Jurisprudentie

De gedwongen biometrische ontgrendeling van een elektronische gegevensdrager: rechtsbescherming gezocht?!

Noot bij HR 9 februari 2021, ECLI:NL:HR:2021:202

Mr. T. Beekhuis en D.A.G. van Toor PhD LLM BSc*

1. De gedwongen biometrische ontgrendeling van een *smartphone* bracht de afgelopen jaren reeds een aantal digitale pennen in beweging.[1] Op 9 februari jongstleden was het aan de Hoge Raad om een oordeel over deze ontgrendelingswijze te geven.[2] De Hoge Raad werd hiertoe opgeroepen doordat het Openbaar Ministerie cassatie in het belang der wet had ingesteld.[3] Advocaat-generaal (hierna: A-G) Bleichrodt diende twee cassatiemiddelen in, namelijk dat de gedwongen biometrische ontgrendeling van een *smartphone* (1) gebaseerd is op een ontoereikende wettelijke grondslag (zijnde de bepalingen in het Wetboek van Strafvordering (hierna: Sv) met betrekking tot de algemene bevoegdheid tot inbeslagneming); en (2) in strijd is met het nemo-teneturbeginsel. In de conclusie van A-G Bleichrodt alsmede in het arrest van de Hoge Raad staat de biometrische *ontgrendeling* centraal. Dat wil zeggen, het gaat in de procedure alleen over de toegangsverschaffing tot elektronische gegevensdragers.

2. Bijzonder aan de ontgrendeling van een elektronische gegevensdrager is dat daarin eigenlijk twee vraagstukken zitten verscholen, die vaak niet uit elkaar worden gehaald. De toegangsverschaffing is niet het doel, maar een middel. Het uiteindelijke doel is het verkrijgen en analyseren van de *inhoud* van de elektronische gegevensdrager. Vragen die gesteld zouden moeten worden, zijn onder welke voorwaarden toegang tot een in beslag genomen elektronische gegevensdrager kan worden verkregen én als eenmaal toegang tot de inhoud van de elektronische gegevensdrager is verkregen, op welke wijze en onder welke voorwaarden mag dan onderzoek worden gedaan naar de inhoud van de elektronische gegevensdrager? Die laatste vraag speelt, volgens ons ten onrechte, in de rechtszaak nauwelijks een rol van betekenis. Immers, de enige reden waarom men toegang wenst tot de inhoud van een elektronische

* Mr. T. 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. D.A.G. van Toor PhD LLM BSc is verbonden als universitair docent straf(proces)recht aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtstaat en Rechtspleging van de Universiteit Utrecht.

1. Bijv. D.A.G. van Toor, 'De vergrendelde smartphone als object van strafvorderlijk onderzoek', *Computerrecht* 2017, 1, p. 3-11; A. Bood, 'Geef ze een vinger …', *NJB* 2018, 36, p. 2744-2748; 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; 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; D.A.G. van Toor, W. Albers, C.M. Taylor Parkins-Ozephius & T. Beekhuis, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131; T. Beekhuis, C.M. Taylor Parkins-Ozephius, W. Albers & D.A.G. van Toor, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 2)', *Computerrecht* 2020/179.
2. HR 9 februari 2021, ECLI:NL:HR:2021:202.
3. Conclusie A-G Bleichrodt 13 oktober 2020, ECLI:NL:PHR:2020:927.

doi: 10.5553/TBSenH/229567002021007003009

gegevensdrager, is dat daarmee de daarop aanwezige data beschikbaar komen voor analyse: het is niet de enkele toegangsverschaffing waarmee een inbreuk op grondrechten wordt gemaakt, maar voornamelijk de analyse van de inhoud van de elektronische gegevensdrager. Dit is het centrale punt dat in deze annotatie wordt gemaakt. Alvorens dit nader wordt uitgewerkt (rn. 6-10), wordt eerst stilgestaan bij de rechtsgang (rn. 3-5).

3. Aan het genoemde arrest van de Hoge Raad is het oordeel van de rechtbank Noord-Holland van 28 februari 2019 voorafgegaan inzake het onderzoek *Cyber007*, waarin een verdachte onder meer terechtstond wegens *phishing*.[4] In deze uitspraak oordeelde de rechtbank dat de opsporingsambtenaren op rechtmatige wijze toegang tot de in beslag genomen *iPhone* van de verdachte hadden verkregen en dat de wettelijke grondslag hiertoe gelegen is in de artikelen 94 jo. 95 en 96 Sv.[5] Als het enkel mogelijk is om toegang tot een in beslag genomen voorwerp (zoals in casu een *iPhone*) te verkrijgen met medewerking van een verdachte, kan een verdachte tot medewerking worden gedwongen, tenzij het nemo-teneturbeginsel of de beginselen van proportionaliteit en subsidiariteit zich hiertegen verzetten, aldus de rechtbank.[6] In de onderhavige zaak werden deze beginselen volgens de rechtbank niet geschonden geacht door een afgedwongen biometrische ontgrendeling van een *iPhone* door het plaatsen van de vinger van de verdachte op zijn *iPhone* en hem daartoe te boeien.[7] Tegen dit oordeel is – zoals gezegd – door het Openbaar Ministerie cassatie in het belang der wet ingediend.[8]

4. Volgens A-G Bleichrodt getuigt het oordeel van de rechtbank Noord-Holland niet van een onjuiste rechtsopvatting, maar hij acht een oordeel van de Hoge Raad over de gedwongen biometrische ontgrendeling met gebruikmaking van fysieke dwang noodzakelijk voor de opsporingspraktijk en de rechtsontwikkeling, mede in het licht van aanstaande wetgeving.[9] Volgens de A-G kan de gedwongen biometrische ontgrendeling – in lijn met het oordeel van de rechtbank Noord-Holland – worden gebaseerd op de artikelen 94 jo. 95 en 96 Sv en artikelen 141 en 148 Sv.[10] Ook stelt de A-G dat de gedwongen biometrische ontgrendeling niet in strijd is met het nemo-teneturbeginsel, omdat de vingerafdruk onafhankelijk van de wil van de verdachte bestaat, beperkte dwang wordt uitgeoefend bij de gedwongen ontgrendeling en geen actieve medewerking van de verdachte is vereist voor de ontgrendeling (duldplicht).[11]

5. De Hoge Raad volgt de A-G in zijn analyse en verwerpt beide cassatiemiddelen.[12] Ten aanzien van het eerste cassatiemiddel oordeelt de Hoge Raad dat het genoemde samenstel van bepalingen waarin de inbeslagname van voorwerpen is geregeld (art. 94 jo. 95 en 96 Sv en art. 141 en 148 Sv) ook de wettelijke basis is voor het onderzoek *aan* de in beslag genomen voorwerpen én dat proportioneel fysiek geweld mag worden toegepast om de voorwerpen in beslag te nemen.[13] De Hoge Raad concludeert voorts dat de biometrische toegangsverschaffing tot in beslag genomen voorwerpen met het doel om daaraan onderzoek te verrichten eveneens op grond van deze bepalingen mogelijk is.[14] In de beoordeling van het tweede cassatiemiddel komt de Hoge Raad tot de conclusie dat, wanneer een zeer geringe mate van dwang wordt gebruikt teneinde een *smartphone* biometrisch te ontgrendelen, dit geen inbreuk op het nemo-teneturbeginsel oplevert. Het ondergaan van beperkte fysieke dwang (in *casu* het boeien van een verdachte en het plaatsen van zijn duim op de vingerafdrukscanner (dit alles tegen de wil van de verdachte)) levert volgens de Hoge Raad slechts een 'geringe inbreuk op de lichamelijke integriteit van de verdachte' op, waardoor het nemo-teneturbeginsel niet in gedrang komt.[15] Belangrijk hierbij is dat de Hoge Raad – net als de A-G – bij de beoordeling van het nemo-teneturbeginsel voor het eerst uitvoerig citeert uit het *Jalloh*-arrest van het EHRM, en geen verwijzingen opneemt naar het welbekende *Saunders*-arrest.[16]

6. Dat de Hoge Raad de discussie over de wettelijke grondslag van de gedwongen biometrische ontgrendeling en de eventuele strijdigheid met het nemo-teneturbeginsel heeft beslecht, betekent echter niet dat de discussie over deze twee aspecten is verstomd. Want, wat betekent dit oordeel nu voor de rechtsbescherming van een verdachte? Als hij zijn elektronische gegevensdrager afschermt met een numerieke code of wachtwoord, komt hem een

4. Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568.
5. Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568, r.o. 3.4.1.3.2. Op grond van art. 141, aanhef en onder a en art. 148 Sv komt deze bevoegdheid eveneens toe aan de officier van justitie.
6. Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568, r.o. 3.4.1.3.2.
7. Rb. Noord-Holland 28 februari 2019, ECLI:NL:RBNHO:2019:1568, r.o. 3.4.1.3.2.
8. Conclusie A-G Bleichrodt 13 oktober 2020, ECLI:NL:PHR:2020:927.
9. Conclusie A-G Bleichrodt 13 oktober 2020, ECLI:NL:PHR:2020:927, punt 3. Voor wat betreft de aankomende wetgeving verwijst de A-G naar het in de Modernisering van het Wetboek van Strafvordering voorgestelde art. 2.7.4.1.4 lid 2 (zie zijn uiteenzetting vanaf punt 23 van zijn conclusie). In de laatste gepubliceerde ambtelijke versie van het wetsvoorstel Wetboek van Strafvordering (juli 2020) is deze bepaling vernummerd naar art. 2.7.44.
10. Conclusie A-G Bleichrodt 13 oktober 2020, ECLI:NL:PHR:2020:927, punt 22.
11. Conclusie A-G Bleichrodt 13 oktober 2020, ECLI:NL:PHR:2020:927, punt 47-54.
12. HR 9 februari 2021, ECLI:NL:HR:2021:202, r.o. 8.
13. HR 9 februari 2021, ECLI:NL:HR:2021:202, r.o. 6.2.1 en 6.2.2.
14. HR 9 februari 2021, ECLI:NL:HR:2021:202, r.o. 6.2.2 en 6.3.
15. HR 9 februari 2021, ECLI:NL:HR:2021:202, r.o. 7.3.
16. Zie hierover D.A.G. van Toor & T. Beekhuis, annotatie bij HR 9 februari 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63.

doi: 10.5553/TBSenH/229567002021007003009

beroep toe op het nemo-teneturbeginsel.[17] Echter, in geval van biometrische ontgrendeling is dit niet het geval en kunnen de autoriteiten de verdachte dwingen toegang te verschaffen tot zijn elektronische gegevensdrager (mits de daarbij gehanteerde dwang beperkt is). Vervolgens verkrijgen de autoriteiten de toegang tot een schat aan gegevens, die zij kunnen bekijken en analyseren (waarbij zij uiteraard de lijn die de Hoge Raad in de *Smartphone*-arresten heeft uitgezet in acht moeten nemen). Is dit anno 2021 nog wel wenselijk? Moeten er in geval van biometrische vergrendeling van een elektronische gegevensdrager niet bepaalde waarborgen gelden die de verdachte beschermen tegen de datahonger van de strafvorderlijke autoriteiten?[18]

7. Zoals reeds eerder opgemerkt, beschermt het nemo-teneturbeginsel de verdachte die zijn *smartphone* op biometrische wijze heeft vergrendeld niet tegen ongewenste toegangsverschaffing tot die *smartphone* door de strafvorderlijke autoriteiten. Dit komt, omdat het nemo-teneturbeginsel alleen bescherming biedt indien (1) de strafvorderlijke autoriteiten ongeoorloofde dwang gebruiken ter verkrijging van bewijs; (2) er geen relevante waarborgen bestaan tegen deze voor de verdachte nadelige wijze van bewijsverkrijging; en (3) het verkregen bewijs tegen de verdachte wordt gebruikt in een strafrechtelijke procedure.[19] Ook als sprake is van wilsonafhankelijk materiaal kan het nemo-teneturbeginsel bescherming bieden, namelijk indien de aard en de mate van dwang zodanig zijn, dat sprake is van ongeoorloofde dwang.[20] Het EHRM heeft reeds in 2016 drie voorbeelden gegeven van vormen van ongeoorloofde dwang, namelijk:

> '*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 (…).*'[21]

Van een dergelijke mate van dwang is in het geval van een gedwongen biometrische ontgrendeling van een elektronische gegevensdrager in de regel geen sprake.

8. Op het gebied van de biometrische toegangs*verschaffing* staat de verdachte, die niet wil dat de strafvorderlijke autoriteiten toegang krijgen tot zijn elektronische gegevensdrager, aldus met lege handen. Hij moet dulden (al dan niet onder (fysieke) dwang of druk) dat de autoriteiten toegang krijgen tot de inhoud van zijn elektronische gegevensdrager. Nadat de autoriteiten toegang hebben gekregen tot deze inhoud, geldt zoals gezegd het toetsingskader dat de Hoge Raad heeft gegeven in de zogeheten *Smartphone*-arresten waarin hij handvatten geeft voor de vaststelling wanneer een rechtmatig onderzoek aan een *smartphone* kan plaatsvinden. Echter, ook deze arresten kunnen op de nodige kritiek rekenen, onder meer omdat de Hoge Raad veel nadruk legt op de *kwantiteit* van de op de *smartphone* aangetroffen gegevens in plaats van de *kwaliteit* (aard) van de gegevens.[22] Daarnaast is niet op voorhand concreet duidelijk wanneer de toestemming van de officier van justitie of de rechter-commissaris noodzakelijk is.[23] En dan hebben we het nog niet over de consequenties die een onrechtmatige doorzoeking met zich brengt: een beroep op artikel 359a Sv blijkt in de praktijk immers zelden tot nooit succesvol te zijn.[24] De vraag die opkomt is op welke wijze tegemoet kan worden gekomen aan deze gebrekkige of wellicht ontbrekende rechtsbescherming van de verdachte. Wordt het geen tijd om de toegangs*verschaffing* tot de *smartphone* en het daaropvolgende onderzoek aan de inhoud op de *smartphone* uit elkaar te trekken en voor de verschillende handelingen uiteenlopende waarborgen te creëren? Hierbij kan worden gedacht aan het creëren van twee specifieke wettelijke grondslagen die de beide handelingen nader reguleren, waarin onder andere de eis wordt gesteld dat een bevel van de officier van justitie of een machtiging van de rechter-commissaris noodzakelijk is.

9. Wanneer we onze blik verleggen naar de Verenigde Staten van Amerika, dan volgt uit de beslissing van het *Supreme Court of the United States* (hierna:

17. Vgl. D.A.G. van Toor, W. Albers, C.M. Taylor Parkins-Ozephius & T. Beekhuis, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131.
18. Dit neemt uiteraard niet weg dat er gevallen kunnen zijn waarin het wenselijk en noodzakelijk is de toegang tot een elektronische gegevensdrager af te kunnen dwingen, namelijk in het geval van een verdenking van zware misdrijven in georganiseerd verband. Zie daartoe ons betoog in: T. Beekhuis, C.M. Taylor Parkins-Ozephius, W. Albers & D.A.G. van Toor, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 2)', *Computerrecht* 2020/179.
19. Vgl. D.A.G. van Toor, W. Albers, C.M. Taylor Parkins-Ozephius & T. Beekhuis, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131, p. 238-239.
20. Vgl. D.A.G. van Toor, W. Albers, C.M. Taylor Parkins-Ozephius & T. Beekhuis, 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131, p. 238-239.
21. EHRM 13 september 2016, appl. nos. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim e.a./het Verenigd Koninkrijk*).
22. O.a. L. Stevens, 'Onderzoek in een smartphone: zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing', *AA* 2017, p. 730-735; T. Beekhuis, 'Mag ik even in uw smartphone kijken? De visie van de Hoge Raad gelet op het recht op privacy op grond van artikel 8 EVRM', *TBSH* 2017/4, p. 4.
23. Stevens, *AA* 2017, p. 734; Beekhuis, *TBSH* 2017/4, p. 4.
24. O.a. E. Devroe, M. Malsch, J. Matthys & G. Minderman, *Toezicht op strafvorderlijk overheidsoptreden*, Den Haag: WODC 2017-2686, p. 60; CAG 25 oktober 2016 ECLI:NL:PHR:2016:1048, punt 78; J. Nan, 'Kroniek van het straf(proces)recht', *NJB* 2017/35, p. 2541.

doi: 10.5553/TBSenH/229567002021007003009

SCOTUS) inzake *Riley v. California* dat wanneer de politie bij de aanhouding van een verdachte een telefoon in beslag neemt, in beginsel eerst een *warrant* verkregen moet worden vóórdat zij onderzoek mag doen aan deze telefoon.[25] Voor telefoons (zoals *smartphones*) geldt in de Verenigde Staten van Amerika sinds deze beslissing een afwijkende regeling van de regeling die geldt voor het in beslag nemen van andere objecten die een verdachte bij zijn aanhouding bij zich draagt (bijvoorbeeld papieren en/of wapens). De rechtvaardiging voor een dergelijke aparte, afwijkende regeling is hierin gelegen dat op *smartphones* niet alleen veel gegevens (kwantitatief) staan, maar ook gegevens die enorm privacygevoelig (kwalitatief) zijn.[26] SCOTUS overweegt zelfs '*a cell phone search would typically expose to the government far more than the most exhaustive search of a house*'.[27] Derhalve is volgens SCOTUS een extra waarborg noodzakelijk en deze wordt gevonden in een voorafgaande *warrant*.

10. Kijken we vooruit, en dan doelen wij op de modernisering van het Wetboek van Strafvordering, dan stelt het voorgestelde artikel 2.7.39 dat het onderzoek in digitale-gegevensdragers of geautomatiseerde werken in geval van stelselmatig onderzoek[28] enkel mag gebeuren op bevel van de officier van justitie.[29] Indien sprake is van een *ingrijpend* stelselmatig onderzoek is een machtiging van de rechter-commissaris vereist.[30] Blijkens de concept memorie van toelichting zal 'alleen in uitzonderingsgevallen sprake (…) zijn van ingrijpende stelselmatigheid' en 'het is zeker niet de bedoeling dat uit voorzorg in veel gevallen een machtiging van de rechter-commissaris zal worden aangevraagd om te voorkomen dat eventuele toevallig in beeld komende gegevens een onderzoek met terugwerkende kracht onrechtmatig zouden maken'.[31] Hieruit kan de conclusie worden getrokken dat ook onder de nieuwe wetgeving – mocht deze worden aangenomen – de doorzoeking van een 'vaste' woning met meer waarborgen is omgeven (altijd machtiging rechter-commissaris) dan de 'draagbare' woning (*smartphone)*. De meeste mensen regelen hun bankzaken via een applicatie en hebben bankafschriften niet meer in een map in de kast staan. Dit geldt ook voor het contact met de zorgverzekering en andere gezondheidsgerelateerde onderwerpen (*fitness apps* en de apotheek). Via *dating apps* kan eenvoudig iemands seksuele geaardheid en relationeel leven in kaart worden gebracht. En dit is slechts het topje van de ijsberg van informatie die op een *smartphone* is te vinden. Wij vragen ons af of het verschil tussen de rechtsbescherming van een woning versus een *smartphone* nog wel van deze tijd is en of de wetgever het onderzoek aan de *smartphone* niet met meer waarborgen moet omgeven. Dit geldt des te meer in geval van een afgedwongen biometrische ontgrendeling van een *smartphone*: de verdachte dient dit te dulden, waardoor de deur naar de op de *smartphone* aanwezige gegevens wagenwijd openstaat.[32] Als de opsporingsambtenaren dan ook nog in veel gevallen zelfstandig of op bevel van de officier van justitie,[33] onderzoek mogen doen, kunnen kanttekeningen worden gezet bij de mate van rechtsbescherming die een verdachte toekomt.

25. Supreme Court of the United States Riley v. California (No. 13-132), 25th June 2014. In beginsel is een *warrant* verplicht, maar de omstandigheden van het geval kunnen een onderzoek zonder *warrant* rechtvaardigen. Zie Supreme Court of the United States Riley v. California, 25th June 2014, p. 26-27.
26. Supreme Court of the United States Riley v. California (No. 13-132), 25th June 2014, p. 17 e.v.
27. Supreme Court of the United States Riley v. California (No. 13-132), 25th June 2014, p. 20.
28. Blijkens de memorie van toelichting gaat het om 'onderzoek van gegevens waarbij op voorhand redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven kan ontstaan'. Zie Ambtelijke versie juli 2020 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 245 en 411. Zie ook de definitie in art. 2.1.1 onder j Ambtelijke versie juli 2020 Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (Boek 2). Een uitleg van de zinsnede 'redelijkerwijs voorzienbaar' kan worden gevonden in de Ambtelijke versie juli 2020 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 412.
29. Artikel 2.7.39 lid 1 Ambtelijke versie juli 2020 Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (Boek 2). Indien het onderzoek geen stelselmatig karakter heeft, mag de opsporingsambtenaar zelfstandig onderzoek verrichten (zonder bevel van de officier van justitie). Zie Ambtelijke versie juli 2020 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 410-411.
30. Artikel 2.7.39 lid 2 Ambtelijke versie juli 2020 Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (Boek 2). Zie ook de definitie van 'ingrijpend stelselmatig onderzoek' in art. 2.1.1 onder j Ambtelijke versie juli 2020 Wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering (Boek 2).
31. Ambtelijke versie juli 2020 Memorie van toelichting bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering, p. 414.
32. Nogmaals benadrukken wij dat dit onderzoek in veel gevallen noodzakelijk en wenselijk is voor het verkrijgen van bewijsmateriaal. Waar het om gaat is dat dit onderzoek met voldoende waarborgen dient te zijn omgeven.
33. Het bevel van de officier van justitie kan ook worden gezien als een waarborg, maar de vraag is of de verdachte dan een voldoende mate van rechtsbescherming toekomt.

doi: 10.5553/TBSenH/229567002021007003009