de vraag of dit gaat gebeuren.

Als onderdeel van het moderniseringstraject strafvordering is ook de opsporing tegen het licht gehouden. Het nieuwe Boek 2 regelt het opsporingsonderzoek.[64] Opsporingsbevoegdheden die relevant zijn in het kader van de bestrijding van cybercriminaliteit en cyber-gefaciliteerde criminaliteit hebben dan ook hun plaats in dit boek. Boek 2 herstructureert en stroomlijnt de regels voor het opsporingsonderzoek en breidt het arsenaal aan opsporingsbevoegdheden uit. Met betrekking tot digitale opsporing is de moderniseringsslag echter beperkt. De twee belangrijkste wijzigingen in relatie tot de digitale opsporing zijn:

1) de modernisering van de regeling voor de inbeslagname van en het onderzoek aan gegevensdragers (hoofdstuk 7); en

2) toevoeging van nieuwe heimelijke bevoegdheden tot het stelselmatig overnemen van gegevens uit openbare bronnen en het stelselmatig bepalen van de locatie van een persoon (hoofdstuk 8).

De modernisering van de regels voor de inbeslagname en het onderzoek aan gegevensdragers zijn primair een reactie op het *Smartphone* arrest van de Hoge Raad.[65] Hoewel de nieuwe regeling een belangrijke verbetering vormt voor de opsporing en de bescherming van de persoonlijke levenssfeer, adresseert zij geen van de problemen die ik hierboven heb besproken.

Datzelfde geldt voor de heimelijke bevoegdheden uit hoofdstuk 8 van het nieuwe Boek 2. De insteek van de wetgever voor deze bevoegden is het herstructureren, stroomlijnen en moderniseren van de bijzondere opsporingsbevoegdheden.[66] De nadruk ligt daarbij duidelijk op het herstructureren en stroomlijnen, niét op het moderniseren van het arsenaal aan bevoegdheden. Er zijn slechts twee volledig nieuwe bevoegdheden aan het wetboek toegevoegd: het stelselmatig overnemen van gegevens uit openbare bronnen en de stelselmatige locatiebepaling. Het moge duidelijk zijn dat deze nieuwe bevoegdheden en de daarbij behorende waarborgen niet alle door mij gesignaleerde problemen (overnemen grijze infrastructuren, analyse van bulkgegevens, en het gebruik van bevoegdheden voor *intelligence* en verstoring) adresseren. Een deel van de door mij gesignaleerde problematiek (stapelingen van bevoegdheden, het belang van specifieke regels bij bulkverzameling) wordt overigens wel gezien door de wetgever. Als oplossing worden nadere regels bij algemene maatregel van bestuur voorgesteld (bijvoorbeeld over de omgang met zogenaamde 'combibevelen' waarin meerdere bevoegdheden tegelijkertijd worden toegepast, of waarborgen voor de analyse van open bronnen met behulp van computerprogramma's).[67] Maar naar mijn mening adresseren deze aanvullende regels niet de kern van de problematiek zoals geschetst in deze oratie.

Aan de hand van de voorbeelden die ik hierboven heb gegeven is het duidelijk dat verscheidene knelpunten die de Commissie Koops in 2018 signaleerde niet langer theoretisch zijn. Op grond van hetgeen ik met u vandaag besproken heb, concludeer ik dat zowel voor de effectiviteit van de bestrijding van cybercriminaliteit en cyber-gefaciliteerde criminaliteit als voor de bescherming van de rechten van de burger, een modern kader voor strafvordering noodzakelijk is. Daarmee bedoel ik een nog moderner kader dan het voorgestelde Boek 2 van het nieuwe Wetboek van Strafvordering ons gaat bieden. Mijns inziens lijkt het erop dat voor de bestrijding, opsporing en verstoring van cybercriminaliteit en cyber-gefaciliteerde criminaliteit het nieuwe Boek 2 al achterhaald is voordat het goed en wel is ingevoerd.

12 Oplossingsrichtingen

De vraag is: hoe dan verder?

In haar advies deed de Commissie Koops een aantal aanbevelingen om de drie door mij hierboven besproken problemen te adresseren.

Met betrekking tot de *cumulatieve inzet van bevoegdheden* adviseerde de Commissie een machtigingsconstructie waarbij de rechter-commissaris wordt betrokken wanneer het op voorhand redelijkerwijs voorzienbaar is dat de voorgenomen inzet van een set aan bevoegdheden een indringend beeld van iemands privéleven zal opleveren.[68] Idealiter blijft de rechter-commissaris nauw betrokken bij opsporingsonderzoeken met potentieel verstrekkende gevolgen zoals het hacken van grijze infrastructuren. In aanvulling daarop denk ik ook dat een meer specifieke regeling voor het runnen van grijze infrastructuren verstandig is.

Met betrekking tot *de bulkverzameling en -analyse van gegevens* adviseerde de Commissie de wetgever om een integrale visie te ontwikkelen op zowel de gegevensvergaring als het gebruik, waarbij het Wetboek van Strafvordering en de Wpg in samenhang moeten worden bezien.[69] Tot op heden ontbreekt een dergelijke integrale visie, maar met de recente jurisprudentie van het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europe Unie in gedachten, lijkt het voor de wetgever nu onontkoombaar om met een reactie te komen in de vorm van een wetswijziging.[70] Naar mijn mening is de aanscherping van het onafhankelijke toezicht (door de rechter of een andere instantie) in het bijzonder van belang. Verder is het verstandig om duidelijkere criteria te formuleren voor het verrijken, analyseren en delen van gegevens.[71]

Wat betreft het vraagstuk van *de inzet van opsporingsbevoegdheden* zonder dat er een serieus vooruitzicht is op een daadwerkelijke vervolging adviseerde de Commissie Koops om naar een nieuwe balans te zoeken in de waarborgen.[72] Een mogelijke oplossingsrichting kan liggen in het onder speciale voorwaarden inzetten van (bijzondere) opsporingsbevoegdheden voor intelligence- en verstoringsdoeleinden. Een nieuwe regeling zou allereerst moeten afbakenen wanneer opsporingsbevoegdheden voor verstoringsdoeleinden ingezet mogen worden. De toepassing zou beperkt kunnen worden tot serieuze en acute cyberdreigingen en alleen wanneer duidelijk is dat opsporing geen resultaten gaat opleveren (bijvoorbeeld omdat het gaat om buitenlandse actoren). Verder moeten er nieuwe waarborgen komen die het ontbreken van *ex post* toezicht door een zittingsrechter kunnen compenseren. Bij deze waarborgen moeten moet dan in ieder geval gedacht wordt aan een stevigere *ex ante* rechterlijke toetsing van de toepassing. Maar ook periodieke controles door een rechter of onafhankelijke toezichthouder, notificatieplichten en een toegankelijke klachtenregeling behoren tot de opties. Tenslotte moeten in lijn met hetgeen hierboven is gezegd duidelijke eisen aan het verwerken en delen van gegevens worden gesteld.

13 Vragen voor de toekomst

Ik kom tot een afronding.

Zoals aan het begin van deze oratie is geconstateerd, vormt de technologie een katalysator voor verandering. Nieuwe technologieën leiden tot nieuwe vormen van criminaliteit en werpen nieuwe vragen op voor de opsporing. Het is aan de strafvordering om een balans te zoeken tussen de materiële waarheidsvinding enerzijds en het beschermen van de rechten van de burger anderzijds. Ik hoop met mijn benoeming hier in Leiden aan deze belangrijke taak een bijdrage te kunnen leveren.

In deze oratie heb ik slechts drie vragen op het snijvlak van privacy en cybercrime kunnen stellen. Er zijn er nog veel meer en er komen er in de loop van de tijd ongetwijfeld nog veel meer bij. Enkele voorbeelden:

- Mag de opsporing *zero days* blijven gebruiken?
- Kun je een bionische arm in beslag nemen?
- Hoe gaat opsporing in de *Metaverse* eruit zien?
- Hoe vorderen we gegevens bij een *Decentralised Autonomous Organisation* (DAO)?

- Hoe gaan we om met de effecten van quantum encryptie?

Genoeg vragen om meerdere leerstoelen, carrières en vakgroepen mee te vullen.

Zeer gewaardeerde studenten. Het zal nu en in de toekomst in belangrijke mate op jullie aankomen om deze belangrijke, ingewikkelde en intrigerende vragen te beantwoorden. Het vinden van een balans tussen de belangen van de opsporing enerzijds en de bescherming van de persoonlijke levenssfeer anderzijds vergt een zorgvuldige en genuanceerde afweging. Kijk daarom met de nodige argwaan naar claims van opsporingsinstanties dat verstrekkende bevoegdheden en achterdeurtjes nodig zijn, alsook naar claims van privacy absolutisten dat wij in een totalitaire surveillancestaat vervallen. Blijf nieuwsgierig, kritisch en een tikje wantrouwig.

14 Woorden van dank

Ik sluit af met enkele woorden van dank.

Allereerst wil ik iedereen bedanken die heeft bijgedragen aan de totstandkoming van mijn benoeming. Daarbij noem ik graag specifiek het College van Bestuur, het faculteitsbestuur en de benoemingsadviescommissie.

Een bijzonder woord van dank gaat uit naar Simone van der Hof, Bart Custers en onze decaan Joanne van der Leun. Heel veel dank dat jullie je hard hebben gemaakt voor mijn benoeming en het proces tot een succesvol einde hebben begeleid.

Hoogleraren Janneke Gerards, Bert-Jaap Koops, Ernst Hirsch Ballin en Bart Jacobs. Jullie zijn de absolute top in jullie vakgebied. Het vervult mij daarom met extra trots dat jullie deze benoeming hebben willen ondersteunen.

Hooggeleerde en hooggeschatte promotor Jaap van den Herik. Beste Jaap, nog elke dag profiteer ik van jouw wijze lessen. Dank dat ik op jouw schouders heb mogen staan om hier te komen.

Collega's van eLaw oud en nieuw, het was en is een genoegen om met jullie allen te mogen werken. Ik kijk er naar uit om weer vaker met jullie in het Keyzertje te discussiëren en borrelen.

Familie, vrienden en alle aanwezigen. Dank voor jullie belangstelling in mijn werk en het feit dat jullie deze mooie dag met mij willen delen.

Ton, mijn partner *in crime* sinds mijn studententijd. Dank dat je binnen Considerati altijd ruimte hebt gelaten voor mijn wetenschappelijke ambities en anti-commerciële persoonlijkheidsstoornis.

Hooggeleerde Nan, beste Joost. Je bent niet alleen een onuitputtelijke bron van strafrechtelijke kennis, maar je zorgt er ook voor dat ik nooit *leg day skip*. Dank daarvoor.

Lieve ouders, dank voor alle liefde en het bieden van een stevig fundament voor mijn bestaan. Zonder jullie had ik hier nooit kunnen staan.

Liefste Sas, allereerst excuses dat ik je verjaardag heb gekaapt voor mijn oratie. Het tekent het geduld dat je altijd met mij hebt. Dank voor alles wat je bent en het feit dat ik dat elke dag met je mag delen.

Lucas en Emma, allerliefste rakkers. Papa is oneindig trots op jullie. Ik hoop dat jullie mijn spreekbeurt mooi vonden en jullie ook een beetje trots op mij zijn vandaag.

Ik heb gezegd.

Literatuurlijst

Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018

De Cuyper, R.H., Weijters G. (2016*), Cybercrime in cijfers, Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices*, WODC Memorandum 2016-1,p. 7

Harris, K. J. (1995*), Computer crime an overview*, Technical Bulletin featuring emerging technologies in criminal justice information management, Bureau of Justice Assistance SEARCH,1995 issue 1

Europol (2021), *Internet Organised Crime Threat Assessment (IOCTA),* 2021

Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Amsterdam: Otto Cramwinckel Uitgevers

Galič M. (2022), Bulkbevoegdheden en strafrechtelijk onderzoek: lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse, in: *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2022.

Gerards, J. (2019), *General principles of the European Convention on Human Rights*, New York: Cambridge University Press, p. 199 e.v.

Goos, M. (2019), Vormverzuimen bij de politie, in: *Strafblad* 2019(1)

Kerr, O. S. (2012), The Mosaic Theory of the Fourth Amendment, in: *Michigan Law Review*, Volume 111 Issue 3 2012

Koops, B. J. (2016), *The Internet and its opportunities for cybercrime*

Kuiper, R. (2014). *Vormfouten, juridische consequenties van vormverzuimen in strafzaken,* dissertatie Radboud Universiteit Nijmegen

Nan, J. S., Bektesevic, D. (2017), Structurele vormverzuimen: een structureel probleem?, in: *DD* 2017/22

Nationaal Cybersecurity Centrum (2021), *Cybersecuritybeeld Nederland 2021*, Ministerie van Justitie en Veiligheid

Nieuwenhuis, A. (2014), *Pressing social need: op zoek naar het dwingende karakter van de maatschappelijke behoefte*, in: *NJCM Bulletin* 2014/02

Oerlemans, J. J. (2016), *Investigating Cybercrime*, Dissertatie Universiteit Leiden

Samadi, M. (2018), Het toezicht op de strafvorderlijke overheid: een modern artikel 359a Sv?', in: *Platform Modernisering Strafvordering*, maart 2018

Samadi, M. (2020), *Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen*, dissertatie Universiteit Leiden

Schermer B.W. (2017), Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, in: *Tijdschrift voor Bijzonder Strafrecht en handhaving* 2017(4): 207-216.,

Schermer B.W., Oerlemans J. J. (2020), AI, strafrecht en het recht op een eerlijk proces, in: C*omputerrecht* 2020(1), p. 14-21

Schermer, B. W., Van der Sloot, B. (2020), *Het recht op privacy in horizontale verhoudingen*, WODC juli 2020

Schermer B. W., van Ham, J. (2021), *Regulering van immersieve technologieën*, WODC augustus 2021.

Schermer, B. W., Galič M. (2022), Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?, in: *Tijdschrift voor strafrecht*, aflevering 3 2022

Stevens, L., Hirsch Ballin, M., Galič M. e.a. (2021), Strafvorderlijke normering van preventief optreden op basis van datakoppeling, in: *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2021, p. 234-245

Taylor Parkins-Ozephius, C. M., De Wit, I. N., Van Toor, D.A.G, et al. (2021), De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel, in: Tijdschrift voor Bijzonder Strafrecht & Handhaving 2021, p. 322-333

Van Amersfoort, P., Smit, L., Rietveld, M. (2002), *Criminaliteit in de Virtuele Ruimte*, DSP Groep Amsterdam, mei 2002, p. 13

Van der Sloot, B., Wagensveld, Y., Koops, B. J. (2021), *Deepfakes: De juridische uitdagingen van een synthetische samenleving*, WODC november 2021

Van den Eeden, C.A.J., van Berkel, J. J., Lankhaar, C. C., de Poot, C. J. (2021), Opsporen, vervolgen en tegenhouden van cybercriminaliteit, WODC Cahier 2021-23

Wall, D.S. (2005) The Internet as a Conduit for Criminals, in: *Information Technology and the Criminal Justice System*; Pattavina, A., Ed.; Sage: Thousand Oaks, CA, USA, 2015; p. 77–98 (gereviseerd in 2015)

Noten

1. https://www.om.nl/actueel/nieuws/2021/09/17/verkopers-cryptotelefoons-encrochat-aangehouden (laatst geraadpleegd 19 september 2022)
2. https://www.rtlnieuws.nl/tech/artikel/5303440/gemeente-buren-neder-betuwe-ransomware (laatst geraadpleegd 19 september 2022)
3. https://ibestuur.nl/nieuws/miljoen-documenten-gemeente-buren-op-dark-web (laatst geraadpleegd 19 september 2022)
4. Zie: https://www.rijksoverheid.nl/onderwerpen/nieuwe-wetboek-van-strafvordering/inhoud-nieuwe-wetboek-van-strafvordering (laatst geraadpleegd 19 september 2022)
5. Zie: Van der Sloot, B., Wagensveld, Y., Koops, B. J. (2021), *Deepfakes: De juridische uitdagingen van een synthetische samenleving*, WODC november 2021
6. https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1638179804094 (laatst geraadpleegd 19 september 2022). Zie ook: Jaarverantwoording Politie 2020.
7. Voor een overzicht zie: Koops, B. J. (2016), *The Internet and its opportunities for cybercrime*
8. https://www.nbcnews.com/tech/tech-news/hackers-steal-600-million-maker-axie-infinity-rcna22031
9. Council of Europe, Cybercrime Convention, Budapest 2001 ets. 185. Naast deze twee categorieën onderscheidt het Cybercrime Verdrag ook nog inhoud-gerelateerde delicten (kinderpornografie) en inbreuken op het auteursrecht, maar omdat dit specifieke delicten zijn laat ik deze voor de categorisering verder buiten beschouwing.
10. Explanatory Report – ETS 185 – Cybercrime (Convention), para. 43
11. Zie bijvoorbeeld: van Amersfoort, P., Smit, L., Rietveld, M. (2002), *Criminaliteit in de Virtuele Ruimte*, DSP Groep Amsterdam, mei 2002, p. 13
12. Explanatory Report – ETS 185 – Cybercrime (Convention), para. 79
13. De Cuyper, R.H., Weijters G. (2016*), Cybercrime in cijfers, Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices*, WODC Memorandum 2016-1, p. 7
14. Harris, K. J. (1995*), Computer crime an overview*, Technical Bulletin featuring emerging technologies in criminal justice information management, Bureau of Justice Assistance SEARCH,1995 issue 1
15. Deze definitie vertoont enige overeenkomst met het door de UK Prosecution Service gehanteerde begrip *cyber dependent crime*. Deze definitie omvat echter een groot scala aan criminele gedragingen die ook onder de categorieën uit het Cybercrime Verdrag vallen. Zie: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (laatst geraadpleegd 19 september 2022)
16. Wall spreekt in dit kader van *computer assisted crimes*. Maar in deze definitie wordt het afschermen van de dader en diens gedrag niet als een centraal element genoemd. Zie: Wall, D.S. (2005) The Internet as a Conduit for Criminals, in: *Information Technology and the Criminal Justice System*; Pattavina, A., Ed.; Sage: Thousand Oaks, CA, USA, 2015; p. 77–98 (gereviseerd in 2015)
17. Oerlemans, J. J. (2016), *Investigating Cybercrime*, Dissertatie Universiteit Leiden
18. Zie: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (laatst geraadpleegd 19 september 2022)
19. Om deze reden maak ik ook een onderscheid tussen wat ook wel *computer assisted crime* of *computer enabled crime* wordt genoemd en wat ik cyber-gefaciliteerde criminaliteit noem. Bij *computer assisted crime* en *computer enabled crime* gaat het om het gebruik van alledaagse ICT-middelen in de commissie van een delict. Bij cyber-gefaciliteerde criminaliteit is de gebruikte digitale infrastructuur specifiek ontworpen en gericht op het faciliteren van criminele gedragingen, of daar in het bijzonder voor geschikt.

20. Europol (2021), *Internet Organised Crime Threat Assessment (IOCTA),* 2021
21. Statement of Christopher A. Wray, Director Federal Bureau of Investigation, before the Committee on the Judiciary United States Senate, at a hearing entitled "FBI Oversight", presented March 2 2021, via: https://www.judiciary.senate.gov/imo/media/doc/SJC%20Oversight%20Hearing%20-%20FBI%20Director%20Wray%20SFR%20-%203.2.2021.pdf (laatst geraadpleegd 19 september 2022)
22. Schermer B. W., van Ham, J. (2021), *Regulering van immersieve technologieën*, WODC augustus 2021.
23. Zie: https://www.ad.nl/binnenland/om-over-chatberichten-van-verdachten-moord-peter-r-de-vries-gevenblijk-van-bloeddorst~abab8467/ (laatst geraadpleegd 19 september 2022)
24. Ook legitieme versleutelde communicatiediensten zoals WhatsApp bieden kansen voor de opsporing. Hoewel de inhoud van de communicatie versleuteld is, zijn de verkeersgegevens dat niet. Deze kunnen door de opsporing bijvoorbeeld worden gebruikt om in kaart te brengen met wie een verdachte allemaal contact heeft gehad en wanneer.
25. Samadi, M. (2020), *Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen*, dissertatie Universiteit Leiden, p. 410. Zie ook: Ontwerp Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 766
26. Gutwirth, S. (1998). *Privacyvrijheid! De vrijheid om zichzelf te zijn*, Amsterdam: Otto Cramwinckel Uitgevers, p. 40
27. Zie bijvoorbeeld EHRM, 28 januari 2003, nr. 44647/98 (*Peck t. het Verenigd Koninkrijk*); EHRM, 24 juni 2004, nr. 59320/00 (*Von Hannover t.. Duitsland*); EHRM 24 november 2009, nrs. 16072/06 en 27809/08 (*Friend e.a. t. het Verenigd Koninkrijk; Countryside Alliance e.a. t. het Verenigd Koninkrijk*); EHRM, 21 juni 2011, nr. 30194/09 (*Shimovolos t. Rusland),* EHRM, 16 december 1992, nr. 13710/88 (*Niemitz t. Duitsland*)
28. Zie: Schermer, B. W., Van der Sloot, B. (2020), *Het recht op privacy in horizontale verhoudingen*, WODC juli 2020, p. 33 e.v.
29. Zie o.a.: Schermer, B. W., Van der Sloot, B. (2020), *Het recht op privacy in horizontale verhoudingen*, WODC juli 2020
30. EHRM, 6 december 1976, nr. 5493/72 (*Handyside t. Verenigd Koninkrijk*)
31. Nieuwenhuis, A. (2014), *Pressing social need: op zoek naar het dwingende karakter van de maatschappelijke behoefte*, in: *NJCM Bulletin* 2014/02
32. Gerards, J. (2019), *General principles of the European Convention on Human Rights*, New York: Cambridge University Press, p. 199 e.v.
33. Gerards, J. (2019), *General principles of the European Convention on Human Rights*, New York: Cambridge University Press, p. 199 e.v., *General principles of the European Convention on Human Rights*, p. 199
34. Zie: EHRM 6 september 1978, nr. 5029/71 (*Klass e.a. t. Duitsland)*; EHRM, 29 juni 2006, nr. 54934/00 (*Weber en Saravia t. Duitsland)*; EHRM, 4 december 2015, nr. 47143/06 (*Roman Zakharov t. Rusland*)
35. In het wetsvoorstel voor een nieuw boek 4 van het Wetboek van Strafvordering wordt de regeling van artikel 359a Sv aangepast. De artikelen 4.3.12 tot en 4.3.15 beschrijven de processuele sancties. Zie voor een toelichting: Samadi, M. (2018),
36. Het toezicht op de strafvorderlijke overheid: een modern artikel 359a Sv?', in: *Platform Modernisering Strafvordering*, maart 2018
37. Samadi, M. (2020), *Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen*, dissertatie Universiteit Leiden

38. Kuiper, R. (2014). *Vormfouten, juridische consequenties van vormverzuimen in strafzaken,* dissertatie Radboud Universiteit Nijmegen; Nan, J. S., Bektesevic, D. (2017), Structurele vormverzuimen: een structureel probleem?, in: *DD* 2017/22; Samadi, M. (2020), *Normering en toezicht in de opsporing Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen*, dissertatie Universiteit Leiden. Voor een ander geluid zie: Goos, M. (2019), Vormverzuimen bij de politie, in: *Strafblad* 2019(1)
39. EHRM 12 mei 2000, nr. 35394/97, (*Khan t. Verenigd Koninkrijk*), m.nt. T.M. Schalken NJ 2002/180
40. Hoge Raad, 7 juli 2009, zaaknummer 08/00807, ECLI:NL:HR:2009:BH8889
41. Goos, M. (2019), Vormverzuimen bij de politie, in: *Strafblad* 2019(1)
42. https://magazines.openbaarministerie.nl/opportuun/2018/02/boevenberichten-ontsleuteld (laatst geraadpleegd 19 september 2022)
43. https://www.om.nl/actueel/nieuws/2017/07/20/ondergrondse-hansa-market-overgenomen-en-neergehaald (laatst geraadpleegd 19 september 2022)
44. https://www.rtlnieuws.nl/tech/artikel/5168819/encrochat-gekraakt-meelezen-criminelen-politie-europol; https://nos.nl/artikel/2371961-arrestaties-na-kraken-sky-ecc-criminele-communicatie-is-niet-meer-onbespied (laatst geraadpleegd 19 september 2022
45. https://www.techtarget.com/searchsecurity/news/252502127/FBI-used-encrypted-Anom-app-in-international-crime-bust; https://www.security.nl/posting/693757/Politie+kon+meelezen+met+miljoenen+versleutelde+berichten+Sky+ECC (laatst geraadpleegd 19 september 2022
46. Daarnaast roept deze methode ook vragen op met betrekking tot de integriteit en beheersbaarheid van de opsporing en mogelijke uitlokking (artikel 6 EVRM).
47. Voor een beoordeling van de legitimiteit van acties tegen grijze infrastructuren zie onder andere: Taylor Parkins-Ozephius, C. M., De Wit, I. N., Van Toor, D.A.G, et al. (2021), De politie als winkelier van smartphones met 'versleutelde' communicatiemiddelen: de inzet van de opsporingshandelingen getoetst aan het legaliteitsbeginsel, in: *Tijdschrift voor Bijzonder Strafrecht & Handhaving,* aflevering 5 2021, p. 322-333
48. Kerr, O. S. (2012), The Mosaic Theory of the Fourth Amendment, in: *Michigan Law Review*, Volume 111 Issue 3 2012
49. https://www.politie.nl/nieuws/2021/juni/8/politie-onderschept-opnieuw-massaal-crimineel-berichtenverkeer.html (laatst geraadpleegd 19 september 2022)
50. Zo zijn de gegevens uit het onderzoek 26Lemont (het onderzoek naar EncroChat) gebruikt als bewijs in diverse drugs- en liquidatiezaken. Denk bijvoorbeeld aan het onderzoek naar Piet Costa.
51. Zie: Hoge Raad 1 december 2020, ECLI:NL:HR:2020:1889
52. Zie onder andere: EHRM, 4 december 2015, nr. 47143/06 (*Roman Zakharov t. Rusland*); EHRM, 25 mei 2021, nrs 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk)*; EHRM 25 mei 2021, nr. 35252/18 (*Centrum för Rättvista t. Zweden*). Zie ook: HvJ-EU, 8 april 2014, C293/12 en C594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), HvJ-EU 21 december 2016. C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele 2 Sverige)*; HvJ-EU, 6 oktober 2020, C511/18, C512/18 en C520/18, ECLI:EU:C:2020:791, (*La Quadrature du Net e.a.*); HvJ-EU, 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*Prokuratuur*); HvJ-EU, 5 april 2022, C140/20, ECLI:EU:C:2022:258 (*Commissioner of An Garda Síochána*)
53. Memorie van toelichting bij de Wet politiegegevens, Tweede Kamer, vergaderjaar 2005–2006, 30 327, nr. 3, p. 3
54. Ontwerp Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 48

55. Zie: Stevens, L., Hirsch Ballin, M., Galič M. e.a. (2021), Strafvorderlijke normering van preventief optreden op basis van datakoppeling, in: *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2021, p. 234-245; Galič M. (2022), Bulkbevoegdheden en strafrechtelijk onderzoek: lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse', in: *Tijdschrift voor Bijzonder Strafrecht en Handhaving*, 2022 nr. 3; Schermer B.W., Oerlemans J. J. (2020), AI, strafrecht en het recht op een eerlijk proces, in: C*omputerrecht* 2020(1), p. 14-21 en Schermer, B. W., Galič M. (2022), Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?, in: *Tijdschrift voor strafrecht*, aflevering 3 2022
56. Zie: Schermer, B. W., Galič M. (2022), Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?, in: *Tijdschrift voor strafrecht*, aflevering 3 2022
57. EHRM, 25 mei 2021, nrs 58170/13, 62322/14 en 24960/15 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk)*; EHRM 25 mei 2021, nr. 35252/18 (*Centrum för Rättvista t. Zweden*)
58. Nationaal Cybersecurity Centrum (2021), *Cybersecuritybeeld Nederland 2021*, Ministerie van Justitie en Veiligheid
59. Europol (2021), *Internet Organised Crime Threat Assessment (IOCTA),* 2021, p. 40
60. Zie bijvoorbeeld: Van den Eeden, C.A.J., van Berkel, J. J., Lankhaar, C. C., de Poot, C. J. (2021), *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*, WODC Cahier 2021-23
61. Ontwerp Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 60
62. Ontwerp Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 60
63. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018 (Commissie Koops), p. 23 en 24
64. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018 (Commissie Koops)
65. Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, Boek 2: het opsporingsonderzoek
66. Hoge Raad der Nederlanden, 4 april 2017, zaaknummer 15/03882, ECLI:NL:HR:2017:584 (*Smartphone arrest*)
67. Voorstel van wet tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering inhoudende bepalingen over het opsporingsonderzoek in verband met de modernisering van het Wetboek van Strafvordering (Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering (Het opsporingsonderzoek)), Memorie van Toelichting, p. 65 (oorspronkelijke versie MvT uit 2017)
68. Ontwerp Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 506 en p. 523
69. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018 (Commissie Koops), p. 54
70. Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018 (Commissie Koops), 24
71 Schermer, B. W., Galič M. (2022), Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?, in: *Tijdschrift voor strafrecht*, aflevering 3 2022
72. Zie in dit kader Schermer B.W. (2017), Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens, in: *Tijdschrift voor Bijzonder Strafrecht en handhaving* 2017(4): 207-216., Schermer B.W., Oerlemans J. J. (2020), AI, strafrecht en het recht op een eerlijk proces, in: C*omputerrecht* 2020(1), p. 14-21 en Schermer, B. W., Galič M. (2022), Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen?, in: *Tijdschrift voor strafrecht*, aflevering 3 2022
73 Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, juni 2018 (Commissie Koops), p. 24

Prof.mr.dr. Bart W. Schermer

Bart Schermer (1978) is als hoogleraar Privacy & Cybercrime verbonden aan eLaw, Centrum voor Recht en Digitale technologie. Hij studeerde Recht en Informatietechnologie en Strafrecht in Leiden. In 2007 promoveerde hij op een onderzoek naar het recht op privacy bij het gebruik van kunstmatige intelligentie voor opsporingsdoeleinden.

Bart doet binnen eLaw onderzoek naar privacy en cybercrime. Meer specifiek richt hij zich op de verhouding tussen grondrechten en (strafrechtelijke) handhaving van de rechtsorde op internet. Hij is als fellow verbonden aan het E. M. Meijers Instituut voor Rechtswetenschappelijk Onderzoek, lid van het Kenniscentrum Cybercrime van het Gerechtshof Den Haag en lid van de Commissie Mensenrechten (CMR) van de Adviesraad voor Internationale Vraagstukken.

Naast zijn werk bij eLaw is Bart partner bij Considerati, een juridisch adviesbureau gespecialiseerd in gegevensbescherming en digitaal vertrouwen.

Universiteit Leiden