T. Beekhuis, C.M. Taylor Parkins-Ozephius, W. Albers & D.A.G. van Toor[1]

De ontgrendelplicht in rechtsvergelijkend perspectief (deel 2)

Computerrecht 2020/179

Deze bijdrage bevat het tweede deel van het door de auteurs verrichte onderzoek naar de ontgrendelplicht in België, Duitsland en Nederland. In het eerste deel concludeerden zij dat de regelingen omtrent de gedwongen ontgrendeling van elektronische gegevensdragers in de drie buurlanden sterk uiteenlopen. De noodzaak om in het Nederlandse recht een algemene ontgrendelplicht voor elektronische gegevensdragers te introduceren wordt door de auteurs in het tweede deel van hun bijdrage behandeld.

1. Inleiding

Deze bijdrage bevat het tweede deel van het door ons verrichte onderzoek naar de ontgrendelplicht in België, Duitsland en Nederland.[2] In het eerste deel hebben wij geconcludeerd dat de regelingen omtrent de gedwongen ontgrendeling van elektronische gegevensdragers in deze drie buurlanden sterk uiteenlopen. Daarbij hebben wij de drie regelingen getoetst aan het nemo-teneturbeginsel, zoals uitgewerkt in de jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM). De Nederlandse interpretatie van dit beginsel volgt de Straatsburgse lijn vrij strikt, met als gevolg dat het voor opsporingsambtenaren onmogelijk is om tegen de wil van een verdachte toegang te verkrijgen tot elektronische gegevensdragers die zijn beveiligd met een wachtwoord of pincode. In België bestaat wel een wettelijke grondslag voor het uitvaardigen van een ontgrendelplicht van elektronische gegevensdragers aan een verdachte en in Duitsland is een wetsvoorstel ingediend waarbij de verdachte de wachtwoorden van virtuele identiteiten moet prijsgeven.

Deze discrepantie in het instrumentarium van de opsporingsautoriteiten doet de vraag rijzen of in de Nederlandse rechtsorde een algemene ontgrendelplicht voor elektronische gegevensdragers dient te worden geïntroduceerd en zo ja, hoe een dergelijke regeling moet worden vormgegeven. De conclusie die getrokken kan worden naar aanleiding van het eerste deel van ons onderzoek is dat noch de Duitse noch de Belgische ontgrendelplicht in een eensluidende vorm naar Nederland overgeheveld zou moeten of mogen worden. Deze ontgrendelplichten zijn te begrijpen vanuit het oogpunt van een efficiënte en effectieve opsporing, aangezien het kunnen afdwingen van toegang tot een elektronische gegevensdrager (of een virtuele identiteit) in vergelijking met de inzet van politiële mankracht en manuren een eenvoudige en snelle methode is om strafrechtelijk relevant bewijs te vergaren. Echter, de Belgische ontgrendelplicht is volgens ons in strijd met het nemo-teneturbeginsel en de Duitse ontgrendelplicht – die wordt gecombineerd met een bewijsuitsluiting – zal enkel in overeenstemming zijn met het nemo-teneturbeginsel indien daaraan een *Beweisverwendungsverbot* wordt gekoppeld. Wel kan de Duitse ontgrendelplicht inspiratie verschaffen voor een wettelijke regeling die de Nederlandse wetgever onzes inziens in overweging zou kunnen nemen. De vraag die in deze bijdrage centraal staat is of een algemene ontgrendelplicht voor elektronische gegevensdragers in Nederland dient te worden geïntroduceerd en zo ja, onder welke voorwaarden.

Daartoe gaan wij in paragraaf twee van deze bijdrage kort in op de noodzaak tot invoering van een dergelijke algemene ontgrendelplicht. De door ons voorgestelde regeling, die tegemoetkomt aan deze noodzaak, maar tevens voldoende waarborgen bevat zodat geen strijd met het nemo-teneturbeginsel onstaat als het verkregen bewijs ook daadwerkelijk wordt gebruikt in de strafrechtelijke context, staat centraal in paragraaf drie. Wij stellen namelijk voor om het ontgrendelen onder omstandigheden te verplichten (en bij niet-meewerken de gijzelingsregeling van weigerachtige getuigen van overeenkomstige toepassing te verklaren) waarbij de ontgrendelaar immuniteit verkrijgt ter voorkoming van de schending van het nemo-teneturbeginsel.

2. De noodzaak tot invoering van een algemene ontgrendelplicht

Het integraal onderzoeken van elektronische gegevensdragers, zoals een *smartphone*, een computer of een *tablet*, legt in vrijwel alle gevallen niet alleen veel (persoonlijke) gegevens bloot van de gebruiker en zijn handelingen,[3] maar ook van diens familie, vrienden, kennissen en/of werkrelaties. Om deze reden vormen dergelijke elektronische gegevensdragers een bron van relevante informatie

1 Mr. Tekla Beekhuis is verbonden als promovenda aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Utrecht Centre for Accountability and Liability Law (Ucall) van de Universiteit Utrecht. Mr. Celine Taylor Parkins-Ozephius en mr. Willemijn Albers zijn beiden verbonden als docent Straf(proces)recht aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht. Mr. dr. Dave van Toor is verbonden als universitair docent aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtstaat en Rechtspleging van de Universiteit Utrecht.

2 D.A.G. van Toor, W. Albers, C.M. Taylor Parkins-Ozephius & T. Beekhuis, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131.

3 J. Henseler & C. de Poot, 'De betekenis van digitale sporen voor bewijs op activiteitniveau', *EeR* 2020, 2, p. 50-59.

en potentieel bewijs[4] voor een strafvorderlijk onderzoek. Oerlemans en Koops stellen dat digitaal bewijs (dat bijvoorbeeld op een *smartphone* aanwezig is) in *cybercrime*-onderzoeken een cruciale rol speelt en dat dergelijk bewijs ook in niet-*cybercrime*zaken steeds belangrijker wordt.[5] Vaak gaat het daarbij om bewijs op bronniveau, bijvoorbeeld om de vraag: wie is de persoon achter een virtuele identiteit of pseudoniem?[6] Inmiddels wordt ook de waarde van het digitale spoor voor het *activiteitniveau* benadrukt, waarmee wordt bedoeld dat gegevensdragers ook bijhouden wanneer *apps* en gebruikers actief zijn, waar de gegevensdrager zich op een bepaald moment bevond en welke bestanden zijn geraadpleegd.[7] Er bestaat derhalve een groot belang voor de opsporingsautoriteiten om toegang te verkrijgen tot elektronische gegevensdragers als deze versleuteld zijn.

2.1 *Het in kaart brengen van criminele organisaties en digitale netwerken*

Het verkrijgen van toegang tot elektronische gegevensdragers lijkt met name essentieel te zijn bij criminaliteit waarop geen goed zicht is in de fysieke wereld. Voorbeelden hiervan zijn criminele organisaties met een maffiastructuur, zoals die van Ridouan T.,[8] waarbij het voor de opsporingsautoriteiten vrijwel onmogelijk is om informatie over het netwerk te verkrijgen. Dit heeft te maken met de geslotenheid van veel criminele organisaties en de zorgvuldigheid in de communicatie die meestal wordt betracht. Zo is de PGP-*smartphone* van Ridouan T.'s handlanger Naoufal F. in 2016 in beslag genomen, maar pas in maart 2020 door het NFI gekraakt.[9] Het opsporingsonderzoek rondom Ridouan T. is in een stroomversnelling geraakt nadat begin 2017 een kroongetuige zich meldde bij de politie,[10] terwijl de ten laste gelegde moorden begonnen in 2015 en de drugscriminaliteit nog veel eerder startte. Ridouan T. en zijn organisatie zijn dus jarenlang onder de radar gebleven en justitie kreeg pas vat op de organisatie door een behulpzame kroongetuige in combinatie met jarenlang onderzoek naar de in beslag genomen *smartphones*.

Ook het onderzoek naar de *Hells Angels* laat zien hoe moeilijk het is om bewijs tegen bepaalde organisaties te verkrijgen: namelijk zo moeilijk dat het Openbaar Ministerie (hierna: OM) voor het eerst sinds decennia weer een burgerinfiltrant heeft ingezet (nadat de inzet van burgerinfiltranten een van de belangrijkste redenen was die leidde tot de IRT-affaire).[11] Het OM stelde dat de inzet van deze opsporingsbevoegdheid in dit onderzoek noodzakelijk was om een inkijkje in de organisatie te krijgen, aangezien de leden van de motorclub zich professioneel afschermden.[12]

Daarnaast zijn de onderzoeken naar digitale netwerken eveneens tijdrovend en complex, maar in beginsel minder risicovol voor de integriteit van de opsporing en minder gevaarlijk voor de gezondheid van de *undercover*-agenten of -burgers. Zo is ten minste maandenlang gewerkt aan de overname van de *Hansa Market*,[13] een *darknet* marktplaats, voordat de autoriteiten daadwerkelijk de controle verkregen over deze marktplaats. Ook het kraken van de met het encryptieprogramma *TrueCrypt* beveiligde computer van Robert M. (verdacht van het misbruiken van een groot aantal minderjarigen en het bezitten van een grote hoeveelheid kinderporno) had vele tientallen, zo niet honderden jaren[14] langer kunnen duren als Robert M. zijn wachtwoorden niet had prijsgegeven.[15] Tevens duurde de zoektocht naar de oprichter en beheerder van een andere *darknet* marktplaats, *Silk Road*, lang. Ross Ulbricht werd na jaren van onderzoek gearresteerd als het brein achter een van de eerste en grootste *darknet* marktplaatsen.[16]

Deze voorbeelden geven aan dat het opsporen van criminele organisaties ingewikkeld en tijdrovend is en dat de autoriteiten alle mogelijkheden die bij de opsporing hiervan dienstbaar zijn, kunnen gebruiken. De ontgrendel-

4 Zoals Henseler in zijn lectorale rede heeft betoogd, maken smartphones tot wel 80 procent uit van het digitale bewijs in strafzaken: J. Henseler, 'De (R)evolutie van Digitaal Bewijs', lectorale rede 21 november 2017, Hogeschool Leiden, p. 13; J.J. Oerlemans, 'Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk', *Platform Modernisering Strafvordering* 2018.

5 B.J. Koops & J.J. Oerlemans, *Strafrecht en ICT* (Monografieën recht en informatietechnologie), Den Haag: Sdu 2019, p. 125; zie ook S. Royer & J.J. Oerlemans, 'Naar een nieuwe regeling voor beslag op gegevensdragers', *Computerrecht* 2017/200, p. 277. Dat het digitale bewijs ook daadwerkelijk wordt gebruikt in niet-*cybercrime*zaken blijkt onder meer uit 'Digitaal bewijs in moordzaken', *Computerrecht* 2019/125, p. 225-226 en 'Digitaal bewijs in strafzaken', *Computerrecht* 2020/38, p. 69-70.

6 Denk aan het pseudoniem *Dread Pirate Roberts*, de oprichter en beheerder van *Silk Road* (1).

7 Henseler & De Poot, *EeR* 2020, 2, p. 51.

8 Ridouan Taghi is een Nederlandse verdachte die in verband wordt gebracht met meerdere gewelddadige misdrijven waaronder moorden en pogingen daartoe. Hij wordt door het Nederlandse Openbaar Ministerie verdacht van het leidinggeven aan een criminele organisatie in de zaak Marengo. Taghi was jarenlang de meest gezochte crimineel van Nederland, hij werd internationaal gezocht en stond op internationale opsporingslijsten. Zie ook: https://web.archive.org/web/20191101220042/ en https://eumostwanted.eu/taghi-ridouan-0 (laatst geraadpleegd op 22 juli 2020).

9 https://www.parool.nl/amsterdam/om-alsnog-leesbaar-gemaakte-berichten-extra-bewijs-tegen-rico-de-chileen~bea73c02/, laatst geraadpleegd op 16 juni 2020.

10 https://www.trouw.nl/binnenland/waar-gaat-het-marengo-onderzoek-om~b7fc520f/, laatst geraadpleegd op 16 juni 2020.

11 https://nos.nl/artikel/2337035-justitie-inzet-crimineel-als-infiltrant-bij-friese-hells-angels-was-verantwoord.html, laatst geraadpleegd op 16 juni 2020.

12 https://www.om.nl/actueel/nieuws/2020/03/27/inzet-criminele-burgerinfiltrant-onderzoek-internationale-drugshandel, laatst geraadpleegd op 16 juni 2020.

13 J.J. Oerlemans & R.S. Wegberg, 'Opsporing en bestrijding van online drugsmarkten', *Strafblad* 2019/45, p. 30.

14 https://www.ad.nl/binnenland/kraken-computer-robert-m-had-6000-jaar-kunnen-duren~a8344a9d/ (laatst geraadpleegd op 22 juli 2020).

15 https://www.volkskrant.nl/nieuws-achtergrond/robert-m-wiste-deel-bestanden~bdaf0e05/ (laatst geraadpleegd op 22 juli 2020).

16 Oerlemans & Wegberg, *Strafblad* 2019/45, p. 25.

plicht lijkt daarvoor geschikt. Immers, op de *smartphone* (of een andere elektronische gegevensdrager) kunnen onder meer gegevens staan over de leden van de criminele organisatie, de contacten die zowel binnen als buiten de organisatie worden onderhouden, de plekken waar de *smartphone* is geweest en wellicht zijn ook voor de opsporing relevante inhoudelijke gesprekken te achterhalen.

2.2 *De efficiëntie en effectiviteit van de ontgrendelplicht*

Het is voor de strafvorderlijke autoriteiten echter niet altijd eenvoudig om deze informatie in handen te krijgen, omdat de toegang van *smartphones* en andere elektronische gegevensdragers veelal is beveiligd door middel van ofwel een biometrische[17] vergrendeling, ofwel een numerieke pincode of een wachtwoord. Zoals in deel 1 van onze bijdrage uitgebreid aan bod is gekomen, is het vanwege de bescherming die het nemo-teneturbeginsel biedt niet mogelijk een *verdachte* te dwingen zijn numerieke pincode of wachtwoord af te geven.[18] Dit levert uiteraard een grote beperking op voor de opsporingsautoriteiten, aangezien het vaak alleen de gebruiker (i.c. de verdachte) is die kennis draagt van de pincode of het wachtwoord.[19] Natuurlijk is het mogelijk om de elektronische gegevensdrager zonder medewerking van de verdachte te ontgrendelen, door deze bijvoorbeeld te *hacken*.[20] Elektronische gegevensdragers kunnen echter zodanig beveiligd zijn, dat de inzet van de hackbevoegdheid niet tot het gewenste resultaat leidt of een enorme inspanning kost. Derhalve bepleiten wij een wettelijke regeling die het mogelijk maakt de verdachte te dwingen zijn wachtwoord (pincode of numerieke gegevens) af te geven aan de opsporingsautoriteiten, zodat zij zichzelf toegang kunnen verschaffen tot de elektronische gegevensdrager. Alvorens wij (in de volgende paragraaf) overgaan tot de uitwerking van de nieuwe regeling vinden hieronder enkele instrumentele overwegingen plaats: een nieuwe opsporingsbevoegdheid moet namelijk in voldoende mate efficiënt en effectief zijn voordat de autoriteiten de beschikking krijgen over die bevoegdheid.[21]

De begrippen effectiviteit en efficiëntie gaan over de doeltreffendheid en doelmatigheid van een opsporingsmethode. Om te beoordelen in hoeverre een bevoegdheid effectief en efficiënt is, dient te worden bekeken wat de *input*, *throughput*, *output*, *outcome* (en *impact*) is.[22] De *efficiëntie* van een bevoegdheid hangt af van de hoeveelheid middelen (*input*), taken, processen en activiteiten die worden uitgevoerd (*throughput*) die noodzakelijk zijn om de resultaten van de methode (*output*) te verkrijgen. De berekening van de *effectiviteit* van het proces begint bij het resultaat (*output*). De effectiviteit van een bevoegdheid hangt af van de vraag of het doel (waarheidsvinding) wordt bereikt. Als het resultaat van de methode een bijdrage levert aan het doel, dan is de methode (in bepaalde mate) effectief. Dit is de *outcome* van de bevoegdheid. De *impact* van de methode ziet op neveneffecten die worden bereikt door de methode te gebruiken. Zo kan worden gedacht aan het toenemen van het veiligheidsgevoel onder burgers of het toenemen van het vertrouwen in de strafrechtspleging als een nieuwe opsporingsmethode wordt gecreëerd of een generaal preventieve werking doordat de samenleving weet dat beter kan worden opgespoord.[23]

De vraag naar de *effectiviteit* van een opsporingsbevoegdheid gaat over de invloed van de methode op de doelen van de strafrechtspleging. Een opsporingsmethode is doeltreffend als de toepassing ervan een bijdrage levert aan de waarheidsvinding. Om te voorkomen dat fouten worden gemaakt – het onjuist uitsluiten van daderschap (een vals-negatieve fout) of onjuist aannemen van daderschap (een vals-positieve fout) – dient de informatie die door de inzet van opsporingsbevoegdheden wordt verkregen betrouwbaar en conform de werkelijkheid te zijn. Een opsporingsmethode is derhalve effectiever naarmate de bevoegdheid met een grotere mate van zekerheid bijdraagt aan de waarheidsvinding. Binnen dit onderdeel zijn de *validiteit* en *betrouwbaarheid* van de methode essentiële aandachtspunten om een opsporingsbevoegdheid op zijn effectiviteit te toetsen. Betrouwbare resultaten van een valide methode bepalen namelijk mede de waarde van de verkregen informatie. Validiteit houdt in dat de methode meet wat zij behoort te meten, dat met de methode accurate resultaten worden verkregen. Alleen als een opsporingsbevoegdheid in voldoende mate betrouwbaar en valide is, wordt met een bepaalde mate van zekerheid de waarheid vastgesteld. Anders zijn de kansen te groot dat vals-negatieve of vals-positieve informatie de beslissingen

17 Dit is een methode waarbij – voor het ontgrendelen – gebruik wordt gemaakt van meetbare persoonsgebonden eigenschappen. Denk hierbij aan een vingerafdruk of de vorm van de iris. Vgl. W. Albers, T. Beekhuis & C.M. Taylor Parkins-Ozephius, 'Geef mij toegang tot uw smartphone! Een zoektocht naar de wettelijke grondslag van de gedwongen biometrische ontgrendeling van de smartphone', *TBS&H* 2019, 3, p. 173.

18 Dit ligt anders in geval van biometrische vergrendeling, nu biometrische kenmerken niet door dit beginsel worden beschermd: zie deel 1 van deze bijdrage (Van Toor, Albers, Taylor Parkins-Ozephius & Beekhuis, *Computerrecht* 2020/131).

19 Zie ook Koops & Oerlemans 2019, p. 137. Koops & Oerlemans wijzen er terecht op dat een strafzaak niet hoeft stuk te lopen op encryptie: een verdachte kan bijvoorbeeld vrijwillig zijn wachtwoord afgeven of het wachtwoord kan ergens anders worden achterhaald, zie Koops & Oerlemans 2019, p. 139.

20 Koops & Oerlemans 2019, p. 174 e.v.

21 Zie hierover uitgebreid D.A.G. van Toor, *Het schuldige geheugen? Een onderzoek naar het gebruik van hersenonderzoek als opsporingsmethode in het licht van eisen van instrumentaliteit en rechtsbescherming* (diss. RUN), Deventer: Wolters Kluwer 2017, H. 3.

22 P.M. Wright & G.C. McMahan, 'Theoretical Perspectives for Strategic Human Resource Management', *JOM* 1992, 2, p. 295-320, p. 306; I. Proeller, 'Outcome-orientation in performance contracts: empirical evidence from Swiss local governments', *IRAS* 2007, 1, p. 95-111, p. 97; C.Pollit & G. Bouckaert, *Public Management Reform: A Comparative Analysis*, Oxford: Oxford University Press 2011, p. 16; M.D. Taverne, J.F. Nijboer, M.F. Abdoel & S. Farooq, *DNA in de databank: de moeite waard?*, Den Haag: WODC 2012, p. 50; B.P.A. van Mil, A.E. Dijkzeul & M. Noordink, 'Beoordeling effectiviteit "Nieuwe Stijl"', *Tijdschrift voor Toezicht*, 2012, 2, p. 82; K. van Beek & M. Kommer, 'De staat van veiligheid en rechtvaardigheid', *NJB* 2015, 16, p. 1058.

23 Taverne e.a. 2012, p. 51.

van de officier van justitie of de rechter beïnvloeden. Dus hoe hoger de validiteit en betrouwbaarheid van een methode, hoe belangrijker de bijdrage aan de waarheidsvinding en hoe effectiever die is.

2.2.1 *De te verwachten effectiviteit*

Om de effectiviteit van de door ons voorgestane ontgrendelplicht te beargumenteren, dienen we na te gaan of het doel, zijnde waarheidsvinding, door de inzet van deze ontgrendelplicht kan worden bereikt. In theorie is de effectiviteit van de inzet van deze ontgrendelplicht groot. Immers, door het ontgrendelen van een elektronische gegevensdrager krijgen de autoriteiten toegang tot een schat aan informatie. Deze informatie kan in potentie, zoals eerder werd opgemerkt, in belangrijke mate bijdragen aan de waarheidsvinding. Bovendien is de waarheidsgetrouwheid (en daarmee de bewijswaarde) van de verkregen informatie groot. De autoriteiten treffen de informatie namelijk aan op de elektronische gegevensdrager: zij hoeven – om deze gegevens te verkrijgen – geen handelingen te verrichten die de validiteit van deze gegevens schaadt of zou kunnen schaden.[24] Dit is bijvoorbeeld anders indien opsporingsautoriteiten pressie uitoefenen tijdens een verhoor of fictief bewijs aandragen. Bij deze voorbeelden leveren de autoriteiten een actieve, inhoudelijke bijdrage voorafgaand aan de totstandkoming van verklaringen. Dergelijke *inhoudelijke bemoeienissen* werken mogelijkerwijs valse bekentenissen in de hand.[25] Hiervan is geen sprake bij de door ons voorgestelde ontgrendelverplichting.

Of de effectiviteit van de door ons voorgestane ontgrendelplicht ook in de praktijk groot is, hangt af van de mate waarin de verdachten willen meewerken aan deze ontgrendelplicht. Wanneer de door ons voorgestane ontgrendelplicht wordt toegepast, wil de verdachte blijkbaar niet vrijwillig zijn inloggegevens afstaan (mogelijk wegens angst voor repercussies vanuit de criminele organisatie waartoe de verdachte behoort) en is het ook niet gelukt om de toegang tot de elektronische gegevensdrager op een andere wijze te verkrijgen. Daarom staan wij, zoals wij in paragraaf drie zullen betogen, een ontgrendelplicht voor die kan worden afgedwongen. Als een verdachte niet wil voldoen aan de ontgrendelplicht, dan kan hij worden gegijzeld.[26] Voorts ligt de prikkel voor de verdachte om mee te werken ook in het aanbieden van immuniteit. Hierdoor is de verdachte wellicht eerder geneigd om mee te werken aan de ontgrendelplicht. Derhalve is de te verwachten effectiviteit, zowel in theorie als in praktijk, in voldoende mate aanwezig om het creëren van een dergelijke opsporingsbevoegdheid te rechtvaardigen.

2.2.2 *De te verwachten efficiëntie*

Niet alleen de te verwachten effectiviteit is groot, maar wij verwachten ook dat de door ons voorgestane ontgrendelplicht heel efficiënt is. Immers, in het voor-digitale tijdperk waren observaties, infiltraties en (kroon)getuigen noodzakelijk om criminele organisaties in kaart te brengen en te ontmantelen. De kosten hiervan – voornamelijk in de zin van mankracht – zijn hoog. De gevaren – en dat zijn ook kosten – zijn voor informanten, infiltranten en (kroon)getuigen enorm. Met andere woorden, alleen met risicovolle methoden die veel manuren kosten, konden criminele organisaties worden ontmanteld. De inzet van de ontgrendelplicht neemt daarentegen niet veel tijd in beslag. Er zullen afspraken moeten worden gemaakt tussen het OM en de verdachte (en zijn advocaat). Zetten we de ontgrendelplicht af tegen de eerdergenoemde methoden, dan is de *input* die noodzakelijk is om het gewenste resultaat te verkrijgen aanzienlijk lager. Het nadeel van de ontgrendelplicht in verhouding tot de hierboven beschreven methoden is dat het werk pas begint nadat de gegevensdrager is ontgrendeld. De autoriteiten moeten de wirwar aan informatie ordenen en analyseren, terwijl de verklaringen van informanten, infiltranten of kroongetuigen direct als bewijs bruikbaar zijn. Daar staat echter tegenover dat die verklaringen altijd op hun waarheidsgetrouwheid worden bestreden, terwijl de waarheidsgetrouwheid van de gegevens op een elektronische gegevensdrager in beginsel vaststaat.

Een kanttekening die moet worden gemaakt is dat elektronische gegevensdragers zoveel informatie bevatten over de gebruiker van de gegevensdragers en over de personen met wie de gebruiker contact onderhoudt, dat (met een druk op de knop) gigabytes of terabytes aan informatie kan worden vergaard. Dat gaat niet gepaard met risico's voor de opsporingsautoriteiten, maar mogelijk wel met risico's voor de persoon die, als gebruiker van een elektronische gegevensdrager, onvrijwillig bijdraagt aan de ontmanteling van een criminele organisatie. Eventuele getuigenbescherming valt evenwel buiten het bestek van deze bijdrage: die ziet enkel op de rol van de ontgrendelaar als getuige. De getuigenbescherming wordt ook bij de kroongetuigenregeling als een aanverwant maar inhoudelijk compleet ander onderwerp gezien.[27]

24 Belangrijk hierbij is dat de opsporingsambtenaren nauwkeurig omschrijven wat zij op de elektronische gegevensdrager hebben aangetroffen, welke bestanden zij hebben geraadpleegd en wat zij met de geraadpleegde bestanden hebben gedaan. Deze waarborg kan worden gerealiseerd door de uitgebreide motiveringsplicht ex art. 126aa Sv van toepassing te verklaren op de door ons voorgestane ontgrendelplicht.

25 Zie bijvoorbeeld CAG 18 juni 2019, ECLI:NL:PHR:2019:648, waarin A-G Bleichrodt in punt 27 e.v. kritisch is over de betrouwbaarheid van de met behulp van de Mr. Big-methode verkregen verklaringen; zie ook M. Sauerland, J.M. Schell, H. Otgaar & E.H. Meijer, 'Hoe misleiding tijdens het verhoor (valse) bekentenissen in de hand kan werken', *EeR* 2013/6, p. 210: in dit artikel bespreken de auteurs dat uit onderzoek blijkt dat druk tijdens het verhoor of het mededelen van fictief bewijs tot valse bekentenissen kan leiden.

26 Vgl. de regeling van de weigerachtige getuige in art. 221 en 294 Sv.

27 Vgl. J.H. Crijns, M.J. Dubelaar, K.M. Pitcher & D.A.G. van Toor, 'Comparative analysis', in: J.H. Crijns, M.J. Dubelaar & K.M. Pitcher (red.), *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*, Den Haag: WODC 2017, par. 7.6.

2.3 *Tussenconclusie*

Volgens ons is een ontgrendelplicht dan ook een efficiënte wijze om veel waarheidsgetrouwe informatie te vergaren, die (tenminste in theorie) een hoge te verwachten effectiviteit heeft. Het voorstel om een ontgrendelplicht te introduceren is overigens niet geheel nieuw. Koops heeft in 2012 drie verschillende opties beschreven voor een ontsleutelplicht.[28] Zijn optie B 'een decryptiebevel met bewijsuitsluiting' vertoont gelijkenissen met ons voorstel, maar daarin bestaat echter alleen aandacht voor de informatie die onder de bewijsuitsluiting zou moeten vallen[29] en wat de verwachte effectiviteit van zo'n regel is.[30] Ons voorstel gaat een stap verder en behandelt, naast de omvang van de bewijsuitsluiting, ook de wettelijke voorwaarden voor een dergelijke opsporingsbevoegdheid.

3. Een nieuwe algemene regeling tot het verplicht ontgrendelen van elektronische gegevensdragers

Zoals hierboven is beargumenteerd, kan het ontgrendelen van elektronische gegevensdragers dienstbaar zijn voor de opsporing van criminaliteit en dan met name criminaliteit die zich aan het oog van de opsporingsautoriteiten onttrekt. Voor de opsporing van strafbare feiten gepleegd door criminele organisaties zijn vaak ingrijpende en risicovolle bevoegdheden – zoals de (burger)infiltratie en de kroongetuige – en tijdrovende en complexe bevoegdheden – zoals het kraken van een PGP-*smartphone* of het ontmantelen en overnemen van een *darknet* marktplaats – noodzakelijk. Om de structuur van een organisatie in kaart te brengen en eventueel ook inhoudelijke communicatie te bemachtigen, kan een ontgrendelplicht uitkomst bieden. Hiermee kan, zonder gebruik te hoeven maken van een persoon die zijn leven op het spel zet en zonder tijdrovend en kostbaar (technisch) onderzoek naar de vergrendeling en encryptie, veel informatie worden verkregen. Daar staat tegenover dat een ontgrendelplicht waarbij een wachtwoord of pincode moet worden overgedragen door een verdachte in strijd is met het nemo-teneturbeginsel. Om de balans tussen de noodzaak van het instrument en de daardoor veroorzaakte problemen omtrent de rechtsbescherming van de verdachte te herstellen, stellen wij een ontgrendelplicht onder immuniteit voor, die hieronder nader wordt uitgewerkt.[31]

3.1 *Het verkrijgen van toegang*

De door ons voorgestelde ontgrendelplicht zal tot gevolg kunnen hebben dat er onder andere veel privacygevoelige informatie wordt verkregen door de opsporingsambtenaren. Nu dit een grote inbreuk op de persoonlijke levenssfeer van de verdachte kan opleveren, dient de inzet van deze opsporingsbevoegdheid strikt gereguleerd te worden.[32] Het ligt dan ook in de rede om in eerste instantie enkel de verdachte als onderzoekssubject op te nemen in deze nieuwe regeling.[33]

Wil een opsporingsambtenaar toegang verkrijgen[34] tot een elektronische gegevensdrager die eigendom is van, of in gebruik is bij de *verdachte*,[35] dan dienen twee situaties te worden onderscheiden. Allereerst de situatie dat de elektronische gegevensdrager is vergrendeld door middel van een biometrisch kenmerk. Thans kan dan een passieve medewerking tot ontgrendeling worden afgedwongen op grond van de artikelen 94 jo. 95 jo. 96 Wetboek van Strafvordering (hierna: Sv) en in de toekomst (mogelijk) op basis van artikel 2.7.3.2.7 Sv.[36] Het verdient in het licht van het subsidiariteitsbeginsel de voorkeur om tot ontgrendeling over te gaan door middel van het biometrische kenmerk, aangezien het op deze wijze ontgrendelen het minst belastend is voor de gebruiker van de gegevensdrager (zolang de gebruikte dwang beperkt is) en hiermee ook geen strafvorderlijke beginselen (zoals het nemo-teneturbeginsel) worden geschonden.

De tweede situatie betreft een door een pincode of wachtwoord vergrendelde elektronische gegevensdrager. Hieronder valt ook het geval dat meermaals is geprobeerd de gegevensdrager via het biometrische kenmerk te ontgrendelen zonder het gewenste resultaat en dat de gegevensdrager enkel nog via een pincode of wachtwoord te ontgrendelen is. Het afdwingen van de inloggegevens is in deze situatie – zoals eer-

28 B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel*, Den Haag: WODC 2012, p. 147-150.

29 Koops 2012, p. 148-149.

30 Koops 2012, p. 149-150.

31 Wij laten hierbij de positie van de getuige die "samenwerkt" met de autoriteiten en daardoor mogelijk getuigenbescherming nodig heeft buiten beschouwing. Het ontgrendelen brengt risico's met zich voor de getuige, en de Staat heeft o.g.v. art. 2 EVRM de verplichting de getuige te beschermen. Het onderwerp van de getuigenbescherming is echter een andere zijde van de medaille. Vgl. J.H. Crijns, M.J. Dubelaar, K.M. Pitcher & D.A.G. van Toor, 'Comparative analysis', in: J.H. Crijns, M.J. Dubelaar & K.M. Pitcher (red.), *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*, Den Haag: WODC 2017, par. 7.6.

32 Vgl. art. 126nba lid 1 Sv. In de memorie van toelichting bij dit artikel is hieromtrent het volgende overwogen: 'De voorgestelde bevoegdheid vormt een ingrijpende aantasting van de persoonlijke levenssfeer van de betrokkene, het ligt dan ook in de rede dat strikte voorwaarden worden verbonden aan de inzet daarvan. Vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer is het niet goed verdedigbaar dat een computer wordt binnengedrongen die niet in gebruik is bij de persoon die wordt verdacht van betrokkenheid bij ernstige misdrijven.' Zie *Kamerstukken II* 2015/16, 34372, 3, p. 99.

33 Uit het oogpunt van de efficiëntie is het wellicht wenselijk dat de door ons voorgestelde ontgrendelplicht aan eenieder kan worden gericht. Wij verwachten echter dat deze uitbreiding eigen problemen met zich brengt, zoals de overlap met andere bevoegdheden. Deze mogelijkheid zal dan ook nader onderzocht moeten worden op onder andere haalbaarheid en wenselijkheid.

34 En wij bedoelen hiermee ook daadwerkelijk *enkel* het toegang verkrijgen. Vervolgstappen – zoals het bekijken van de informatie, kopiëren van de informatie, het gebruiken van aan de elektronische gegevensdrager gekoppelde accounts *et cetera* – kunnen alleen op basis van een daarvoor geschikte wettelijke grondslag worden gezet.

35 Te bediscussiëren valt of de ontgrendelplicht moet kunnen worden gericht aan alle personen en bedrijven die informatie bezitten waarmee de gegevensdrager kan worden ontgrendeld. Wij laten de plicht om de gegevensdragers via een derde te laten ontgrendelen voorlopig rusten.

36 Van Toor, Albers, Taylor Parkins-Ozephius & Beekhuis, *Computerrecht* 2020/131.

der betoogd – ongeoorloofd in het licht van het nemo-teneturbeginsel. Aangezien ook in een dergelijke situatie de toegang tot de inhoud van de elektronische gegevensdrager wenselijk is voor de effectiviteit en efficiëntie van de opsporing, stellen wij voor om alsnog de toegang in strijd met het nemo-teneturbeginsel af te dwingen door de verdachte te verplichten de inloggegevens te verstrekken, zodat de informatie die op de elektronische gegevensdrager aanwezig is voor strafrechtelijke doeleinden kan worden verzameld.

Een consequentie van deze afgedwongen toegangsverschaffing is dat hierdoor strijd met het nemo-teneturbeginsel ontstaat indien de verkregen informatie ook wordt gebruikt in een strafrechtelijke procedure tegen de gebruiker van deze gegevensdrager. Daarom dient de door ons voorgestelde wettelijke regeling gepaard te gaan met het geven van strafrechtelijke immuniteit aan de gebruiker van de elektronische gegevensdrager, zodat de verkregen informatie op geen enkele wijze jegens hem mag worden gebruikt in een strafrechtelijke procedure. Deze waarborg is in lijn met die welke in de Duitse regeling wordt voorgesteld, namelijk het *Verdwendungsverbot* wat inhoudt dat een bewijsmiddel niet – in de zin van: op geen enkele wijze – mag worden gebruikt. Alvorens nader in te gaan op de reikwijdte van deze immuniteitsregeling (in par. 3.4), worden eerst de wettelijke voorwaarden voor de inzet van de door ons voorgestelde wettelijke regeling besproken.

3.2 *Toepassingsvoorwaarden voor ontgrendeling door middel van een wachtwoord of pincode*

Voor de desbetreffende regeling moet volgens ons zoveel mogelijk worden aangesloten bij regelingen omtrent de meest ingrijpende bevoegdheden, zoals de bijzondere opsporingsbevoegdheden en de in Nederland gehanteerde kroongetuigenregeling, aangezien ook deze nieuwe bevoegdheid streng moet worden genormeerd. In het bijzonder wordt aangesloten bij de kroongetuigenregeling, omdat het koppelen van immuniteit aan de verplichting tot medewerking vergelijkbaar is bij het geven van immuniteit aan kroongetuigen in andere landen.[37] De inzet van deze bevoegdheden is strikt genormeerd, omdat deze opsporingsbevoegdheden ofwel een meer dan beperkte inbreuk maken op de grondrechten van de verdachte, ofwel dat de inzet van de bevoegdheden een risico vormt voor de integriteit en beheersbaarheid van het overheidsoptreden.[38]

De door ons voorgestelde informatieverplichting die leidt tot ontgrendeling mag daarom enkel worden ingezet indien 'uit feiten en omstandigheden een *redelijk vermoeden* voortvloeit dat misdrijven, als omschreven in *artikel 67, eerste lid*, van het Wetboek van Strafvordering[39] die gepleegd zijn in *georganiseerd verband* en gezien hun aard of de samenhang met andere door de verdachte begane misdrijven een *ernstige inbreuk op de rechtsorde* opleveren [onze cursivering].' Wij vinden de 'afspraak' om aan een persoon immuniteit te verlenen alleen gerechtvaardigd als daarmee een groter doel wordt bereikt, in de zin van het verkrijgen van informatie over een georganiseerd verband.[40] Dit betekent dat de ontgrendelplicht ingezet kan worden als uit de reeds beschikbare informatie blijkt van een redelijk vermoeden van schuld dat bepaalde strafbare feiten in georganiseerd verband worden gepleegd. Verder moet de inzet van de ontgrendelplicht strikt noodzakelijk zijn. Het belang van het onderzoek moet de inzet van deze bevoegdheid dringend vorderen,[41] omdat de immuniteit alleen gerechtvaardigd kan worden in situaties waarin andere opsporingsmethoden niet tot hetzelfde bewijs kunnen leiden. Daarnaast dient de elektronische gegevensdrager in gebruik te zijn bij, of eigendom te zijn van een *verdachte*.

Bovendien kan niet enkel worden volstaan met een bevel van de officier van justitie, maar dient tevens een machtiging van de rechter-commissaris te worden verkregen. Wij kiezen hier voor een minder uitgebreide toetsing door de betrokken autoriteiten dan bij de kroongetuigenovereenkomst, waar ook het College van procureurs-generaal en onder bepaalde omstandigheden zelfs de Minister van Justitie en Veiligheid bij betrokken is.[42] De immuniteit voor de 'ontgrendelaar' is een verdergaande 'beloning', echter de waarheidsgetrouwheid van het bewijs staat veel minder ter discussie. Daarnaast is het ontgrendelen niet zozeer risicovol voor de integriteit van de opsporing. Daarom achten wij nadere controlemechanismes niet noodzakelijk. De machtiging van, en de daarmee gepaard gaande controle door, de rechter-commissaris is wel noodzakelijk, aangezien strafrechtelijke immuniteit moet worden verleend aan de gebruiker van de elektronische gegevensdrager vanwege de strijd met het nemo-teneturbeginsel als het bewijs tegen de verdachte wordt gebruikt. De rol van de rechter-commissaris uit de kroongetuigenregeling is hierbij als uitgangspunt genomen. Tevens moet, om adequaat toezicht op de toepassing van deze regeling mogelijk te maken, de verscherpte verbaliseringsplicht zoals neergelegd in artikel 126aa Sv gelden. Ten slotte lijkt het onmisbaar dat de verdachte/getuige

37 Vgl. J.H. Crijns, M.J. Dubelaar & K.M. Pitcher, 'Concluding observations', in: J.H. Crijns, M.J. Dubelaar & K.M. Pitcher (red.), *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*, Den Haag: WODC 2017, par. 8.4.3.

38 *Kamerstukken II* 1996/97, 25403, 3, p. 3.

39 Na de modernisering zou dit gewijzigd dienen te worden in misdrijven waarop naar wettelijke omschrijving vier jaar of meer gevangenisstraf staat.

40 Dezelfde rechtvaardiging wordt gebruikt bij de kroongetuigenregeling: je moet iets bieden om bij de allergrootste vissen van de organisatie uit te komen.

41 Vgl. art. 126p e.v. en art. 226g Sv.

42 Zie uitgebreid J.H. Crijns, M.J. Dubelaar & K.M. Pitcher, 'Collaboration with Justice in the Netherlands', in: J.H. Crijns, M.J. Dubelaar & K.M. Pitcher (red.), *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*, Den Haag: WODC 2017, par. 3.4.4.

verplicht gebruik moet maken van rechtsbijstand[43] zodat hij de gevolgen van het wel of niet meewerken kan overzien. Overigens heeft de persoon die tot ontgrendeling wordt gedwongen met aan zekerheid grenzende waarschijnlijk al contact gehad met een advocaat omdat hij in eerste instantie als verdachte wordt behandeld.

3.3 *De reikwijdte van de immuniteit*

Voor wat betreft de door ons voorgestane immuniteitsregeling geldt het volgende. Zoals reeds beschreven, is een consequentie van de regeling dat het bewijs dat wordt verzameld op de ontgrendelde elektronische gegevensdrager niet kan worden gebruikt in een strafrechtelijke procedure jegens de gebruiker. Echter, als de informatie, waarvan redelijkerwijs kan worden vermoed aanwezig te zijn op de elektronische gegevensdrager, van cruciaal belang is voor het verkrijgen van strafrechtelijk relevante informatie over de leden van de criminele groepering waartoe de verdachte behoort, dient deze informatie alsnog te worden vrijgegeven. Dan zou het belang van een effectieve en efficiënte strafrechtspleging jegens de georganiseerde misdaad (eenvoudig en snel toegang krijgen tot een gegevensdrager waarop strafrechtelijk relevante gegevens staan over een georganiseerde groep) moeten prevaleren boven het belang om één enkel individu te kunnen vervolgen en te veroordelen.

In een dergelijke situatie zal de gebruiker van de elektronische gegevensdrager een afspraak maken met het OM waarbij hij zichzelf verplicht tot het verstrekken van de inloggegevens onder de voorwaarde van strafrechtelijke immuniteit.[44] De op de elektronische gegevensdrager aangetroffen gegevens kunnen dan enkel worden gebruikt in een strafrechtelijke procedure jegens een derde (in de regel een persoon die onderdeel is van het criminele netwerk van de gebruiker van de telefoon).[45] De gebruiker van de elektronische gegevensdrager verkrijgt aldus twee hoedanigheden: hij is *verdachte* van een ernstig strafbaar feit dat in georganiseerd verband is gepleegd en hij is in het kader van de door ons voorgestelde regeling een *getuige* (in een strafrechtelijke procedure tegen een lid of leden van het georganiseerde verband waartoe hij behoort).[46] In zijn hoedanigheid als verdachte kan hij niet worden gedwongen zichzelf te belasten en zal hij door het afgeven van zijn inloggegevens niet (verder) worden vervolgd. Hierdoor verkrijgt hij voordeel: hij ontloopt immers een strafrechtelijke procedure en een mogelijke veroordeling door de strafrechter.

Hij zal dan wel in zijn hoedanigheid als getuige de inloggegevens van zijn elektronische gegevensdrager moeten verschaffen. In laatstgenoemde procedure zal geen strijd met het nemo-teneturbeginsel ontstaan.[47] In het voorkomen van een strafrechtelijke vervolging ligt de prikkel voor de verdachte om aan de informatieverplichting – die leidt tot ontgrendeling – mee te werken. Echter, niet in alle situaties zal de gebruiker van een elektronische gegevensdrager willen meewerken aan deze verplichting. Daarom moet hij ook kunnen worden gedwongen mee te werken. Aangezien de gebruiker in de door ons voorgestelde regeling niet als verdachte, maar als getuige wordt aangemerkt, kan de gijzelingsregeling in de zin van artikel 221 Sv van toepassing worden verklaard.

De vraag is echter wel tot hoever die strafrechtelijke immuniteit moet reiken. Immers, op de gebruiker van de telefoon rust ook een strafrechtelijke verdenking op grond van één of meerdere ernstige strafbare feiten in georganiseerd verband. Wegens dat strafbare feit (of die strafbare feiten) wordt hij betrokken in een opsporingsonderzoek en ontstaat de noodzaak bij het Openbaar Ministerie om inzage te verkrijgen in de elektronische gegevensdrager om te bezien of er informatie op staat die zij kunnen gebruiken voor een nader onderzoek jegens een derde die tot dezelfde criminele organisatie als de verdachte behoort. De immuniteit die de verdachte verkrijgt dient primair te gelden voor de strafbare feiten die in het kader van deze organisatie door de verdachte zelf zijn verricht. Echter, het is niet ondenkbaar dat op de elektronische gegevensdrager ook informatie te vinden is over andere strafbare feiten die niet in relatie staan tot de criminele organisatie. Dient de immuniteit dan ook voor deze strafbare feiten te gelden? Voor deze strafbare feiten zou bepleit kunnen worden dat de informatie niet gebruikt mag worden als bewijsmateriaal, maar dat de informatie wel gebruikt mag worden als startinformatie (zoals bijvoor-

43 Dit is paternalistisch, maar om de gevolgen van de ontgrendelplicht goed te kunnen overzien, lijkt partijdig advies noodzakelijk. Hiervan kan alleen worden afgezien na consultatie met een raadsman. Wat ons betreft, is enig contact met een raadsman noodzakelijk.

44 Hierbij zouden nog de volgende twee situaties onderscheiden kunnen worden: (i) het bewijs is niet noodzakelijk voor de vervolging en berechting van de tot ontgrendeling gedwongen verdachte; (ii) het bewijs is wel noodzakelijk voor de vervolging en berechting van de tot ontgrendeling gedwongen verdachte. In het eerste geval zou immuniteit een te verstrekkende afspraak kunnen zijn, waarbij misschien aangesloten kan worden bij de huidige kroongetuigenregeling (maximaal vijftig procent strafvermindering). In het tweede geval geldt dat immuniteit noodzakelijk is om schending van het nemo-teneturbeginsel te voorkomen en het netwerk (in grote mate) op te rollen.

45 Vgl. de regeling voor kroongetuigen in art. 226g e.v. Sv; J.H. Crijns, M.J. Dubelaar & K.M. Pitcher, 'Collaboration with Justice in the Netherlands', in: J.H. Crijns, M.J. Dubelaar & K.M. Pitcher (red.), *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*, Den Haag: WODC 2017, par. 3.2.1.

46 Vgl. J.H. Crijns, M.J. Dubelaar & K.M. Pitcher, 'Collaboration with Justice in the Netherlands', in: J.H. Crijns, M.J. Dubelaar & K.M. Pitcher (red.), *Collaboration with Justice in the Netherlands, Germany, Italy and Canada*, Den Haag: WODC 2017, par. 3.2.1..

47 Overigens geldt wel dat ook aan een getuige die zichzelf incrimineert de waarborgen moeten toekomen die een verdachte heeft (vgl. art. 27d lid 2 Sv). De gegevens mogen dus niet alsnog aan hem worden tegengeworpen.

beeld ook geldt voor TCI-informatie en anonieme meldingen[48]).[49]

4. Afronding

Wij beseffen dat de door ons voorgestelde regeling wegens de daaraan gekoppelde immuniteitsregeling vergaand is. Thans geldt dat de inloggegevens van een elektronische gegevensdrager niet kunnen worden afgedwongen en dat het daarom niet altijd mogelijk is voor opsporingsambtenaren om toegang te krijgen tot een elektronische gegevensdrager. Het voor de strafvordering relevante bewijs zal dan op andere manieren verzameld moeten worden. De toegang tot een elektronische gegevensdrager kan echter *cruciaal* zijn voor het verkrijgen van het noodzakelijke bewijs in een strafrechtelijke procedure. Daarnaast verzet het nemo-teneturbeginsel zich tegen het afdwingen van een pincode of een wachtwoord en – wanneer een pincode of wachtwoord alsnog is afgedwongen – tot het gebruik van het bewijs wat is verkregen door een schending van het voornoemde beginsel.[50] De door ons beschreven immuniteitsregeling is daarom noodzakelijk in het licht van het nemo-teneturbeginsel en draagt bij aan een voortvarende strafrechtspleging. Dit laatste is ook geheel in lijn met de hoofddoelstelling van de modernisering van het Wetboek van Strafvordering: 'te voorzien in een wetboek waarin zo veel mogelijk bevorderd wordt dat een *adequate justitiële reactie* kan worden gegeven op strafbaar gedrag, en dat onjuiste justitiële beslissingen zoveel mogelijk worden voorkomen. Daarbij dient zo goed mogelijk geborgd te zijn dat het onderzoek in een strafzaak vanaf het begin zowel *zorgvuldig als voortvarend* plaatsvindt, met *inachtneming van de (grond)rechten van burgers* [onze cursivering].'[51]

48 S. Brinkhoff, *Startinformatie in het strafproces*, Deventer: Kluwer 2014, par. 4.5.2.4 & 5.5.3.4. TCI staat voor Team Criminele Inlichtingen. Voor TCI-informatie geldt overigens dat deze in uitzonderlijke situaties wel als bewijsmiddel kan dienen, zie Brinkhoff 2014, par 5.5.3.4.

49 In de Duitse bewijsrechtelijke doctrine wordt dit een *Beweisverwertungsverbot* genoemd. Het bewijs mag niet worden gebruikt om een bewezenverklaring op te stoelen (*Verwertung*), maar mag wel op andere wijzen worden gebruikt (geen *Verwendungsverbot*).

50 Vgl. Van Toor, Albers, Taylor Parkins-Ozephius & Beekhuis, *Computerrecht* 2020/131.

51 *Kamerstukken II* 2015/16, 29279, 278, p. 4.