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

Artikelen

De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)

Computerrecht 2020/131

In deze bijdrage worden de regelingen met betrekking tot de ontgrendelplicht van Nederland, België en Duitsland vergeleken. Het verplicht meewerken aan het ontgrendelen is ten minste prima facie problematisch in het licht van het zwijgrecht en het nemo-teneturbeginsel. De noodzaak om in het Nederlandse recht een algemene ontgrendelplicht voor elektronische gegevensdragers te introduceren onderzoeken de auteurs in het tweede deel van hun bijdrage.

1. Inleiding

Het gedwongen ontgrendelen van *smartphones* blijft de strafrechtswetenschap en de rechtspraktijk (in binnen- en buitenland) bezighouden. In 2017 beargumenteerde Van Toor dat het gedwongen ontgrendelen van een smartphone met een *biometrisch kenmerk* geen schending oplevert van het nemo-teneturbeginsel.[2] In 2018 betoogde Bood het tegenovergestelde,[3] een standpunt waarop reacties van verschillende auteurs kwamen.[4] In de tijd rondom die discussie zijn meerdere vonnissen gewezen waarbij rechtbanken in het gedwongen ontgrendelen van een *smartphone* met een biometrisch kenmerk geen schending van het recht op een eerlijk proces zagen.[5] Omdat deze ontgrendeling met een biometrisch kenmerk plaatsvindt zonder expliciete wettelijke grondslag leidden deze vonnissen ook tot onderzoek naar de wettelijke grondslag in Nederlandse strafrechtzaken en de vraag of die als voldoende toereikend moet worden gezien in verband met de criteria uit artikel 8 lid 2 Europees Verdrag voor de Rechten van de Mens (EVRM).[6]

In België en Duitsland speelt een vergelijkbare discussie. In België werd onlangs in een tweetal uitspraken geoordeeld dat het gedwongen ontgrendelen van een *smartphone* met een wachtwoord of pincode geen schending van het nemo-teneturbeginsel oplevert.[7] In het Duitse wetsvoorstel *IT-Sicherheitsgesetz 2.0* is een bepaling opgenomen die de gedwongen ontgrendeling (onder bepaalde omstandigheden) van virtuele identiteiten met een wachtwoord of pincode mogelijk maakt (paragraaf 163g Strafprozessordnung (StPO)).[8]

Uit dit korte overzicht blijkt dat Nederland en zijn twee buurlanden de ontgrendelplicht allen anders reguleren. Om twee redenen is het van belang nader aandacht te besteden aan deze verschillen. Ten eerste, hebben of krijgen de autoriteiten in onze twee buurlanden een onderscheidend instrumentarium ter beschikking om strafbare feiten, waarover informatie op elektronische gegevensdragers of via telecommunicatiediensten is te vinden, op te helderen. De discussie of het criminaliteitsinstrumentarium toereikend is, mede om in te spelen op de veranderde criminaliteit, stopt niet en stopt ook niet bij landsgrenzen. Het is belangrijk gedegen aandacht aan de onderbouwing van de noodzaak en de wenselijkheid van het instrumentarium te besteden.[9] Ten tweede moeten alle drie de landen aan de minimumwaarborgen van het EVRM voldoen, aangezien zij lid zijn van de Raad van Europa. Gezien de verschillende verplichtingen in de buurlanden lijkt onenigheid te bestaan over de interpretatie van het recht tegen gedwongen zelfincriminatie in relatie tot de ontgrendelplicht. Het is van belang deze verschillen in kaart te brengen en vervolgens te analyseren of de Nederlandse interpretatie moet worden aangepast, ook in het licht van de modernisering van het Wetboek van Strafvordering.

In deze bijdrage worden daarom de regelingen met betrekking tot de ontgrendelplicht van Nederland, België en Duitsland vergeleken. In de tweede paragraaf wordt de *wettelijke grondslag* van de ontgrendelplicht bespro-

1 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. Mr. Willemijn Albers en mr. Celine Taylor Parkins-Ozephius zijn beiden ook verbonden als docent Straf(proces)recht aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht. 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. Wij danken Sofie Royer voor haar hulp met betrekking tot het onderwerp naar Belgisch recht.

2 D.A.G. van Toor, 'De vergrendelde smartphone als object van strafvorderlijk onderzoek', *Computerrecht* 2017/2, p. 3-11.

3 A. Bood, 'Geef ze een vinger …', *NJB* 2018/1880, p. 2744-2748.

4 L. Stevens, 'Gedwongen biometrische toegangsverschaffing is niet in strijd met nemo tenetur', *NJB* 2019/315; M. Egberts & W. Ferdinandusse, 'Reactie op Alex Bood', *NJB* 2019/316; D.A.G. van Toor, 'Het gedwongen ontgrendelen van een smartphone in het licht van het nemo-teneturbeginsel', *NJB* 2019/317.

5 Rb. Den Haag 12 maart 2018, ECLI:NL:RBDHA:2018:2983; Rb. Rotterdam 14 december 2018, ECLI:NL:RBROT:2018:10283; Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568, *Computerrecht* 2019/94, m.nt. D.A.G. van Toor.

6 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. 173-181.

7 Hof van Cassatie van België 4 februari 2020, P.19.1086.N/1; Grondwettelijk Hof 20 februari 2020, 28/2020.

8 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0).

9 D.A.G. van Toor, 'Het doel heiligt het middel? Over de noodzaak van uniforme criteria voor evaluatie van de effectiviteit en efficiëntie van de opsporing', *Proces* 2015, 4, p. 229-239.

ken. In de derde paragraaf wordt het *verplicht meewerken* aan het ontgrendelen besproken, dat ten minste *prima facie* problematisch is in het licht van het zwijgrecht en het nemo-teneturbeginsel. In paragraaf vier vindt de rechtsvergelijking plaats, waarna wij concluderen dat er een noodzaak bestaat nader onderzoek te verrichten naar de mogelijkheid om in het Nederlandse recht een algemene ontgrendelplicht voor elektronische gegevensdragers te introduceren. Die discussie komt echter aan bod in het tweede deel van dit tweeluik.

2. Het verplicht ontgrendelen van elektronische gegevensdragers vanuit instrumenteel perspectief

In deze paragraaf worden achtereenvolgens de Nederlandse, Belgische en Duitse ontgrendelplichten besproken. Bij deze bespreking staan de wettelijke grondslag van de ontgrendelplicht en de toepassingsvoorwaarden centraal.

2.1 *Nederland*

De toegang tot de inhoud van een *smartphone* kan op verschillende wijzen, namelijk zowel met als zonder medewerking van een verdachte, worden verkregen.[10] In deze paragraaf wordt enkel stilgestaan bij de ontgrendelplicht waarbij medewerking van de verdachte is vereist. Dit levert een beantwoording op van de vraag of en zo ja, op basis van welke (toekomstige) Nederlandse wettelijke grondslag strafvorderlijke autoriteiten de medewerking van een verdachte kunnen bevelen of afdwingen tot (1) biometrische ontgrendeling en/of (2) afgifte van een code of wachtwoord ter ontgrendeling van elektronische gegevensdragers.

2.1.1 *Biometrische ontgrendeling*

Thans bestaat (nog) geen expliciete wettelijke grondslag op basis waarvan een verdachte kan worden gedwongen tot biometrische toegangsverschaffing van zijn elektronische gegevensdrager. Uit de feitenrechtspraak blijkt echter dat rechters hiernaar op zoek zijn, nu de praktijk uitwijst dat dergelijke ontgrendelverzoeken tot verdachten worden gericht.[11] Albers, Beekhuis en Taylor Parkins-Ozephius hebben in dat kader beargumenteerd dat de algemene bevoegdheid tot inbeslagneming zoals neergelegd in de artikelen 94 jo. 95 jo. 96 Wetboek van Strafvordering (Sv) – nu zij tevens dienen als grondslag voor het onderzoek *aan* de *smartphone*[12] – in dat geval de meest geschikte wettelijke grondslag vormt.[13] Opsporingsambtenaren kunnen op grond van het samenstel van deze bepalingen een verdachte – eventueel onder dreiging met, of met gebruik van, gepast geweld – dwingen tot biometrische toegangsverschaffing. In de praktijk blijkt dat de bewegingsvrijheid van de verdachte bijvoorbeeld wordt beperkt door hem te boeien, zodat zijn vinger met een proportionele geweldstoepassing op de ontgrendelknop kan worden gelegd,[14] of dat, indien een elektronische gegevensdrager is vergrendeld met een irisscan of gezichtsherkenning, het hoofd van een verdachte wordt vastgehouden en zijn oogleden met enige dwang te openen.[15] In de hiervoor beschreven scenario's wordt de elektronische gegevensdrager door de verdachte ontgrendeld, zonder dat de autoriteiten zelf de (biometrische) ontgrendelgegevens verkrijgen.

2.1.2 *Ontgrendeling via een code of wachtwoord*

Toegangsverkrijging via een code of wachtwoord vertoont gelijkenissen met het decryptiebevel[16] zoals was voorgesteld ter opname in de Wet Computercriminaliteit III.[17] In het conceptwetsvoorstel werd namelijk een bepaling voorgesteld om de verdachte te verplichten zijn elektronische gegevensdrager te ontgrendelen door het afgeven of intoetsen van zijn *pincode* of *wachtwoord* ter ontsleuteling van op elektronische gegevensdragers beschikbare gegevens. Dit werd evenwel in strijd geacht met het nemo-teneturbeginsel, waardoor dit bevel uit het conceptwetsvoorstel Computercriminaliteit III is geschrapt.[18] Thans ontbreekt in Nederland aldus een grondslag op basis waarvan een verdachte kan worden gedwongen tot het afgeven of intoetsen van een *wachtwoord* of *pincode* ter ontgrendeling van een elektronische gegevensdrager.

10 Zie voor een uitgebreide analyse van deze mogelijkheden: Van Toor 2017a, p. 3-11.

11 Vgl. Rb. Noord-Holland 14 december 2018, ECLI:NL:RBNHO:2018:11578, waarin de rechtbank stelde dat art. 3 Politiewet 2012 of art. 61a Sv mogelijk voldoende basis vormen om de biometrische toegangsverschaffing op te baseren. Zie ook Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568, *Computerrecht* 2019/94, m.nt. D.A.G. van Toor, waarin de officier van justitie (r.o. 3.4.1.2.) beargumenteerde dat de grondslag voor het bevel tot ontgrendeling aan de verdachte was gelegen in art. 61a Sv en de rechtbank beargumenteerde dat art. 94 jo. 95 jo. 96 Sv de wettelijke grondslag voor toegangsverschaffing vormen.

12 Vgl. Albers, Beekhuis & Taylor Parkins-Ozephius 2019, p. 174. Hierbij moet worden opgemerkt dat het samenstel van deze bepalingen enkel een legitieme wettelijke grondslag is in het geval de door het onderzoek aan de *smartphone* gerealiseerde inbreuk op het recht op privéleven slechts van geringe dan wel beperkte aard is. Zie ook de welbekende *Smartphone*-arresten: HR 4 april 2017, ECLI:NL:HR:2017:584, *NJ* 2017/229, m.nt. T. Kooijmans; HR 4 april 2017 ECLI:NL:HR:2017:592, *NJ* 2017/230, m.nt. T. Kooijmans.

13 Albers, Beekhuis & Taylor Parkins-Ozephius 2019, p. 180. De auteurs hebben in dit artikel onderzocht wat de meest geschikte wettelijke grondslag zou kunnen zijn. Hiertoe hebben de auteurs drie verschillende, meer algemene wettelijke grondslagen onderzocht, te weten: art. 3 Pw 2012 jo. art. 141 en 142 Sv, art. 61a Sv en tot slot art. 94 jo. 95 jo. 96 Sv.

14 Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568, *Computerrecht* 2019/94, m.nt. D.A.G. van Toor.

15 Albers, Beekhuis & Taylor Parkins-Ozephius 2019, p. 179.

16 Op het niet-meewerken aan het bevel zou een gevangenisstraf worden gesteld van ten hoogste drie jaren.

17 D.A.G. van Toor 2013, 'Het decryptiebevel en het nemo-teneturbeginsel', *NJB* 2013/385; Van Toor 2017a, p. 4; *Kamerstukken II* 2012/13, 33400, 68. Zie ook B.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Den Haag: Boom Lemma uitgevers 2012.

18 *Kamerstukken II* 2015/16, 34372, 3, p. 6, 84.

2.1.3 *De toekomstige wettelijke grondslag voor biometrische ontgrendeling*

In de praktijk blijft de biometrische vergrendeling van *smartphones* van verdachten problemen opleveren.[19] In artikel 125k van het huidige Wetboek van Strafvordering is reeds een medewerkingsverplichting tot ontsleuteling opgenomen. Dit bevel tot decryptie kan worden gericht aan degene van wie redelijkerwijs kan worden vermoed kennis te dragen van de wijze van versleuteling van deze gegevens (lid 2), maar niet aan een verdachte (lid 3). Ook kan dit bevel *niet* worden gegeven ten aanzien van een *in beslag genomen* elektronische gegevensdrager, daar deze bevoegdheid vooralsnog alleen is gericht op het onderzoek naar een – tijdens een doorzoeking van een plaats van onderzoek – aangetroffen elektronische gegevensdrager.[20]

In de consultatieversie van het conceptwetsvoorstel tot vaststelling van Boek 2 van het Wetboek van Strafvordering is in artikel 2.7.3.2.7 voorgesteld dit ontgrendelbevel te verruimen naar in beslag genomen elektronische gegevensdragers. In het verlengde daarvan wordt in de vernieuwde redactie van het artikel tevens rekening gehouden met technische ontwikkelingen op het gebied van biometrie, zoals het ontgrendelen door middel van een irisscan of vingerafdruk.[21] De commissie-Koops acht – in het kader van de modernisering van boek 2 van het Wetboek van Strafvordering – het opnemen van de bevoegdheid tot het geven van een *bevel* aan verdachten tot biometrische ontgrendeling van een elektronische gegevensdrager onwenselijk.[22] Om de problematiek rondom de biometrische toegangsverkrijging tot *smartphones* van verdachten toch het hoofd te bieden, heeft de commissie derhalve de *afgedwongen* toegangsverschaffing op bevel van een officier van justitie voorgesteld als werkbaar alternatief voor het geven van een *bevel* tot toegangsverschaffing aan een verdachte.[23]

Meer concreet houdt dit in dat de verdachte, in plaats van dat hij zelf (als gevolg van een bevel) actief moet bijdragen aan de biometrische toegangsverschaffing tot de *smartphone*, slechts (al dan niet gedwongen) passief dient te dulden dat zijn *smartphone* op biometrische wijze wordt ontgrendeld.[24] De commissie-Koops stelt dat de hiervoor reeds besproken mate van dwang die wordt gebruikt bij het forceren van de biometrische ontgrendeling (onder dwang een vinger op de sensor van de telefoon leggen, of het ooglid openen ter ontgrendeling met een irisscanner), vanwege de relatief geringe inbreuk op de lichamelijke integriteit dan ook toelaatbaar is, mits deze binnen de grenzen van proportionaliteit, subsidiariteit en artikel 3 EVRM blijft.[25]

2.1.4 *Afronding*

Kortom: een verdachte kan (vooralsnog) op grond van een algemene bevoegdheidsgrondslag, zoals de artikelen 94 jo. 95 jo. 96 Sv, worden gedwongen medewerking te verlenen aan het op biometrische wijze ontgrendelen van een elektronische gegevensdrager. Indien het conceptwetsvoorstel tot vaststelling van boek 2 van het Wetboek van Strafvordering in huidige vorm wordt aangenomen, zal de nieuwe versie van artikel 125k Sv, namelijk artikel 2.7.3.2.7, in deze bevoegdheidsgrondslag voorzien. Ook bestaat er geen wettelijke grondslag op basis waarvan een verdachte in Nederland kan worden gedwongen tot het ter ontgrendeling intoetsen of afgeven van een wachtwoord of pincode.

2.2 ***België***

Waar in Nederland de actuele discussie vooral is gericht op het op biometrische wijze ontgrendelen van elektronische gegevensdragers, ziet de discussie in België voornamelijk op het ontgrendelen met inloggegevens (zoals een wachtwoord of een pincode).[26] Sinds 2001 zijn in het Belgische Wetboek van Strafvordering (hierna: BSv) in artikel 88*quater* een informatieverplichting (§ 1) en een medewerkingsverplichting (§ 2) opgenomen.[27] Paragraaf 3 bevat vervolgens de strafbaarstelling voor het niet-meewerken aan de in paragraaf 1 en 2 opgenomen verplichtingen. De invoering van dit artikel was onderdeel van een wetswijziging die volgens de memorie van toelichting beoogde adequate juridische instrumenten te verschaffen tegen computercriminaliteit.[28]

19 Commissie Koops 2018, p. 105-106, 198.

20 Vgl. de consultatieversie van het conceptwetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering art. 2.7.3.2.7, p. 35.

21 Omdat – zoals ook te lezen is in het conceptwetsvoorstel bij art. 2.7.3.2.7 – niet te voorzien is welke wijzen van biometrische vergrendeling in de toekomst mogelijk zijn, is het bijgevolg ook niet te voorzien wat de mate van inbreuk op de persoonlijke levenssfeer van de betrokkene is die dit op kan leveren. Om die reden is ervoor gekozen enkel deze twee wijzen van ontgrendeling onder de reikwijdte van deze bepaling te laten vallen.

22 Vgl. Commissie Koops 2018, p. 105-106. Het niet-meewerken aan een dergelijk bevel is in dat geval strafbaar op grond van art. 184 Sr. Derhalve acht de commissie het risico dat verdachten de drie maanden gevangenisstraf (voor het overtreden van art. 184 Sr) verkiezen boven de mogelijk veel hogere gevangenisstraf die verdachten door het ontsluiten van het bewijsmateriaal op de smartphone boven het hoofd hangt, groot.

23 Commissie Koops 2018, p. 106.

24 Vgl. Commissie Koops 2018, p. 107-108, 198.

25 Commissie Koops 2018, p. 105-106, 198.

26 Zie onder andere: C. Conings & N. Wagemans, 'Uiteenlopende rechtspraak over de ontsleutelplicht en het non-incriminatiebeginsel', *Computerrecht* 2018/103, afl. 2, p. 124-125; K. de Schepper, 'Toegangscode is wilsonafhankelijk bewijsmateriaal', *Computerrecht* 2018/248, afl. 5, p. 306-307; K. de Schepper, 'Opnieuw veroordeling voor schending medewerkingsplicht', *Computerrecht* 2018/283, afl. 6, p. 382; C. Conings, 'De ontsleutelplicht: hof van beroep stelt prejudiciële vraag – rechtbank blijft overtuigd', *Computerrecht* 2019/126, afl. 3, p. 226-227; C. Conings, 'De ontsleutelplicht: uiteenlopende rechtspraak', *Computerrecht* 2019/171, afl. 4, p. 307-308; C. van de Heyning, 'Het zwijgrecht in digitale tijden: de strijd om decryptiesleutels naar het Grondwettelijk Hof', *T.Strafr.* 2019 (6), p. 307-319.

27 Art. 88*quater* BSv is onderverdeeld in paragrafen en de paragrafen zijn onderverdeeld in ongenummerde leden.

28 *Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, p. 3.

Blijkens paragraaf 1 van bovengenoemde bepaling kan een onderzoeksrechter *eenieder* van wie hij vermoedt dat hij bijzondere kennis van een informatiesysteem heeft, bevelen inlichtingen te verstrekken over de wijze waarop toegang kan worden verkregen tot dit informatiesysteem.[29] Uit de memorie van toelichting blijkt dat hierbij vooral werd gedacht aan informatie over toegangsmogelijkheden, configuratie, beveiliging en cryptografische sleutels.[30] Op grond van deze paragraaf kan een pincode worden verkregen waarmee een vergrendelde *smartphone* ontgrendeld kan worden, indien de onderzoeksrechter aannemelijk kan maken dat de verdachte deze toegangscode weet, door bijvoorbeeld aan te tonen dat de verdachte de gebruiker is van de telefoon.

Deze informatieverplichting kan dus – in tegenstelling tot de hierna te bespreken medewerkingsverplichting – ook aan een verdachte worden opgelegd, nu paragraaf 1 spreekt over *eenieder*. Verder ontbreekt ieder voorbehoud in de bepaling. Immers, het bevel tot medewerking uit artikel 88*quater* § 2 BSv kan ingevolge het tweede lid van paragraaf 2 niet aan de verdachte en zijn familieleden worden gegeven. Deze exceptie verwijst specifiek naar het eerste lid van paragraaf 2 en geldt daardoor niet voor de informatieverplichting uit de eerste paragraaf. De uitzondering dat de medewerking van een verdachte niet kan worden bevolen, geldt volgens de memorie van toelichting omdat de verdachte hier zijn zwijgrecht moet kunnen laten gelden.[31] Uit de memorie van toelichting volgt dat dit voorbehoud expliciet niet geldt voor de informatieverplichting uit § 1 aangezien wordt gesteld dat de informatieverplichting verenigbaar is met de eisen van het EVRM inzake bescherming tegen gedwongen zelfincriminatie.[32]

Uit het verschil in bewoordingen – bevelen inlichtingen te verschaffen en bevelen het systeem te bedienen – tussen de informatieverplichting uit artikel 88*quater* § 1 BSv en de medewerkingsverplichting uit § 2 van dat artikel kan worden opgemaakt dat de verdachte niet kan worden bevolen zelf zijn telefoon te ontgrendelen door het intypen van zijn pincode, nu dit zou vallen onder het bedienen van het systeem en dus onder de medewerkingsverplichting. De verdachte kan enkel worden gedwongen tot het verschaffen van inlichtingen over de wijze waarop zijn *smartphone* is beveiligd, waardoor hij gedwongen kan worden tot het opschrijven of uitspreken van zijn pincode. Wij laten verder onbesproken dat dit een gekunstelde tweedeling is.

Het niet-meewerken aan deze informatieverplichting en medewerkingsverplichting is op grond van § 3 strafbaar gesteld en kan leiden tot een gevangenisstraf van zes maanden tot drie jaar en een geldboete van € 26 tot € 20.000. Het niet-meewerken aan een van beide verplichtingen terwijl medewerking de uitvoering van een wanbedrijf[33] of misdaad kan verhinderen, of de gevolgen ervan kan beperken, is ingevolge lid 2 een strafverzwarende omstandigheid. De strafbedreiging is in een dergelijk geval een gevangenisstraf van één tot vijf jaar en een geldboete van € 500 tot € 50.000. Deze sanctionering heeft als doel de afdwingbaarheid van deze verplichtingen te garanderen.[34]

2.3 *Duitsland*

Ook in Duitsland bestaat politieke aandacht voor de toegang tot gegevens die zich achter een vergrendeling bevinden en de haalbaarheid van een medewerkingsverplichting om de toegang tot die gegevens mogelijk te maken. Met het conceptwetsvoorstel *IT-Sicherheitsgesetz 2.0* – vergelijkbaar met de Wet Computercriminaliteit in Nederland – heeft de Duitse regering begin 2019 een tweede wetsvoorstel voorbereid die het materiële en formele straf-(proces)recht moet wijzigen vanuit de noodzaak om beter op *cybercrime* te kunnen reageren.[35] Met de *IT-Sicherheitsgesetz 2.0* worden wijzigingen in allerlei Wetboeken voorgenomen, waaronder de StPO (het Duitse Wetboek van Strafvordering). Een van de wijzigingen is de nieuw in het StPO in te voegen §[36] 163g, dat enkel nog in concept voorligt. Tegen dit concept is al enig verzet geuit door de rechtspraktijk[37] en de media.[38] Al hetgeen hieronder wordt besproken betreft dus een conceptwetsvoorstel, waarvan nog geen parlementaire behandeling heeft plaatsgevonden en waarbij geen uitvoerige memorie van toelichting is gepubliceerd. Hoe dan ook, de Duitse regering zet – net zoals het later verwijderde decryptiebevel in het conceptwetsvoorstel Computercriminaliteit III – in op het verkrijgen van wachtwoorden. Een van de redenen daarvoor is dat in de praktijk al regelmatig wachtwoorden worden verkregen onder 'vrijwillige' medewerking en zonder wettelijke grondslag in ruil voor strafvermindering.[39] Met het nieuwe § 163g StPO wordt deze praktijk dus gelegitimeerd.

29 Daarnaast heeft de onderzoeksrechter ook de mogelijkheid om opdracht hiertoe te geven aan de verschillende actoren die in deze bepaling worden genoemd.

30 *Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, p. 27.

31 *Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, p. 27.

32 *Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, p. 27.

33 In het Belgische strafrecht bestaan drie soorten strafbare feiten, van minst naar meest ernstig: overtredingen, wanbedrijven en misdaden.

34 *Parl. St.*, Kamer, 1999-2000, DOC 50-0213/001 en DOC 50-0214/001, p. 26.

35 De tekst kan (in het Duits) hier worden geraadpleegd: https://intrapol.org/wp-content/uploads/2019/04/IT-Sicherheitsgesetz-2.0-_-IT-SiG-2.0.pdf, laatst geraadpleegd op 19 maart 2020.

36 In het Duitse recht is het woord 'artikel' voorbehouden aan bepalingen uit de Grondwet. Bepalingen uit andere wetten worden paragraaf genoemd en afgekort met §.

37 A. Oehmichen & B. Weißenberger, 'Digitaloffensive im Strafrecht! Verbesserte Bekämpfung von Cyberkriminalität durch das IT-Sicherheitsgesetz 2.0?', *KriPoz* 2020/1.

38 https://www.sueddeutsche.de/digital/passwort-it-sicherheit-gesetz-seehofer-beugehaft-gefaengnis-1.4401627, laatst geraadpleegd op 20 maart 2020.

39 § 46b StGB: in het Duitse materiële strafrecht is bepaald dat het gedrag van de verdachte tijdens de opsporing mee moet worden gewogen bij de strafbepaling.

De eerste volzin van de voorgestelde paragraaf stelt een aantal beperkingen aan de toepassing van de bevoegdheid. Ten eerste is de bevoegdheid beperkt tot het overnemen van een *virtuele identiteit* en alle daarbij behorende functies (waaronder de chatfunctie, zie volzin 2) en is daarmee *prima facie* beperkter dan een ontgrendelplicht van een elektronische gegevensdrager, omdat in dat geval toegang wordt verkregen tot de gehele inhoud van de gegevensdrager. Ten tweede moet de virtuele identiteit verbonden zijn aan een account dat de verdachte heeft bij een *Telekommunikations- oder Telemediendienstes*, waarvoor een wettelijke definitie te vinden is in respectievelijk § 3 onder 6 *Telekommunikationsgesetz* en § 2 onder 1 *Telemediengesetz*. In die bepalingen gaat het om commerciële (ondersteunende) dienstverleners in de telecommunicatiebranche (*Telekommunikation*) en (andere) elektronische informatie- en communicatiediensten (*Telemedien*). Ten derde kan § 163g StPO alleen worden toegepast bij de limitatief in § 100g lid 1 juncto § 100a lid 2 StPO opgenomen misdrijven.

Hieronder vallen twee categorieën delicten: (i) delicten die met behulp, of gebruikmaking van (tele)communicatie zijn begaan, zonder nadere begrenzing in de strafmaat (Oehmichen en Weißenberger geven het voorbeeld van een eenvoudige belediging via een chatbox, waarbij deze verstrekkende bevoegdheid kan worden ingezet omdat het delict is begaan met gebruik van een communicatiedienst);[40] of (ii) ernstige misdrijven zoals genoemd in § 100a lid 2 StPO, zonder dat deze delicten zijn begaan in verband met (tele)communicatie. Onder de laatste categorie vallen onder andere levensdelicten, geweldsmisdrijven, opiumwetmisdrijven en vermogensdelicten. Een *verband* tussen de virtuele identiteit en de verdenking is dus niet altijd nodig (categorie-ii-delicten). Hierdoor brengt de bepaling ook geen beperking aan in de over te nemen virtuele identiteiten: *alle* virtuele identiteiten van een verdachte kunnen worden overgenomen als is voldaan aan de criteria.[41]

In de derde volzin wordt bepaald dat deze bevoegdheid ook tegen de wil van de verdachte kan worden gebruikt, en dat de verdachte de toegangsinformatie prijs *moet* geven. De weigering kan worden bestraft met een geldboete en gijzeling (zoals wij die kennen bij weigerachtige getuigen) (§ 70 StPO). De gijzeling kan op grond van § 70 StPO juncto § 95 StPO maximaal zes maanden duren, maar wordt eerder opgeheven als de verdachte zwicht en de informatie prijsgeeft tijdens de gijzeling.

In de vijfde volzin wordt een belangrijke rechtsbeschermende voorwaarde opgenomen. De via deze bevoegdheid verkregen bewijsmiddelen kunnen alleen dan tegen de verdachte worden gebruikt als hij daarvoor toestemming geeft. De precieze betekenis van deze volzin, alsmede hoe deze volzin past bij de Duitse uitleg van het recht om niet gedwongen mee te hoeven werken aan de eigen veroordeling, wordt in paragraaf 3.4 besproken.

Afwezig als toepassingscriteria, die meestal wel bij andere vergaande Duitse opsporingsbevoegdheden te vinden zijn, zijn de proportionaliteit en noodzakelijkheid. De afwezigheid van deze begrenzing is ook te zien in de ongelimiteerde overname van *alle* virtuele identiteiten van een verdachte, zonder dat deze identiteiten te linken zijn aan het delict waarvoor de verdenking bestaat. Dit wekt des te meer verbazing omdat in de korte toelichting op § 163g StPO vooral het belang van deze bevoegdheid voor de ontmanteling van *darknet*-activiteiten wordt gestipuleerd,[42] maar de beperking van de inzet van deze bevoegdheid voor *enkel* die delicten niet in de concepttekst is opgenomen.

Oehmichen en Weißenberger bekritiseren ook de afwezigheid van een rechterlijke toets – de bevoegdheid kan door alle opsporingsambtenaren worden uitgevoerd – en de afwezigheid van de (absolute) *Kernbereichsschutz*.[43] De bescherming van de privésfeer in het Duitse recht is ingedeeld in drie te beschermen gebieden – de sferentheorie: bestaande uit de sociale, de private en de intieme sfeer – die naargelang de gevoeligheid van de daar aan te treffen informatie meer (de private sfeer) of absolute (de intieme sfeer) bescherming genieten.[44] Met het overnemen van een virtuele identiteit en de daaraan gekoppelde chatfunctie kunnen de autoriteiten, bijvoorbeeld als de virtuele identiteit op een datingwebsite wordt overgenomen, toegang krijgen tot de intieme sfeer. Met andere woorden, met deze, naar Duits recht, atypische bevoegdheid kunnen de autoriteiten de verdachte dwingen alle toegangsgegevens van alle virtuele identiteiten over te dragen, waarna de autoriteiten de virtuele identiteiten volledig over kunnen nemen.

2.4 *Vergelijking en conclusie*

Ondanks dat het doel van de drie hierboven beschreven regelingen (min of meer) gelijk is,[45] is de uitwerking van de voorwaarden waaronder een ontgrendelplicht wordt ingezet verschillend. De Nederlandse wetgever acht het geven van een bevel aan een verdachte tot het afgeven of intoetsen van een *wachtwoord* of *pincode* ter ontgrendeling van een elektronische gegevensdrager in strijd met

40 Oehmichen & Weißenberger 2020, par. III.4.
41 Oehmichen & Weißenberger 2020, par. III.4.
42 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), p. 86-87.
43 Oehmichen & Weißenberger 2020, par. III.4.
44 Zie uitvoerig M. Lindemann & D.A.G. van Toor, 'Protection of a Suspect's Privacy in Criminal Procedures: Does the Conceptual Approach of the German Federal Constitutional Court Make a Difference?', *AA* 2018, 5, p. 376-384.
45 Namelijk het bemachtigen van toegang tot elektronische gegevensdragers of virtuele identiteiten ten behoeve van de opsporing van (cyber)criminaliteit, zodat de autoriteiten de beschikking verkrijgen over aan de gegevensdrager of identiteit gekoppelde informatie.

het nemo-teneturbeginsel. Daar staat tegenover dat de biometrische ontgrendeling van een elektronische gegevensdrager in de lagere rechtspraak is geaccepteerd (terwijl de wettelijke grondslag daarvan, totdat het nieuwe Wetboek van Strafvordering in werking treedt, onduidelijk is), maar ook hierover bestaat discussie in de literatuur.[46]

Hierdoor bestaat een duidelijk verschil met onze buurlanden. In België en Duitsland kunnen verdachten, kort gezegd, onder omstandigheden wel worden gedwongen *inloggegevens* aan de autoriteiten te overhandigen. In België kan het daardoor verkregen bewijs op de elektronische gegevensdrager worden gebruikt in een strafrechtelijke procedure, terwijl in Duitsland is gekozen voor bewijsuitsluiting van de bewijzen die zijn verkregen via een aan de verdachte gerichte ontgrendelplicht. In Duitsland is de bevoegdheid ook op een andere wijze verder begrensd: de ontgrendelplicht is bedoeld voor virtuele identiteiten (en alle functies die daarmee te besturen zijn). Met de Belgische en Nederlandse ontgrendelplicht verkrijgen de autoriteiten toegang tot gegevens die zijn gekoppeld aan een gegevensdrager. Of hierdoor een daadwerkelijk verschil ontstaat, is onduidelijk. Als bijvoorbeeld alle gegevens van een *smartphone* in een *cloud* zijn opgeslagen en verdachtes virtuele identiteit kan worden gebruikt om in de *cloud* in te loggen, dan verkrijgen de Duitse autoriteiten ook alle informatie die verkregen zou worden door de ontgrendeling van een apparaat.

3. Het verplicht ontgrendelen van elektronische gegevensdragers vanuit rechtsbeschermend perspectief

Een van de belangrijkste kritiekpunten die in alle drie de landen wordt geuit, is dat de ontgrendelplicht op gespannen voet staat met het nemo-teneturbeginsel. Doordat de verdachte zijn elektronische gegevensdrager of virtuele accounts moet ontgrendelen, verkrijgen de autoriteiten toegang tot zijn volledige elektronische voetafdruk. Aangezien de verdachte zelf het apparaat of het account moet ontgrendelen, kan *prima facie* het idee ontstaan dat die handeling een schending is van het beginsel dat iemand niet mee hoeft te werken aan zijn eigen veroordeling. In deze paragraaf wordt dit voor de drie in deze bijdrage behandelde rechtsordes getoetst. Daarvoor wordt eerst aandacht besteed aan de rechtspraak van het Europese Hof voor de Rechten van de Mens (hierna: het EHRM), omdat het veelvuldig arresten heeft gewezen over het toepassingsbereik van het nemo-teneturbeginsel.

3.1 *De rechtspraak van het EHRM*

Het *Saunders*-arrest is in de literatuur over het nemo-teneturbeginsel waarschijnlijk de meest aangehaalde uitspraak. Het is echter juist dit arrest, en dan met name rechtsoverweging 69, dat tot veel verwarring heeft geleid over de reikwijdte en inhoud van het nemo-teneturbeginsel.[47] De kern van genoemde rechtsoverweging wordt gevormd door het criterium 'bewijs dat (on)afhankelijk van de wil bestaat' en bij de interpretatie van het arrest is hier dan ook veel aandacht aan besteed.

Kort gezegd, kwam de consensus over de interpretatie van deze rechtsoverweging op het volgende neer: (1) bewijs dat afhankelijk van de wil bestaat, waarvoor een bewuste spierbeweging noodzakelijk is, valt onder de bescherming van het beginsel; (2) materiaal dat onafhankelijk van de wil bestaat, waarover een mens met *enkel* zijn wil of zijn gedachten geen controle heeft, valt *niet* onder de bescherming van het beginsel.[48] Het verschil tussen deze twee soorten bewijsmiddelen wordt bepaald aan de hand van de vraag of het bewijs al (in fysieke zin) bestaat of dat het nog moet worden geproduceerd. Als iets bestaat, bijvoorbeeld een document in een kluis, dan is dat bewijsstuk niet onderhevig aan verandering of vernietiging *enkel* door middel van de wil van een persoon. Dit is anders voor bewijs dat nog niet bestaat, zoals het gesproken woord of een te schrijven tekst.[49] Hiervoor is bewust, gewild en gepland gedrag nodig en een verklaring of geschreven tekst komt alleen 'tot leven' als de verdachte dat wil. Zoals hierboven beschreven, valt volgens de consensus het bewijs dat onafhankelijk van de wil bestaat *niet* onder de bescherming van het nemo-teneturbeginsel en bewijs dat afhankelijk van de wil bestaat wel. Dat deze uitleg destijds aan *Saunders* is gegeven, is gezien het arrest *Funke*[50] al verwonderlijk, maar is absoluut in strijd met de *post-Saunders*-jurisprudentie.

In het arrest *Funke*, dat een aantal jaar *voor Saunders* is gewezen, werden namelijk documenten gevorderd op last van een dwangsom. Deze documenten zijn in het verleden geproduceerd. Dat betekent voor het heden dat documenten onafhankelijk van de wil bestaan, aangezien een persoon met *enkel* zijn bewustzijn of gedachten het bestaan van papier niet kan controleren of beïnvloeden. Hoe hard iemand ook probeert om documenten (letterlijk) weg te denken, dat gaat hem nooit lukken (tenzij hij over onwaarschijnlijke paranormale gaven beschikt). In de hierboven weergegeven uitleg van het *Saunders*-criterium zou Funke niet worden beschermd onder het nemo-teneturbeginsel. Toch werd in *Funke* een schending van het nemo-teneturbeginsel aangenomen, omdat de overdracht van

46 Zie bijv. Bood 2018.

47 D.A.G. van Toor, *Het schuldige geheugen?* (diss. RUN), Deventer: Wolters Kluwer 2017, p. 370 e.v.

48 Zie voor een dergelijke uitleg van het *Saunders*-criterium: T. Ward & P. Gardner, 'The privilege against self incrimination: in search of legal certainty', *EHRLR* 2003, 4, p. 392; A. Andreangeli, *EU Competition Enforcement and Human Rights*, Cheltenham: Edward Elgar Publishing 2008, p. 138; EHRM 17 december 1996, *NJ* 1997, 699, m.nt. Knigge, punt 4 (*Saunders/het Verenigd Koninkrijk*).

49 D.A.G. van Toor, 'Het nemo-teneturbeginsel in de conceptwetsvoorstellen van het Wetboek van Strafvordering', *TBS&H* 2018, 4, p. 249-254.

50 EHRM 25 februari 1993, appl. no. 10828/84 (*Funke/Frankrijk*).

documenten werd gevorderd waarvan het bestaan onduidelijk was (*fishing expedition*). De zaak *J.B.*,[51] die enkele jaren *na Saunders* werdgewezen, vertoont qua feiten grote gelijkenis met *Funke*. Ook daar werden documenten gevorderd en moest J.B. boetes betalen voor het niet-verschaffen van inlichtingen en nam het EHRM (ondanks dat sprake was van materiaal dat onafhankelijk van de wil van de verdachte bestaat)[52] een schending van het nemo-teneturbeginsel aan. Wat het geheel nog complexer maakt, is dat het EHRM een schending van het nemo-teneturbeginsel heeft aangenomen in een zaak waar het ging om bewijs dat onafhankelijk van de wil bestaat (*Jalloh*[53]) en *geen* veroordeling heeft uitgesproken in zaken waarin het materiaal betrof dat afhankelijk van de wil bestaat (*O'Halloran & Francis*,[54] *Khan*[55] & *Bykov*[56]). Hierdoor lijkt niet het *Saunders*-criterium – de vraag of het verkregen bewijsmateriaal (on)afhankelijk van de wil bestaat – bepalend of leidend bij de beoordeling, maar de toets die vooral in de *post-Saunders*-jurisprudentie is geformuleerd.

Latere EHRM-rechtspraak, onder andere *Jalloh*, *O'Halloran & Francis* en *Ibrahim en anderen*, maken duidelijker wat volgens het EHRM onder de reikwijdte van het nemo-teneturbeginsel valt. Uit deze rechtspraak blijkt dat het EHRM een drietal criteria gebruikt om te toetsen of een bepaalde overheidshandeling het nemo-teneturbeginsel schendt. Dit zijn: (1) de mate en aard van *dwang* die werd gebruikt om het bewijs te verkrijgen; (2) relevante *waarborgen* in de procedure; en (3) de manier waarop het bewijs wordt *gebruikt*.[57] Hierin wordt de aard van het bewijs niet als toetsingscriterium genoemd, maar wel de aard en mate van *dwang*. Het nemo-teneturbeginsel is derhalve *means based*. Het beschermt tegen *bepaalde wijzen van verkrijging* van bewijsmateriaal.

In 2016 heeft de Grote Kamer van het EHRM het volgende overzicht opgesteld met betrekking tot ongeoorloofde dwang. Gezien het belang en de duidelijkheid van die overweging wordt die hier weergegeven: 'The Court, through its case-law, has identified at least three kinds of situations which give rise to concerns as to improper compulsion in breach of Article 6. The first is where a suspect is obliged to testify under threat of sanctions and either testifies in consequence (…) or is sanctioned for refusing to testify (…). The second is where physical or psychological pressure, often in the form of treatment which breaches Article 3 of the Convention, is applied to obtain real evidence or statements (…). The third is where the authorities use subterfuge to elicit information that they were unable to obtain during questioning (…) (onze onderstreping)'.[58] Een vorm van ongeoorloofde dwang is een noodzakelijke voorwaarde voor een schending van het nemo-teneturbeginsel, waarbij het EHRM in de hierboven geciteerde overweging de drie voorbeelden op een rij heeft gezet die tot op heden in de rechtspraak van het Hof als ongeoorloofde dwang zijn gecategoriseerd.

De relevante waarborgen kunnen er echter voor zorgen dat dwang – die in beginsel ongeoorloofd zou zijn – toch geoorloofd is. Een voorbeeld daarvan kan worden gevonden in de zaak *Van Weerelt*.[59] Blijkens deze zaak is een voldoende effectieve waarborg tegen 'improper compulsion' dat wilsafhankelijk materiaal wel kan worden afgedwongen met het oog op een juiste belastingheffing, mits deze informatie niet ook voor fiscale beboeting of strafvervolging wordt gebruikt.[60]

Samenvattend is dus pas sprake van een schending van het nemo-teneturbeginsel volgens de rechtspraak van het EHRM als de autoriteiten (i) ongeoorloofde dwang gebruiken ter verkrijging van het bewijs, terwijl er (ii) geen relevante waarborgen tegen deze voor de verdachte nadelige verkrijging bestaat en (iii) het verkregen bewijs tegen hem in een strafzaak wordt gebruikt.

3.2 *Nederland*

Zoals beschreven bestaan er tot op heden twee verschillende mogelijkheden[61] op basis waarvan een elektronische gegevensdrager kan worden ontgrendeld, namelijk door middel van: (1) het invoeren van een pincode of wachtwoord en (2) een biometrische ontgrendeling. In § 2.1 is reeds besproken dat de Nederlandse wetgeving niet voorziet in een grondslag op basis waarvan een verdachte kan worden bevolen of gedwongen tot het afgeven of intoetsen van een *wachtwoord* of *pincode* ter ontgrendeling van een *smartphone*. Dit heeft alles te maken met het feit dat de wetgever een dergelijke bevoegdheid in strijd acht met het nemo-teneturbeginsel.[62] Een pincode

51 EHRM 3 mei 2001, appl. no. 31827/96 (*Jalloh/Zwitserland*).
52 Overigens overweegt de tweede sectie van de Kamer van het Hof in rechtsoverweging 68 over 'materiaal dat onafhankelijk van de persoon bestaat'. Deze term, waarin 'onafhankelijk van *de wil van de verdachte* bestaand materiaal' wordt vervangen door 'onafhankelijk van *de persoon* bestaand materiaal' komt in geen enkel ander arrest of ontvankelijkheidsbeslissing terug, terwijl de Grote Kamer zich daarna consequent houdt aan de in *Saunders* geïntroduceerde terminologie. Ik ga ervan uit dat met 'de persoon' hetzelfde wordt bedoeld als met 'de wil van de verdachte'. Zowel de persoon als entiteit als de wil van een verdachte heeft als zodanig geen controle over het al dan niet bestaan van een document. Anders B.J. Koops & L. Stevens, 'J.B. versus Saunders. De groeiende duisternis rond nemo tenetur', *DD* 2003, 33 (3), p. 292-293.
53 EHRM (GK) 11 juli 2006, appl. no. 54810/00 (*Jalloh/Duitsland*).
54 EHRM (GK) 29 juni 2007, appl. nos. 15809/02 en 25624/02 (*O'Halloran & Francis/het Verenigd Koninkrijk*).
55 EHRM 12 mei 2000, *NJ* 2002, 180; appl. no. 35394/97 (*Khan/het Verenigd Koninkrijk*).
56 EHRM 10 maart 2009, appl. no. 4378/02 (*Bykov/Rusland*).
57 EHRM 29 juni 2007, appl. nos. 15809/02 en 25624/02, par. 55 (*O'Halloran & Francis/het Verenigd Koninkrijk*). Zie over dit toetsingskader Van Toor 2017b, p. 410-413.
58 EHRM 13 september 2016, appl. nos. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim e.a./het Verenigd Koninkrijk*).
59 EHRM 16 juni 2015, appl. no. 784/14 (*Van Weerelt/Nederland*) (beslissing).
60 HR 12 juli 2013, ECLI:NL:HR:2013:BZ3640, r.o. 3.9; EHRM 16 juni 2015, appl. no. 784/14, par. 66 (*Van Weerelt/Nederland*) (beslissing).
61 De mogelijkheden tot ontgrendeling door middel van medewerking van een derde daargelaten.
62 *Kamerstukken II* 2015/16, 34372, 3, p. 6 en 84; Commissie Koops 2018, p. 105.

of wachtwoord bestaat – indien deze niet elders is opgeslagen – afhankelijk van de wil van de verdachte. Om dit wilsafhankelijke materiaal te verkrijgen is een actieve bijdrage van de verdachte vereist in de vorm van een gewilde spierbeweging.[63] Derhalve valt dit materiaal binnen de reikwijdte van het nemo-teneturbeginsel. Dit beginsel is zoals reeds besproken *means based* en biedt bescherming tegen bepaalde wijzen van verkrijging van bewijsmateriaal.[64] Dat betekent in het geval van wilsafhankelijk materiaal dat elke mate van dwang[65] ter verkrijging ervan schending van het nemo-teneturbeginsel oplevert en dus onrechtmatig is, indien het verkregen materiaal als bewijs in een strafzaak tegen de verdachte wordt gebruikt.[66]

Het nemo-teneturbeginsel biedt, vanwege het *means based*-karakter, in bepaalde gevallen ook bescherming tegen het met dwang verkrijgen van wilsonafhankelijk materiaal van de verdachte.[67] Vingerafdrukken en een scan van de iris of het gelaat zijn bij uitstek voorbeelden van wilsonafhankelijk materiaal,[68] daar zij al in fysieke zin bestaan en de wil van de verdachte geen noodzakelijke schakel[69] is voor de verkrijging ervan. De vraag is dus of de wijze waarop de verkrijging van dit materiaal ter ontgrendeling van een *smartphone* in Nederland is of zal worden geregeld, onder de bescherming van het nemo-teneturbeginsel valt, waarbij de aard en mate van dwang ter verkrijging van het wilsonafhankelijk materiaal bepalend zijn.

De huidige (op basis van de artikelen 94 jo. 95 jo. 96 Sv) en (mogelijk) toekomstige bevoegdheid (artikel 2.7.3.2.7 Sv) komen in de kern op hetzelfde neer, namelijk een *afgedwongen* toegangsverschaffing. Dit houdt in dat de verdachte moet dulden dat zijn elektronische gegevensdrager wordt ontgrendeld met een biometrisch kenmerk. De bevoegdheid tot *afgedwongen* toegangsverschaffing zal ertoe leiden dat het biometrische materiaal van de verdachte buiten diens wil om wordt verkregen.

Ter verkrijging van wilsonafhankelijk materiaal mag, ingevolge de Straatsburgse jurisprudentie, een bepaalde mate van dwang worden uitgeoefend, mits deze blijft binnen de grenzen van de beginselen van proportionaliteit, subsidiariteit en artikel 3 EVRM. Daarbij is het van belang dat de wil van de verdachte om geen actieve bijdrage te leveren aan het vergaren van de informatie wordt gerespecteerd.[70] Deze wil van de verdachte wordt, in tegenstelling tot een bevoegdheidsgrondslag op basis waarvan een opsporingsambtenaar een *bevel* kan geven tot ontgrendeling (actief), in onze ogen gerespecteerd bij de bevoegdheid tot het afdwingen van toegangsverschaffing (passief). De verdachte hoeft in het laatste geval zijn wil om zelf de gegevens niet te verstrekken immers niet te herzien.[71] Daarnaast maakt het onder dwang vasthouden van een vinger of openen van de oogleden geen substantiële inbreuk op de lichamelijke integriteit van een verdachte en zal het (in beginsel) niet leiden tot een schending van artikel 3 EVRM. Ook brengt het onder dwang vasthouden van een vinger of het openen van de oogleden geen significante risico's met zich mee voor de gezondheid van de verdachte.[72] Tevens is van belang dat de hiervoor beschreven mate van dwang ter verkrijging van de biometrische gegevens niet significant hoger is dan het met dwang afnemen van bloed, urine en lichaamsweefsel.[73] Derhalve vallen de wilsonafhankelijke biometrische gegevens die worden verkregen door middel van een (passief) *afgedwongen toegangsverschaffing*, gezien de geringe dwang die wordt toegepast, niet binnen de reikwijdte van het nemo-teneturbeginsel, met als gevolg dat ook van een schending van het voornoemde beginsel geen sprake zal zijn.

Dit moge (intuïtief) enige bevreemding opwekken. In *Jalloh* werd veel lichamelijke dwang gebruikt – het met geweld, door vier agenten, vastpinnen van de verdachte zodat via zijn neus braakmiddel kan worden toegediend – terwijl weinig informatie werd verkregen: namelijk dat de verdachte 0,2 gram cocaïne in zijn bezit had. Bij een biometrische ontgrendeling wordt slechts in zeer beperkte mate een inbreuk op de fysieke integriteit gemaakt, terwijl gigabytes of terabytes aan informatie wordt verkregen. Dat het EHRM in *Jalloh* tot een schending van het nemo-teneturbeginsel komt, en naar onze inschatting bij een biometrische ontgrendeling niet, is te verklaren vanuit het *means based*-perspectief – de dwang in *Jalloh* is significant hoger – maar biedt gezien de hoeveelheid informatie weinig rechtsbescherming.

3.3 *België*

Waar de Nederlandse situatie stabiel en duidelijk is, was de rechtspraak over artikel 88*quater* § 1 BSv wispelturig.[74]

63 S.L.T.J. Ligthart, 'Het recht tegen zelfincriminatie ex art. 6 EVRM. Doorwerking van het nemo tenetur-beginsel in enkele gedachte-experimenten volgens de benadering van het EHRM en van de Hoge Raad', *DD* 2019/16, p. 221.

64 Zie § 3.1.

65 Uitzonderingen zoals in het geval van EHRM 16 juni 2015, appl. no. 784/14 (*Van Weerelt/Nederland*) (beslissing), par. 66 en EHRM 29 juni 2007, appl. nos. 15809/02 en 25624/02 (*O'Halloran en Francis/Groot-Brittannië*) daargelaten.

66 Van Toor 2017a, p. 5; Ligthart 2019, p. 220.

67 EHRM 11 juli 2006, appl. no. 54810/00 (*Jalloh/Duitsland*).

68 Commissie Koops 2018, p. 105.

69 L. Stevens, *Het nemo-teneturbeginsel in strafzaken: van zwijgrecht naar containerbegrip* (diss. Tilburg), Nijmegen: *WLP* 2005, p. 158; Ligthart 2019, p. 222.

70 Ligthart 2019, p. 232.

71 Ligthart 2019, p. 222.

72 Zoals wel het geval was in EHRM 11 juli 2006, appl. no. 54810/00 (*Jalloh/Duitsland*), par. 114.

73 Ligthart (2019, p. 223) stelt dat de rechtspraak van het EHRM in de zaak *Jalloh* de suggestie wekt dat het recht tegen zelfincriminatie ook van toepassing kan zijn op het afdwingen en gebruiken van wilsonafhankelijk materiaal, indien de mate van dwang significant hoger is dan bij het met dwang afnemen van bloed, urine en/of lichaamsweefsel.

74 Zie bijvoorbeeld de bespreking van twee zaken van het Hof van Beroep te Gent in C. Conings 2019a, p. 307-308; Zie hierover ook: Conings & Kerkhofs, 'U hebt het recht te zwijgen. Uw login kan en zal tegen u worden gebruikt? Over ontsleutelplicht, zwijgrecht en *nemo tenetur*', *Nullum Crimen* 2018, p. 457-472.

De in de inleiding genoemde uitspraken van februari 2020 van het Hof van Cassatie van België (hierna: Hof van Cassatie) en het Grondwettelijk Hof hebben tot eenheid geleid, aangezien uit beide uitspraken volgt dat de informatieverplichting uit artikel 88*quater* § 1 BSv aan een verdachte kan worden opgelegd.[75]

Het grootste twistpunt in de Belgische discussie is de status van de pincode als wils(on)afhankelijk. Het Grondwettelijk Hof laat, na een korte bespreking van de EHRM-zaken, in het midden of de pincode wilsonafhankelijk materiaal is.[76] Het Hof van Cassatie gaat hier, zonder bespreking van de jurisprudentie, wel op in en stelt dat de toegangscode onafhankelijk van de wil bestaat, aangezien de code onveranderd blijft, ongeacht de mededeling ervan.[77] Daarnaast komt de code volgens het Hof van Cassatie in aanmerking voor onmiddellijke controle en daardoor bestaat geen risico op onbetrouwbaar bewijsmateriaal.[78]

Royer en Yperman stellen (onzes inziens terecht) dat deze redenering leidt tot de conclusie dat er bijna geen wilsafhankelijk materiaal meer bestaat.[79] Daardoor wordt ook de beoogde bescherming van het nemo-teneturbeginsel uitgehold.[80] Het Hof van Cassatie lijkt zich vooral te baseren op het *Saunders*-criterium en niet op de latere invulling van de toets of een overheidshandeling het nemo-teneturbeginsel schendt. Ook het zwijgrecht blijft onbesproken, terwijl het verschaffen van de pincode zal plaatsvinden door een gesproken of geschreven verklaring. Het bevelen een verklaring af te leggen zal dan, naast een mogelijke schending van het nemo-teneturbeginsel, ook een inbreuk op het zwijgrecht opleveren.

In tegenstelling tot de stelling van het Hof van Cassatie dat de pincode wilsonafhankelijk is, hebben wij in § 3.2 betoogd dat een pincode wel wilsafhankelijk is en dus onder de bescherming van het nemo-teneturbeginsel valt. Voorts staat op het niet-meewerken aan het bevel tot het verschaffen van deze informatie zoals eerder opgemerkt een gevangenisstraf van een half jaar tot ten hoogste drie jaren, dan wel in geval van strafverzwarende omstandigheden één tot vijf jaar. Het in het vooruitzicht stellen van een dermate hoge gevangenisstraf is in het licht van het nemo-teneturbeginsel een vorm van ongeoorloofde dwang.[81] Bovendien lijken de relevante waarborgen (bevel wordt gemotiveerd en afgegeven door een onderzoeksrechter aan een persoon waarvan de onderzoeksrechter aannemelijk kan maken dat hij de toegangscode weet) in het licht van de jurisprudentie van het EHRM onvoldoende te zijn.[82]

Concluderend kan worden gesteld dat de in artikel 88*quater* § 1 BSv neergelegde bevoegdheid om een verdachte onder dreiging van een gevangenisstraf te bevelen zijn wilsafhankelijke pincode te openbaren waarna het bewijs dat daardoor wordt verkregen wordt gebruikt in een strafrechtelijke procedure, volgens onze analyse van de jurisprudentie van het EHRM een schending oplevert van het nemo-teneturbeginsel.

3.4 *Duitsland*

In tegenstelling tot de hierboven gepresenteerde Belgische situatie, is het naar Duits recht zonneklaar dat het onder dwang van boete of gijzeling overdragen van inloggegevens, niet zijnde biometrische kenmerken, een inbreuk op het zwijgrecht oplevert.[83] Ook de regering ziet dit zo, en zij ziet in de bewijsuitsluiting de enige manier om de inbreuk te rechtvaardigen.[84] In Duitsland wordt dus 'vol' ingezet op de ontwikkeling van een inbreuk makende bevoegdheid met een relevante waarborg. Net zoals in de hierboven besproken zaak *Van Weerelt*, mag het door de meewerkplicht verkregen bewijsmateriaal – in het geval van § 163g StPO het overdragen van inloggegevens – niet tegen de verdachte worden gebruikt. In de toelichting op § 163g StPO wordt namelijk overwogen dat aan de onderhavige bevoegdheid een *Verwendungsverbot* moet worden verbonden. Een *Verwendungsverbot* houdt in dat het bewijsmiddel niet – in de zin van: op geen enkele wijze – mag worden gebruikt (*verwenden* betekent letterlijk gebruiken). Dit zou een zeer ruime, noodzakelijke en relevante waarborg opleveren voor de verdachte omdat hierdoor ook onder andere toevallige vondsten niet mogen worden gebruikt.

4. Vergelijking en conclusie

Uit het voorgaande blijkt dat Nederland, België en Duitsland een ontgrendelplicht zien als een geschikt *instrument* ten behoeve van de opsporing. Dat is niet verwonderlijk gezien de rol die elektronische gegevensdragers en virtuele identiteiten in de huidige samenleving

75 De uitspraak van het Grondwettelijk Hof beantwoordt een prejudiciële vraag die met name zag op de verhouding tussen art. 88*quater* § 1 en § 2 BSv. Daarom is het decryptiebevel getoetst aan het gelijkheidsbeginsel. De rechtspraak van het EHRM is kort aangehaald, maar niet betrokken in de toetsing.

76 Grondwettelijk Hof 20 februari 2020, arrest nr. 28/2020, rolnr. 7075.

77 Het kan zijn dat het Hof van Cassatie hier doelt op het feit dat de inloggegevens onafhankelijk van de wil van de verdachte *bestaan* – en dat is natuurlijk ook zo – maar die kunnen alleen afhankelijk van zijn wil worden *verkregen*.

78 Hof van Cassatie 4 februari 2020, P.19.1086.N/1, *Computerrecht* 2020/137, zie verder in dit nummer.

79 S. Royer & W. Yperman, 'Wankele argumenten van hoogste Belgische hoven in uitspraken over decryptiebevel', nog te verschijnen, p. 4.

80 Zie hierover ook: Van de Heyning 2019, p. 314-317; J. Meese, 'Recht om te zwijgen maar toch verplicht om te spreken?', *Rechtskundig Weekblad* 2019-20, nr. 34, p. 1322.

81 EHRM 13 september 2016, appl. nos. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim e.a./het Verenigd Koninkrijk*), par. 267.

82 EHRM 21 december 2000, appl. nr. 36887/97 (*Quinn/Ierland*), par. 51; EHRM 21 december 2000, appl. nr. 34720/97 (*Heaney & McGuinness/Ierland*), par. 51.

83 Zie voor literatuurverwijzingen L. Franck, 'Herausgabe von Passwörtern und der nemo-tenetur-Grundsatz', *RDV* 2013, 6, p. 289. Zie ook Oehmichen & Weißenberger 2020, par. III.4.

84 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0), p. 86-87.

spelen. Bij veel (individuele) strafbare feiten spelen de elektronische gegevens, zoals communicatie en afbeeldingen, een grote rol van betekenis. Bij de ontmanteling van criminele organisaties zijn deze gegevens zelfs onmisbaar, omdat alleen met communicatie tussen personen het verband tussen deze personen en de verhoudingen binnen de organisatie kunnen worden blootgelegd. Wij zien derhalve de noodzakelijkheid voor de ontwikkeling van instrumenten om toegang te krijgen tot gegevens.

Ondanks dat in de drie buurlanden het doel gelijk is, is het enigszins verwonderlijk dat de regelingen zo uiteenlopen. In Nederland wordt de minimumwaarborg uit de Straatsburgse jurisprudentie braaf gevolgd: een ontgrendelplicht is alleen mogelijk als geringe (geoorloofde) dwang wordt gebruikt door een elektronische gegevensdrager te ontgrendelen via het afdwingen van een biometrisch kenmerk (dat onafhankelijk van de wil van de verdachte bestaat). Vervolgens kan de ontgrendelde gegevensdrager nader worden onderzocht en mogen de daarop aangetroffen gegevens als bewijs tegen de verdachte worden gebruikt. Een verdere inbreuk op het nemo-teneturbeginsel, door ook het ontgrendelen van een elektronische gegevensdrager met inloggegevens te kunnen bevelen of afdwingen, wordt onrechtmatig geacht.

In België zien de wetgever en verschillende rechtscolleges daarin juist geen probleem. Waar in Nederland het opschrijven of uitspreken van inloggegevens wordt gezien als een gedraging die afhankelijk van de wil van de verdachte is, hebben Belgische rechtscolleges overwogen dat de toegangscodes onafhankelijk van de wil van de verdachte bestaan, aangezien de codes onveranderd blijven. Dat moge zo zijn, maar de Belgische rechters laten hierbij volledig onbenoemd dat de toegangscodes niet zonder een van de wil van de verdachte afhankelijke gedraging kunnen worden verkregen (althans tenzij de Belgische rechters ervan uitgaan dat de toegangscode ook altijd via een derde (bijvoorbeeld een telecommunicatiedienst) kan worden verkregen). Met andere woorden, er is altijd een actieve gedraging van de verdachte vereist terwijl dat onzes inziens in strijd is met de Straatsburgse jurisprudentie.

Dat standpunt wordt gedeeld in Duitsland. De Duitse regering ziet in het tweede criterium uit het Straatsburgse toetsingskader echter een uitweg. De autoriteiten mogen ongeoorloofde dwang ter verkrijging van afhankelijk van de wil bestaand materiaal gebruiken, mits relevante waarborgen bestaan. Zij 'gebruiken' de rechtsbescherming die de individuele verdachte op grond van artikel 6 EVRM toekomt om veel informatie over andere strafbare feiten te verkrijgen. Deze 'ontgrendelaar' wordt als het ware een soort kroongetuige. In de rechtspraak van het EHRM is een relevante waarborg het uitsluiten van de door dwang verkregen bewijsmiddelen. In Duitsland wordt daarom een 'gebruiksverbod' gekoppeld aan de ontgrendelplicht, die inhoudt dat de verkregen gegevens op geen enkele wijze tegen de verdachte mogen worden gebruikt.

Kortom, de Nederlandse EHRM-conforme interpretatie van de ontgrendelplicht is zodanig dat de toegang tot elektronische gegevensdragers die zijn beveiligd met een wachtwoord of pincode tegen de wil van een *verdachte* tot op heden vrij moeilijk is. Of een regeling die thans in Duitsland is voorgesteld ook noodzakelijk en wenselijk is voor de Nederlandse rechtsorde wordt in het tweede luik bezien.