T. den Os, P. Reumer & D. van Toor[1]

Gezichtsherkenning als lakmoesproef voor biometrisch ontgrendelen van elektronische gegevens

Computerrecht 2022/139

In 2021 heeft de Hoge Raad geoordeeld dat de verdachte mag worden verplicht een vergrendelde gegevensdrager te ontgrendelen, mits de *biometrische* ontgrendeling met geringe fysieke dwang kan worden afgedwongen. De Hoge Raad geeft echter niet aan wat onder biometrie moet worden verstaan. In deze bijdrage wordt nader ingegaan op het begrip biometrie en in hoeverre gezichtsherkenning in overeenstemming met het nemo-teneturbeginsel tegen de verdachte kan worden gebruikt.

1. Inleiding[2]

Op 9 februari 2021 oordeelde de Hoge Raad dat de overweging van de rechtbank Noord-Holland dat de opsporingsambtenaar in het kader van de opsporing naar strafbare feiten een verdachte met lichte fysieke dwang mag dwingen zijn smartphone biometrisch te ontgrendelen niet getuigt van een onjuiste rechtsopvatting.[3] Met andere woorden, vanaf dat moment omarmt ons hoogste rechtscollege hetgeen al langer in de wetenschap[4] en in de lagere rechtspraak[5] het uitgangspunt is: omdat de vingerafdruk biometrisch is en bij de ontgrendeling van een smartphone met lichte fysieke dwang tegen de verdachte kan worden gebruikt, levert de gedwongen ontgrendeling van een smartphone geen schending van het nemo-teneturbeginsel – het beginsel dat iemand niet kan worden gedwongen mee te werken aan zijn eigen veroordeling – op. Tot op heden bestaat geen expliciete grondslag voor de ontgrendelbevoegdheid. Deze wordt ingelezen in de inbeslagnamebevoegdheid: 'voor de waarheidsvinding [mag] onderzoek worden gedaan aan inbeslaggenomen voorwerpen ten einde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen en in computers opgeslagen gegevens [zijn] daarvan niet (…) uitgezonderd.'[6]

Na de modernisering van het Wetboek van Strafvordering (Sv) krijgt de ontgrendelbevoegdheid wel een wettelijke grondslag. Artikel 2.7.44 lid 2 Sv (ambtelijke versie) bepaalt dat (als steundwangmiddel) de biometrische beveiliging of versleuteling ongedaan mag worden gemaakt tegen de wil van degene wiens biometrische kenmerken ontgrendeling mogelijk maken. Zowel in het rapport van de commissie Koops – op wiens advies voor het eerst een ontgrendelbevoegdheid tegen de wil wordt opgenomen[7] – als in het wetsvoorstel wordt geen definitie van het begrip *biometrisch kenmerk* gegeven. Bij algemene maatregel van bestuur moet ten minste worden vastgesteld welke kenmerken als biometrische kenmerken worden gekwalificeerd, zo bepaalt artikel 2.7.44 lid 2 Sv. Dat laat vooralsnog de vraag open wat precies onder het begrip biometrie valt. Dat is in het licht van de steeds verder ontwikkelde beveiligings- of versleutelmethode een belangrijke vraag, waarmee ook de praktijk zal worden geconfronteerd.

Eén van die "nieuwe" methode is gezichtsherkenning als ont-/vergrendelmethode bij smartphones. Nadat de pincode (in ieder geval voor veel gebruikers) is vervangen door de gebruikersvriendelijkere vingerafdruk, is de gezichtsherkenning geïntroduceerd als veiligere verificatiemethode.[8] Het is daarom zeer goed denkbaar dat er al een smartphone gedwongen is ontgrendeld door de autoriteiten, of in ieder geval binnenkort wordt ontgrendeld, door de smartphone van de verdachte zijn gezicht te laten herkennen. De vraag is echter of het gezicht kwalificeert als biometrisch kenmerk. Hiervan wordt vooralsnog, ook door één van de coauteurs, zonder nadere onderbouwing van uitgegaan,[9] terwijl goede gronden bestaan daarover te twijfelen.

Anders dan de vingerafdruk (of de irisscan) baseert gezichtsherkenning zich op een groter gedeelte van het li-

1 Mr. T.P.A. (Thomas) den Os en mr. P. (Patrick) Reumer zijn beide als docent straf(proces)recht verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen van de Universiteit Utrecht.
D.A.G. (Dave) van Toor PhD LLM BSc is als universitair docent verbonden aan het Willem Pompe Instituut voor Strafrechtswetenschappen en het Montaigne Centrum voor Rechtstaat en Rechtspleging van de Universiteit Utrecht.

2 Deze bijdrage borduurt voort op: D.A.G. van Toor, 'De vergrendelde smartphone als object van strafvorderlijk onderzoek', *Computerrecht* 2017/2, p. 3-11; D.A.G. van Toor, 'Het gedwongen ontgrendelen van een smartphone in het licht van het nemo-teneturbeginsel. Reactie op Boods 'Geef ze een vinger …'', *NJB* 2019/317; HR 9 februari 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63, m.nt. Van Toor & Beekhuis; D.A.G. van Toor e.a., 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131.

3 HR 9 februari 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63, m.nt. Van Toor & Beekhuis.

4 D.A.G. van Toor, 'De vergrendelde smartphone als object van strafvorderlijk onderzoek', *Computerrecht* 2017/2; 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.

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.

6 HR 29 maart 1994, ECLI:NL:HR:1994:AD2076, r.o. 9.3. Zie ook HR 4 april 2017, ECLI:NL:HR:2017:584, r.o. 2.5-2.8.

7 Zie artikel 2.7.4.1.4 van het eerste conceptwetsvoorstel en artikel 2.7.3.2.7 van de consultatieversie, in samenhang met artikel 2.7.1.1.4 van beide versie.

8 Zie bijvoorbeeld: 'Over de geavanceerde technologie achter Face ID', support.apple.com, 23 maart 2022.

9 Commissie modernisering opsporingsonderzoek in het digitale tijdperk, *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 21; D.A.G. van Toor e.a., 'De ontgrendelplicht in rechtsvergelijkend perspectief (deel 1)', *Computerrecht* 2020/131, par. 2.1.1.

chaam waarin meerdere spieren zitten die door de wil van de persoon te gebruiken zijn. Zo is een persoon bijvoorbeeld in staat in een bepaalde richting te kijken, zowel door de ogen te draaien als het gehele hoofd te bewegen, waarbij dat mogelijk invloed heeft op de gezichtsherkenning. Om te beoordelen of de gezichtsherkenning onder de biometrische ontgrendelmethoden valt, is het van belang de techniek achter de gezichtsherkenning nader te bekijken. Afhankelijk van de verificatiemethode en afhankelijk van de vraag in hoeverre wilsafhankelijke spierbewegingen invloed hebben op de verificatie moet de gezichtsherkenning als onafhankelijk van de wil bestaand of afhankelijk van de wil bestaand worden gecategoriseerd. Die categorisatie is in het licht van het nemo-teneturbeginsel van groot belang: alleen bij materiaal dat *onafhankelijk* van de wil bestaat, is namelijk een bepaalde mate van dwang toelaatbaar om de verdachte te dwingen mee te werken aan het opsporingsonderzoek.

In deze bijdrage wordt daarom de vraag beantwoord of gezichtsherkenning als verificatiemethode (enkel) gebruikmaakt van biometrische kenmerken en in hoeverre gezichtsherkenning in overeenstemming met het nemo-teneturbeginsel tegen de verdachte kan worden gebruikt. Deze bijdrage is als volgt opgebouwd. In paragraaf 2 beschrijven wij het toetsingskader: als de verdachte wordt gedwongen om zijn elektronische gegevensdrager te ontgrendelen, ligt het in de lijn der verwachting dat dit aan het *nemo-teneturbeginsel* wordt getoetst. Vervolgens definiëren wij in paragraaf 3 het begrip *biometrie*. Naar huidig en toekomstig recht zijn bij de ontgrendelbevoegdheid alleen biometrische kenmerken tegen de wil van de verdachte te gebruiken, maar om te kunnen beoordelen wat daar precies onder valt, is een definitie onontbeerlijk. In paragraaf 4 staat de *gezichtsherkenning als verificatiemethode* centraal. Hierbij besteden wij aandacht aan de achterliggende techniek. Zoals hierboven kort aangestipt, is de precieze werking van de techniek een essentieel element in de beoordeling van de gedwongen ontgrendeling door middel van gezichtsherkenning. In paragraaf 5 beschrijven wij een door ons uitgevoerd onderzoek: wij hebben mensen die gezichtsherkenning gebruiken gevraagd om een aantal procedures te doorlopen en daarbij te noteren of de gezichtsherkenning werkt. Voorbeelden zijn het niet recht in de camera kijken; de ogen sluiten; en een foto gebruiken. In paragraaf 6 ronden wij deze bijdrage af met de analyse en conclusie.

2. Het nemo-teneturbeginsel

Sinds het midden van de jaren negentig is de discussie over de reikwijdte van het nemo-teneturbeginsel en de afbakening van dat beginsel met het zwijgrecht losgebarsten. Het *Saunders*-arrest uit 1996[10] heeft tot veel verwarring en discussie geleid over de reikwijdte en inhoud van het nemo-teneturbeginsel.[11] Daarin wordt het volgende overwogen: 'the privilege against self-incrimination does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood, urine, hair or voice samples and bodily tissue for the purpose of DNA testing' (onderstreping auteurs). Veel van de aandacht bij de interpretatie is besteed aan het criterium 'bewijs dat (on)afhankelijk van de wil bestaat'.

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 nemo-teneturbeginsel; (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.[12] 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.[13] 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 bewijs dat onafhankelijk van de wil bestaat *niet*, en bewijs dat afhankelijk van de wil bestaat *wel* onder de bescherming van het nemo-teneturbeginsel. Dat deze uitleg destijds aan *Saunders* is gegeven, is gezien het hierna te bespreken arrest *Funke*[14] verwonderlijk.

In het arrest *Funke*, dat een aantal jaar vóór *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. In de hierboven weergegeven uitleg van het *Saunders*-criterium zou Funke niet worden beschermd onder het nemo-tenetur-

10 EHRM 17 december 1996, *NJ* 1997/699, m.nt. Kn (*Saunders/het Verenigd Koninkrijk*).

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

12 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. Kn, punt 4 (*Saunders/het Verenigd Koninkrijk*).

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

14 EHRM 25 februari 1993, *BNB* 1993/350, m.nt. Wattel (*Funke/Frankrijk*).

beginsel. Toch werd in *Funke* een schending van het nemo-teneturbeginsel aangenomen, omdat de overdracht van documenten werd gevorderd. De zaak *J.B.*, die enkele jaren ná *Saunders* werd gewezen, vertoont qua feiten grote gelijkenis met *Funke*. Ook daar werden documenten gevorderd en moest J.B. boetes betalen voor het niet verschaffen van inlichtingen. Ook hier nam het EHRM 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*) en *geen* veroordeling heeft uitgesproken in zaken waarin het materiaal betrof dat afhankelijk van de wil bestaat (*O'Halloran & Francis*,[15] *Khan*[16] & *Bykov*[17]). 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*.[18] Hierin wordt de aard van het bewijs niet als toetsingscriterium genoemd, maar wel de aard en mate van *dwang*.

In 2016 heeft de Grote Kamer van het EHRM in *Ibrahim e.a.* het volgende overzicht opgesteld met betrekking tot ongeoorloofde dwang. Gezien het belang en de duidelijkheid van die overweging wordt die hier integraal 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" (onderstreping auteurs en verwijzingen uit het citaat verwijderd).[19]

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 echter ervoor zorgen dat dwang – die ongeoorloofd is – zonder consequenties kan blijven. Een voorbeeld daarvan kan worden gevonden in de zaak *Van Weerelt*.[20] Via de Duitse belastingdienst zijn de Nederlandse collega's op de hoogte gebracht van door Nederlanders geheimgehouden rekeningen in Liechtenstein. De Belastingdienst vordert in juni 2009 informatie over de buitenlandse rekeningen van Van Weerelt, maar hij verklaart dat hij deze informatie niet meer bezit. Na veel communicatie over en weer legt de belastinginspecteur eind 2010, in afwezigheid van gedetailleerde informatie omdat Van Weerelt geen documenten overlegt, een naheffing inkomstenbelasting en vermogensbelasting op plus een vergrijpboete en heffingsrente van in totaal € 371.546 voor één fiscaal jaar (1998-1999). Daarnaast wordt een kort geding gestart om informatie van de belastingplichtige te verkrijgen. Van Weerelt verzet zich hiertegen met een beroep op artikel 6 EVRM. De Hoge Raad oordeelt dat van een belastingplichtige op grond van artikel 47 Algemene wet inzake rijksbelastingen (AWR) afgifte van wilsafhankelijk materiaal kan worden verlangd met het oog op een juiste belastingheffing, met als waarborg dat deze informatie *niet* ook voor fiscale beboeting of strafvervolging wordt gebruikt.[21] Het EHRM oordeelt hierover dat dit een voldoende effectieve waarborg tegen '*improper compulsion*' is.[22]

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 (ii) geen relevante waarborgen tegen deze voor de verdachte nadelige verkrijging bestaan en (iii) het verkregen bewijs tegen hem in een strafzaak wordt gebruikt. Zoals in de inleiding is aangestipt, is het gedwongen ontgrendelen van een smartphone door middel van een vingerafdruk te scannen niet ongeoorloofd in het licht van deze criteria wanneer slechts lichte fysieke dwang wordt gebruikt. De Hoge Raad oordeelt algemener door biometrische ontgrendelmethoden te rechtvaardigen, maar onduidelijk is welke methoden onder dit begrip vallen.

15 EHRM 29 juni 2007, ECLI:NL:XX:2007:BB3173 (*O'Halloran & Francis/het Verenigd Koninkrijk*).
16 EHRM 12 mei 2000, *NJ* 2002/180; appl. no. 35394/97 (*Khan/het Verenigd Koninkrijk*).
17 EHRM 10 maart 2009, appl. no. 4378/02 (*Bykov/Rusland*).
18 EHRM 29 juni 2007, appl. nos. 15809/02 en 25624/02, par. 55 (*O'Halloran & Francis/het Verenigd Koninkrijk*). Zie over dit toetsingskader D.A.G. van Toor, *Het schuldige geheugen?* (diss. RUN), Deventer: Wolters Kluwer 2017, p. 410-413.
19 EHRM 13 september 2016, appl. nos. 50541/08, 50571/08, 50573/08 en 40351/09 (*Ibrahim e.a./het Verenigd Koninkrijk*).
20 EHRM 16 juni 2015, appl. no. 784/14 (*Van Weerelt/Nederland*) (beslissing).
21 HR 12 juli 2013, ECLI:NL:HR:2013:BZ3640, r.o. 3.9.
22 EHRM 16 juni 2015, appl. no. 784/14, par. 66 (*Van Weerelt/Nederland*) (beslissing).

3. De definitie van biometrie

Alvorens te komen tot een beschrijving van de technologie van gezichtsherkenning als verificatiemethode bij de ontgrendeling van smartphones is het wenselijk om eerst een begrip te definiëren dat hierna als hoeksteen van de beschrijving en de analyse fungeert: biometrie of biometrische gegevens. Er kunnen meerdere definities van het begrip biometrie worden gegeven, afhankelijk van welke benadering wordt gehanteerd. Wanneer wordt gekozen voor een grammaticale benadering van het begrip, kan het worden gedefinieerd als het meten van biologische kenmerken en gegevens (afgeleid van de Griekse woorden *bíos*, leven, en *metria*, meten). De digitale Dikke van Dale definieert het begrip biometrisch dan ook als 'met meetbare persoonsgebonden eigenschappen, zoals vingerafdrukken of vorm van de iris: *een biometrisch paspoort*'.

De wetgever kiest voor een uitgebreidere en meer juridische definitie van biometrie, of biometrische gegevens: 'persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragskenmerken van een natuurlijk persoon op grond waarvan de eenduidige identificatie van die persoon mogelijk is of bevestigd wordt, zoals afbeeldingen van het gezicht of dactyloscopische gegevens.'[23] Deze kenmerken, en de verschillende technieken die daarbij horen, worden in de wetenschappelijke literatuur grofweg onderverdeeld in twee categorieën: de fysieke en fysiologische kenmerken van een persoon en de gedragsgerelateerde kenmerken.[24] Bij de fysieke en fysiologische kenmerken dient bijvoorbeeld te worden gedacht aan een vingerafdruk, het aderpatroon van de handpalm, de natuurlijke geur van een persoon, de iris en het onderwerp van dit artikel: de uiterlijke kenmerken van een gezicht.[25] De gedragsgerelateerde kenmerken zien toe op bijvoorbeeld het stemgeluid van een persoon, zijn of haar natuurlijke wijze van bewegen en de wijze waarop die persoon zijn handtekening zet.[26]

De gezichtsherkenningstechnologie is, zoals hiervoor al benoemd, een wijze van biometrische ontgrendeling, in ieder geval onder de juridische definitie. Bij toepassing van de ontgrendeling door gezichtsherkenning is echter niet enkel sprake van *onveranderlijke* fysieke biometrische kenmerken, maar mogelijk ook van *veranderlijke* gedragsgerelateerde biometrische kenmerken, namelijk de spierbewegingen die een persoon afhankelijk van zijn wil maakt. Een bepaald loopje, de wijze waarop een handtekening wordt gezet, of (in dit geval) de houding van een gezicht, zijn juist *veranderlijk*. Hierin lijkt de ontgrendelingsmethode door gezichtsherkenning zich in biometrische zin te onderscheiden van de ontgrendeling door vingerafdruk, handpalm of irisscan, terwijl advocaat-generaal Bleichrodt in zijn conclusie bij het in de inleiding besproken arrest van de Hoge Raad deze wijze van ontgrendelen wel in één adem noemt met de ontgrendeling door middel van de vingerafdruk.[27]

4. Gezichtsherkenning als verificatiemethode

Om te kunnen onderzoeken of de gezichtsherkenningstechnologie bij de ontgrendeling van smartphones in overeenstemming is met het nemo-teneturbeginsel, dient eerst een werkbare beschrijving te worden gegeven van hoe de gezichtsherkenningstechnologie werkt en in hoeverre deze betrouwbaar is. Eerst beschrijven wij hoe de technologie zich heeft ontwikkeld en op dit moment werkt. Vervolgens onderscheiden wij vier categorieën van huidige gezichtsherkenningstechnologieën, een onderscheid waar wij in de analyse op terug zullen komen. Deze technologieën verschillen in de mate waarin *gedragsgerelateerde* kenmerken invloed hebben op de ontgrendeling. Ten slotte behandelen wij de betrouwbaarheid van de technologie.

4.1 *De technologie in het algemeen*

Gezichtsherkenningstechnologie wordt al sinds medio 2011 gebruikt op smartphones, zij het op dat moment slechts door één telefoonmodel en in een meer rudimentaire versie dan de gezichtsherkenningstechnologie die anno 2022 wordt gebruikt.[28] In 2017 introduceerde Apple, met de lancering van de iPhone X, zijn *Face ID*.[29] Met de introductie hiervan wordt de gezichtsherkenningstechnologie betrouwbaarder en makkelijker te gebruiken voor een breed publiek. De rest van de grote smartphoneproducenten volgden kort daarop met hun eigen versies van de geavanceerdere gezichtsherkenningstechnologie. Hoewel verschillen bestaan in de wijze waarop de gezichtsherkenningstechnologie werkt op verschillende smartphones, beschrijven wij eerst de algemene werkwijze van de gezichtsherkenningstechnologie, alvorens wij later in de analyse terugkomen op de kwaliteitsverschillen.

De gezichtsherkenningstechnologie vraagt eerst dat de gebruiker zijn of haar gezicht vanuit verschillende hoeken laat scannen. De gezichtsherkenningstechnologie slaat dan een scan, of een plattegrond, van het gezicht van de gebruiker op voor toekomstig gebruik. Bij de verzamelde gegevens moet worden gedacht aan de stand van de ogen, de afstand tussen het voorhoofd en de kin, de breedte van

23 Toelichting bij de ambtelijke eindversie Wetboek van Strafvordering van juli 2020, p. 425 onder verwijzing naar artikel 1, onderdeel s, Wpg.

24 A. Alzubaidi & J. Kalita, 'Authentication of Smartphone Users Using Behavioral Biometrics', *IEEE Communications Surveys & Tutorials* 2016, p. 2001.

25 A. Alzubaidi & J. Kalita, 'Authentication of Smartphone Users Using Behavioral Biometrics', *IEEE Communications Surveys & Tutorials* 2016, p. 2001.

26 A. Alzubaidi & J. Kalita, 'Authentication of Smartphone Users Using Behavioral Biometrics', *IEEE Communications Surveys & Tutorials* 2016, p. 2014-2019.

27 PHR 13 november 2020, ECLI:NL:PHR:2020:927, punt 26.

28 Hayley Tsukayama, 'Galaxy Nexus debuts with Ice Cream Sandwich, facial recognition', washingtonpost.com 19 oktober 2011.

29 'The future is here: iPhone X', apple.com, 12 september 2017.

de neus en specifieke onderscheidende kenmerken van het gezicht zoals bijvoorbeeld een opvallend litteken.[30] Het scannen van het gezicht van de gebruiker gebeurt door middel van de camera aan de voorzijde van de telefoon. Bij een aantal merken wordt het gebruik van de camera vergezeld door andere ondersteunende technologie (denk aan een infraroodlichtprojector en een infraroodprojector die het gezicht in kaart brengt bij Apple's *Face ID*) die tevens aan de voorzijde van de smartphone zijn gesitueerd.[31] Apple geeft aan dat de gezichtsherkenningstechnologie het beste werkt wanneer de smartphone op een armlengte of minder afstand van het gezicht wordt gehouden, waarbij zij een indicatie geven van een afstand van ongeveer 25-50 centimeter.[32]

Op het moment dat de gebruiker vervolgens de telefoon wil ontgrendelen door middel van de gezichtsherkenningstechnologie, wordt het opgeslagen gezicht vergeleken met wat de camera op dat moment te zien krijgt. Als de gezichtsherkenningstechnologie een overeenkomst constateert, wordt de telefoon ontgrendeld.[33]

4.2 *Verschillen in de technologie*

Zoals zojuist kort aangestipt, werkt niet elke gezichtsherkenningstechnologie hetzelfde en zijn zij niet allemaal even betrouwbaar. In deze sub-paragraaf bespreken wij dat nader en categoriseren wij de verschillende technieken. Dat is belangrijk, omdat niet alle gezichtsherkenningstechnologieën in dezelfde mate gebruikmaken van gedragsgerelateerde kenmerken. Wij onderscheiden vier verschillende categorieën gezichtsherkenningstechnologie, waarvan de eerste drie gebaseerd zijn op de 2D-scan door een frontcamera en de vierde gebaseerd is op de 3D-scan door de frontcamera ondersteund door infraroodtechnologie.

De eerste categorie behelst de meest simpele gezichtsherkenningstechnologie waarbij het tonen van een afbeelding van het gezicht van de smartphonehouder reeds voldoende is om de smartphone te ontgrendelen. Wanneer een categorie 1-gezichtsherkenningstechnologie wordt aangetroffen, zal ontgrendeling eenvoudig kunnen plaatsvinden. Zonder medewerking van de verdachte en zonder dwang kan een opsporingsambtenaar met een afbeelding de telefoon ontgrendelen (denk aan een aangetroffen ID-bewijs of een op het politiebureau aan de ID-zuil genomen foto).

De tweede categorie behelst de verder ontwikkelde gezichtsherkenningstechnologie waarbij een foto te weinig is, doch het vluchtig tonen van (de contouren van) het gezicht reeds voldoende is om de smartphone te ontgrendelen. Wanneer een categorie 2-gezichtsherkenningstechnologie wordt aangetroffen, en dus meer nodig is dan een enkele foto, is de aanwezigheid van verdachte noodzakelijk. Bij deze categorie scant de technologie op een globale, een vage gelaatsuitdrukking. De stand van de ogen en de afstand tussen het voorhoofd en de kin worden hierbij bijvoorbeeld gebruikt.

De derde categorie behelst dezelfde gezichtsherkenningstechnologie waarbij een duidelijk beeld van het gezicht van de smartphonehouder moet worden getoond. Wanneer de gezichtsherkenningstechnologie kennelijk een duidelijker beeld van het gezicht van de smartphonehouder vereist om tot ontgrendeling over te gaan, dan zal niet alleen de aanwezigheid van de verdachte nodig zijn, maar ook diens medewerking, zo nodig onder toepassing van enige dwang, om op deugdelijke wijze een gezicht aan te bieden. Deze categorie 3-gezichtsherkenningstechnologie vereist een duidelijk beeld van het gezicht. Wel zij opgemerkt dat dit nog altijd gaat om een 2D-scan van het gezicht. Het fixeren van het gezicht met behulp van bijvoorbeeld een collega-opsporingsambtenaar die het gezicht met beide handen rechthoudt, kan zodoende een smartphone ontgrendelen.[34]

De vierde en laatste door ons onderscheiden categorie behelst de ontgrendeling door *state of the art* gezichtsherkenningstechnologie voor smartphones. De technologie van Apple loopt hierin momenteel voorop. Op dit moment behelst die categorie 4-gezichtsherkenningstechnologie de technologie die met behulp van infraroodtechnologie een 3D-scan van een gezicht kan maken. In dit geval dient een gezicht *precies* te worden aangeboden. Het gesloten houden van de ogen, een andere richting opkijken of een modellering van het gezicht kunnen ertoe leiden dat de smartphone niet ontgrendelt, afhankelijk van welke houding is ingesteld waarmee moet worden vergeleken. Deze vorm van gezichtsherkenningstechnologie gaat uit van verschillende punten in het gezicht waarbij afstand tot elkaar, maar ook de diepte ervan, wordt gemeten. De modelleringsmogelijkheden van het gezicht gaan dus een stap verder en dat betekent dat het voor verdachten eenvoudiger is om een succesvolle ontgrendeling door opsporingsambtenaren te frustreren. Opsporingsambtenaren moeten zodoende meer fysieke dwang uitoefenen op de eigenaar van de smartphone als zij deze smartphone willen ontgrendelen. Deze vorm van gezichtsherkenningstechnologie is gefocust op fysieke kenmerken, maar gedragsafhankelijke kenmerken kunnen de ontgrendeling beïnvloeden. Dit betekent in theorie dat een smart-

30 Aarzu Khan, 'Is Facial Recognition on Your Smartphone a Good Choice?', dazeinfo.com 12 november 2021; 'What Is Facial Recognition on a Phone?', xfinity.com, 31 januari 2019.

31 Maggie Tillman, 'What is Apple Face ID and how does it work?', pocket-lint.com 3 september 2021.

32 'Over de geavanceerde technologie achter Face ID', support.apple.com, 23 maart 2022.

33 Calvin Wankhede, 'Facial recognition on smartphones: Is it secure and should you use it?', androidauthority.com 7 november 2021; 'About Face ID advanced technology', apple.com 14 september 2021.

34 Ook de wetgever gaat hiervan uit, zie: Toelichting bij de ambtelijke eindversie Wetboek van Strafvordering van juli 2020, p. 426.

phonehouder niet alleen een gezicht kan trekken waardoor de smartphone *niet* ontgrendelt, maar ook dat hij een gemodelleerd gezicht als standaard instelt en de smartphone enkel ontgrendelt als het gezicht in die bewust gemodelleerde vorm wordt aangeboden (bijvoorbeeld dat de mond altijd geopend moet zijn of de wenkbrauwen maximaal opgetrokken). Dit maakt dat deze technologie *de facto* focust op gedragsmatige kenmerken.

4.3 *De betrouwbaarheid van de technologie*

De hierboven besproken verschillende technieken laten een opbouwende mate van betrouwbaarheid zien. De gezichtsherkenningstechnologie is niet feilloos en gebruikers, maar ook ontwikkelaars merken op dat in een aantal gevallen vals-positieve en vals-negatieve ontgrendelingen optreden. Een vals-positieveontgrendeling betekent dat een smartphone foutief wél is ontgrendeld. Een vals-negatieve ontgrendeling betekent dat een smartphone foutief niet ontgrendelt, terwijl het ingestelde gezicht wordt aangeboden. De introductie van het grootschalig commercieel gebruik van de gezichtsherkenningstechnologie door smartphoneaanbieders is aanleiding geweest voor een legio aan (quasi)experimenten en onderzoeken van consumenten, (tech)journalisten en wetenschappelijk onderzoekers naar de betrouwbaarheid, en daarmee gepaarde veiligheidsrisico's, van de gezichtsherkenningstechnologie.

Uit een onderzoek van de Consumentenbond uit 2019 bleek dat het mogelijk was om bij 29 van de 60 onderzochte smartphones de gezichtsherkenningstechnologie te bedriegen door middel van een goede portretfoto.[35] Verschillende nieuwsplatformen verrichten eigen onderzoek waaruit bleek dat de gezichtsherkenningstechnologie niet in staat was om de gebruiker van de smartphone en een tweeling of een broer of zus te onderscheiden. In sommige gevallen lukte het zelfs de dochter de telefoon van haar moeder te ontgrendelen.[36] Onderzoekers die een presentatie gaven bij de veiligheidsconference *Black Hat USA* in 2019 presenteerden resultaten waarmee zij lieten zien dat Apple's *Face ID* kon worden ontgrendeld bij een slapend persoon door een bril op of voor zijn hoofd te plaatsen waarvan de glazen waren bedekt met zwarte en witte tape teneinde de ogen na te bootsen. Volgens de onderzoekers werkt deze methode van omzeiling omdat de gezichtsherkenningstechnologie geen 3D-informatie uit het gebied rondom de ogen haalt als het een bril herkent. Door met de tape een oog te fingeren, kon de telefoon worden ontgrendeld.[37]

35 Peter Kulche, 'Gezichtsherkenning op Smartphone Niet Altijd Veilig' consumentenbond.nl 15 april 2019.

36 'Face ID wel veilig? Deze zussen kunnen elkaars telefoon ontgrendelen', rtlnieuws.nl, 30 november 2020; Ankita Chakravarti, 'Brothers who are not identical twins fool iPhone 12 mini's Face ID', indiatoday.in 9 juni 2021.

37 Lindsey O'Donnell, 'Researchers Bypass Apple FaceID Using Biometrics 'Achilles Heel', threatpost.com 8 augustus 2019.

Uit bovenstaande beschrijving wordt in ieder geval duidelijk dat de gezichtsherkenningstechnologie niet feilloos is. Uit meerdere tests en onderzoeken blijkt dat de technologie gezichten 'herkent', terwijl evident is dat niet de persoon wordt gescand die de gezichtsherkenningstechnologie heeft ingeschakeld. Onduidelijk blijft echter in hoeverre de gezichtsherkenningstechnologie *niet* werkt doordat bewuste spierbewegingen worden gemaakt. Om een impressie te krijgen van de effecten daarvan, hebben wij een vragenlijst uitgezet onder collega's, kennissen en studenten.

5. De proef op de som: is gezichtsherkenning te misleiden?

Gelet op de verschillen die er bestaan in de kwaliteit van de gezichtsherkenningstechnologie onder smartphones, en er geen onderzoeken bestaan die per telefoon onderzoeken wat de feilbaarheid is van de gezichtsherkenningstechnologie hebben wij, zoals aangekondigd, zelf de proef op de som genomen. Wij hebben een vragenlijst afgenomen die per e-mail is verzonden in maart en april 2022.

5.1 *De vragenlijst*

De vragenlijst start met enkele inleidende vragen over het merk en model van de smartphone, de gebruikte softwareversie en of er bijzonderheden zijn aan de telefoon (denk hierbij aan beschadigingen of afgenomen kwaliteit van de frontcamera). Na deze vragen beantwoord te hebben, vangt de respondent aan met het onderzoek. De vraag die bij alle dertien vragen centraal staat, is of de smartphone nog kan worden ontgrendeld in de beschreven situatie of 'gezichtshouding'. De respondent geeft hier antwoord op door middel van het antwoorden van 'ja' of 'nee'. Elke 'gezichtshouding' of situatie dient drie keer te worden getoetst, waarbij 'nee' ingevuld dient te worden indien ontgrendeling van de smartphone niet lukt bij één van de drie pogingen. Het antwoord 'ja' dient te volgen bij drie succesvolle pogingen.

In de eerste elf vragen verzoeken wij de respondent om telkens een andere 'gezichtshouding' aan te nemen. Wij verstaan onder het begrip 'gezichtshouding' de stand, of houding, van het gezicht terwijl de respondent de smartphone probeert te ontgrendelen. Alvorens de in de vragen beschreven 'gezichtshoudingen' aan te nemen, dient de respondent eerst een neutrale 'gezichtshouding' aan te nemen. Hieronder verstaan wij een gesloten mond, open ogen en een horizontaal gezichtsveld. De volgende gezichtshoudingen worden gevraagd van de respondent: de ogen gesloten; de ogen bewogen naar links; rechts; naar boven; of naar onderen; de mond volledig geopend; de wenkbrauwen maximaal opgetrokken en het hoofd bewogen; in een hoek van 45 graden, naar links; rechts; naar boven; of naar onderen. Vervolgens worden nog twee vragen gesteld die toezien op de vraag of de smartphone ook kan worden ontgrendeld door middel van een gedrukte

gestandaardiseerde pasfoto (een officiële pasfoto, een rijbewijs of een paspoort of ID-kaart) en een normale foto.

5.2 *Demografische kenmerken van de respondenten en kenmerken van de gebruikte smartphones*

De vragenlijst die wij per e-mail hebben uitgezet, is door negen respondenten beantwoord. De respondenten vallen in de leeftijdscategorie 22-32 jaar en zijn, zoals geschreven, studenten, kennissen en collega's van de auteurs. De *responserate* onder studenten bedroeg ongeveer 5%, waarbij het onderzoek is uitgevoerd door twee van de 36 aangeschreven studenten. De *responserate* onder collega's bedroeg ook ongeveer 5%, waarbij drie van de 78 collega's de vragenlijst hebben ingevuld. Onder kennissen hadden wij de hoogste *responserate*, waarbij bijna allen voldeden aan het verzoek om het onderzoek uit te voeren en de vragenlijst in te vullen (drie van de vier).

De verdeling binnen de respondenten in het gebruik van de verschillende merken smartphones was als volgt: zes respondenten maken gebruik van een smartphone van Apple, variërend van de iPhone XR tot aan de iPhone 13, met softwareversies variërend van iOS 14.7.1, 14.8.1, 15.2.1 tot aan 15.3.1; één respondent van een OPPO Find X3 Lite met softwareversie Android 11/ColorOS 11.1; één respondent van een Huawei P30 Lite met softwareversie Android 10 en één respondent van een Samsung Galaxy S20 met softwareversie Android 12. Belangrijk om te bespreken in dit kader is dat OPPO, Huawei en Samsung allemaal gebruikmaken van hetzelfde besturingssysteem, namelijk Android. Deze drie merken smartphones gebruiken echter niet dezelfde gezichtsherkenningstechnologie. Hoewel de smartphones hetzelfde besturingssysteem gebruiken, onderscheiden zij zich op andere manieren. De website *Android Authority* vat dit als volgt samen:

> "The speed level of security provided by this technique varies a lot, and many Android OEMs (*original equipment manufacturers*) have worked to improve on it over the years. The quality of the front camera is a determining factor, as is the complexity of the algorithm used to extract facial details. The use of neural network hardware can also accelerate more secure algorithms on high-end smartphones."[38]

5.3 *Resultaten*

Uit het onderzoek zijn de volgende opvallende resultaten gekomen. De respondent die gebruikmaakt van de OPPO geeft aan dat de smartphone kan worden ontgrendeld bij alle 'gezichtshoudingen' en situaties uit de vragenlijst, op de gestandaardiseerde pasfoto na. Dit maakt dat de gezichtsherkenningstechnologie van deze smartphone, met enige afstand, het meest eenvoudig te ontgrendelen én te omzeilen lijkt. De OPPO wordt gevolgd door de Huawei, in het kader van welke smartphone het eenvoudigst ontgrendelbaar en omzeilbaar lijkt. De Huawei is enkel niet ontgrendeld bij gesloten ogen, het hoofd ongeveer 45 graden naar boven en onderen gekanteld en bij de gestandaardiseerde pasfoto en de normale foto. De Huawei wordt weer opgevolgd door de Samsung, die wisselende resultaten laat zien bij de verschillende 'gezichtshoudingen' en wel kan worden ontgrendeld door middel van een normale foto. Hiermee lijken de smartphones die gebruikmaken van het besturingssysteem Android tot de meest feilbare te behoren in die zin dat omzeiling van de technologie goed mogelijk is. Wel zij het dat het verschil tussen sommige smartphones van Apple en de Samsung klein is (één keer minder 'ja' ingevuld).

Bij de smartphones van Apple valt op dat bijna alle modellen niet kunnen worden ontgrendeld terwijl de respondent het hoofd in de vier verschillende 45 graden hoeken beweegt. Alleen de iPhone 13 kan worden ontgrendeld bij elk van de vier verschillende hoofdbewegingen. De iPhone Pro Max kan worden ontgrendeld bij een 45 graden beweging met het hoofd naar links en rechts, maar niet naar boven en onderen. Aangezien de modellen van Apple waarbij bij de verschillende hoofdbewegingen niet tot ontgrendeling leiden oudere versies betreffen dan de iPhone Pro Max en de iPhone 13, zou dit aan de vooruitgang van de gezichtsherkenningstechnologie kunnen liggen. Een ander punt dat opvalt bij de smartphones van Apple is dat geen van de toestellen kan worden ontgrendeld door middel van een gestandaardiseerde pasfoto of een normale foto. Dit betekent dat de Appletoestellen en -software bezien de gezichtsherkenningstechnologie als meest feilloos uit deze test komen.

5.4 *Tussenconclusie*

Op basis van de voorgaande resultaten kunnen wij de volgende, nadrukkelijk onder voorbehoud gemaakte, tussenconclusies trekken. Gebaseerd op deze steekproef blijkt dat de gebruikers van oudere modellen *casu quo* besturingssystemen van Apple de meest onterechte niet-ontgrendelingen registreren (vals-negatief). Bij deze gebruikers leidt *gedrag* regelmatig tot een niet-herkenning.

Bij de nieuwe modellen en besturingssystemen van Apple en de smartphones met een Android-besturingssysteem worden minder niet-herkenningen geregistreerd. Alleen de OPPO werd in alle gevallen, ondanks het gedrag van de respondent, ontgrendeld. Bij de andere smartphones bestaat enige ruimte om met gedrag de herkenning te manipuleren. Het is niet ondenkbaar dat verdachten met wegkijken of door spiermodelering in het gezicht een afgedwongen ontgrendeling kunnen frustreren. In welke gevallen welke mate van dwang mag worden toegepast, bespreken wij in de volgende en tevens laatste paragraaf.

38 Robert Triggs, 'Facial recognition technology explained', androidauthority.com 14 januari 2019.

6. Analyse en conclusie

Wat betekent dit nu voor het ontgrendelen van een smartphone door middel van gezichtsherkenning, waarbij de opsporingsambtenaar de verdachte *verplicht* om in de camera van de smartphone te kijken of een foto van de verdachte gebruikt ter ontgrendeling? Daarvoor zijn twee elementen van belang nader te analyseren, te weten (i) de definitie van biometrie; en (ii) de classificatie van gezichtsherkenning als gedragsgerelateerde biometrie.

6.1 *De definitie van biometrie*

Wat betreft de definitie van biometrie bestaat een duidelijk verschil tussen de grammaticale definitie en de juridische definitie. De grammaticale definitie beslaat alleen *biologische kenmerken* en sluit gedragsgerelateerde kenmerken uit. In de grammaticale definitie van biometrie zou door opsporingsambtenaren alleen mogen worden ontgrendeld wanneer de ontgrendelmethode enkel gebruikmaakt van *biologische kenmerken*. In de juridische definitie omvat biometrie ook *gedragsgerelateerde kenmerken*. Zo is de iris een biologisch kenmerk, maar is het sluiten van de ogen een gedragsgerelateerd kenmerk. De iris is onder beide definities biometrie, maar het bewegen van de oogleden ten behoeve van gezichtsherkenning kan alleen onder de juridische definitie als biometrie worden geclassificeerd. Die definitie heeft daardoor een veel breder bereik en biedt dan ook meer mogelijkheden om allerlei methoden onder het begrip biometrisch ontgrendelen te plaatsen.

De discrepantie tussen de grammaticale en juridische definitie is van groot belang voor de toetsing van gedwongen ontgrendeling onder het nemo-teneturbeginsel. In de rechtspraak van het EHRM staat bij die toetsing de aard en mate van dwang centraal, maar welke aard en mate van dwang is geoorloofd, is mede afhankelijk van de vraag of het materiaal onafhankelijk van de wil van de verdachte bestaat. Bij een grammaticale definitie van biometrie is zonneklaar dat op het moment dat het om onveranderlijke biologische kenmerken gaat, die, vertaald naar de rechtspraak van het EHRM, *onafhankelijk* van de wil van de verdachte bestaan. Bij de juridische definitie van biometrie, waaronder ook gedragsgerelateerde kenmerken vallen, lijken ook gedragingen te vallen die zijn aan te merken als *afhankelijk* van de wil bestaand materiaal (zoals het bewegen van de ogen of oogleden). Dat betekent dat bij de laatste definitie en als gebruik wordt gemaakt van gedragsgerelateerde identificatie geen (tot maximaal zeer geringe) dwang mag worden gebruikt, opdat het nemo-teneturbeginsel niet wordt geschonden. Dat laatste lijkt echter heel lastig: juist doordat gedragsgerelateerde kenmerken invloed hebben op de ontgrendeling – bijvoorbeeld een bepaalde gezichtsmimiek – is meer dwang nodig – namelijk een volledige fixatie zodat de verdachte door gedrag te vertonen de ontgrendeling niet kan frustreren.

Het lijkt daarom raadzaam om in het toetsingskader van het biometrisch ontgrendelen in het licht van het nemo-teneturbeginsel aansluiting te zoeken bij de grammaticale definitie. Alleen de biologische kenmerken kunnen met zekerheid als onafhankelijk van de wil bestaand worden aangemerkt, waardoor die volgens de rechtspraak van de Hoge Raad met enige fysieke dwang tegen de wil van de verdachte kunnen worden gebruikt om een elektronische gegevensdrager te ontgrendelen. Hierbij dient de opsporingsambtenaar óf kennis te hebben van de beveiligingssoftware op de inbeslaggenomen smartphone waardoor hij weet dat hij met weinig dwang een ontgrendeling kan afdwingen, óf moet hij zich terughoudend opstellen in het afdwingen van een ontgrendeling als blijkt dat enige gedragsgerelateerde ontgrendelfrustrering door de verdachte succesvol blijkt.

6.2 *Is gezichtsherkenning een biometrische ontgrendelmethode?*

Dit betekent echter nog niet dat gezichtsherkenning een biometrische ontgrendelmethode is onder de grammaticale definitie. Daarvoor is van belang in welke mate gedragsgerelateerde kenmerken invloed hebben op de herkenning van de correcte persoon. Het gaat er dan dus om of de verdachte, doordat hij recht in de camera moet kijken zonder bepaalde spieren in zijn gezicht te bewegen voor een geslaagde herkenning, met zijn wil invloed heeft op de herkenning.

Uit ons onderzoek en uit de publicaties over de techniek blijkt dat door middel van gedrag de herkenning kan worden gemanipuleerd, in die zin dat het gezicht dat wordt aangeboden en tot ontgrendeling zou moeten leiden, niet tot daadwerkelijke ontgrendeling leidt. Dit geldt vooral wanneer de ogen worden bewogen of gesloten of wanneer het hoofd in een hoek – dus niet frontaal – wordt aangeboden.

Dit maakt het heel moeilijk in algemene zin te beantwoorden in hoeverre gedwongen identificatieverificatie door middel van gezichtsherkenning een schending van het nemo-teneturbeginsel oplevert, omdat dat antwoord sterk afhankelijk is van de stand der techniek. Aan de ene kant lijkt de conclusie gerechtvaardigd dat de verdere ontwikkeling van de techniek waarbij softwareontwikkelaars een afname van vals-negatieve ontgrendelpogingen nastreven, en er dus minder ruimte is voor de niet-herkenning door gedrag, de gezichtsherkenning als biometrisch moet worden bestempeld. De eigenaar van de smartphone zal dan altijd – ongeacht de stand van diens gezicht – worden herkend als de rechtmatig gebruiker-eigenaar van de smartphone. Als de verdachte de herkenning *niet* kan beïnvloeden door gedragsgerelateerde kenmerken dan is de gezichtsherkenning volledig of doorslaggevend gebaseerd op biologische kenmerken. Aan de andere kant ontwikkelt de techniek zich zodanig dat de smartphone alleen wordt ontgrendeld als de ingestelde mimiek wordt aangeboden, en dat is juist gedragsgerelateerd.

Op dit moment is het antwoord of gezichtsherkenning te categoriseren is als biometrisch in de grammaticale zin van het woord niet te geven, maar is dat antwoord volledig afhankelijk van het gebruikte model, besturingssysteem en/of verificatietechniek. Als de verdachte met simpele bewegingen de ontgrendeling kan frustreren, dan betekent dat dat de identificatieverificatie afhankelijk is van zijn wil. Daardoor biedt het nemo-teneturbeginsel een grotere mate van bescherming, namelijk dat in beginsel geen dwang mag worden gebruikt. Dat geldt ook voor de ontgrendeling door middel van een bepaalde mimiek. Alleen als zonder gedragsgerelateerde kenmerken kan worden ontgrendeld, is er volgens ons sprake van geoorloofd biometrisch ontgrendelen.

6.3 *Nadere overwegingen over de aard en mate van dwang*

Wij hebben tot nu toe onbesproken gelaten welke aard en mate van dwang ten behoeve van gezichtsherkenning dan geoorloofd zou zijn. Bij de identificatieverificatie door middel van een vingerafdruk is geoorloofd dat de bewegingsvrijheid van de verdachte wordt beperkt door hem te boeien aan een tafel of stoel en vervolgens met enige kracht zijn hand vast te pakken, zijn duim te strekken en op de scanner te leggen. Aangezien het hier gaat om een klein onderdeel van het lichaam dat moet worden gescand, is het eenvoudiger hierbij (geringe) dwang toe te passen. Deze dwang is *mutatis mutandis* ook toegestaan bij een afgedwongen ontgrendeling door middel van de irisscan.

Bij ontgrendeling van de smartphone door middel van gezichtsherkenning moet meestal frontaal in de camera worden gekeken en geen oogbewegingen worden gemaakt. In het kader van de eerdergenoemde gezichtsherkenningstechnologieën 1 en 2 zou een fixatie van het hoofd door vasthouding van het hoofd door een opsporingsambtenaar onzes inziens toegestane geringe, kortstondige dwang opleveren in de zin van het arrest van februari 2021. Als met behulp van deze fixatie geen ontgrendeling wordt bewerkstelligd, heeft de opsporingsambtenaar dus te maken met een gezichtherkenninsgstechnologie 3 of 4. Bij gedwongen ontgrendeling zou de verdachte in die gevallen eigenlijk volledig moeten worden gefixeerd, inclusief zijn nek en hoofd, omdat hij anders eenvoudig met zijn romp, nek of hoofdbewegingen kan maken. De vraag is of een kortstondige, volledige fixatie nog als een geringe inbreuk op de lichamelijke integriteit kan worden bestempeld. Ook moeten op de een of andere wijze zijn ogen open worden gehouden. Dan is het nog steeds onmogelijk voor opsporingsambtenaren om de bewegingen van de oogbal te voorkomen, en bovendien zullen fixeermechanismen om de ogen open te houden, de ontgrendeling frustreren als deze meetpunten in het gezicht bedekken. Bij perfect werkende *state of the art* technologie zal zelfs elke minimale, doch afwijkende spierbeweging in het gezicht onder dwang moeten worden gemodelleerd ter succesvolle ontgrendeling van de smartphone. Deze vorm van fixatie maakt direct duidelijk dat de gezichtsherkenning waarin gedragsgerelateerde kenmerken invloed hebben op de herkenning een andere aard en mate van dwang noodzakelijk maken. Hoogstwaarschijnlijk kan dit niet als een geringe inbreuk op de lichamelijke integriteit worden gezien.

Ten slotte lijkt, in het kader van de subsidiariteit, het altijd wenselijk en noodzakelijk de smartphone in eerste instantie te proberen te ontgrendelen met een foto of door medewerking van een gelijkend persoon zoals een bereidwillig familielid (behoudens eventuele verschoningsgerechtigden). Uit de berichtgeving over gezichtsherkenning en ons onderzoek blijkt dat dit in sommige gevallen lukt. Omdat hierbij geen enkele lichamelijke dwang wordt gebruikt, is deze vorm van identificatieverificatie een subsidiaire vorm van gezichtsherkenning. Daarbij verdient het ook nog opmerking dat de foto onafhankelijk van de wil van de verdachte bestaat – zoals het geval is bij alle documenten – en dat bij de ontgrendeling door middel van een foto[39] geen schending van het nemo-teneturbeginsel plaatsvindt.

6.4 *Conclusie*

In deze bijdrage zijn wij ingegaan op gezichtsherkenning als biometrische identificatieverificatie omdat het gebruik daarvan op de meeste smartphones mogelijk is (en het daadwerkelijke gebruik zal toenemen). Daarmee ligt het voor de hand dat de praktijk wordt geconfronteerd met de vraag of het ontgrendelen door middel van gezichtsherkenning onder het biometrisch ontgrendelen valt. In de literatuur is tot nu, zonder nadere onderbouwing, ervan uitgegaan dat de ontgrendeling door middel van gezichtsherkenning onder het biometrisch ontgrendelen valt. In dit artikel laten wij zien dat die conclusie voorbarig is. Of gezichtsherkenning een vorm van biometrische ontgrendeling is, hangt namelijk af van de keuze voor een grammaticale of juridische definitie van biometrie en de stand van de verificatietechniek.

Wij opteren voor een grammaticale definitie: de (bredere) juridische definitie omvat namelijk ook gedragsgerelateerde kenmerken. Als de verdachte wordt gedwongen zich op een bepaalde manier te gedragen – bijvoorbeeld door frontaal in de camera te kijken – dan wordt materiaal verkregen dat afhankelijk van de wil van de verdachte bestaat. Bij gedragsgerelateerde biometrische kenmerken is dan veel sneller sprake van een schending van het nemo-teneturbeginsel, nog daargelaten dat een hoge mate van dwang noodzakelijk is om de niet-meewerkende verdachte neutraal en frontaal in een camera te laten kijken.

39 Of een siliconen model: vergelijk deze zaak waarin een 3D geprinte vinger ter ontgrendeling is gebruikt: https://www.theverge.com/2016/7/21/12247370/police-fingerprint-3D-printing-unlock-phone-murder, laatst geraadpleegd op 22 februari 2022.