FACULTEIT
RECHT EN CRIMINOLOGIE

Digitale Controle op Migratie vs. het Recht op Privacy en Gegevensbescherming in België:

De toegang tot smartphones en sociale mediaprofielen in Belgische verzoekprocedures om internationale bescherming

Lore Roels
Studentennummer: 01407012

Promotoren: Prof. Dr. Ellen Desmet, Prof. Dr. Eva Lievens
Commissaris: Lennert Dierickx

Masterproef voorgelegd tot behalen van de graad van Master of Laws in de rechten

Aantal woorden: 50 659

Academiejaar: 2019 – 2020

UNIVERSITEIT
GENT

Voorwoord

Deze masterproef bewandelt, zoals de titel doet vermoeden, de grens tussen het asielrecht en het privacy- en gegevensbeschermingsrecht. In dit sluitstuk van mijn rechtenopleiding ga ik meer bepaald op zoek naar het evenwicht tussen het belang van een overheid, bij het bestrijden van misbruik in procedures om internationale bescherming, en het belang van verzoekers om internationale bescherming, bij de uitoefening van hun recht op privacy en gegevensbescherming. Ik spits me hierbij toe op de recente wetswijziging van de Belgische Vreemdelingenwet (21 november 2017), die het (onder andere) mogelijk maakt voor het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen om zich toegang te verschaffen tot smartphones en sociale mediaprofielen van verzoekers, ter beoordeling van hun verzoek om internationale bescherming.

In "Er zijn geen paarden in Brussel" [1], een bundel met zes vluchtelingenverhalen, beschrijft Rachida Lamrabet hoe een van deze vluchtelingen haar verzoekprocedure om internationale bescherming ervaarde:

> *"Ik kan een tocht door de hel niet minutieus reconstrueren. Ik kan de deur die naar dat verleden leidt, niet openen want achter die deur zijn de stenen waarmee ik mijn verhaal moet heropbouwen gloeiend heet."*
>
> – De dingen waar ik bang voor ben | Rachida Lamrabet

Toch is de Belgische verzoekprocedure om internationale bescherming opgebouwd om die 'deur naar het verleden' open te trekken, ongeacht de manier waarop en vaak ongeacht welke fundamentele rechten daarbij moeten sneuvelen. Het doel blijkt de middelen te heiligen. In dit onderzoek zijn die middelen de sociale mediaprofielen en smartphones van mensen op de vlucht. Aan het ongelimiteerd doorzoeken daarvan om misbruik te bestrijden is volgens mij niets heiligs, en volgens de conclusie van deze masterproef ook niets wettigs.

Ik schreef deze masterproef, geleid door mijn eigen passie voor het migratierecht en de mensenrechten, maar ook door de hoop om hiermee een stem te kunnen zijn voor een groep, wiens stem te vaak gedempt blijft.

Ik wil hierbij in de eerste plaats mijn promotoren, Prof. Dr. Ellen Desmet en Prof. Dr. Eva Lievens, en commissaris, Lennert Dierickx, bedanken voor hun deskundige begeleiding en constructieve feedback gedurende het schrijfproces. Daarnaast wil ik ook mijn ouders, Silke, Jozefien, Maud en Braam bedanken, voor hun bemoedigende woorden en kritische blikken, niet alleen tijdens het schrijven van deze masterproef, maar doorheen mijn hele rechtenopleiding.

[1] Lamrabet, R. "De dingen waar ik bang voor ben" in Al Galidi, R., Lamrabet, R., Demyttenaere, B., Van Beirs, P., Van Ranst, D. en De Cock, M. Er zijn geen paarden in Brussel: Vluchtelingenverhalen. Berchem: Uitgeverij EPO, 2015. P. 29-30.

Abstract

Deze masterproef spitst zich toe op de recente wetswijziging van de Belgische Vreemdelingenwet (21 november 2017), die het (onder andere) mogelijk maakt voor het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen (CGVS) om zich toegang te verschaffen tot smartphones en sociale mediaprofielen van verzoekers, ter beoordeling van hun verzoek om internationale bescherming. In dit kader wordt het evenwicht geanalyseerd tussen het belang van een overheid, bij het bestrijden van misbruik in procedures om internationale bescherming, en het belang van verzoekers om internationale bescherming, bij de uitoefening van hun recht op privacy en gegevensbescherming. Specifiek wordt een antwoord gezocht op de vraag of deze bevoegdheid van het CGVS in overeenstemming is met het toepasselijk (inter)nationaal asiel-, privacy- en gegevensbeschermingsrechtelijk kader en zo nee, onder welke voorwaarden en met welke waarborgen deze schending eventueel kan worden geremedieerd.

Allereerst moet worden vastgesteld dat de conformiteit van de wetswijziging met het toepasselijk (inter)nationaal asiel-, privacy- en gegevensbeschermingsrechtelijk kader niet kan worden bevestigd. Voor de wettelijke vereisten in het asielrechtelijk kader wordt vastgesteld dat de bevoegdheid van het CGVS een verkeerde omzetting vormt van de Europese regelgeving en op onevenwichtige wijze de medewerkingsplicht van de verzoeker om internationale bescherming benadrukt. Wat het privacy- en gegevensbeschermingsrechtelijk kader betreft, vormt de wetswijziging een fundamentele beperking van het recht op gegevensbescherming van verzoekers. De artikelen voldoen op zichzelf namelijk aan geen enkele van de gegevensverwerkingsvereisten in de Algemene Verordening Gegevensbescherming (AVG). Tevens beantwoorden deze artikelen aan geen enkele van de voorwaarden voor een gerechtvaardigde beperking van het recht op privacy en gegevensbescherming. De onderzoeksbevoegdheid van het CGVS met betrekking tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vormt dus een onmiskenbare schending van het recht op privacy en gegevensbescherming van de verzoekers.

Vervolgens worden, op basis van de relevante beginselen en regels in de AVG, het EVRM en het EU-Handvest van de Grondrechten, de geïdentificeerde pijnpunten en een praktijk- en rechtspraakschets, een aantal waarborgen voorgesteld om conformiteit met het asiel-, privacy- en gegevensbeschermingsrechtelijk kader te bewerkstelligen. De voorgestelde waarborgen zouden afzonderlijk bepaalde tekortkomingen in de besproken wetswijziging (kunnen) remediëren. Er bestaan echter substantiële hindernissen voor het implementeren ervan en het aangekondigde KB, om aan de geuite privacybekommernissen tegemoet te komen, blijkt hiervoor geen geschikt instrument. De waarborgen kunnen ten eerste niet cumulatief worden toegepast. Ten tweede brengen bepaalde waarborgen discriminatoire gevolgen met zich mee. Ten derde kan het gebrek aan het wettelijk vereist ‘algemeen belang’ of ‘gerechtvaardigd doel’ door geen enkele waarborg worden geremedieerd. Tot slot moet worden vastgesteld dat de ‘nadelen’ van de bevoegdheid van het CGVS (zowel de flagrante schending van de fundamentele rechten van verzoekers om internationale bescherming, als de effectieve ‘kosten’ van de onderzoeksbevoegdheid) onmogelijk opwegen tegen de minimale bewijswaarde en het empirisch vastgestelde verwaarloosbare ‘succespercentage’ van het doorzoeken van sociale mediaprofielen en smartphones in verzoekprocedures om internationale bescherming.

Inhoudsopgave

Lijst met afkortingen 11

1. Inleiding 13

1.1. Toegang tot smartphones en sociale mediaprofielen in Belgische verzoekprocedures om internationale bescherming: de wetswijziging van 21 november 2017 13

1.2. Benadering van de probleemstelling 16

1.3. Methodologie 19

1.4. Beperkingen van het onderzoek 20

1.5. Wetenschappelijke relevantie van het onderzoek 21

2. Theoretisch kader: toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vanuit asielrechtelijk perspectief 24

2.1. Het Europees asielrechtelijk kader 24

2.1.1. Omzetting van de Procedurerichtlijn 24

2.1.1.1. Artikel 13, lid 2, d) Procedurerichtlijn 24

2.1.1.2. Betwiste toepasselijkheid van de Procedurerichtlijn 24

2.1.2. Omzetting van de Kwalificatierichtlijn 26

2.2. Medewerkingsplicht, samenwerkingsplicht en gedeelde bewijslast binnen verzoekprocedures om internationale bescherming 26

2.2.1. De medewerkingsplicht 27

2.2.2. De samenwerkingsplicht en de daaruit voortvloeiende gedeelde bewijslast 28

3. Theoretisch kader: toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vanuit privacy- en gegevensbeschermingsrechtelijk perspectief 32

3.1. Het recht op privacy versus het recht op gegevensbescherming 32

3.2. Het Europees gegevensbeschermingsrechtelijk kader: de Algemene Verordening Gegevensbescherming 35

3.3. Het Belgisch gegevensbeschermingsrechtelijk kader: de Wet Bescherming Persoonsgegevens 37

4. Voorwaarden voor gegevensverwerking en beperkingen op het recht op gegevensbescherming 38

4.1. Beginselen in de Algemene Verordening Gegevensbescherming 38

4.1.1. Rechtmatige, behoorlijke en transparante verwerking 38

4.1.2. Doelbindingsprincipe, dataminimalisatie, nauwkeurigheid, opslagbeperking, integriteit en vertrouwelijkheid 39

4.2. Rechtmatigheid van de verwerking in de Algemene Verordening Gegevensbescherming 41

4.2.1. Alle persoonsgegevens 41

4.2.1.1. Toestemming 42

4.2.1.2. Unie- of lidstaatrechtelijke wettelijke verplichting 45

4.2.1.3. Taak van algemeen belang 46

4.2.2. Bijzondere categorieën van persoonsgegevens: gevoelige gegevens 47

4.2.2.1. Uitdrukkelijke toestemming 49
4.2.2.2. Uitdrukkelijke openbaarmaking 49
4.2.2.3. Zwaarwegend algemeen belang 49
4.2.3. Overzicht van de verwerkingsgronden voor alle persoonsgegevens en de uitzonderingen voor gevoelige gegevens 49
4.3. Beperkingen op het recht op gegevensbescherming en de daaraan verbonden voorwaarden 51
5. Toepassing van het theoretisch kader: geïdentificeerde pijnpunten 55
5.1. Verkeerde omzetting en onevenwichtige benadrukking van de medewerkingsplicht 55
5.1.1. Verkeerde omzetting van de medeweringsplicht 55
5.1.2. Onevenwichtige benadrukking van de medewerkingsplicht 55
5.2. Niet-gerespecteerde beginselen voor gegevensverwerking in de Algemene Verordening Gegevensbescherming 58
5.2.1. Behoorlijke en transparante verwerking niet gegarandeerd 58
5.2.2. Doelbindingsprincipe niet onbetwistbaar nageleefd 62
5.2.3. Dataminimalisatie niet gegarandeerd 66
5.2.4. Nauwkeurigheid niet gegarandeerd 68
5.2.5. Opslagbeperking niet gegarandeerd 72
5.2.6. Vertrouwelijkheid en integriteit niet gegarandeerd 74
5.2.7. Onrechtmatigheid van de verwerking: drempel (zwaarwegend) algemeen belang niet bereikt 77
5.2.7.1. Publieke (gevoelige) persoonsgegevens: uitdrukkelijke openbaarmaking en algemeen belang 77
5.2.7.2. Private (gevoelige) persoonsgegevens: zwaarwegend algemeen belang 81
5.3. Niet-gerespecteerde voorwaarden voor beperkingen op het recht op privacy en gegevensbescherming 81
5.3.1. Ontbreken van een gerechtvaardigd doel 81
5.3.2. Noodzaak en proportionaliteit in een democratische samenleving 81
5.3.2.1. Niet-noodzakelijkheid in een democratische samenleving 81
5.3.2.2. Disproportionaliteit in een democratische samenleving 84
5.3.3. Disrespect voor de wezenlijke inhoud van de fundamentele rechten 86
6. Praktijk- en rechtspraakschets rond de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming 89
6.1. Praktijkschets 89
6.1.1. Praktijkschets: toegang tot smartphones en onrechtstreeks tot sociale mediaprofielen . 89
6.1.2. Praktijkschets: toegang vanop afstand tot publieke onderdelen van sociale mediaprofielen 89
6.2. Rechtspraakschets 90
6.2.1. Rechtspraakschets: toegang tot smartphones en onrechtstreeks tot sociale mediaprofielen 90

6.2.2. Rechtspraakschets: toegang vanop afstand tot publieke onderdelen van sociale mediaprofielen 90
7. Voorgestelde waarborgen en voorwaarden voor conformiteit met het asiel-, privacy- en gegevensbeschermingsrechtelijk kader 92
7.1. Context van het invoeren van waarborgen en voorwaarden voor conformiteit 92
7.2. Voorgestelde waarborgen en voorwaarden voor conformiteit 93
7.2.1. Voorgestelde waarborgen per geïdentificeerd pijnpunt in de wetswijziging 93
7.2.2. Bemerkingen omtrent de voorgestelde waarborgen 99
8. Conclusie 101

Lijst met afkortingen

AVG	Algemene Verordening Gegevensbescherming
CBPL	Commissie voor de Bescherming van de Persoonlijke Levenssfeer
CGVS	Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen
EHRM	Europees Hof voor de Rechten van de Mens
EU-Handvest	EU-Handvest van de Grondrechten
EVRM	Europees Verdrag voor de Rechten van de Mens
GWH	Grondwettelijk Hof
HvJ	Hof van Justitie van de EU
KB	Koninklijk Besluit
RvV	Raad voor Vreemdelingenbetwistingen
RvSt	Raad van State
UNHCR	VN-Hoog Commissariaat voor de Vluchtelingen
Verzoek OIB	Verzoek om internationale bescherming
Verzoeker OIB	Verzoeker om internationale bescherming
Verzoekprocedure OIB	Verzoekprocedure om internationale bescherming
WGA29	Werkgroep Gegevensbescherming Artikel 29

1. Inleiding

1.1. Toegang tot smartphones en sociale mediaprofielen in Belgische verzoekprocedures om internationale bescherming: de wetswijziging van 21 november 2017

Een aantal staten hebben de voorbije jaren wetgeving aangenomen die het voor asielautoriteiten mogelijk maakt om elektronische gegevensdragers (zoals smartphones, laptops, tablets…) en sociale mediaprofielen van verzoekers om internationale bescherming[2] in het kader van hun verzoekprocedures OIB te doorzoeken.[3] Op 21 november 2017, met de wetswijziging[4] van de Vreemdelingenwet, werd België hier een van. Deze wijziging zorgt ervoor dat verzoekers OIB hun elektronische apparaten en/of sociale mediakanalen niet meer louter kunnen zien als hulpmiddelen in hun zoektocht naar bescherming en vrijheid[5], maar zich nu ook bewust moeten zijn van de manieren waarop deze gegevensbronnen procedureel tegen hen kunnen worden gebruikt.

[2] Hierna: OIB

[3] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 1.; International Committee of the Red Cross (ICRC) en Privacy International. "The Humanitarian Metadata Problem: Doing no harm in the digital era." (oktober 2018). https://reliefweb.int/sites/reliefweb.int/files/resources/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf. P. 62.; European Migration Network (EMN). "Annual Report on Migration and Asylum 2018." (2019). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/00_arm2018_synthesis_report_final_en.pdf. P. 5.

[4] Wet 21 november 2017 tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, BS 12 maart 2018. Hierna: de wetswijziging

[5] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 2.; Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 7.
Elektronische apparaten helpen tijdens het migratieproces (bijvoorbeeld door kaartdiensten te verlenen, migranten te verbinden met smokkelaars of hen er net onafhankelijk van te maken door info over de beste/minst gevaarlijke routes aan te reiken), door migranten in staat te stellen contact te houden met hun familie, door info te verstrekken over beschikbare middelen (vb. water, voedsel, onderdak…), door hen in staat te stellen hulpdiensten rechtstreeks te contacteren of door een rol te spelen als instrument voor integratie.

De invoering van deze nieuwe onderzoeksbevoegdheid ging noch in de media[6], noch tijdens de voorbereidingen van de wetswijziging[7] onopgemerkt voorbij. Over het wetsontwerp werden talrijke amendementen ingediend en adviezen verleend door de Raad van State[8], de Commissie voor de Bescherming van de Persoonlijke Levenssfeer[9] en het VN-Hoog Commissariaat voor de Vluchtelingen[10], waarbij de laatste twee uitgesproken kritisch waren.

Concreet gaat het om de volgende twee artikelen. Het eerste artikel[11] wijzigt artikel 48/6, §1, lid 4 van de Belgische Vreemdelingenwet[12] als volgt:

> *Art. 10. Artikel 48/6 van dezelfde wet, ingevoegd bij de wet van 8 mei 2013, wordt vervangen als volgt:*
>
> *Art. 48/6. § 1. […] Indien de met het onderzoek van het verzoek belaste instanties goede redenen hebben om aan te nemen dat de verzoeker informatie, stukken, documenten of andere elementen achterhoudt die essentieel zijn voor een correcte beoordeling van het verzoek, kunnen zij de verzoeker uitnodigen om deze elementen onverwijld voor te leggen, wat ook hun drager is. De weigering van de verzoeker*

---

[6] Een niet-exhaustieve lijst:
Andries, S. "Smartphones scannen botst op verzet: Francken schendt privacy asielzoekers". www.standaard.be. De Standaard, 18 oktober 2017. https://www.standaard.be/cnt/dmf20171017_03138056?articlehash=FB56DDD30B64BCF21A11603091E24E47C54A8B4BFB98ACBD4A985045E31E834BDDE9CF6FE958527F5BB8F0E25731CCE5C75D9CFE57F4405338A990BB4C2CF861.; De Schutter, S. "De nieuwe asielwet is in aantocht". www.vrt.be. Vrt, 9 november 2017. https://www.vrt.be/vrtnws/nl/2017/11/09/de-nieuwe-asielwet-is-in-aantocht/.; Kihl, L. "Les migrants sommés de montrer leur GSM". www.lesoir.be. Le Soir, 30 juni 2016. https://plus.lesoir.be/art/d-20160629-G8NNLZ.; Meersman, M. "Controle gsm's asielzoekers "geen schending privacy"". www.sceptr.net. Sceptr, 7 februari 2017. https://sceptr.net/2017/10/smartphones-en-sociale-media-asielzoekers-mogen-gescreend-worden/.; "Overheid mag sociale media screenen bij asielaanvraag". www.hln.be. HLN, 21 april 2017. https://www.hln.be/ihln/internet/overheid-mag-sociale-media-screenen-bij-asielaanvraag~a69629fe/.; "Overheid mag sociale media screenen bij asielaanvraag: "Privacy wordt niet geschonden"". www.demorgen.be. De Morgen, 21 april 2017. https://www.demorgen.be/binnenland/overheid-mag-sociale-media-screenen-bij-asielaanvraag-privacy-wordt-niet-geschonden-bad4c1b1/.; Risack, L. "De nieuwe asielwet doorgelicht: plat racisme of gewoon goede wetgeving?" www.rechtenkrant.be. De Rechtenkrant, 11 november 2017. https://rechtenkrant.be/de-nieuwe-asielwet-doorgelicht-plat-racisme-gewoon-goede-wetgeving/.; Sokol, K., Verstraete, J. en Belga. "Overheid mag sociale media screenen bij asielaanvraag: "Geen schending privacy"". www.vrt.be. Vrt, 21 april 2017. https://www.vrt.be/vrtnws/nl/2017/04/21/overheid_mag_socialemediascreenenbijasielaanvraaggeenschendingpr-1-2957454/.; "Vandaag stemt de Kamer over wetsontwerpen die onze asielwetgeving ingrijpend wijzigen". www.vluchtelingenwerk.be. Vluchtelingenwerk Vlaanderen, 9 november 2017. https://www.vluchtelingenwerk.be/nieuws/vandaag-stemt-de-kamer-over-wetsontwerpen-die-onze-asielwetgeving-ingrijpend-wijzigen.

[7] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 70.

[8] Hierna: RvSt; Memorie van toelichting over het wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, gedaan op 22 juni 2017, Parl.St. Kamer 2016-17, nr. 2548/001. P. 219. Hierna: memorie van toelichting bij de wetswijziging

[9] Hierna: CBPL; Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL). "Advies uit eigen beweging betreffende het wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, nr. 57/2017." (oktober 2017). https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/advies_57_2017.pdf. Hierna: Advies CBPL

[10] Hierna: UNHCR; VN-Hoog Commissariaat voor de Vluchtelingen. "Commentaires du Haut Commissariat des Nations Unies pour les réfugiés (HCR) relatifs aux : le projet de loi 2548/003 modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines catégories d'étrangers et le Projet de loi 2548/003 modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers." (oktober 2017). http://www.dekamer.be/FLWB/PDF/54/2548/54K2548004.pdf. Hierna: Advies UNHCR

[11] Artikel 10 van de wetswijziging

[12] Wet 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen, BS 31 december 1980. Hierna: Vreemdelingenwet

om deze elementen voor te leggen zonder bevredigende verklaring kan een aanwijzing zijn van zijn weigering om te voldoen aan zijn medewerkingsplicht zoals bedoeld in het eerste lid.

Het tweede artikel[13] wijzigt artikel 57/7, §2 van de Belgische Vreemdelingenwet als volgt:

Art .48. In artikel 57/7 van dezelfde wet, ingevoegd bij de wet van 14 juli 1987, worden de volgende wijzigingen aangebracht:

[…] §2. De Commissaris-generaal voor de Vluchtelingen en de Staatlozen kan informatie van alle aard die via elektronische weg is verstuurd of ontvangen door de verzoeker om internationale bescherming en die niet persoonlijk voor de Commissaris-generaal voor de Vluchtelingen en de Staatlozen is bestemd, maar die publiek toegankelijk is, raadplegen en gebruiken voor de beoordeling van het verzoek om internationale bescherming.

Op die manier maken beide artikelen het mogelijk voor het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen[14] om (al dan niet met toestemming) toegang te verkrijgen tot digitale gegevensdragers en sociale mediaprofielen van de betrokken verzoeker OIB. Het onderscheid tussen beide artikelen ligt in het publieke of private karakter van de informatie en de fysieke aard van de maatregel. Enerzijds kunnen de persoonsgegevens van de betrokkene worden geraadpleegd door middel van het fysiek in beslag nemen en doorzoeken van (digitale) gegevensdragers, waarbij zowel private als publiek gemaakte info kan worden geraadpleegd (met toestemming). Anderzijds kan digitale communicatie (bijvoorbeeld op sociale mediaprofielen) ook vanop afstand worden geraadpleegd (zonder toestemming), zonder de gegevensdragers ook effectief in beslag te moeten nemen. Hierbij gaat het noodzakelijkerwijs enkel om publiek gemaakte informatie.

Artikel 57/7, §2 van de Vreemdelingenwet vermeldt 'informatie van alle aard die via elektronische weg is verstuurd of ontvangen'. De memorie van toelichting verduidelijkt dat met een 'publiek medium' niet enkel (de publieke onderdelen van) facebookaccounts worden bedoeld, maar ook discussie- en internetfora die niet afgeschermd of beveiligd zijn.[15] Er is voor het gebruik van deze gegevens geen toestemming van de betrokkene vereist.[16] De verwerking ervan zou volgens de memorie van toelichting namelijk gerechtvaardigd worden door belangrijke redenen van publiek belang.[17]

Artikel 48/6, §1, lid 4 van de Vreemdelingenwet daarentegen heeft betrekking op alle soorten informatie, ongeacht de drager of het publieke/private karakter ervan, en geeft daardoor ook (nog) meer aanleiding tot controverse. De memorie van toelichting verduidelijkt dat het kan gaan om 'een materiële of een immateriële drager, met inbegrip van elk stuk, elk voorwerp, elke communicatietoestel (gsm, tablet, draagbare computer, …), elke toegang tot een sociale netwerksite op internet (Facebook…), elke uitwisseling van briefwisseling (inclusief elektronische), elke elektronische informatiedrager (Usb-sleutel, cd-(rom), geheugenkaartje, …)'.[18] Voor het raadplegen van deze informatie is echter wel toestemming van de betrokkene vereist. De weigering om toestemming te geven kan echter een aanwijzing zijn van de weigering tot het voldoen aan de medewerkingsplicht[19] en een negatief element

[13] Artikel 48 van de wetswijziging
[14] Hierna: CGVS
[15] Memorie van toelichting bij de wetswijziging P. 137.
[16] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 196.
[17] Memorie van toelichting bij de wetswijziging P. 137-138.
[18] Ibid. P. 35.
[19] Term wordt verder onder '2.2.1.' verduidelijkt

vormen in de beoordeling van de vraag OIB.[20] Ter rechtvaardiging van deze maatregel wordt dan ook hoofdzakelijk de uitdrukkelijke toelating van de verzoeker OIB aangehaald, die impliciet uit de tekst van het artikel zou kunnen worden afgeleid.[21]

In de voorbereidende werken van de wetswijziging wordt gesteld dat beide artikelen in overeenstemming[22] zijn met de (toen nog geldende) Wet Bescherming Persoonsgegevens [23]. Daarnaast verklaart het CGVS zelf dat 'alle verwerkingen van persoonsgegevens die aan het CGVS worden toevertrouwd verlopen conform de Algemene Verordening Gegevensbescherming 2016/679 van 27 april 2016 van het Europees Parlement en de Raad'.[24] Hoewel de bedoeling van kritische adviesverleners en ngo's was om hun bezorgdheden en voorgestelde aanpassingen ingevoegd te zien in de gewijzigde wetsartikelen zelf, bestond het antwoord van de toenmalige Staatssecretaris voor Asiel en Migratie in de aankondiging van een Koninklijk Besluit[25], dat aan de ongunstige adviezen tegemoet zou komen.[26] Daarnaast werd op 12 september 2018 een beroep tot gedeeltelijke vernietiging van de wetswijziging ingediend bij het Grondwettelijk Hof[27], door onder andere[28] de Orde van Franstalige en Duitstalige balies van België.[29] Onder de aangevochten artikelen van de wetswijziging bevinden zich artikel 10 en 48, die zoals hierboven aangegeven de focus van dit onderzoek vormen.

Het is dus allesbehalve een vanzelfsprekendheid dat de wetswijziging is opgesteld in overeenstemming met de Belgische en Europese asiel-, privacy- en gegevensbeschermingsregelgeving. Het opzet van dit onderzoek is dan ook om deze conformiteit te analyseren en om na te gaan of de wetswijziging bijgevolg een schending van het recht op privacy en gegevensbescherming van de verzoeker OIB uitmaakt of niet.

1.2. Benadering van de probleemstelling

Een groot deel van de persoonsgegevens waar we vandaag mee geconfronteerd worden, komen elektronisch tot stand. Waar smartphone- en sociale mediagebruikers zich niet altijd van bewust zijn, is dat hun toestellen en profielen als het ware een gecentraliseerde database van private informatie

[20] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 195.

[21] Verslag over het wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, gedaan op 27 oktober 2017, Parl.St. Kamer 2016-17, nr. 2548/008. P. 9. Hierna: Verslag 2 bij de wetswijziging

[22] Memorie van toelichting bij de wetswijziging P. 36 en 137.
Verslag 2 bij de wetswijziging P. 5 en 27.

[23] Wet 8 december 1992 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens; Momenteel geldende versie: Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna: Wet Bescherming Persoonsgegevens
Deze wet geldt samen met en moet gezien worden als gedeeltelijk implementatiewet van de Europese Algemene Verordening Gegevensbescherming en de Europese Richtlijn Politie en Justitie

[24] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[25] Hierna: KB

[26] Verslag 2 bij de wetswijziging P. 5.; European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 70.

[27] Hierna: GWH

[28] De andere organisaties die mee het beroep instelden zijn: de vzw 'Association pour le droit des Etrangers', de vzw 'Coordination et Initiatives pour et avec les Réfugiés et les Etrangers', de vzw 'Jesuit Refugees Service - Belgium', de vzw 'Liga voor Mensenrechten', de vzw 'Ligue des Droits de l'Homme', de vzw 'Point d'appui. Service d'aide aux personnes sans papiers', de vzw 'Bureau d'Accueil et de Défense des Jeunes', de vzw 'Syndicat des Avocats pour la Démocratie' en de vzw 'Vluchtelingenwerk Vlaanderen'.

[29] GWH (Hangend) Rolnr. 7008 (FR) van 12 september 2018. BS 11 oktober 2018.

vormen[30], wat van enorm nut kan zijn voor asielautoriteiten[31] en overheden in het algemeen[32]. Wat echter niet uit het oog mag worden verloren, is dat de aard van deze digitale informatie (persoonsgegevens verspreid via sociale mediaprofielen) en de digitale dragers waarop deze informatie raadpleegbaar is (smartphones, laptops…) erg privacygevoelig kunnen zijn.[33]

Ten eerste moet worden gewezen op de gemakkelijke toegangswijze tot deze digitale informatie[34], de grote hoeveelheid ervan en de vaak niet-gecategoriseerde en ongestructureerde wijze waarop dergelijke persoonsgegevens worden aangetroffen. Het kan uiteraard geen doel zijn om zoveel mogelijk persoonlijke gegevens te verzamelen en zoveel mogelijk actoren toegang te geven tot deze gegevens zonder dat dit een duidelijke toegevoegde waarde heeft.[35] Ten tweede legt het UNHCR de nadruk op het feit dat digitaal en elektronisch bewijsmateriaal in bepaalde gevallen maar beperkt betrouwbaar of accuraat is en gemakkelijk gewijzigd kan worden.[36]

Ten derde mag niet uit het oog verloren worden dat verzoekers OIB kwetsbare personen zijn[37], die het slachtoffer zijn van een acute humanitaire situatie en op de vlucht zijn voor oorlog, vervolging of ontbering in hun land van herkomst[38]. Deze personen komen dus vaak uit traumatiserende situaties en dit rechtvaardigt dan ook hun nood aan bijzondere procedurele waarborgen[39]. Deze bijzondere bescherming wordt tegenover de procedurele plicht van verzoekers OIB geplaatst om hun medewerking te verlenen tijdens het verloop van de verzoekprocedure. Het wordt in de memorie van toelichting als vanzelfsprekend beschouwd dat verzoekers OIB hun medewerkingsplicht ten volle vervullen door het vrijgeven van persoonlijke gegevens. Verzoekers zijn echter vaak gevlucht van omstandigheden waar ze net omwille van bepaalde persoonlijke informatie vervolgd werden (zoals godsdienst, nationaliteit,

---

[30] "Sociale netwerken en privacy". www.gegevensbeschermingsautoritieit.be. Gegevensbeschermingsautoriteit. https://www.gegevensbeschermingsautoriteit.be/sociale-netwerken.

[31] Chetrit, S. L. "Surviving an Immigration Marriage Fraud Investigation: All You Need is Love, Luck, and Tight Privacy Controls." Brooklyn Law Review vol. 77, no. 2 (2012). https://heinonline.org/HOL/P?h=hein.journals/brklr77&i=713. P. 709-744.; Verslag 2 bij de wetswijziging P. 8, 16 en 18.; Verslag over het wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, gedaan op 10 augustus 2017, Parl.St. Kamer 2016-17, nr. 2548/002. P. 84. Hierna: Verslag 1 bij de wetswijziging

[32] Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 12.

[33] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 197.

[34] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2.

[35] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 76.

[36] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2.

[37] VN- Hoog Commissariaat voor de Vluchtelingen. "Guidance on the Protection of Personal Data of Persons of Concern to UNHCR." (augustus 2018). https://www.refworld.org/docid/5b360f4d4.html. P. 36.
Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 4.; European Data Protection Supervisor (EDPS). "Formal consultation on EASO's social media monitoring reports (case 2018-1083)." (2019). https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf. P. 6.; "Communities at risk: How governments are using tech to target migrants". www.privacyinternational.org. Privacy International. https://privacyinternational.org/blog/2781/how-governments-are-using-tech-target-migrants.

[38] Verslag 2 bij de wetswijziging P. 16.

[39] Ibid. P. 21.

het behoren tot een bepaalde sociale groep of politieke overtuiging[40]) en willen daarom (deze aspecten van) hun identiteit net verbergen.[41] Ook zijn vluchtmotieven van verzoekers vaak van die aard dat het niet vanzelfsprekend is om ze vanaf de aanvang van het onderzoek volledig uiteen te zetten (vb. verkrachting, seksuele geaardheid…).[42] De prangende situaties waarin verzoekers OIB zich bevonden/bevinden maakt het voor hen dus niet altijd eenvoudig te determineren in welk geval medewerking verlenen aan autoriteiten een gevaar kan inhouden of niet.[43]

In verzoekprocedures OIB kan digitale informatie, bijvoorbeeld gevonden op smartphones of sociale mediaprofielen, dienen als bijkomende informatiebron voor verzoekers met een tekort aan documenten om hun identiteit te bewijzen. Echter, het kan ook dienen als middel om verzoekers uit te sluiten van de mogelijkheid om internationale bescherming te verwerven, op grond van ideologische, etnische of religieuze vooroordelen of op basis van verkeerde interpretaties.[44] De samenloop van bovenstaande aandachtspunten gebiedt dan ook bijkomende waakzaamheid bij het doorzoeken, beoordelen en verwerken van de persoonlijke digitale gegevens van de verzoeker binnen diens verzoekprocedure.[45] Deze waakzaamheid zou zich moeten weerspiegelen in de wetgeving met betrekking tot de technieken voor herkomstonderzoek, die tijdens die verzoekprocedure worden gehanteerd. In het (inter)nationaal asielbeleid zijn de strengste normen op het gebied van privacy en gegevensbescherming op hun plaats[46] om te garanderen dat de gegevens van migranten niet verkeerdelijk als wapen tegen hen kunnen worden gebruikt.[47]

In de parlementaire stukken bij het wetsontwerp wordt verduidelijkt dat de wetswijziging vooral focust op duidelijke, efficiënte, snelle en kwaliteitsvolle procedures met een nadruk op de strijd tegen misbruik van verzoekprocedures OIB.[48] Er moet *in casu* echter een duidelijke evenwichtsoefening worden gemaakt tussen het belang van de overheid bij de bestrijding van misbruik in verzoekprocedures OIB en het belang van de verzoeker bij de uitoefening van diens recht op privacy en gegevensbescherming.[49] Het is deze evenwichtsoefening die de maatschappelijke relevantie van dit onderzoek duidt en er ook het leidmotief van vormt.

---

[40] Artikel 1 VN Vluchtelingenverdrag

[41] European Union Agency for Fundamental Rights (FRA). "Fundamental rights and the interoperability of EU information systems: borders and security." (2017). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf. P. 8.

[42] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 542.

[43] Verslag 2 bij de wetswijziging P. 17.

[44] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 33.

[45] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018).
https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 2-3.

[46] Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 4.

[47] "Communities at risk: How governments are using tech to target migrants". www.privacyinternational.org. Privacy International. https://privacyinternational.org/blog/2781/how-governments-are-using-tech-target-migrants.

[48] Memorie van toelichting bij de wetswijziging P. 6 en 7.; Verslag 2 bij de wetswijziging P. 22.; Verslag 1 bij de wetswijziging P. 5.

[49] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017).
https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 77.

1.3. Methodologie

Het uitgangspunt voor het ontwikkelen van een beter inzicht in een bepaalde problematiek, is een goed begrip van wat reeds bekend is. Om die reden vertrekt dit onderzoek vanuit het deductief analyseren van bestaande relevante academische literatuur, toepasselijke (nationale en internationale) regelgeving, beleidsdocumenten en nieuwsberichtgeving in verband met digitale controle op migratie in relatie tot het recht op privacy en gegevensbescherming, en in het bijzonder over de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures OIB. Om de Belgische situatie hieromtrent te schetsen, werden de voorbereidende werken van de besproken wetswijziging als uitvalsbasis gebruikt. Gezien de relatief recente aard van de wetswijziging, is de academische literatuur omtrent dit specifieke onderzoeksonderwerp in België eerder schaars. Om die reden werd de literatuurstudie ook uitgebreid naar andere landen, zoals Duitsland, Nederland, Noorwegen, Denenmarken, Oostenrijk, de VS ... Dit gebeurde niet met de ambitie om een rechtsvergelijkende en/of alomvattende situatieschets van de problematiek in deze landen weer te geven, maar om het maatschappelijk en academisch debat op verschillende plaatsen ter wereld als inspiratie te gebruiken voor de probleemanalyse in België.

De literatuurstudie, die de basis voor dit onderzoek vormt, beslaat (inter)nationale wetgeving[50], rechtsleer (o.a. juridische basiswerken; academische papers; rapporten, adviezen en richtlijnen opgesteld door (inter)nationale asiel- en gegevensbeschermingsinstanties)[51] en rechtspraak[52]. Daarnaast werden ook minder klassieke rechtsbronnen geraadpleegd, zoals krantenartikelen/nieuwspagina's[53], blogs[54] en informatieve webpagina's[55]. Dit om een zo volledig mogelijk beeld te krijgen, zowel van de juridisch-technische, als van de maatschappelijke aspecten van de problematiek van de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures OIB.

Eerst en vooral wordt in dit onderzoek het theoretisch kader rond 'digitale controle op migratie in relatie tot het recht op privacy en gegevensbescherming' geschetst, zowel vanuit asielrechtelijk[56], als vanuit privacy- en gegevensbeschermingsrechtelijk perspectief[57]. Vervolgens worden de toepasselijke beginselen en regels in de Algemene Verordening Gegevensbescherming[58] (en het Europees Verdrag voor de Rechten van de Mens[59]) bepaald, die relevant zijn voor de gegevensverwerking door het CGVS van persoonsgegevens op sociale mediaprofielen en smartphones van verzoekers OIB.[60] Vanuit deze opsomming, worden de 'geïdentificeerde pijnpunten' in de Belgische wetswijziging uiteengezet.[61] Deze pijnpunten geven aan op welke manier en in welke mate de huidige wettekst (ingevoerd door de

[50] Geraadpleegd via o.a. 'www.ejustice.just.fgov.be' voor Belgische wetgeving, 'www.dekamer.be' voor de parlementaire stukken van Belgische wetgeving, 'www.eur-lex.europa.eu' voor Europese wetgeving, 'www.gesetze-im-internet.de' voor Duitse wetgeving, …

[51] Geraadpleegd via o.a. 'www.lib.ugent.be', 'www.jurisquare.be', 'www.scholar.google.com', 'www.google.com', 'www.refworld.org', 'www.unhcr.org', 'www.home.heinonline.org', 'www.echr.coe.int', 'www.easo.europa.eu', 'www.edps.europa.eu', 'www.ec.europa.eu', 'www.fra.europa.eu', 'www.emnbelgium.be', 'www.gegevensbeschermingsautoriteit.be', 'www.dhs.gov'…

[52] Geraadpleegd via o.a. 'www.rvv-cce.be', 'www.raadvst-consetat.be', 'www.const-court.be', 'www.hudoc.echr.coe.int', 'www.curia.europa.eu'…

[53] Geraadpleegd via o.a. De Standaard, De Morgen, Vrt, Le Soir, De Rechtenkrant, BBC, The Guardian, The New York Times…

[54] Geraadpleegd via o.a. 'www.unhcr.org/blogs', 'www.vluchtelingenwerk.be/nieuws'…

[55] Geraadpleegd via o.a. 'www.agii.be', 'www.cgvs.be', 'www.dofi.ibz.be', 'www.gegevensbeschermingsautoriteit.be', 'www.edps.europa.eu', 'www.ec.europa.eu'…

[56] Hoofdstuk '2. Theoretisch kader: toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vanuit asielrechtelijk perspectief'

[57] Hoofdstuk '3. Theoretisch kader: toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vanuit privacy- en gegevensbeschermingsrechtelijk perspectief'

[58] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), hierna: AVG

[59] Hierna: EVRM

[60] Hoofdstuk '4. Voorwaarden voor gegevensverwerking en beperkingen op het recht op gegevensbescherming'

[61] Hoofdstuk '5. Toepassing van het theoretisch kader: geïdentificeerde pijnpunten'

wetswijziging) tekortkomingen vertoont in het licht van het privacy- en gegevensbeschermingsrechtelijk regelgevend kader. Vervolgens wordt kort ingegaan op de wijze waarop de besproken wetsartikelen zich manifesteren in de praktijk van het CGVS en in de rechtspraak van de Raad voor Vreemdelingenbetwistingen[62], zonder hiermee een diepgaande analyse voor ogen te houden. Tot slot worden, op basis van de relevante beginselen en regels in de AVG (en het EVRM), de geïdentificeerde pijnpunten en de praktijk- en rechtspraakschets, een aantal waarborgen voorgesteld om conformiteit met het asiel-, privacy- en gegevensbeschermingsrechtelijk kader te bewerkstelligen.[63] In de bemerkingen omtrent de voorgestelde waarborgen wordt duiding gegeven rond een aantal substantiële hindernissen voor het opnemen ervan in het aangekondigd KB en het praktisch implementeren ervan.

1.4. Beperkingen van het onderzoek

Dit onderzoek wordt strikt begrensd door de hoofdonderzoeksvraag ervan:

> '*Is de bevoegdheid van het CGVS om smartphones en sociale mediaprofielen te doorzoeken voor de beoordeling van Belgische verzoekprocedures om internationale bescherming in overeenstemming met het toepasselijk (inter)nationaal asiel-, privacy- en gegevensbeschermingsrechtelijk kader en zo nee, onder welke voorwaarden en met welke waarborgen kan deze schending eventueel worden geremedieerd?'*

Een eerste beperking ligt dus in het feit dat het onderzoek zich toespitst op het raadplegen van smartphones en sociale mediaprofielen. De alomtegenwoordigheid van beide mediums in de huidige samenleving verklaart waarom maatregelen van digitale controle op migratie hoofdzakelijk deze gegevensbronnen raken. De wetswijziging definieert een ruimer toepassingsgebied, namelijk 'informatie, stukken, documenten of andere elementen, wat ook hun drager is' en 'informatie van alle aard die via elektronische weg is verstuurd of ontvangen'. Hoewel tijdens de literatuurstudie rekening wordt gehouden met dit ruimere toepassingsgebied, wordt de verzamelde informatie specifiek toegepast op 'smartphones en sociale mediaprofielen' om de onderzoekvraag te beantwoorden.

Ten tweede focust de onderzoeksvraag zich enkel op de Belgische verzoekrpocedures OIB. Ondanks het feit dat ook de situatie in andere landen en/of in andere migratieprocedures wordt geanalyseerd, wordt de bijeengebrachte informatie hieromtrent aangewend om de Belgische situatie te beoordelen.

Ten derde wordt geen toetsing uitgevoerd van de wetswijziging aan de Europese Richtlijn Politie en Justitie[64], aangezien deze *in casu* niet van toepassing is[65]. Ook de de Belgische wet van 13 juni 2005

[62] Hierna: RvV; Hoofdstuk '6. Praktijk- en rechtspraakschets rond de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming'

[63] Hoofdstuk '7. Voorgestelde waarborgen en voorwaarden voor conformiteit met het asiel-, privacy- en gegevensbeschermingsrechtelijk kader'

[64] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, hierna: Richtlijn Politie en Justitie

[65] Quintel, T. A. "EDPS and Article 29 Working Party Opinions about the Commission Proposals on the Interoperabity of Database." European Data Protection Law Review (EDPL) vol. 4, no. 2 (2018). https://heinonline.org/HOL/P?h=hein.journals/edpl4&i=232. P. 218.; Quintel, T. A. en Sajfert, J. "Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities." (2017). http://hdl.handle.net/10993/38833. P. 3.; "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.; Advies CBPL P. 7.; European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 61.

betreffende de elektronische communicatie (Wet Elektronische Communicatie)[66] blijft buiten beschouwing, vanwege de niet-toepasselijkheid ervan[67].

Als laatste wordt louter de juridische overeenstemming met het (inter)nationaal asiel-, privacy- en gegevensbeschermingsrechtelijk kader geëvalueerd. Er wordt hierbij niet ingegaan op de rechten van de betrokkene (zoals gedefinieerd in hoofdstuk III van de AVG), noch op de hoogtechnologische aspecten van de gegevensbeschermingsrechtelijke kwesties die in dit onderzoek naar boven komen. Uit deze laatste beperking vloeit voort dat de wetswijziging ook niet aan het regelgevend kader van de 'geautomatiseerde individuele besluitvorming, waaronder profilering' in de AVG[68], wordt getoetst.

1.5. Wetenschappelijke relevantie van het onderzoek

Zoals vermeld in '1.3.', is de besproken wetswijziging relatief recent, waardoor de academische *state of the art* omtrent dit specifieke onderzoeksonderwerp in België eerder schaars is. Aangezien de problematiek van de gegevensbeschermingsrechtelijke legitimiteit van digitale controle op migratie geen grenzen kent, is er wel wetenschappelijke literatuur te vinden in andere landen en op Europees niveau. Net zoals België, begeven nog heel wat staten zich op glad ijs als het gaat om de gegevensrechtelijke bescherming van verzoekers OIB. Het Verenigd Koninkrijk bijvoorbeeld, bepaalde resoluut dat (essentiële delen van) het Europeesrechtelijk gegevensbeschermingskader niet van toepassing zijn voor migranten en hen dus geen bescherming kunnen bieden.[69] Zowel o.a. Duitsland, Noorwegen, Nederland, Oostenrijk, Denenmarken, als de VS hebben gelijkaardige wetgeving als de Belgische omtrent de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures OIB. Hierop kwam onder andere reactie in de vorm van wetenschappelijk onderzoek of rapportering van gegevensbeschermingsrechtelijke instanties.[70] Een aantal studies vergelijken ook de situatie in meerdere landen[71] of focussen op het gedigitaliseerd systeem van grenscrontroles van de EU (o.a. Eurosur en

[66] Wet 13 juni 2005 betreffende de elektronische communicatie, hierna: Wet Elektronische Communicatie
[67] Artikel 124 4° jo. 125, § 1, 1° Wet Elektronische Communicatie
[68] Artikel 22 AVG: De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.
[69] Moraes, C. "New UK data protection rules are a cynical attack on immigrants". www.theguardian.com. The Guardian, 5 februari 2018. https://www.theguardian.com/commentisfree/2018/feb/05/brexit-data-protection-rules-immigrants.
[70] Het Verengd Koninkrijk: vb. White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl.
Duitsland: vb. Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf.
Noorwegen: vb. European Migration Network (EMN) National Contact Point Norway. "EMN Synthesis Report for EMN Focused Study 2017: Challenges and practices for establishing the identity of third-country national in migration procedures, Report from Norway." (2017). https://www.udi.no/globalassets/global/european-migration-network_i/studies-reports/emn-id--norwegian-response.pdf.
Nederland: vb. Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf.
Oostenrijk: vb. Knapp, A. en European Council on Refugees and Exiles (ECRE). "Country Report: Austria." Asylum Information Database (AIDA) (2018). https://www.asylumineurope.org/sites/default/files/report-download/aida_at_2018update.pdf.
Denenmarken: vb. VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Observations on the proposed amendments to the Danish Aliens legislation." (januari 2016). https://www.refworld.org/pdfid/5694ed3a4.pdf.
De VS: vb. Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf.
[71] Vb. Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-

Eurodac)[72]. Andere studies analyseren dan weer het gebruik van smartphones door verzoekers OIB zelf tijdens hun asielroute[73] of het gebruik van gegevens op smartphones door ngo's om humanitaire redenen[74].

In de eerste plaats verschilt de wetgeving omtrent de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures in alle hierboven vermelde landen. Er zijn aanzienlijke verschillen op vlak van het doel waarvoor de gegevens worden gebruikt, de frequentie waarmee de maatregelen worden uitgevoerd, de mate waarin de gegevens worden geraadpleegd, de autoriteit die verantwoordelijk is voor het lezen van de gegevensdragers …[75] Hierdoor is buitenlands wetenschappelijk onderzoek of rapportering hieromtrent per definitie niet toepasselijk op de Belgische situatie. Daarnaast gaat het merendeel van de reeds aangehaalde studies niet verder dan het louter vermelden of beschrijven van de bestaande praktijk van digitale controle op migratie. Wat het nagaan van de overeenstemming met het toepasselijk (inter)nationaal privacy- en gegevensbeschermingsrechtelijk kader betreft, wordt vaak slechts de noodzakelijkheids- en proportionaliteitstoets uitgevoerd, zoals verankerd in het EVRM.[76] Ook de studies die uiterst grondig ingaan op de privacygerelateerde bezorgdheden omtrent de praktijk van digitale controle op migratie[77], bevatten geen complete toetsing aan het Europees gegevensbeschermingsrechtelijk kader. In onderzoeken en rapporten worden ook aanbevelingen voor verbetering of *best practices* geïdentificeerd, maar dit gebeurt slechts selectief. Correcte, uitgebreide en volledige kosten-batenanalyses van deze digitale controle op migratie is echter in de meeste landen niet,

content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf.; Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf.

[72] Vb. European Union Agency for Fundamental Rights (FRA). "Fundamental rights and the interoperability of EU information systems: borders and security." (2017). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf.

[73] Vb. Zijlstra, J. en van Liempt, I. "Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys." Int. J. Migration and Border Studies, Vol. 3, Nos. 2/3 (2017). https://www.ris.uu.nl/ws/files/27630646/IJMBS0302_0304_ZIJLSTRA.pdf.

[74] Vb. International Committee of the Red Cross (ICRC) en Privacy International. "The Humanitarian Metadata Problem: Doing no harm in the digital era." (oktober 2018). https://reliefweb.int/sites/reliefweb.int/files/resources/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf.

[75] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 43.

[76] Vb. Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf.; White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl.

[77] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf.; Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 43.

of in ieder geval niet openbaar, beschikbaar.[78] Dit verhindert bijgevolg dat men aanbevelingen kan formuleren omtrent de praktijk van het raadplegen van sociale mediaprofielen en smartphones van verzoekers in haar geheel.[79]

De wetenschappelijke relevantie van dit onderzoek ligt dan ook in de allesomvattende toetsing van de Belgische wetswijziging aan het volledige toepasselijk (inter)nationaal asiel-, privacy- en gegevensbeschermingsrechtelijk kader (hoofdzakelijk relevante wetgeving *in casu*: de Kwalificatierichtlijn[80], de AVG en het EVRM). Bovendien brengt dit onderzoek op complete wijze voorgestelde waarborgen samen, die betrekking hebben op elk van de geïdentificeerde pijnpunten uit de toetsing aan het wettelijk kader.

[78] Uitzondering: Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf.

[79] Bolhuis, M. en van Wijk, J. "Practices in establishing the identity and screening on national security and exclusion aspects in Syrian asylum cases in five European countries." Migration Policy Practice (april-juni 2019). https://publications.iom.int/system/files/pdf/mpp_38.pdf. P.16.

[80] Richtlijn 2011/95/EU van het Europees Parlement en de Raad van 13 december 2011 inzake normen voor de erkenning van onderdanen van derde landen of staatlozen als personen die internationale bescherming genieten, voor een uniforme status voor vluchtelingen of voor personen die in aanmerking komen voor subsidiaire bescherming, en voor de inhoud van de verleende bescherming, hierna: Kwalificatierichtlijn

2. Theoretisch kader: toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vanuit asielrechtelijk perspectief

2.1. Het Europees asielrechtelijk kader

De relevante artikelen van de wetswijziging passen de Vreemdelingenwet aan met betrekking tot de onderzoeksbevoegdheden van het CGVS in het kader van verzoeken OIB[81], met name de verzoeken tot erkenning van de vluchtelingenstatus[82] of tot toekenning van de subsidiaire beschermingsstatus[83]. Voor de wijziging/invoering van artikelen 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet worden in de desbetreffende wetswijziging twee Europese rechtsgronden aangehaald[84]: de (gedeeltelijke) omzetting van enerzijds de Procedurerichtlijn[85], en anderzijds de Kwalificatierichtlijn[86].

2.1.1. Omzetting van de Procedurerichtlijn

2.1.1.1. Artikel 13, lid 2, d) Procedurerichtlijn

De memorie van toelichting stelt dat artikel 48/6, §1, lid 4 van de Vreemdelingenwet een gedeeltelijke omzetting vormt van artikel 13, lid 2, d) van de Procedurerichtlijn[87]. Dit artikel voorziet in de mogelijkheid voor de asielautoriteiten om de verzoeker uit te nodigen de elementen voor te leggen, die essentieel zijn voor een correcte evaluatie van het verzoek OIB. Het is dus te kaderen binnen de medewerkingsplicht van de verzoeker OIB, waarover in '2.2.1.' verder wordt uitgeweid.

> *Artikel 13: Verplichtingen van de verzoekers*
>
> *2. De lidstaten kunnen met name bepalen dat:*
>
> *d) de bevoegde autoriteiten de verzoeker en de voorwerpen die hij bij zich draagt mogen fouilleren, respectievelijk doorzoeken. Onverminderd fouilleringen die plaatsvinden om veiligheidsredenen, wordt een fouillering van de verzoeker uit hoofde van deze richtlijn verricht door een persoon van hetzelfde geslacht met volledige eerbiediging van de beginselen van menselijke waardigheid en van de lichamelijke en psychische integriteit;*

2.1.1.2. Betwiste toepasselijkheid van de Procedurerichtlijn

Hoewel de memorie van toelichting de toepasselijkheid van deze Europese rechtsgrond als onbetwist gegeven vermeldt, is deze niet vanzelfsprekend. Het is namelijk in twijfel te trekken of artikel 13, lid 2, d) Procedurerichtlijn, dat over fouillering handelt, wel in verband te brengen is met artikel 48/6, §1, lid 4 van de Vreemdelingenwet. Fouilleringen/doorzoekingen van iemands private bezittingen gebeuren namelijk per definitie zonder diens toestemming[88], terwijl in artikel 48/6, §1, lid 4 van de

[81] Artikel 1, 16° Vreemdelingenwet; Artikel 2(a) Kwalificatierichtlijn
[82] Artikel 48/3 Vreemdelingenwet; Artikel 1 VN Vluchtelingenverdrag; Artikel 2 (d) Kwalificatierichtlijn
[83] Artikel 48/4 Vreemdelingenwet; Artikel 2 (f) Kwalificatierichtlijn
[84] Artikel 2 van de wetswijziging
[85] Richtlijn 2013/32/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende gemeenschappelijke procedures voor de toekenning en intrekking van de internationale bescherming, hierna: Procedurerichtlijn
[86] Richtlijn 2011/95/EU van het Europees Parlement en de Raad van 13 december 2011 inzake normen voor de erkenning van onderdanen van derde landen of staatlozen als personen die internationale bescherming genieten, voor een uniforme status voor vluchtelingen of voor personen die in aanmerking komen voor subsidiaire bescherming, en voor de inhoud van de verleende bescherming, hierna: Kwalificatierichtlijn
[87] Memorie van toelichting bij de wetswijziging P. 33.
[88] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 527.

Vreemdelingenwet de toestemming als hoofdverwerkingsgrond wordt aangehaald. Het fouilleren, materieel speuren in, op of onder de kleding van een aanwezige persoon of de controle van de bagage van die persoon, om na te gaan of die bepaalde voorwerpen of zaken bij zich heeft, wordt in België geregeld in artikel 28 van de Wet op het Politieambt.[89] Noch in dit artikel, noch in artikel 13, lid 2, d) Procedurerichtlijn wordt de toestemming van de gefouilleerde vereist.

Daarnaast worden veiligheidsfouilleringen volgens de Wet op het Politieambt ook enkel uitgevoerd in deze limitatief opgesomde en sterk aan criminaliteit gelinkte gevallen: er is een vermoeden van bezit van een wapen of ander gevaarlijk voorwerp; de persoon is het voorwerp van een bestuurlijke arrestatie of gerechtelijke vrijheidsbeneming; de persoon neemt deel aan een bijeenkomst die een dreiging vormt voor de openbare orde; en de persoon heeft toegang tot een plaats waar de openbare orde wordt bedreigd. Verder kunnen gerechtelijke fouilleringen worden uitgevoerd indien er aanwijzingen zijn dat de persoon bewijsmateriaal van een misdaad of wanbedrijf bij zich draagt. Ten derde kunnen personen vooraleer ze in een cel worden geplaatst door de politie worden gefouilleerd.[90] Geen van deze gevallen zijn echter van toepassing als het gaat om het doorzoeken van smartphones en sociale mediaprofielen in verzoekprocedures OIB. De CBPL stelt trouwens ook dat medewerkers van het CGVS niet opgeleid zijn om taken uit te voeren die initieel thuishoren in de strafwetgeving.[91] De enige finaliteit van de doorzoeking door het CGVS is het verzamelen van gegevens ter verificatie van het asielrelaas van de verzoeker OIB en zo het voorkomen van misbruik.

Ten slotte bestaat er een fundamenteel verschil tussen het doorzoeken van niet-digitale voorwerpen enerzijds, en digitale gegevensdragers anderzijds. Dit werd reeds in de Belgische rechtsleer omtrent informaticazoekingen in het kader van de strafrechtspleging aangehaald[92], maar werd ook verduidelijkt door het Amerikaanse Hooggerechtshof. Het Hof stelde het substantiële verschil vast tussen het in beslag nemen van fysieke goederen en van elektronische gegevensdragers om deze te doorzoeken in het arrest 'Riley t. Californië'. Letterlijk stelde het Hof daarin dat mobiele telefoons zowel in kwantitatief als in kwalitatief opzicht verschillen van andere objecten die van een persoon in beslag kunnen worden genomen bij een zoeking.[93] Een niet-digitale zoeking wordt namelijk steeds beperkt door de fysieke realiteit ervan en vormt zo volgens het Hof slechts een beperkte inbreuk op het recht op privacy. Elektronische gegevensdragers daarentegen, hebben een eindeloze opslagcapaciteit (miljoenen pagina's tekst, duizenden foto's of honderden video's…) en een zoeking daarin kan dus ook veel verregaandere gevolgen hebben. De hoeveelheid gegevens, de combinatie van verschillende soorten gegevens, het feit dat de gegevens jaren kunnen teruggaan en de alomtegenwoordigheid van mobiele telefoons en andere digitale gegevensdragers verantwoorden een verhoogd risico op serieuze inbreuken op iemands recht op privacy.[94] Individuele privacybekommernissen worden dus versterkt door de alomtegenwoordigheid van smartphones en het volume en type van persoonlijke informatie die ze kunnen bevatten of waartoe ze toegang kunnen geven via cloud-gebaseerde toepassingen. Dit wordt nogmaals bevestigd door het 'US Department of Homeland Security' in een gegevensbeschermingseffectbeoordeling over

[89] Bockstaele, M. et al. De Zoeking Onderzocht. Antwerpen: Maklu, 2009. P. 117.
[90] Artikel 28 Wet op het Politieambt
[91] Advies CBPL P. 7.
[92] Royer, S. en Oerlemans, J.J. "Naar een nieuwe regeling voor beslag op gegevensdragers." Computerrecht 2017/200 (2017). https://www.law.kuleuven.be/strafrecht/BijlagenNEDL/Sroyer_Computerrecht_2017_20.pdf. P. 280.
[93] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 26-27.
[94] Supreme Court of the United States (SCOTUS), Riley t. Californië, nr. 13–132, 25 juni 2014. https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf. P. 17-21.

grensonderzoeken van elektronische apparaten, uitgevoerd bij vreemdelingen die de VS binnenkomen door de U.S. Customs and Border Protection.[95]

Artikel 48/6, §1, lid 4 van de Vreemdelingenwet en artikel 13, lid 2, d) Procedurerichtlijn vertonen, op vlak van de toestemmingsvereiste, de finaliteit (herkomstonderzoek vs. strafrechterlijk onderzoek) en het voorwerp van de maatregel (digitale gegevensdragers vs. niet-digitale voorwerpen), niet te betwisten verschillen. Het aangehaalde artikel van de Procedurerichtlijn kan dus geen rechtsgrond vormen voor de invoering van artikel 48/6, §1, lid 4 van de Vreemdelingenwet.

2.1.2. Omzetting van de Kwalificatierichtlijn

Daarnaast vermeldt de memorie van toelichting dat met het nieuwe artikel 48/6, §1, lid 4 van de Vreemdelingenwet zo nauw mogelijk wordt aangesloten bij de tekst van artikel 4 van de Kwalificatierichtlijn[96]. Ook in het advies over het wetsontwerp van het UNHCR wordt dit bevestigd.[97]

> *Artikel 4: Beoordeling van feiten en omstandigheden*
>
> *1. De lidstaten mogen van de verzoeker verlangen dat hij alle elementen ter staving van het verzoek om internationale bescherming zo spoedig mogelijk indient. De lidstaat heeft tot taak om de relevante elementen van het verzoek in samenwerking met de verzoeker te beoordelen.*

De toepasselijkheid van de Kwalificatierichtlijn als rechtsgrond wordt bevestigd in de uiteenzetting over de medewerkingsplicht (zie '2.2.1.'), zoals vertegenwoordigd in de eerste zin van artikel 4, §1 Kwalificatierichtlijn, en over de samenwerkingsplicht en gedeelde bewijslast (zie '2.2.2.'), zoals vertegenwoordigd in de tweede zin van artikel 4, §1 Kwalificatierichtlijn.

2.2. Medewerkingsplicht, samenwerkingsplicht en gedeelde bewijslast binnen verzoekprocedures om internationale bescherming

De praktijken beschreven in artikel 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet zijn niet los te koppelen van een aantal essentiële concepten uit het asielrecht, namelijk de medewerkingsplicht, de samenwerkingsplicht en de gedeelde bewijslast. Enerzijds maakt de bevoegdheid van het CGVS om smartphones en andere gegevensdragers te doorzoeken, zoals voorzien in artikel 48/6, §1, lid 4 van de Vreemdelingenwet, deel uit van de medewerkingsplicht van de verzoeker OIB. Anderzijds kadert de bevoegdheid van het Commissariaat om sociale mediaprofielen vanop afstand te screenen, omschreven in artikel 57/7, §2 van de Vreemdelingenwet, binnen de samenwerkingsplicht (ook onderzoeks- of beoordelingsplicht genoemd) van het CGVS.

[95] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 2.
[96] Memorie van toelichting bij de wetswijziging P. 29.
[97] Advies UNHCR P. 5.

2.2.1. De medewerkingsplicht

De medewerkingsplicht van de verzoeker OIB wordt erkend[98] door het UNHCR[99], het Hof van Justitie van de EU[100] en het Europees Hof voor de Rechten van de Mens[101]. Het is in de Vreemdelingenwet opgenomen in de eerste zin van het eerste lid van artikel 48/6, §1 en in artikel 51. Deze plicht houdt in dat verzoekers vanaf het doen van hun verzoek OIB verplicht zijn om mee te werken met de bevoegde overheden om hun identiteit en andere elementen ter staving van hun verzoek vast te stellen. Er wordt van hen volledige medewerking verwacht bij het verstrekken van gegevens en bewijzen over hun identiteit, nationaliteit, reisweg, asielrelaas, vluchtmotieven … om zo een correcte beoordeling van het verzoek OIB mogelijk te maken.[102] De medewerkingsplicht is gesteund op het beginsel *actori incumbit probatio*. Het betreft een algemeen beginsel van de bewijslast: de persoon die zich op een recht beroept, moet er het bewijs van leveren.[103] Er dient echter opgemerkt te worden, dat een al te strikt gebruik van dit beginsel in asielcontexten volgens het EHRM niet op z'n plaats is, rekening houdend met de intrinsieke moeilijkheden van het leveren van bewijs voor verzoekers OIB.[104]

Verzoekers OIB worden volop onderworpen aan controle door asielautoriteiten aan de hand van identificatiestrategieën. Deze manifesteren zich vandaag als een gigantisch informatienetwerk, waar persoonlijke gegevens volop door nationale en internationale asielautoriteiten worden uitgewisseld en verwerkt. Het is bijgevolg die elektronische informatie, die volgens de besproken wetswijziging onderdeel uitmaakt van de medewerkingsplicht van de verzoeker. De link tussen artikel 48/6, §1, lid 4 van de Vreemdelingenwet en de medewerkingsplicht wordt in het eerste verslag over het wetsontwerp ook uitdrukkelijk bevestigd. De aanpassingen worden gekaderd in de strijd tegen misbruik van de verzoekprocedure OIB. Hiervoor wordt getracht om een groter belang te hechten aan de medewerkingsplicht 'waarvan elke verzoeker OIB zich ten volle bewust dient te zijn'.[105]

Het UNHCR dringt er op aan het gebrek aan documenten niet automatisch te linken aan een gebrek aan medewerking.[106] Ook het EHRM is van mening dat niet al te veel gewicht mag worden gehecht aan het ontbreken van documentatie en bewijsmateriaal. Het Hof erkent dat het voor een asielzoeker moeilijk, zo niet onmogelijk, kan zijn om binnen een korte termijn bewijzen te leveren, vooral als die bewijzen

[98] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 195.
[99] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Guide des procédures et critères à appliquer pour déterminer le statut de réfugié." (december 2011). https://www.refworld.org/docid/4fc5db782.html. § 196.
[100] Hierna: HvJ; HvJ, C-465/07, Elgafaji t. Staatssecretaris van Justitie, 2009. §10.; HvJ, C-277/11, M.M. t. Ierland, 2012. §16.
[101] Hierna: EHRM; EHRM, Saadi t. Italië, nr. 37201/06, 28 februari 2008, § 129.; EHRM, NA t. VK, nr. 25904/07, 17 juli 2008, § 111.; EHRM, N. t. Finland, nr. 38885/02, 26 juli 2005. § 167.
[102] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 195.
[103] Nansen (The Belgian Refugee Council). "Beoordeling van de bewijsmiddelen inzake asiel: de actualiteit sinds het arrest Singh e.a. v. België." (maart 2018). https://nansen-refugee.be/wp-content/uploads/2019/01/nansen-note-2018-3-asielprocedure-beoordeling-bewijsmiddelen.pdf. P. 7.
[104] Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 6.
[105] Verslag 1 bij de wetswijziging P. 5-6.
[106] Advies UNHCR P. 10.; VN- Hoog Commissariaat voor de Vluchtelingen. "Note on Burden and Standard of Proof in Refugee Claims." (december 1998). https://www.refworld.org/docid/3ae6b3338.html. P. 3.

moeten worden verkregen van het land waaruit de verzoeker beweert te zijn gevlucht. Het ontbreken van directe bewijsstukken kan dus niet *in se* doorslaggevend zijn.[107]

2.2.2. De samenwerkingsplicht en de daaruit voortvloeiende gedeelde bewijslast

Tegenover de medewerkingsplicht speelt nog een ander concept: de samenwerkingsplicht[108], die zowel gericht is tot de verzoeker, als tot de autoriteit die met het onderzoek van het verzoek OIB is belast. Het UNHCR categoriseert de samenwerkingsplicht als een kernbeginsel van het vluchtelingenrecht.[109] De bewijslast in verzoekprocedures OIB ligt slechts 'in beginsel' bij de verzoeker. Daarnaast rust de plicht om alle relevante feiten vast te stellen en te beoordelen op de instantie die het verzoek beoordeelt.[110] In de Belgische Vreemdelingenwet wordt de samenwerkingsplicht als 'onderzoeks- of beoordelingsplicht' uiteengezet in artikel 48/6, §5. Volgens dit artikel moet het CGVS de verzoeken beoordelen op individuele, objectieve en onpartijdige wijze en wordt onder andere rekening gehouden met: de relevante landeninfo (op het moment van het verzoek), de door de verzoeker aangebrachte verklaringen en stukken en de individuele situatie van de verzoeker.

De rechtspraak van het EHRM bevestigt de vaststelling dat de 'slechts principiële' medewerkingsverplichting van de verzoeker steeds moet worden gekoppeld aan de samenwerkingsverplichting van de asielautoriteit.[111] Daarnaast benadrukte het Hof dat lidstaten de beoordeling van een risico op een schending van het recht op leven of het verbod van foltering nauwkeurig en rigoureus moeten uitvoeren.[112] Daarom moet deze beoordeling niet alleen worden uitgevoerd in het licht van de door de verzoeker aangeleverde elementen, maar ook van de door nationale autoriteiten aangevoerde informatie om twijfels omtrent dit bewijsmateriaal weg te nemen.[113] Het EHRM stelt dus dat bevoegde asielautoriteiten de positieve verplichting[114] hebben om onderzoek in te stellen naar beweerde materiële feiten, die met redelijke middelen kunnen worden bevestigd of

---

[107] EHRM, Bahaddar t. Nederland, nr. 145/1996/764/965, 19 februari 1998. §45.; EHRM, Said t. Nederland, nr. 2345/02, 5 juli 2005. §49.; Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 6.

[108] Artikel 4, lid 1 in fine Kwalificatierichtlijn

[109] VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 35.

[110] VN- Hoog Commissariaat voor de Vluchtelingen. "Handbook on Procedures and Criteria for Determining Refugee Status under the 1951 Convention and the 1967 Protocol relating to the Status of Refugees." (januari 1992).
https://www.unhcr.org/4d93528a9.pdf. §195-196.; Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 524-525.

[111] EHRM, Saadi t. Italië, nr. 37201/06, 28 februari 2008, § 129.; EHRM, NA t. VK, nr. 25904/07, 17 juli 2008, § 111.; EHRM, N. t. Finland, nr. 38885/02, 26 juli 2005. § 167.; EHRM, R.C. t. Zweden, nr. 41827/07, 9 maart 2010. §50.; EHRM, A.A. t. Frankrijk, nr. 18039/11, 15 januari 2015. §53.; EHRM, R.K. t. Frankrijk, nr. 61264/11, 9 juli 2015. §59.; EHRM, JK e.a. t. Zweden, nr. 59166/12, 23 augustus 2016. §96-98.; Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 4.

[112] EHRM, Shamayev e.a. t. Georgië en Rusland, nr. 36378/02, 12 april 2005. §40.; EHRM, M.S.S. t. België, nr. 30696/09, 21 januari 2011. §387.; EHRM, M. e.a. t. Bulgarije, nr. 41416/08, 26 juli 2011. §127.; EHRM, Chahal t. VK, nr. 70/1995/576/662, 15 november 1996. §96.; EHRM, NA t. Verenigd Koninkrijk, nr. 25904/07, 17 juli 2008. §111.; EHRM, Jabari t. Turkije, nr. 40035/98, 11 juli 2000. §39.; EHRM, Hirsi Jamaa e.a. t. Italië, nr. 27765/09, 23 februari 2012. §116.; EHRM, R.C. t. Zweden, nr. 41827/07, 9 maart 2010. §50.; Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 5.

[113] EHRM, F.H. t. Zweden, nr. 32621/06, 20 januari 2009. §95.; EHRM, NA t. VK, nr. 25904/07, 17 juli 2008. §111.; EHRM, R.C. t. Zweden, nr. 41827/07, 9 maart 2010. §50.; EHRM, N. t. Zweden, nr. 23505/09, 20 juli 2010. §53.; EHRM, Saadi t. Italië, nr. 37201/06, 28 februari 2008, § 129.

[114] EHRM, JK e.a. t. Zweden, nr. 59166/12, 23 augustus 2016. §98.

weerlegd. Indien relevante bewijsstukken dus relatief gemakkelijk kunnen worden geverifieerd door het raadplegen van een objectieve en betrouwbare bron, dan vereist de samenwerkingsplicht dat de asielautoriteit dit ook doet, om zo de bestaande twijfels erover weg te werken.[115]

Aan deze plicht tot het wegwerken van twijfels omtrent het aangevoerde bewijsmateriaal, wordt in bepaalde situaties zelfs nog bijkomend gewicht toegekend. Het gaat om de situaties waarin de verzoeker OIB het risico op refoulement[116] door een verwijderingsmaatregel *prima facie* heeft kunnen aantonen. De bewijslast wordt in dit geval verlaagd. Het volstaat dat de verzoeker aantoont dat de aangevoerde elementen 'kunnen' bewijzen dat er een risico op schending van artikel 3 EVRM is, in plaats van de 'gegronde redenen' voor zulk bewijs die normaal vereist zijn.[117] In dat geval gaat het niet alleen om een samenwerkingsplicht, maar is er zelfs sprake van een 'verschuiving van de bewijslast' naar de beslissingsautoriteit.[118] In de Belgische Vreemdelingenwet wordt deze verschuiving van de bewijslast echter enkel erkend indien de verzoeker in het verleden reeds werd blootgesteld aan vervolging of ernstige schade.[119]

Daarnaast heeft ook het HvJ verklaard dat, hoewel het in het algemeen aan de aanvrager is om alle elementen ter staving van het verzoek voor te leggen, het de plicht blijft van de lidstaat om met de verzoeker samen te werken in het stadium van de vaststelling van de relevante elementen van dat verzoek.[120] Deze verplichting tot samenwerking betekent dus in de praktijk dat, indien er, om welke reden dan ook, sprake is van onvolledige, niet-actuele of niet-relevante aangebrachte elementen door de verzoeker, er medewerking van de asielautoriteiten vereist is. Deze medewerking houdt in dat de

[115] EHRM, Salah Sheekh t. Nederland, nr. 1948/04, 23 mei 2007. §136.; EHRM, Garabayev t. Rusland, nr. 38411/02, 7 juni 2007. §74.; Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 5 en 13.; VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013).
https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 132.; Severijns, R.W.J. "Zoeken naar Zekerheid: Een onderzoek naar de vaststelling van feiten door hoor- en beslismedewerkers van de Immigratie- en Naturalisatiedienst in de Nederlandse asielprocedure." Radboud University (2019).
https://repository.ubn.ru.nl/bitstream/handle/2066/207000/207000.pdf?sequence=1. P. 82-83.

[116] Geen enkele staat mag personen uitzetten of terugzenden ("refouler") naar of uitleveren aan een andere staat wanneer er gegronde redenen zijn om aan te nemen dat zij daar gevaar zouden lopen te worden onderworpen aan foltering; onmenselijke of vernederende behandelingen of bestraffingen; of dat hun leven of vrijheid daar bedreigd zou worden op grond van ras, godsdienst, nationaliteit, het behoren tot een bepaalde sociale groep of politieke overtuiging.
Het non-refoulementbeginsel vindt zijn grond in mensenrechteninstrumenten (artikel 3, §1 VN Antifolterverdrag; artikel 3 EVRM), het vluchtelingenrecht (artikel 33, §1 VN Vluchtelingenverdrag; artikel 21 Kwalificatierichtlijn) en in het internationaal gewoonterecht.

[117] Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 5-6.

[118] EHRM, R.C. t. Zweden, nr. 41827/07, 9 maart 2010. §5.; Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 5 en 8.; Reneman, A.M. "EU Asylum Procedures and the Right to an Effective Remedy." VU Amsterdan (2014).
https://openaccess.leidenuniv.nl/bitstream/handle/1887/20403/Reneman.Thesis%20def.pdf?sequence=26. P. 204.; Spijkerboer, T. "Subsidiarity and 'Arguability': the European Court of Human Rights' Case Law on Judicial Review in Asylum Cases." 21 International Journal of Refugee Law (2009). http://thomasspijkerboer.eu/wp-content/uploads/2015/01/Subsidiarity-and-Arguability-The-European-Court-of-Human-Rights-Case-Law-on-Judicial-Review-in-Asylum-Cases.pdf. P. 61-62.

[119] Artikel 48/7 Vreemdelingenwet; "De beoordeling van de asielaanvraag". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/de-beoordeling-van-de-asielaanvraag.

[120] HvJ, C-277/11, M.M. t. Ierland, 2012. §65.; HvJ, C-148/13, C-149/13 en C-150/13, A, B en C t. Staatssecretaris van Veiligheid en Justitie (Nederland), 2014. §56.

autoriteit zich actief inzet om ervoor te zorgen dat alle elementen, die nodig zijn om het verzoek te staven, worden verzameld.[121]

Het CGVS moet dus meewerken bij het verzamelen van gegevens om de relevante elementen in het verzoek te bepalen en te beoordelen en om bestaande twijfels omtrent het aangeleverde bewijsmateriaal weg te werken. Het is echter niet correct om de reikwijdte van deze plicht te beperken tot het inwinnen van informatie over het herkomstland.[122] Op de nationale asielautoriteiten rust namelijk een dubbele verplichting: de plicht om de algemene toestand in het land van oorsprong te onderzoeken en de plicht om de individuele situatie van de verzoeker te bekijken.[123] De rechtsgrond voor deze plichten is respectievelijk te vinden in artikel 10, lid 3, b) Procedurerichtlijn en in artikel 4, lid 1 Kwalificatierichtlijn. Het is dus de taak van de instantie die het verzoek moet beoordelen om, in het licht van de individuele en contextuele omstandigheden van de verzoeker, de gepaste verantwoordelijkheid op zich te nemen om met eigen middelen bewijsmateriaal te verzamelen met betrekking tot het verzoek.[124]

Deze samenwerkingsplicht wordt door een aantal elementen gerechtvaardigd[125], namelijk: de moeilijkheden die de verzoeker kan ondervinden bij het vergaren van bewijsmateriaal[126], de zwaarwichtige gevolgen die een verkeerde beoordeling van de aanvraag kan hebben en de plicht van asielinstanties om een verzoek OIB objectief, onpartijdig en nauwgezet te onderzoeken[127]. Ook is het voor de overheid vaak gemakkelijker toegang tot bepaalde soorten documenten te krijgen dan voor de verzoeker.[128] De samenwerkingsplicht houdt tevens in dat de verzoeker en de instantie die het verzoek beoordeelt samenwerken om een gemeenschappelijk doel te bereiken. Dit gemeenschappelijke doel bestaat erin om zoveel mogelijk relevant bewijsmateriaal te verzamelen om een zo solide als mogelijke basis te hebben van waaruit de geloofwaardigheid van de aangevoerde feiten kan worden beoordeeld en de behoefte aan internationale bescherming kan worden vastgesteld.[129]

Uit deze samenwerkingsplicht tussen verzoeker en onderzoeker vloeit dan ook een gedeelde bewijslast[130] voort. Tijdens een verzoekprocedure OIB worden ‘de feiten en omstandigheden

---

[121] HvJ, C-277/11, M.M. t. Ierland, 2012. §66 en Advies van Advocaat-Generaal Bot (26 april 2012) §67.

[122] De Wilde, A. “Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen” in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 190.

[123] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 525.; VN- Hoog Commissariaat voor de Vluchtelingen. “Beyond Proof: Credibility Assessment in EU Asylum Systems.” (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 134.

[124] VN- Hoog Commissariaat voor de Vluchtelingen. “Beyond Proof: Credibility Assessment in EU Asylum Systems.” (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 126.

[125] De Wilde, A. “Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen” in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 195.

[126] HvJ, C-277/11, M.M. t. Ierland, 2012, Advies van Advocaat-Generaal Bot (26 april 2012) §§ 64-66.; EHRM, Said t. Nederland, nr. 2345/02, 5 juli 2005. §49.; EHRM, N. t. Zweden, nr. 23505/09, 20 juli 2010. §53.

[127] HvJ, C-277/11, M.M. t. Ierland, 2012, § 88.

[128] Ibid. § 66.

[129] Ibid. Advies van Advocaat-Generaal Bot (26 april 2012) §59.

[130] Artikel 4, eerste lid Kwalificatierichtlijn; EHRM, JK e.a. t. Zweden, nr. 59166/12, 23 augustus 2016. §96-98.
VN- Hoog Commissariaat voor de Vluchtelingen. “Note on Burden and Standard of Proof in Refugee Claims.” (december 1998). https://www.refworld.org/docid/3ae6b3338.html. P. 2.; Belgisch Comité voor de Hulp aan Vluchtelingen (BCHV). “Trauma, geloofwaardigheid en bewijs in de asielprocedure.” (2014). http://www.medimmigrant.be/uploads/Publicaties/externe%20documenten/CBARAnalysepsy.pdf. P. 30.; Nansen (The Belgian Refugee Council). “Beoordeling van de bewijsmiddelen inzake asiel: de actualiteit sinds het arrest Singh e.a. v. België.” (maart 2018). https://nansen-refugee.be/wp-content/uploads/2019/01/nansen-note-2018-3-asielprocedure-beoordeling-bewijsmiddelen.pdf. P. 8.; Severijns, R.W.J. “Zoeken naar Zekerheid: Een onderzoek naar de vaststelling van

beoordeeld'[131] en dit gebeurt in twee fasen. In de eerste fase worden de feitelijke omstandigheden die vasthangen aan het verzoek OIB vastgesteld. Daarna, in de tweede fase, worden deze gegevens in rechte beoordeeld en beslist men of voldaan is aan de voorwaarden in de Kwalificatierichtlijn voor de toekenning van een statuut van internationale bescherming. Deze tweede fase is de uitsluitende bevoegdheid van de asielinstanties. In de eerste fase zijn, *a contrario*, zowel de verzoeker als de asielinstanties medeverantwoordelijk en hebben zij gezamenlijk de taak om alle relevante feiten van het verzoek OIB vast te stellen en te beoordelen.[132] Dit beginsel is van algemene toepassing binnen verzoekprocedures OIB, zelfs wanneer de verklaringen van de verzoeker onwaarschijnlijk, inconsistent of onvoldoende onderbouwd lijken[133].

feiten door hoor- en beslismedewerkers van de Immigratie- en Naturalisatiedienst in de Nederlandse asielprocedure." Radboud University (2019). https://repository.ubn.ru.nl/bitstream/handle/2066/207000/207000.pdf?sequence=1. P. 82.

[131] Titel artikel 4, eerste lid Kwalificatierichtlijn

[132] HvJ, C-277/11, M.M. t. Ierland, 2012, §64-65, 69 en 70.; Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 525.

[133] Advies UNHCR P. 5.

3. Theoretisch kader: toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming vanuit privacy- en gegevensbeschermingsrechtelijk perspectief

3.1. Het recht op privacy versus het recht op gegevensbescherming

Bij het doorzoeken en gebruiken van informatie op smartphones en sociale mediaprofielen in het kader van verzoekprocedures OIB worden gegevens van de verzoeker door de autoriteiten verwerkt. Deze gegevens maken onder andere deel uit van het privé-, familie- en gezinsleven en bevatten informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Deze omschrijvingen komen enerzijds overeen met het toepassingsgebied van bet Europees en Belgisch regelgevend kader rond het recht op privacy en anderzijds met dat van het recht op gegevensbescherming. Dit werd ook door de toenmalige Staatssecretaris voor Asiel en Migratie tijdens de voorbereidingen van het wetsontwerp bevestigd.[134] Het is echter belangrijk het onderscheid tussen deze twee rechten te verduidelijken.

Het recht op privacy is erkend als een universeel mensenrecht[135] en werd doorheen de geschiedeis conceptueel gelinkt aan begrippen als 'menselijke waardigheid', 'persoonlijke vrijheid'[136], 'onschendbaarheid van de woning'[137], 'vertrouwelijkheid van correspondentie' …[138] Het individueel recht omvat onder andere het recht op een privéleven, het recht op autonomie, het recht op controle over persoonlijke informatie en het recht om met rust gelaten te worden.[139] Privacy wordt in meerdere internationale instrumenten verankerd als 'het recht op eerbiediging van privé-, familie- en gezinsleven', waaronder artikel 8 EVRM, artikel 7 EU-Handvest van de Grondrechten[140], artikel 12 UVRM[141], artikel 17 VBPR[142] en artikel 16 VRK[143].

In het licht van de technologische vooruitgang ontstond de nood aan gegevensbescherming, een bijkomende kwalificering van privacy als 'informationele privacy' of 'het recht op informationele zelfbeschikking'[144]. De gegevensbescherming vormt een antwoord op de nood aan het opleggen van verplichtingen voor informatieverwerkers en het verlenen van rechten en bescherming[145] aan individuen wiens informatie wordt verwerkt.[146] Het recht op bescherming van persoonsgegevens is binnen het kader

---

[134] Verslag 2 bij de wetswijziging P. 4.

[135] "Data Protection". www.edps.europa.eu. European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection_en.

[136] Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 10, 12.

[137] Floridi, L. Protection of Information and the Right to Privacy – A New Equilibrium? Law, Governance and Technology Series, volume 17. Cham: Springer, 2014. P. 43.

[138] González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 23-24, 48.; Van Alsenoy, B. Data Protection Law in the EU: Roles, Responsibilities and Liability. Intersentia, 2019. P. 158.

[139] Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 9.; "Data Protection". www.edps.europa.eu. European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection_en.; Van Alsenoy, B. Data Protection Law in the EU: Roles, Responsibilities and Liability. Intersentia, 2019. P. 158.

[140] Hierna: EU-Handvest

[141] Universele Verklaring voor de Rechten van de Mens

[142] Verdrag inzake Burgergelijke en Politieke Rechten

[143] Verdrag inzake de Rechten van het Kind

[144] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 18.; Council of Europe/European Court of Human Rights. "Guide on Article 8 of the European Convention on Human Rights." (augustus 2019). https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf. §170.

[145] Van Alsenoy, B. Data Protection Law in the EU: Roles, Responsibilities and Liability. Intersentia, 2019. P. 157-158.

[146] González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 48.

van de Europese Unie als een aparte bepaling[147] terug te vinden in artikel 8 van het EU-Handvest en in artikel 16 van het VWEU[148].

Hoewel dit recht in het EVRM niet uitdrukkelijk apart wordt vermeld, is het ook onder het privacy-artikel van het EVRM (artikel 8) onder te brengen[149] en vormt het een fundamenteel recht op zichzelf[150]. Met de opkomst van de digitale gegevensverwerking[151] ontstond namelijk ook binnen de Raad van Europa de nood om een bijkomende bescherming in te bouwen. Artikel 8 EVRM werd aanvankelijk als ongeschikt beschouwd om bescherming te bieden voor het hele gegevensbeschermingscontentieux.[152] Hierop werd een apart verdrag aan de gegevensbescherming gewijd, met name het Verdrag 108 van de Raad van Europa voor de bescherming van individuen met betrekking tot de automatische verwerking van persoonlijke gegevens[153].[154] Ondanks deze initiële visie dat het recht op gegevensbescherming niet in artikel 8 EVRM kon worden ondergebracht, gebeurde dit geleidelijk aan door de rechtspraak van het EHRM (deels) toch.[155] Het EHRM heeft in de loop der jaren zijn interpretatie van artikel 8 uitgebreid tot de bescherming van personen tegen bepaalde informatiepraktijken, maar heeft nooit uitdrukkelijk het volledige toepassingsgebied van Verdrag 108 opgenomen.[156]

In verschillende arresten bracht het Hof gegevensbeschermingskwesties in nauw verband met het recht op privacy.[157] In de zaak Leander[158] oordeelde het Hof bijvoorbeeld dat de loutere opslag door de politie van informatie betreffende het privéleven van een persoon neerkomt op inmenging in het recht op privacy.[159] Ook in de zaak Amann[160] en Rotaru[161] werd artikel 8 EVRM toegepast om een recht op gegevensbescherming te doen ontstaan.[162] In 2007 werd in de zaak Copland t. VK[163] door het Hof

[147] Leenes, R., van Brakel, R., Gutwirth, S. en De Hert, P. Data protection and privacy: the age of intelligent machines. Oxford: Hart Publishing, 2017. P. 3 en 7.
[148] Verdrag betreffende de werking van de Europese Unie
[149] Council of Europe/European Court of Human Rights. "Guide on Article 8 of the European Convention on Human Rights." (augustus 2019). https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf. §159.
[150] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 19.; Leenes, R., van Brakel, R., Gutwirth, S. en De Hert, P. Data protection and privacy: the age of intelligent machines. Oxford: Hart Publishing, 2017. P. 3.
[151] Leenes, R., van Brakel, R., Gutwirth, S. en De Hert, P. Data protection and privacy: the age of intelligent machines. Oxford: Hart Publishing, 2017. P. 5.
[152] González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 84.
[153] Verdrag 108 van de Raad van Europa voor de bescherming van individuen met betrekking tot de automatische verwerking van persoonlijke gegevens, 1981. Hierna: Verdrag 108
[154] Kokott, J. en Sobotta, C. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR." International Data Privacy Law (2013). https://doi.org/10.1093/idpl/ipt017. P. 223.
[155] Leenes, R., van Brakel, R., Gutwirth, S. en De Hert, P. Data protection and privacy: the age of intelligent machines. Oxford: Hart Publishing, 2017. P. 3.; González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 94.; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 154.
[156] González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 104.
[157] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 37.
[158] EHRM, Leander t. Zweden, nr. 9248/81, 26 maart 1987. §48.
[159] González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 97.
[160] EHRM, Amann t. Zwitserland, nr. 27798/95, 16 februari 2000. § 65.
[161] EHRM, Rotaru t. Roemenië, nr. 28341/95, 4 mei 2000. §43, 46.
[162] Kokott, J. en Sobotta, C. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR." International Data Privacy Law (2013). https://doi.org/10.1093/idpl/ipt017. P. 223.
[163] EHRM, Copland t. VK, nr. 62617/00, 3 april 2007, §44.

uiteengezet dat het verzamelen en opslaan van persoonlijke informatie uit de telefoon, het e-mailverkeer en het internetgebruik van de verzoeker, zonder diens medeweten, een inbreuk vormt op artikel 8 EVRM.[164] In de zaak S en Marper t. VK[165] stelde het EHRM dat de bescherming van persoonsgegevens van fundamenteel belang is voor de uitoefening van het recht op privacy, zoals gewaarborgd door artikel 8 van het EVRM.[166] Finaal erkende het Hof in de zaak Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland dat artikel 8 EVRM voorziet in een 'recht op informationele zelfbeschikking'.[167] Het Hof besluit zo dat het verzamelen, opslaan of openbaar maken van informatie met betrekking tot de persoonlijke levenssfeer een inmenging vormt in het recht op privacy.[168] Het HvJ interpreteert de rechtspraak van het EHRM dan ook als volgt: het privéleven omvat de bescherming van persoonsgegevens, gedefinieerd als informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[169]

Hoewel het dus gaat om twee onderscheiden rechten[170], bestaat er een duidelijke conceptuele overlap en samenhang tussen de twee[171]. Naast de integratieve interpretatie in de rechtspraak, wordt ook het regelgevend kader van de gegevensbescherming sterk gekoppeld aan dat van de privacy[172], de gegevensbescherming wordt vaak weergegeven als een element van privacy[173], als een instrument van privacy[174] of als een voortvloeisel uit het recht op privacy[175] en beide termen worden vaak samen vermeld[176].

---

[164] White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl. P. 31.

[165] EHRM, S en Marper t. VK, nr. 30562/04 en 30566/04, 4 december 2008, §103.

[166] White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl. P. 29.

[167] EHRM, Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland, nr. 931/13, 27 juni 2017. § 137.

[168] EHRM, Rotaru t. Roemenië, nr. 28341/95, 4 mei 2000. §46.; EHRM, Amann t. Zwitserland, nr. 27798/95, 16 februari 2000. § 69 en 80.

[169] Kokott, J. en Sobotta, C. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR." International Data Privacy Law (2013). https://doi.org/10.1093/idpl/ipt017. P. 223.

[170] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 18.; Kokott, J. en Sobotta, C. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR." International Data Privacy Law (2013). https://doi.org/10.1093/idpl/ipt017. P. 222.; González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 268.

[171] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 19.

[172] Van Alsenoy, B. Data Protection Law in the EU: Roles, Responsibilities and Liability. Intersentia, 2019. P. 158. González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 75.

[173] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 37.; White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl. P. 26. González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the Eu. Cham: Springer, 2014. P. 86.

[174] Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 13.; Council of Europe/European Court of Human Rights. "Guide on Article 8 of the European Convention on Human Rights." (augustus 2019). https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf. §166.; EHRM, Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland, nr. 931/13, 27 juni 2017. §133.

[175] "Data Protection". www.edps.europa.eu. European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection_en

[176] Leenes, R., van Brakel, R., Gutwirth, S. en De Hert, P. Data protection and privacy: the age of intelligent machines. Oxford: Hart Publishing, 2017. P. 5.; González-Fuster, G. The Emergence of Personal Data Protection As a Fundamental Right of the

Het onderscheid tussen beide rechten ligt echter in hun formulering en toepassingsgebied. Het recht op privacy is allesomvattend geformuleerd en bestaat uit een algemeen verbod op inmenging in het privéleven van een persoon. Het recht op gegevensbescherming is een moderner concept[177], waarbij een evenwichtssysteem wordt geïnstalleerd om personen te beschermen, enkel en telkens wanneer hun persoonsgegevens worden verwerkt.[178] Het privéleven zoals bedoeld in het recht op privacy omvat dus niet noodzakelijkerwijs alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, wat wel het toepassingsgebied van het recht op gegevensbescherming vormt.[179] In die zin is het recht op gegevensbescherming ruimer dan dat van het recht op privacy.[180] Gegevensbescherming heeft namelijk betrekking op alle soorten gegevens en gegevensverwerking, ongeacht de verhouding en impact hiervan op het privéleven van de betrokkene. Een dergelijke impact op iemands privéleven is dan weer wel vereist om te kunnen spreken over het recht op privacy.[181]

Uit dit alles vloeit voort dat voor het recht op gegevensbescherming zowel artikel 8 van het EU-Handvest als artikel 8 van het EVRM relevant zijn. Dit wordt bevestigd in overweging 73 van de AVG, dat stelt dat beperkingen op het gegevensbeschermingsrecht in overeenstemming moeten zijn met de vereisten van het Handvest én het EVRM.[182]

3.2. Het Europees gegevensbeschermingsrechtelijk kader: de Algemene Verordening Gegevensbescherming

Het Belgisch recht wordt, als het gaat om de verwerking van persoonsgegevens, beheerst door de Europese Algemene Verordening Gegevensbescherming. Het gaat om een set regels rond de bescherming van persoonsgegevens[183] die via deze verordening in de hele Europese Unie geharmoniseerd worden. De AVG heeft onder andere geprobeerd tegemoet te komen aan de uitdagingen die door de opkomst van sociale media in onze samenleving zijn binnengeslopen.[184] Ten tijde van de voorbereidingen van de hier besproken wetswijziging (21 november 2017) was deze Europese regelgeving met betrekking tot gegevensbescherming nog niet van toepassing (dit was pas het geval vanaf 25 mei 2018). Dit niet 'van toepassing' zijn, verhinderde echter niet dat de AVG wel al 'van kracht' was (sinds 24 mei 2016). Het verschil tussen beide ligt erin dat de verordening nog niet strikt juridisch afdwingbaar was, maar wel reeds een positieve en negatieve verplichting aan de lidstaten oplegde. De negatieve verplichting bestond in een onthoudingsplicht om nationale wetgeving uit te

Eu. Cham: Springer, 2014. P. 270.; Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 12.

[177] Leenes, R., van Brakel, R., Gutwirth, S. en De Hert, P. Data protection and privacy: the age of intelligent machines. Oxford: Hart Publishing, 2017. P. 5.; HvJ, C-92/09 en C-93/02C-465/07, Volker und Markus Schecke GbR t. Land Hessen, 2010. Conclusie van advocaat-generaal Sharpston, §71.

[178] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 19.

[179] Kokott, J. en Sobotta, C. "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR." International Data Privacy Law (2013). https://doi.org/10.1093/idpl/ipt017. P. 225.

[180] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 37.

[181] Ibid. P. 20.

[182] White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl. P. 26.

[183] Artikel 1 AVG

[184] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 364.

vaardigen die het door de AVG beoogde resultaat ernstig in gevaar zou brengen. De positieve verplichting hield in dat alle nodige uitvoeringsbepalingen dienden te worden genomen om de Verordening uitwerking te geven.[185] Rekening houdend met deze toen geldende verplichtingen, zal de wetswijziging worden besproken in het licht van de huidige gegevensbeschermingsregelgeving, de AVG.

Wat het territoriaal toepassingsgebied van de AVG betreft, kan het Belgische CGVS gecategoriseerd worden als een verwerkingsverantwoordelijke[186] of verwerker[187] gevestigd in de EU[188]. De hier besproken praktijken die door de wetswijziging worden ingevoerd vallen dus territoriaal gezien binnen het toepassingsgebied van de AVG.

Materieel gezien beslaat het toepassingsgebied van de AVG 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen'[189].

'Persoonsgegevens' worden gedefinieerd als 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene)'[190]. Voorbeelden van soorten persoonsgegevens zijn volgens het CGVS en de Dienst Vreemdelingenzaken: identificatiegegevens (naam, adres, telefoonnummer …), persoonlijke kenmerken (leeftijd, geslacht, geboortedatum, burgerlijke staat, nationaliteit …), leefgewoonten (reizen en verplaatsingen, sociale contacten, bezittingen …), samenstelling van het gezin, vrijetijdsbesteding en interesses, lidmaatschappen (clubs, organisaties, verenigingen, vakbondsmaatschappen …), studie en opleiding, beroep en betrekking, raciale of etnische gegevens, politieke opvattingen, filosofische en religieuze overtuigingen, financiële situatie, gerechtelijke gegevens, gegevens met betrekking tot het seksueel gedrag of seksuele gerichtheid en gegevens betreffende de gezondheid.[191] Deze soorten persoonsgegevens zijn veelvuldig op smartphones en sociale mediaprofielen terug te vinden. Via deze digitale kanalen kan de informatie aan de betrokken verzoekers OIB worden gelinkt, wat de gegevens tot 'informatie over een geïdentificeerde of identificeerbare natuurlijke persoon' maakt.

Met 'de betrokkene' wordt de geïdentificeerde of identificeerbare persoon bedoeld, wiens persoonsgegevens worden verwerkt.[192] Deze identificering kan gebeuren aan de hand van een naam, een identificatienummer, locatiegegevens, een online-identificator of eigenschappen en factoren die specifiek zijn voor de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit van de betrokkene in kwestie.[193] Het verwerken van iemands persoonsgegevens op smartphones en sociale mediaprofielen vormt dus een van de gevallen waarbij de betrokkene identificeerbaar is. Wanneer het echter gaat om anonieme informatie of gepseudonimiseerde

[185] Advies CBPL P. 2.; European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 73.
[186] Wordt verder in dit onderdeel verduidelijkt.
[187] Wordt verder in dit onderdeel verduidelijkt.
[188] Artikel 3 AVG
[189] Artikel 2 (1) AVG
[190] Artikel 4 (1) AVG
[191] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.; "Verwerking van persoonsgegevens". www.dofi.ibz.be. Dienst Vreemdelingenzaken. https://dofi.ibz.be/sites/dvzoe/NL/Over-ons/Pages/Verwerking-van-persoonsgegevens.aspx.
[192] Artikel 4 (1) AVG
[193] Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 55.

gegevens[194], die (zelfs bij het gebruik van aanvullende informatie) niet kunnen leiden tot enige identificering, is er geen sprake van een identificeerbare persoon of betrokkene.[195]

Om te kunnen spreken van 'verwerking' van die persoonsgegevens, volstaat het volgens artikel 4 (2) AVG al dat de gegevens worden opgevraagd, geraadpleegd of gebruikt op al dan niet geautomatiseerde wijze. Bij het doorzoeken en gebruiken van informatie op smartphones en sociale mediaprofielen door het CGVS kan dus gesproken worden van de verwerking van persoonsgegevens.

Het CGVS kan worden beschouwd als 'verwerkingsverantwoordelijke', aangezien het gaat om een overheidsinstantie die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt[196] en tegelijkertijd als 'verwerker' van persoonsgegevens, aangezien deze de persoonsgegevens verwerkt in de zin van artikel 4 (2) AVG[197].

De AVG bevat verder geen expliciete overwegingen over hoe de gegevensbeschermingsrechtelijke situatie van betrokkenen er moet uitzien in de context van verzoeken OIB (of in een migratiecontext in het algemeen).[198] Uit bovenstaande analyse vloeit dus voort dat de AVG van toepassing is op alle entiteiten die persoonsgegevens verzamelen en verwerken van betrokken die in de EU verblijven, ongeacht hun verblijfsrechtelijke status.

3.3. Het Belgisch gegevensbeschermingsrechtelijk kader: de Wet Bescherming Persoonsgegevens

In België wordt het rechtsgebied van de gegevensbescherming beheerst door de AVG (zoals vermeld in '3.2.'), maar ook door de Kaderwet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Wet Bescherming Persoonsgegevens)[199]. Deze Kaderwet is een Belgische implementatiewet die een gedeeltelijke omzetting vormt van de AVG en de Richtlijn Politie en Justitie, voor zaken die voormelde instrumenten aan de discretionaire bevoegdheid van de lidstaten hebben overgelaten (de zogenaamde 'open clausules'[200]). Ten tijde van het besproken wetsvoorstel gold nog de Kaderwet van 8 december 1992 en het is deze versie waarvan in de voorbereidende werken van het wetsontwerp wordt gesteld dat artikel 48/6, §1, lid 4 en artikel 57/7, §2 van de Vreemdelingenwet ermee in overeenstemming zijn[201]. Nu is dus echter de aangepaste wet van 30 juli 2018 van kracht, die in overeenstemming is gebracht met de AVG.

---

[194] Pseudonimisering is het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. (Artikel 4 (5) AVG)

[195] Overweging 26 AVG

[196] Artikel 4 (7) AVG

[197] Artikel 4 (8) AVG

[198] Latonero, M., Hiatt, K., Napolitano, A., Clericetti, G. en Penagos, M. "Digital Identity in the Migration & Refugee Context: Italy case study." Data & Society (2019). https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf. P. 18.

[199] Wet 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, hierna: Wet Bescherming Persoonsgegevens

[200] "Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Kaderwet)". www.gegevensbeschermingsautoriteit.be. Gegevensbeschermingsautoriteit. https://www.gegevensbeschermingsautoriteit.be/wet-betreffende-de-bescherming-van-natuurlijke-personen-met-betrekking-tot-de-verwerking-van#overlay-context=wet-van-3-december-2017-tot-oprichting-van-de-gegevensbeschermingsautoriteit.

[201] Memorie van toelichting bij de wetswijziging P. 36 en 137.; Verslag 2 bij de wetswijziging P. 5 en 27.

4. Voorwaarden voor gegevensverwerking en beperkingen op het recht op gegevensbescherming

4.1. Beginselen in de Algemene Verordening Gegevensbescherming

Allereerst moet de gegevensverwerking conform de algemene beginselen van de AVG gebeuren. In artikel 5 AVG worden deze beginselen uiteengezet, die cumulatief in acht moeten worden genomen. Zelfs als een bepaalde gegevensverwerking rechtmatig gebeurt (d.w.z. op grond van een geldige verwerkingsgrond voor het verwerken van de persoonsgegevens), moeten de andere beginselen voor gegevensverwerking in de AVG tevens worden gerespecteerd.[202]

4.1.1. Rechtmatige, behoorlijke en transparante verwerking

Het moet allereerst gaan om een rechtmatige, behoorlijke en transparante verwerking.[203] De rechtmatigheidsvereiste slaat op het bestaan van een verwerkingsgrond voor het raadplegen en gebruiken van de persoonsgegevens, zoals in '4.2.' verder wordt uiteengezet. De behoorlijke en transparante verwerking vereist een eerlijk en loyaal gegevensverwerkingsproces.

Het 'behoorlijke karakter' van de gegevensverwerking slaat op de relatie tussen de betrokkene en de verwerkingsverantwoordelijke. Verwerkingsverantwoordelijken moeten betrokkenen en het grote publiek ervan in kennis stellen dat zij gegevens op een wettige en transparante wijze zullen verwerken en moeten ook kunnen aantonen dat de verwerkingen in overeenstemming zijn met de AVG. Zo moeten de betrokkenen op de hoogte worden gesteld van de verwerking zelf en van de mogelijke risico's die deze met zich meebrengt.[204]

Wat de transparantie van de gegevensverwerking betreft, zijn verwerkingsverantwoordelijken verplicht alle passende maatregelen te nemen om de betrokkenen integraal op de hoogte te brengen en houden, zowel van de manier waarop en het doel waarvoor hun gegevens worden verwerkt, als van de risico's, regels, waarborgen en rechten die op deze verwerking van toepassing zijn. De communicatie omtrent de transparantievereiste moet gebeuren op een gemakkelijk toegankelijke en begrijpelijke manier, met gebruik van simpele en duidelijke taal.[205] Daarnaast is het tijdig verstrekken van informatie, dit wil zeggen: ten laatste wanneer de gegevensverzameling plaatsvindt, een essentieel onderdeel van de verplichting tot transparante en behoorlijke gegevensverwerking.[206]

De concrete invulling van de soorten informatie die aan de betrokkene moeten worden verstrekt bij een gegevensverwerking worden in artikel 13 en 14 van de AVG uitgewerkt en zijn *in casu* beiden relevant. Enerzijds beschrijft artikel 14 AVG welke informatie moet worden meegegeven wanneer de persoonsgegevens niet van de betrokkene zelf zijn verkregen. Dit is het geval wanneer asielautoriteiten vanop afstand, zonder het fysiek in beslag nemen van (digitale) gegevensdragers, sociale mediaprofielen

---

[202] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 4.

[203] Artikel 5 (1) a) jo. overweging 39 AVG

[204] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 118.

[205] Overweging 39 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 120.; Werkgroep gegevensbescherming artikel 29. "Guidelines on transparency under Regulation 2016/679 17/EN WP260." (november 2017). https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025. P. 7-10.

[206] Werkgroep gegevensbescherming artikel 29. "Guidelines on transparency under Regulation 2016/679 17/EN WP260." (november 2017). https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025. P. 14-15.

van verzoekers OIB doorzoeken (artikel 57/7, §2 van de Vreemdelingenwet). Het gaat hoofdzakelijk om de volgende informatie: de identiteit en contactgegevens van de verwerkingsverantwoordelijke (en de functionaris voor gegevensbescherming), de verwerkingsdoeleinden, de rechtsgrond voor de verwerking, de betrokken categorieën van persoonsgegevens, de eventuele ontvangers van de persoonsgegevens, of de persoonsgegevens zullen worden doorgegeven aan een derde land/internationale organisatie, de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, de rechten die de betrokkene heeft met betrekking tot de gegevensverwerking, de (eventueel openbare) bron van de persoonsgegevens en het eventuele bestaan van geautomatiseerde besluitvorming (en nuttige informatie over de onderliggende logica, het belang en de verwachte gevolgen voor de betrokkene).

Artikel 13 AVG somt dan weer op welke informatie precies moet worden verstrekt wanneer persoonsgegevens bij de betrokkene zelf worden verzameld. Dit is van toepassing wanneer smartphones (en andere (digitale) gegevensdragers) effectief in beslag worden genomen en worden doorzocht (artikel 48/6, §1, lid 4 van de Vreemdelingenwet). Het gaat om dezelfde lijst informatiesoorten als in artikel 14, met uitzondering van 'de betrokken categorieën van persoonsgegevens' en 'de (eventueel openbare) bron van de persoonsgegevens'. Voor deze elementen wordt er namelijk vanuit gegaan dat ze reeds duidelijk zijn wanneer de gegevens bij de betrokkene zelf worden verzameld.[207] Daarnaast bevat artikel 13 AVG nog de te verstrekken informatiesoort 'of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt', wat niet in artikel 14 AVG wordt aangehaald.

Hoewel de AVG geen concrete modaliteiten voorschrijft voor het communiceren van bovenstaande informatie aan de betrokkene, is het wel de verantwoordelijkheid van de verwerkingsverantwoordelijke om passende maatregelen te nemen voor het correct vervullen van alle transparantievereisten, rekening houdend met de specifieke omstandigheden van de gegevensverzameling.[208]

4.1.2. Doelbindingsprincipe, dataminimalisatie, nauwkeurigheid, opslagbeperking, integriteit en vertrouwelijkheid

Volgens het doelbindingsprincipe[209] moet elke verwerking een 'specifiek, geëxpliciteerd en gerechtvaardigd doel' nastreven, dat moet worden afgebakend voordat de verwerking een aanvang neemt. Bij de verwerking van persoonsgegevens zonder een bepaald doel, alleen op basis van de overweging dat ze eventueel in de toekomst nuttig kunnen zijn, is niet aan de vereiste van een 'specifiek doel' voldaan.[210] Daarnaast moet het doeleinde van de gegevensverzameling niet alleen worden gespecificeerd door de verwerkingsverantwoordelijke. Het moet ook expliciet worden meegedeeld aan de betrokkenen, door het in begrijpelijke vorm voor hen uiteen te zetten. Het uiteindelijke oogmerk van het doelbindingsprincipe is ervoor zorgen dat de doelen worden gespecificeerd zonder vaagheid of onduidelijkheid te laten over de betekenis of bedoeling ervan.[211] De eis van een 'gerechtvaardigd doel', slaat niet alleen op het feit dat de verwerking rechtmatig gebeurt (in de zin van artikel 6 AVG, wat in '4.2.' uiteen wordt gezet), maar ook op het feit dat het doel zelf 'wettig' is en dit in de meest brede zin

[207] Werkgroep gegevensbescherming artikel 29. "Guidelines on transparency under Regulation 2016/679 17/EN WP260." (november 2017). https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025. P. 36.
[208] Ibid. P. 14.
[209] Artikel 5 (1) b) jo. overweging 39 AVG
[210] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 123.
[211] Werkgroep gegevensbescherming artikel 29. "Opinion 03/2013 on purpose limitation 00569/13/EN WP 203." (2013). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. P. 17.

van het woord[212]. Tot slot mogen de verwerkte persoonsgegevens niet verwerkt worden voor andere doeleinden, die onverenigbaar zijn met het oorspronkelijk aangegeven doel. Hierop bestaan enkel uitzonderingen voor archiveringsdoeleinden in het algemeen belang, voor wetenschappelijke of historische onderzoeksdoeleinden en voor statistische doeleinden.[213] In artikel 6, lid 4 AVG worden de factoren gedefinieerd waarmee rekening moet worden gehouden om te bepalen of een ander doel al dan niet verenigbaar is met het oorspronkelijke doel. De AVG geeft echter geen concrete definitie voor de term 'verenigbaarheid'. In essentie houdt het doelbindingsprincipe dus in dat gegevensverwerking enkel kan plaatsvinden voor een specifiek, geëxpliciteerd en gerechtvaardigd doel en enkel voor bijkomende doeleinden, indien deze verenigbaar zijn met het initiële doel.[214]

Het beginsel van de dataminimalisatie[215] schrijft voor dat de verzamelde persoonsgegevens toereikend moeten zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. De voor de verwerking te verzamelen categorieën gegevens moeten dus zowel noodzakelijk zijn, als rechtstreeks relevant om het aangegeven verwerkingsdoeleinde te bereiken. Het noodzakelijkheidsaspect van de dataminimalisatie houdt tevens in dat de verwerking van persoonsgegevens alleen mag plaatsvinden wanneer het doel van de verwerking redelijkerwijs niet met andere middelen kan worden bereikt. Ook mag de verwerking van gegevens geen onevenredige invloed hebben op de belangen, rechten en vrijheden van de betrokkene.[216] Het beginsel van de dataminimalisatie heeft betrekking op zowel de massa verzamelde gegevens als de massa verwerkte gegevens.[217] Met andere woorden: dataminimalisatie houdt in dat niet meer gegevens mogen worden verzameld en verwerkt dan nodig is om het vooropgestelde doel van de gegevensverwerking te bereiken.

Artikel 5 (1) d) van de AVG[218] omschrijft het beginsel van de nauwkeurigheid of juistheid van persoonsgegevens. Dit beginsel moet door de verwerkingsverantwoordelijke voor elke gegevensverwerking in acht worden genomen, in het licht van de gedefinieerde verwerkingsdoelstellingen. Het vereist dat men persoonsgegevens zo nauwkeurig mogelijk registreert om ervoor te zorgen dat deze doelstellingen kunnen worden bereikt.[219] Alle redelijke maatregelen moeten worden getroffen om onjuiste gegevens onmiddellijk te wissen of te corrigeren en gegevens moeten regelmatig worden gecontroleerd om ze actueel te houden en de nauwkeurigheid ervan te waarborgen. Een verwerkingsverantwoordelijke mag verzamelde persoonsgegevens dus niet gebruiken zonder stappen te ondernemen om met redelijke zekerheid te garanderen dat de gegevens accuraat en actueel zijn.[220]

---

[212] alle vormen van geschreven en gewoonterecht, primair en secundair recht, gemeentelijke besluiten, precedenten in de rechtspraak, grondwettelijke beginselen, fundamentele rechten en andere juridische beginselen
Werkgroep gegevensbescherming artikel 29. "Opinion 03/2013 on purpose limitation 00569/13/EN WP 203." (2013). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. P. 20.

[213] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 122-123.

[214] Ibid. P. 122-123.

[215] Artikel 5 (1) c) jo. overweging 39 AVG

[216] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 125.

[217] European Union Agency for Fundamental Rights (FRA). "Fundamental rights and the interoperability of EU information systems: borders and security." (2017). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf. P. 21.

[218] Artikel 5 (1) d) jo. overweging 39 AVG

[219] VN- Hoog Commissariaat voor de Vluchtelingen. "Guidance on the Protection of Personal Data of Persons of Concern to UNHCR." (augustus 2018). https://www.refworld.org/docid/5b360f4d4.html. P. 20.

[220] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European

Het beginsel van de opslagbeperking[221] schrijft voor dat de gegevens moeten worden bewaard in een vorm waardoor de betrokkene niet langer identificeerbaar is dan nodig voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Persoonsgegevens kunnen voor langere perioden worden opgeslagen louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. In dat geval moeten wel passende technische en organisatorische maatregelen worden genomen om de rechten en vrijheden van de betrokkenen te beschermen. Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan nodig, moet de verwerkingsverantwoordelijke termijnen vaststellen voor het wissen van gegevens of voor een periodieke toetsing ervan. Met andere woorden: persoonsgegevens moeten worden gewist of geanonimiseerd zodra ze niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld. Gegevens die niet meer nodig zijn, kunnen dus nog steeds rechtmatig worden opgeslagen, zolang de betrokkenen niet meer identificeerbaar zijn.[222]

Tot slot legt artikel 5 (1) f) AVG integriteit en vertrouwelijkheid[223] op bij de verwerking van persoonsgegevens. De verwerkingsverantwoordelijke moet een passende beveiliging en vertrouwelijkheid van de gegevens waarborgen door technische of organisatorische maatregelen te nemen. Deze beveiliging en vertrouwelijkheid moeten zorgen voor bescherming, zowel tegen ongeoorloofde toegang en gebruik van de gegevens en de apparatuur die voor de verwerking wordt gebruikt, als tegen onopzettelijk verlies, vernietiging of beschadiging ervan. Bij het uitvoeren van dergelijke maatregelen moet men onder andere rekening houden met de risico's voor de rechten en vrijheden van de betrokkene ten gevolge van de vernietiging, het verlies, de wijziging of de ongeoorloofde toegang tot verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.[224] Dergelijke maatregelen kunnen bijvoorbeeld bestaan uit het pseudonimiseren en versleutelen van persoonsgegevens en/of het regelmatig testen en evalueren van de effectiviteit van de maatregelen om ervoor te zorgen dat de gegevensverwerking veilig is.[225] Ten slotte moeten verwerkingsverantwoordelijken of verwerkers maatregelen treffen om ervoor te zorgen dat personen onder hun gezag, die toegang hebben tot persoonsgegevens, deze enkel en alleen in hun opdracht verwerken, tenzij zij daartoe Unierechtelijk of lidstaatrechtelijk zijn gehouden.[226]

4.2. Rechtmatigheid van de verwerking in de Algemene Verordening Gegevensbescherming

4.2.1. Alle persoonsgegevens

Zoals omschreven in '4.1.1.', vormt ook de rechtmatigheidsvereiste[227] een van de verwerkingsbeginselen in de AVG. Naast de algemene beginselen uitgewerkt in artikel 5 AVG, moet er

Union, 2018. P. 127.; European Union Agency for Fundamental Rights (FRA). "Fundamental rights and the interoperability of EU information systems: borders and security." (2017). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf. P. 29.; European Union Agency for Fundamental Rights (FRA). "Under watchful eyes: biometrics, EU IT systems and fundamental rights." (april 2018). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf. P. 81.

[221] Artikel 5 (1) e) jo. overweging 39 AVG

[222] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 129.

[223] Artikel 5 (1) f) jo. overweging 39 AVG

[224] Artikel 32 (2) AVG

[225] Artikel 32 (1) AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 131.

[226] Artikel 32 (4) AVG

[227] Artikel 5 (1) a) AVG

voor elke verwerking van persoonsgegevens een gerechtvaardigde verwerkingsgrond bestaan, zoals verder verduidelijkt in artikel 6 AVG. Voor het gebruik van smartphones en sociale mediaprofielen binnen verzoekprocedures OIB zijn de volgende rechtvaardigingsronden relevant[228]: toestemming van de betrokkene, een unie- of lidstaatrechtelijke verplichting en een taak van algemeen belang. Deze gronden worden hieronder uiteengezet en de toepasselijkheid ervan op artikel 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet wordt besproken.

4.2.1.1. Toestemming

Artikel 6 (1) a) van de AVG vermeldt de verwerkingsgrond van de toestemming. De betrokkenen moeten toestemming geven voor de verwerking van hun persoonsgegevens voor een of meer specifieke doeleinden. Hoewel de bewoordingen van artikel 48/6, §1, lid 4 van de Vreemdelingenwet geen expliciete toestemmingsvereiste vermelden, moet deze er volgens de parlementaire stukken wel uit worden afgeleid[229]. Het was dus wel degelijk de bedoeling van de wetgever om de toegang tot smartphones en sociale mediaprofielen afhankelijk te stellen van de toestemming hiertoe van de betrokkene.[230] Het bleek uit de parlementaire stukken echter allesbehalve vanzelfsprekend dat het hier wel degelijk om een 'toestemming' gaat zoals deze in de AVG wordt gedefinieerd.[231] Volgens artikel 7 en 4 (11) en overweging 42 en 43 van de AVG moet het gaan om een vrije, geïnformeerde, herroepbare, specifieke, ondubbelzinnige, actieve en aantoonbare toestemming.

Om van een vrije/autonome toestemming te kunnen spreken, moet de betrokkene volgens de Werkgroep Gegevensbescherming Artikel 29[232] een werkelijke keuze en controle hebben over de verwerking van diens persoonsgegevens.[233] De toestemming kan *in casu* echter niet worden losgekoppeld van de plicht tot medewerking van de verzoeker OIB.[234] De weigering van de verzoeker om zijn medewerking te verlenen zal namelijk worden opgevat als een aanwijzing die de verdere beoordeling van het verzoek OIB negatief kan beïnvloeden.[235] In deze omstandigheden kan niet worden aangenomen dat de toestemming volledig vrij wordt verleend.[236] Daarnaast bevindt de betrokkene zich in een afhankelijke

[228] De andere (niet-relevante) verwerkingsgronden zijn: gegevensverwerking uit noodzaak om een contract aan te gaan; gegevensverwerking uit noodzaak om de vitale belangen van de betrokkene of een ander persoon te beschermen; gegevensverwerking uit noodzaak voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde partij, indien zij niet tenietgedaan worden door de belangen en rechten van de betrokkene (niet voor de verwerking door overheidsinstanties in kader van de uitoefening van hun taken)

[229] Verslag 2 bij de wetswijziging P. 4 en 9.; Memorie van toelichting bij de wetswijziging P. 37.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 88.

[230] Memorie van toelichting bij de wetswijziging P. 37.

[231] Verslag 1 bij de wetswijziging P. 169.; Amendement (HELLINGS en DE VRIENDT) op wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, gedaan op 17 oktober 2017, Parl.St. Kamer 2016-17, nr. 2548/005. P. 3. Hierna: Amendement 1 bij de wetswijziging; Amendementen (PAS, KIR, DE CONINCK, PONCELET en MAINGAIN) op wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen en van de wet van 12 januari 2007 betreffende de opvang van asielzoekers en van bepaalde andere categorieën van vreemdelingen, gedaan op 9 november 2017, Parl.St. Kamer 2016-17, nr. 2548/011. P. 14. Hierna: Amendement 2 bij de wetswijziging

[232] Hierna: WGA29

[233] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6.

[234] Advies CBPL P. 8.

[235] Artikel 48/6, §1, lid 4 Vreemdelingenwet

[236] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6.; Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 529.

positie tegenover het CGVS waardoor de mogelijkheid tot toestemming geven snel als plicht of gebod zal worden ervaren.[237] Waar er een duidelijk (machts)onevenwicht bestaat tussen de verwerker en de betrokkene, is de toestemming dan ook ongeldig.[238] De WGA29 en overweging 43 van de AVG stellen hieromtrent zelfs dat het onwaarschijnlijk is dat overheidsinstanties zich kunnen beroepen op de verwerkingsgrond 'toestemming' voor verwerkingen, omdat er in dat geval vaak een wanverhouding bestaat in de relatie tussen de betrokkene en de verwerkingsverantwoordelijke.[239]

Een geïnformeerde toestemming vereist volgens de WGA29 kennis en begrip van de feiten en implicaties van de toestemming tot het verwerken.[240] Algemeen gezien worden de volgende informatieonderdelen als noodzakelijk beschouwd om van een geïnformeerde toestemming te kunnen spreken[241]: de identiteit van de verwerkingsverantwoordelijke, het doel van de verwerkingen, de gevolgen van de toestemming, de aard van de gebruikte gegevens, het recht om de toestemming in te trekken (en de andere rechten van de betrokkene) en de entiteiten aan wie de gegevens mogelijks worden doorgegeven. Indien dit niet het geval is, is de gegeven toestemming door de betrokkene slechts schijn en kan deze niet als verwerkingsgrond dienen.[242] Deze informatie moet in heldere taal, op toegankelijke wijze[243] en in aangepaste vorm aan het doelpubliek ervan worden overgebracht.[244] Bijzondere aandacht is dus bijvoorbeeld geboden bij het informeren van anderstaligen (wat voor verzoekers OIB meestal het

[237] Advies CBPL P. 8.

[238] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6.; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 144.; "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers". www.privacyinternational.org. Privacy International. https://privacyinternational.org/node/2776.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 24.; Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.

[239] Overweging 43 van de AVG; Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6.

[240] Werkgroep gegevensbescherming artikel 29. "Working Document on the processing of personal data relating to health in electronic health records (HER) WP 131." (2007). https://www.garanteprivacy.it/documents/10160/10704/1386451. P. 9.

[241] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 15.; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 146.

[242] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 14.

[243] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 146.

[244] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 16.

geval zal zijn) of van kinderen[245] (en niet-begeleide minderjarigen in het bijzonder[246]). Het blijkt voor verzoekers OIB (en voor migranten in het algemeen) echter vaak een obstakel om de wettelijke draagwijdte van privacy en gegevensbescherming te bevatten[247] in de communicatie met overheidsambtenaren. Dit wordt onder andere gelinkt aan een gebrek aan begrip van de specifieke juridische terminologie, culturele verschillen, eventuele kennishiaten en ongelijke machtsverhoudingen binnen de situatie van verzoeken OIB, wat het voldoen aan de geïnformeerde toestemmingsvereiste substantieel bemoeilijkt.[248]

Overweging 42 van de AVG verduidelijkt de vereiste van een 'herroepbare toestemming'. De toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene die toestemming niet kan weigeren of intrekken zonder nadelige gevolgen, wat ook door de WGA29 wordt benadrukt. Daarnaast stelt artikel 7, lid 3 van de AVG dat de verwerkingsverantwoordelijke ervoor moet zorgen dat het intrekken van een toestemming door de betrokkene even eenvoudig moet zijn als het geven ervan.[249] Aangezien de wetswijziging letterlijk stelt dat het weigeren toestemming te geven een negatieve aanwijzing is voor de beoordeling van het verzoek OIB, is de vereiste van de herroepbaarheid van de toestemming *in casu* dus niet vervuld.

Ten slotte moet de toestemming specifiek, ondubbelzinnig, actief en aantoonbaar zijn. Deze voorwaarden zijn erop gericht een zekere transparantie en controle voor de betrokkene met betrekking tot de verwerking van diens persoonsgegevens te creëren.[250] Om een specifieke toestemming mogelijk te maken, moet de verwerkingsverantwoordelijke de betrokkene dus vooraf duidelijk informeren over het welbepaald, uitdrukkelijk omschreven doel voor de beoogde verwerkingsactiviteit. Met de ondubbelzinnigheidsvereiste wordt bedoeld dat de toestemming steeds aan de hand van een actieve handeling of verklaring moet worden verleend.[251] Overweging 32 AVG verduidelijkt deze vereiste door te stellen dat eraan kan worden voldaan door middel van bijvoorbeeld een schriftelijke of een (opgenomen) mondelinge verklaring.[252] Uit deze laatste vereiste vloeien ook de voorwaarden van een 'actieve' en 'aantoonbare' toestemming voort.

Artikel 48/6, §1, lid 4 van de Vreemdelingenwet voorziet op geen enkele wijze een 'toestemming' in de zin van de AVG (een vrije, geïnformeerde, herroepbare, specifieke, ondubbelzinnige, actieve en aantoonbare toestemming). In artikel 57/7, §2 van de Vreemdelingenwet ontbreekt de toestemmingsvereiste volledig. Bovendien moet worden opgemerkt dat het bij het screenen van sociale mediaprofielen en smartphones onvermijdelijk is dat ook persoonsgegevens worden verwerkt van

[245] Overweging 39 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 149.; Walters, R., Trakman, L. en Zeller, B. Data Protection Law: A Comparative Analysis of Asia-pacific and European Approaches. Springer Singapore, 2019. P. 68.; Werkgroep gegevensbescherming artikel 29. "Advies 5/2009 over online sociale netwerken 01189/09/NL WP 163." (2009). https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/01.02.04.02.01-wp163_nl.pdf. P. 13.

[246] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 189.

[247] European Union Agency for Fundamental Rights (FRA). "Under watchful eyes: biometrics, EU IT systems and fundamental rights." (april 2018). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf. P. 9.

[248] Latonero, M., Hiatt, K., Napolitano, A., Clericetti, G. en Penagos, M. "Digital Identity in the Migration & Refugee Context: Italy case study." Data & Society (2019). https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf. P. 31.

[249] Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6, 12 en 25.

[250] Ibid. P. 13.

[251] Ibid. P. 18.

[252] Overweging 32 AVG

andere personen dan de verzoekers OIB zelf, met wie zij (al dan niet gewenst) in contact staan.[253] Hierdoor worden hoe dan ook persoonsgegevens verwerkt van personen die hier geen toestemming toe hebben gegeven.[254]

4.2.1.2. Unie- of lidstaatrechtelijke wettelijke verplichting

In artikel 6 (1) c) van de AVG wordt de verwerkingsgrond van de wettelijke verplichting uiteengezet. Als de gegevensverwerking aan de verwerker/verwerkingsverantwoordelijke wordt opgelegd op grond van een Unie- of lidstaatrechtelijke bepaling, geldt dit als rechtvaardiging. In artikel 6 (3) en overwegingen 41 en 45 van de AVG wordt verduidelijkt dat het moet gaan om een rechtsgrond, die op de verwerkingsverantwoordelijke van toepassing is en die duidelijk, nauwkeurig en voorzienbaar is geformuleerd. Bijgevolg moet de wetsbepaling op voldoende specifieke wijze verwijzen naar het doel van de verwerking.[255] Daarnaast moet de wetsbepaling beantwoorden aan een doelstelling van algemeen belang (zie '4.2.1.3.') en evenredig zijn met het nagestreefde gerechtvaardigde doel (zie '5.3.2.2.').[256]

De besproken artikelen worden inderdaad duidelijk in de Belgische wet geformuleerd. De formulering van de artikelen stemt echter niet overeen met de vereiste van een unie- of lidstaatrechtelijke wettelijke verplichting. Beide artikelen laten de vrije keuze voor het CGVS om de besproken persoonsgegevens al dan niet te gebruiken en te verwerken. Artikel 48/6, §1, lid 4 van de Vreemdelingenwet stelt: 'indien […] kunnen zij de verzoeker uitnodigen om deze elementen onverwijld voor te leggen' en artikel 57/7, §2 van de Vreemdelingenwet stelt: 'kan informatie van alle aard die via elektronische weg is verstuurd of ontvangen […] raadplegen en gebruiken'. De wet voorziet dus in de optie voor het CGVS om toegang tot digitale persoonsgegevens te vragen aan de betrokkene, maar legt hiertoe geenszins de verplichting op.[257] De WGA29 stelt in een van haar adviezen[258] letterlijk dat, om te voldoen aan de voorwaarde van de wettelijke verplichting, de verwerkingsverantwoordelijke niet de keuze mag hebben om al dan niet aan de verplichting te voldoen. Daarnaast mag de verwerkingsverantwoordelijke geen te grote beoordelingsmarge hebben met betrekking tot de wijze waarop aan de wettelijke verplichting moet voldaan worden.

Als voorbeelden van een dergelijke wettelijke verplichting worden gegeven: de voor advocaten verplichte vermeldingen in procedurestukken, de voor advocaten of financiële instellingen verplichte mededeling van informatie en verdachte transacties aan de Cel voor Financiële Informatieverwerking

[253] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 6 en 14.
Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.; EHRM, Szabo & Vissy t. Hongarije, nr. 37138/14, 12 januari 2016. §89.
[254] RvV nr. 175 324 van 26 september 2016. § 1, 3.2.2. en 3.2.3.
[255] Werkgroep gegevensbescherming artikel 29. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. P. 22.
[256] Artikel 6 (3) jo. overweging 45 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 152.
[257] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 196.
[258] Werkgroep gegevensbescherming artikel 29. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. P. 19.
Hier dient te worden opgemerkt dat dit advies werd geschreven ten tijde van de Richtlijn 95/46/EC (de voorganger van de AVG). Artikel 7 (c) van deze Richtlijn bevatte echter dezelfde verwerkingsgrond voor wettelijke verplichtingen als in de huidige AVG.

belast met de bestrijding van het witwassen van geld, de voor de werkgever verplichte melding van de salarisgegevens van hun werknemers aan de sociale zekerheids-[259] of belastingdienst[260], de voor lokale autoriteiten verplichte verzameling van voertuiggegevens met het oog op de behandeling van parkeersancties[261], gegevensverwerking door belasting- of douaneautoriteiten, financiële onderzoeksdiensten, onafhankelijke bestuurlijke autoriteiten of financiële marktautoriteiten die belast zijn met de regulering van en het toezicht op de effectenmarkten[262] …

Uit deze vaststellingen volgt dat de verwerkingsgrond van de unie- of lidstaatrechtelijke wettelijke verplichting voor artikel 48/6, §1, lid 4 en artikel 57/7, §2 van de Vreemdelingenwet niet van toepassing is.

4.2.1.3. Taak van algemeen belang

Artikel 6 (1) e) AVG rechtvaardigt de gegevensverwerking voor persoonsgegevens als deze noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Te benadrukken valt, dat de gegevensverwerking dus effectief noodzakelijk moet zijn voor de uitoefening van het openbaar gezag.[263] De verwerkingsgrond van 'de taak van algemeen belang', beslaat een zeer ruim toepassingsgebied, waardoor een strikte interpretatie en een duidelijke 'geval per geval' beoordeling moet plaatsvinden van het algemeen belang in kwestie en de officiële autoriteit die de verwerking rechtvaardigt.[264] Ook moet de gegevensverwerking die wordt gerechtvaardigd door de verwerkingsgrond van 'de taak van algemeen belang' een grondslag hebben in het unie- of lidstaatrechtelijk recht, dat aan dezelfde voorwaarden moet voldoen als deze uiteengezet in '4.2.1.2.'.[265]

Het UNHCR erkent dergelijke algemene belangen van staten in het kader van verzoeken OIB, zoals het identificeren van verzoekers op hun territorium, met inbegrip van personen die mogelijks handelingen hebben gesteld die hen van het statuut van internationale bescherming uitsluiten of die een bedreiging voor de nationale veiligheid kunnen betekenen. Daarnaast erkent het UNHCR het belang van staten om ervoor te zorgen dat beoordelingen van verzoeken OIB gebaseerd zijn op de meest volledige en nauwkeurige informatie die beschikbaar is.[266] Ook de Europese Toezichthouder voor Gegevensbescherming sprak zich hierover uit in een advies over de gegevensbeschermingsimplicaties

[259] "When can personal data be processed?" www.ec.europa.eu. Europese Commissie. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en.
[260] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 151.
[261] Werkgroep gegevensbescherming artikel 29. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. P. 19.; Gegevensbeschermingsautoriteit (GBA). "Overzicht van de begrippen verwerkingsverantwoordelijke/verwerker in het licht van de Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens (AVG) en enkele specifieke toepassingen voor vrije beroepen zoals advocaten." Gegevensbeschermingsautoriteit. https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Begrippen_VW_OA.pdf. P. 6.
[262] overweging 31 van de AVG
[263] Werkgroep gegevensbescherming artikel 29. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. P. 21-22.
[264] Ibid. P. 22.
[265] Artikel 6 (3) jo. overwegingen 41 en 45 AVG
[266] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 1.

van het creëren van een European Union Agency for Asylum in het kader van het Common European Asylum System (CEAS). De 'taak van algemeen belang' werd voor de gegevensverwerking door het European Union Agency for Asylum van de persoonsgegevens van verzoekers OIB als voldoende verwerkingsgrond beschouwd.[267] Het feit dat bovenvermelde instanties op algemene wijze erkennen dat voor bepaalde verwerkingsactiviteiten in het kader van verzoeken OIB een 'taak van algemeen belang' een voldoende verwerkingsgrond grond is, wil echter niet zeggen dat dit ook voor de specifieke doorzoekingen van sociale mediaprofielen en smartphones door het CGVS het geval is.

4.2.2. Bijzondere categorieën van persoonsgegevens: gevoelige gegevens

In de AVG wordt een groep persoonsgegevens geïdentificeerd waarvoor bijkomende vereisten gelden: de bijzondere categorieën van persoonsgegevens (de 'gevoelige gegevens'). Deze gegevens zijn door hun aard bijzonder gevoelig en verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan inhouden voor de grondrechten en de fundamentele vrijheden.[268] Het gaat om persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische informatie, biometrische informatie, informatie over gezondheid en informatie over seksueel gedrag of seksuele gerichtheid blijken. [269]

Het CGVS bevestigt op zijn officiële website zelf dat (onder andere) de volgende persoonsgegevens door het Commissariaat worden verwerkt: raciale of etnische gegevens, politieke opvattingen/lidmaatschap van een vakvereniging, filosofische en religieuze overtuigingen, gegevens met betrekking tot het seksueel gedrag of seksuele gerichtheid en gegevens betreffende de gezondheid.[270] Alle gegevens uit deze opsomming zijn te categoriseren als 'gevoelige gegevens'.

Enerzijds zijn gevoelige gegevens veelvuldig op sociale mediaprofielen en smartphones te vinden[271]. Op sociale mediaprofielen gaat het om gegevens als naam, locatie, leeftijd, opleiding en/of professionele loopbaan, interesses, politieke en religieuze voorkeuren, burgerlijke staat, seksuele voorkeur, gedeelde teksten, foto's, video's … [272] Smartphones vormen een persoonlijke databank, die gegevens kan bevatten

---

[267] European Data Protection Supervisor (EDPS). "EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations) nr. 07/2016." (september 2016). https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf.. P. 17.

[268] Overweging 51 AVG

[269] Artikel 9 (1) AVG

[270] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[271] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 2.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 9.; European Data Protection Supervisor (EDPS). "Formal consultation on EASO's social media monitoring reports (case 2018-1083)." (2019). https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf. P. 7.; "Gemeenschappelijke kenmerken van socialenetwerkdiensten". www.gegevensbeschermingsautoritieit.be. Gegevensbeschermingsautoriteit. https://www.gegevensbeschermingsautoriteit.be/gemeenschappelijke-kenmerken-van-socialenetwerkdiensten.; Dekker, R., Vonk, H., Klaver, J. en Engbersen, G. "Syrische asielmigranten in Nederland en het gebruik van sociale media bij migratiebesluitvorming." Erasmus Universiteit Rotterdam (juli 2016). https://www.wodc.nl/binaries/2682-volledige-tekst_tcm28-131598.pdf. P. 2.

[272] Lewis, B. K. "Social media and strategic communication: Attitudes and perceptions among college students." Public Relations Journal vol. 4, Isuue 3 (2009). https://shareok.org/bitstream/handle/11244/7479/School%20of%20Teaching%20and%20Curriculum%20Leadership_191.pdf?sequence=1&isAllowed=y. P. 29.; Dekker, R., Vonk, H., Klaver, J. en Engbersen, G. "Syrische asielmigranten in Nederland en

die jaren terug gaan en licht kunnen werpen op bijna elk aspect van het leven van een persoon[273], zoals identificatiegegevens, account- en betalingsgegevens, geschiedenis van zoekmachines, verblijfsgegevens, beeldmateriaal, documenten …[274] Beide mediums (sociale mediaprofielen en smartphones) bieden ook de mogelijkheid om dankzij communicatietools rechtstreeks en afgesloten met anderen te converseren.[275] Zo bevatten ze persoonlijke communicatie van de gebruiker, zoals berichten naar familieleden, contactgegevens (waaronder bijvoorbeeld informatie over en naar advocaten), e-mailaccounts …[276] Anderzijds is het vaak net die informatie, die pertinent is voor het beoordelen van een verzoek OIB en van de 'gegronde vrees voor vervolging'[277] (voor de erkenning van de vluchtelingenstatus) of van het 'reëel risico op ernstige schade'[278] (voor de toekenning van de subsidiaire beschermingsstatus).

De verwerking van gevoelige gegevens is principieel verboden[279], hoewel artikel 9 (2) AVG een aantal uitzonderingen op deze regel invoert. Naast een algemene verwerkingsgrond[280], die bij elke verwerking van persoonsgegevens aanwezig moet zijn[281], moet de verwerking van gevoelige gegevens onder één van de uitzonderingen opgenomen in artikel 9 (2) AVG vallen om te mogen plaatsvinden. Hieronder worden de voor de besproken artikelen in de Vreemdelingenwet relevante uitzonderingen aangehaald[282]: de uitdrukkelijke toestemming van de betrokkene, de uitdrukkelijke openbaarmaking van de persoonsgegevens door de betrokkene en het zwaarwegend algemeen belang. Naast de bijzondere regels die van toepassing zijn op verwerkingen van gevoelige gegevens, dienen ook de algemene beginselen en andere regels van de AVG steeds in acht te worden genomen.[283]

---

het gebruik van sociale media bij migratiebesluitvorming." Erasmus Universiteit Rotterdam (juli 2016). https://www.wodc.nl/binaries/2682-volledige-tekst_tcm28-131598.pdf. P. 2.; "Gemeenschappelijke kenmerken van socialenetwerkdiensten". www.gegevensbeschermingsautoriteit.be. Gegevensbeschermingsautoriteit. https://www.gegevensbeschermingsautoriteit.be/gemeenschappelijke-kenmerken-van-socialenetwerkdiensten.

[273] Supreme Court of the United States (SCOTUS), Riley t. Californië, nr. 13–132, 25 juni 2014. https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf. P. 2-3.

[274] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 22.

[275] "Gemeenschappelijke kenmerken van socialenetwerkdiensten". www.gegevensbeschermingsautoriteit.be. Gegevensbeschermingsautoriteit. https://www.gegevensbeschermingsautoriteit.be/gemeenschappelijke-kenmerken-van-socialenetwerkdiensten.; International Committee of the Red Cross (ICRC) en Privacy International. "The Humanitarian Metadata Problem: Doing no harm in the digital era." (oktober 2018). https://reliefweb.int/sites/reliefweb.int/files/resources/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf. P. 43.

[276] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 22.

[277] Artikel 48/3 Vreemdelingenwet jo. artikel 1 VN Vluchtelingenverdrag

[278] Artikel 48/4 Vreemdelingenwet

[279] Artikel 9 (1) AVG

[280] Artikel 6 AVG

[281] Overweging 51 AVG

[282] De andere (niet-relevante) uitzonderingen zijn: gegevensverwerking door een organisatie zonder winstoogmerk met politieke, levensbeschouwelijke, godsdienstige of vakbondsdoeleinden en alleen betreffende haar (vroegere) leden of op personen die regelmatig contact met haar opnemen voor zulke doeleinden; gegevensverwerking noodzakelijk op gebied van het arbeidsrecht en socialezekerheidsrecht; gegevensverwerking noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, de beoordeling van de arbeidsgeschiktheid van de werknemer of medische diagnoses; gegevensverwerking noodzakelijk om redenen van algemeen belang op het gebied van volksgezondheid; gegevensverwerking noodzakelijk is om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen; gegevensverwerking noodzakelijk om rechtsvorderingen vast te stellen, uit te voeren of te verdedigen of wanneer gerechtelijke instanties handelen in rechterlijke hoedanigheid; gegevensverwerking noodzakelijk voor archivering in het algemeen belang, voor wetenschappelijk of historisch onderzoek of statistische doeleinden

[283] Overweging 51 AVG

4.2.2.1. Uitdrukkelijke toestemming

Een eerste relevante uitzondering betreft het geval waarin de betrokkenen uitdrukkelijke toestemming hebben gegeven tot de verwerking van hun gevoelige persoonsgegevens.[284] Voor de invulling van deze uitzondering wordt verwezen naar artikel 7 en 4 (11) AVG en naar de uiteenzetting onder '4.2.1.1.'.

4.2.2.2. Uitdrukkelijke openbaarmaking

Ook kan het gaan om gegevens die uitdrukkelijk door de betrokkene openbaar zijn gemaakt.[285] Hoewel het concept 'uitdrukkelijke openbaarmaking' niet in de AVG wordt gedefinieerd, moet het strikt worden geïnterpreteerd, aangezien het een uitzondering vormt op het verbod op de verwerking van gevoelige gegevens. De gevoelige gegevens moeten dus door de betrokkene opzettelijk openbaar zijn gemaakt om onder deze uitzondering te vallen.[286] Deze uitzondering is van toepassing op gegevens op sociale mediaprofielen of andere online fora die door de betrokkene bewust voor iedereen publiek toegankelijk zijn gemaakt (artikel 57/7, §2 en artikel 48/6, §1, lid 4 van de Vreemdelingenwet). Het geldt echter niet voor de private of afgeschermde informatie op sociale mediaprofielen of smartphones (artikel 48/6, §1, lid 4 van de Vreemdelingenwet).

4.2.2.3. Zwaarwegend algemeen belang

Ten derde wordt in artikel 9 (2) g) AVG een uitzondering gemaakt voor de verwerking van gevoelige gegevens met redenen van zwaarwegend algemeen belang.[287] De invulling van het algemeen belang werd hierboven reeds toegelicht onder '4.2.1.3.'. Belangrijk is dat de lat om van 'redenen van zwaarwegend algemeen belang' te kunnen spreken bij de uitzondering voor de verwerking van gevoelige gegevens hoger ligt dan bij de algemene verwerkingsrond voor alle persoonsgegevens. Het volstaat dus niet om louter vast te stellen dat er sprake is van een taak van algemeen belang.

Daarenboven veresit artikel 9 (2) g) AVG dat de verwerking voor een zwaarwegend algemeen belang wettelijk verankerd is, waarbij de proportionaliteit met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. Deze laatste voorwaarden worden verder onder '4.3.' behandeld.

4.2.3. Overzicht van de verwerkingsgronden voor alle persoonsgegevens en de uitzonderingen voor gevoelige gegevens

Uit bovenstaande bespreking van de relevante algemene verwerkingsgronden en de uitzonderingen op het principieel verbod op verwerking van gevoelige gegevens, kunnen een aantal tussentijdse conclusies worden getrokken.

Wat de algemene verwerkingsronden betreft:

---

[284] Artikel 9 (2) a) AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 161.

[285] Artikel 9 (2) e) AVG

[286] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 162.

[287] Artikel 9 (2) g) AVG

- Toestemming: Artikel 48/6, §1, lid 4 van de Vreemdelingenwet voldoet niet aan de voorwaarden voor toestemming in de AVG en artikel 57/7, §2 van de Vreemdelingenwet vereist geen toestemming.
- Wettelijke verplichting: Artikel 48/6, §1, lid 4 en artikel 57/7, §2 van de Vreemdelingenwet houden geen 'verplichting' voor het CGVS in.
- Taak van algemeen belang: Deze verwerkingsgrond is op artikel 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet van toepassing.

ALLE PERSOONSGEGEVENS	ARTIKEL 48/6, §1, LID 4 VW.	ARTIKEL 57/7, §2 VW.
PRIVATE GEGEVENS	o ~~toestemming~~ o ~~wettelijke verplichting~~ o taak van algemeen belang	
PUBLIEKE GEGEVENS	o ~~toestemming~~ o ~~wettelijke verplichting~~ o taak van algemeen belang	o ~~toestemming~~ o ~~wettelijke verplichting~~ o taak van algemeen belang

Naast bovenstaande verwerkingsgronden voor alle persoonsgegevens, is voor de verwerking van gevoelige gegevens nog vereist dat deze onder een van de uitzonderingen op het principieel verbod op verwerking van gevoelige gegevens valt:

- Uitdrukkelijke toestemming: Artikel 48/6, §1, lid 4 van de Vreemdelingenwet voldoet niet aan de voorwaarden voor (uitdrukkelijke) toestemming in de AVG en artikel 57/7, §2 van de Vreemdelingenwet vereist geen (uitdrukkelijke) toestemming.
- Uitdrukkelijke openbaarmaking: Deze uitzondering is op artikel 57/7, §2 en artikel 48/6, §1, lid 4 van de Vreemdelingenwet van toepassing, voor de uitdrukkelijk publiek gemaakte gegevens op sociale mediaprofielen of andere online fora.
- Zwaarwegend algemeen belang: Deze uitzondering is op artikel 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet van toepassing. Daarnaast moet worden voldaan aan de andere voorwaarden in artikel 9 (2) g) AVG[288].

GEVOELIGE GEGEVENS	ARTIKEL 48/6, §1, VIERDE LID	ARTIKEL 57/7, §2
PRIVATE GEGEVENS	o ~~uitdrukkelijke toestemming~~ o ~~uitdrukkelijke openbaarmaking~~ o zwaarwegend algemeen belang	
PUBLIEKE GEGEVENS	o ~~uitdrukkelijke toestemming~~ o uitdrukkelijke openbaarmaking o zwaarwegend algemeen belang	o ~~uitdrukkelijke toestemming~~ o uitdrukkelijke openbaarmaking o zwaarwegend algemeen belang

Het niet-gecategoriseerde karakter van de digitale persoonsgegevens op sociale mediaprofielen en smartphones vormt een cruciaal gegeven voor de beoordeling van de rechtmatigheid van de verwerking ervan. De grote massa aan informatie en de quasi-onmogelijkheid om preventief het raadplegen van bepaalde gevoelige gegevens uit te sluiten, zorgt ervoor dat de grens in de AVG tussen 'gewone persoonsgegevens' en 'gevoelige persoonsgegevens' *in casu* niet kan worden aangehouden. Alle

[288] Deze worden hieronder behandeld in '4.5.'.

gegevens op smartphones en sociale mediaprofielen moeten bijgevolg worden onderworpen aan de strengere vereisten voor de verwerking van gevoelige gegevens. Enkel zo kan worden gegarandeerd dat de rechtmatigheid van de verwerking van bijzondere categorieën van persoonsgegevens correct wordt getoetst. Voor de verwerking van publieke persoonsgegevens moeten dus de uitzondering van 'uitdrukkelijke openbaarmaking' en de verwerkingsgrond van 'taak van algemeen belang' worden gehanteerd. Private persoonsgegevens moeten aan de uitzondering van 'het zwaarwegend algemeen belang' worden getoetst.

4.3. Beperkingen op het recht op gegevensbescherming en de daaraan verbonden voorwaarden

Indien voor een bepaalde gegevensverwerking niet aan de voorwaarden in de AVG is voldaan (de beginselen, verwerkingsgronden en uitzonderingsgronden), maakt deze verwerking een beperking op het recht op gegevensbescherming uit. Sterker nog, in principe vormt elke gegevensverwerking een beperking van het recht op gegevensbescherming, ongeacht of die beperking gerechtvaardigd kan zijn.[289] Het HvJ oordeelde zelfs in de overgrote meerderheid van de zaken die betrekking hebben op gegevensverwerkingen, vastgelegd in de wet, dat een verwerking zowel het recht op gegevensbescherming als het recht op privacy beperkt. Ook stelde het Hof reeds dat het voor de vaststelling van een dergelijke beperking irrelevant is of het om gevoelige persoonsgegevens gaat of dat de betrokkenen ook effectief hinder hebben ondervonden.[290] De bescherming van persoonsgegevens is namelijk van fundamenteel belang voor de uitoefening van het recht op privacy van een persoon.[291] Er kan dus worden aangenomen dat het doorzoeken van smartphones en sociale mediaprofielen van verzoekers OIB een inperking vormt op het recht op gegevensbescherming en op privacy. Noch het recht op gegevensbescherming, noch het recht op privacy zijn absolute rechten, waardoor deze beperkingen onder bepaalde voorwaarden kunnen gerechtvaardigd worden.[292]

Zoals uiteengezet in '3.1.', zijn zowel artikel 8 EU-Handvest als artikel 8 EVRM relevant voor het recht op gegevensbescherming. Hieruit vloeit voort dat, in verband met de voorwaarden voor beperkingen op het recht op gegevensbescherming en het recht op privacy, zowel moet rekening gehouden worden met artikel 52 (1) en (3) EU-Handvest, als met artikel 8 (2) EVRM. De beperkingsclausule in artikel 8 EVRM moet strikt geïnterpreteerd worden[293] en iedere beperking moet overtuigend vastgesteld worden[294]. Een

[289] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 7.
[290] HvJ, C-92/09 en C-93/09, Volker und Markus Schecke, 2010. § 55.; HvJ, C-468/10 en C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD), v Administración del Estado, 2011. § 41.; HvJ, C-465/00, C-138/01 en C-139/01, Rechnungshof et al v. Österreichischer Rundfunk, 2003. §75.; HvJ, C-293/12 en C-594/12, Digital Rights Ireland Ltd t. Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a., 2014. § 33.; European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 7.
[291] EHRM, S en Marper t. VK, nr.30562/04 en 30566/04, 4 december 2008. § 103.
[292] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 35-36.; European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 4.
[293] EHRM, Silver e.a. t. VK, nr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 en 7136/75, 25 maart 1983. §97.; EHRM, Gawęda t. Polen, nr. 26229/95, 14 maart 2002. § 32.
[294] EHRM, Otto-Preminger-Institut t. Oostenrijk, nr. 13470/87, 20 september 1994. § 50.; EHRM, Dupuis e.a. t. Frankrijk, nr. 1914/02, 7 juni 2007. § 36.

inperking van de uitoefening van deze rechten is volgens deze beperkingsclausules enkel toegestaan voor zover deze[295] (cumulatief):

- wettelijk is voorzien
- een gerechtvaardigd doel nastreeft
    - in het EVRM limitatief uitgewerkt als: in het belang zijn van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen
    - in het EU-Handvest ruimer[296] uitgewerkt als: beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen
- noodzakelijk (en proportioneel) is (in een democratische samenleving)
- de wezenlijke inhoud van de ingeperkte rechten en vrijheden eerbiedigt

Wat de wettelijkheidsvereiste betreft, wordt het doorzoeken van smartphones en sociale mediaprofielen van verzoekers OIB via de besproken wetswijziging ingeschreven in de Vreemdelingenwet en is de praktijk dus voorzien van een (toegankelijke en voorzienbare)[297] wettelijke basis. Het feit dat de maatregel uitdrukkelijk in een wetsbepaling is opgenomen, is echter niet voldoende om de rechtvaardiging ervan te waarborgen.[298]

Tevens moet de maatregel die het recht op privacy en gegevensbescherming inperkt genomen zijn om een gerechtvaardigd doel na te streven. Het EVRM bevat hieromtrent een limitatieve opsomming, terwijl het EU-Handvest ‘de door de Unie erkende doelstellingen van algemeen belang of de bescherming van rechten en vrijheden van anderen’ vermeldt. Specifiek in het kader van de AVG, wordt het criterium van ‘een gerechtvaardigd doel’ in artikel 23 (1) AVG verduidelijkt.[299] Gerechtvaardigde doelen die daarin worden vermeld zijn onder andere: nationale veiligheid en defensie, misdaadpreventie, de bescherming van belangrijke economische en financiële belangen van de EU of de lidstaten, volksgezondheid en sociale zekerheid … In het kader van het doorzoeken van digitale communicatie

[295] Artikel 8 (2) EVRM en artikel 52 (1) EU-Handvest; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 35-36.
[296] Kokott, J. en Sobotta, C. “The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR.” International Data Privacy Law (2013). https://doi.org/10.1093/idpl/ipt017. P. 224.
[297] Haeck, Y. en Burbano Herrera, C. Procederen voor het Europees Hof voor de Rechten van de Mens (2e editie). Antwerpen: Intersentia, 2011. P. 54.
[298] Jumbert, M. G., Bellanova, R. en Gellert, R. “Smart Phones for Refugees: Tools for Survival, or Surveillance?” The Peace Research Institute Oslo (Prio) (2018).
https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P.4.
[299] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 49.; European Data Protection Supervisor (EDPS). “Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.” (april 2017). P. 10.

door overheidsinstanties, moet dit gerechtvaardigd doel overeenstemmen met een juridische doelstelling van zwaarwegend belang.[300]

De noodzakelijkheid van de maatregel (in een democratische samenleving) impliceert volgens het EHRM dat de inmenging overeenkomt met een 'dringende maatschappelijke behoefte'.[301] Het aan te pakken probleem moet dus niet alleen reëel, aanwezig of dreigend zijn, maar ook problematisch voor het functioneren van de samenleving.[302] Bij de beoordeling of een maatregel noodzakelijk is om in een dringende maatschappelijke behoefte te voorzien, onderzoekt het EHRM de relevantie en geschiktheid ervan in verhouding tot het nagestreefde doel.[303] In het licht van het EU-Handvest, is een beperking pas noodzakelijk als het nagestreefde gerechtvaardigde doel niet kan worden bereikt met minder ingrijpende maatregelen.[304] Voor het doorzoeken van digitale communicatie door overheidsinstanties in het bijzonder, mogen enkel de maatregelen worden gehanteerd die strikt en aantoonbaar noodzakelijk zijn om het vooropgestelde legitiem doel te bereiken.[305]

Met betrekking tot de proportionaliteit van de maatregel (in een democratische samenleving), is vereist dat een inperking op het recht niet verregaander is dan nodig om het nagestreefde gerechtvaardigd doel te bereiken. Belangrijke factoren waarmee rekening moet worden gehouden bij het uitvoeren van deze evenredigheidstoets zijn de omvang van de inperking (vb. het aantal betrokken personen) en de waarborgen die zijn ingebouwd om de impact ervan te beperken of de schadelijke gevolgen voor de rechten van personen te beperken.[306] Met andere woorden, de voordelen die voortvloeien uit de inperking van het fundamenteel recht moeten opwegen tegen de nadelen die deze inperking met zich meebrengt voor de uitoefening van het recht door de betrokkene.[307]

Ten slotte moet bij de inperking van een fundamenteel recht de wezenlijke inhoud ervan geëerbiedigd blijven. De inperking mag volgens het HvJ niet te beschouwen zijn als 'een onevenredige en onduldbare ingreep, waardoor de gewaarborgde rechten in hun kern worden aangetast'.[308] Dit laatste betekent dat inperkingen die zo ingrijpend zijn dat ze de kern of basisinhoud van het fundamenteel recht ontnemen[309],

[300] Necessary & Proportionate. "International Principles on the Application of Human Rights to Communications Surveillance." Necessary & Proportionate (mei 2014). https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. P. 7.
[301] EHRM, Leander t. Zweden, nr. 9248/81, 26 maart 1987. §58.
[302] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 15
[303] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 40.
[304] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 46
[305] Necessary & Proportionate. "International Principles on the Application of Human Rights to Communications Surveillance." Necessary & Proportionate (mei 2014). https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. P. 7.
[306] Werkgroep gegevensbescherming artikel 29. "Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 536/14/EN WP 211." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. P. 9-11.
[307] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 5.
[308] HvJ, 5/88, Wachauf, 1989. § 18.
[309] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 4.; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 44.

waardoor het individu het recht niet kan uitoefenen[310], niet te rechtvaardigen zijn. Wat het EVRM betreft, ontbreekt het begrip 'essentie', 'kern' of 'basisinhoud' van de fundamentele rechten en vrijheden in de tekst van het Verdrag, maar komt het in de rechtspraak van het EHRM regelmatig voor. Artikel 52 (1) van het EU-Handvest vond dan ook zijn oorsprong in de rechtspraak van het EHRM omtrent dit concept. De 'essentie' van de grondrechten in het EVRM vormt volgens deze rechtspraak de absolute grens, die door middel van inperkingen niet mag overschreden worden, wat ook kan worden afgeleid uit artikel 17 EVRM (Verbod van misbruik van recht).[311]

[310] European Data Protection Supervisor (EDPS). "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data." (december 2019). https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf. P.8.

[311] Sinds EHRM, Case relating to certain aspects of the laws on the use of languages in education in Belgium t. België, nr. 1474/62, 1677/62, 1691/62, 1769/63, 1994/63 en 2126/64, 23 juli 1968.; Van Drooghenbroeck, S. en Rizcallah, C. "The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?" German Law Journal 20 (2019). https://www.cambridge.org/core/services/aop-cambridge-core/content/view/594CA9F2A83DF4B52A1FB6B638339FB4/S2071832219000683a.pdf/echr_and_the_essence_of_fundamental_rights_searching_for_sugar_in_hot_milk.pdf. P. 904 en 907-908.

5. Toepassing van het theoretisch kader: geïdentificeerde pijnpunten

5.1. Verkeerde omzetting en onevenwichtige benadrukking van de medewerkingsplicht

5.1.1. Verkeerde omzetting van de medeweringsplicht

De elementen aan de hand waarvan de verzoeker de medewerkingsplicht moet vervullen worden in artikel 48/6, §1, lid 1 en 2 en artikel 51 van de Vreemdelingenwet omschreven. Het gaat onder meer om verklaringen en documenten/stukken met betrekking tot de identiteit, nationaliteit(en), leeftijd, achtergrond, land(en) en plaats(en) van eerder verblijf, eerdere verzoeken, reisroutes, reisdocumentatie en de redenen voor het verzoek OIB van de verzoeker en diens relevante familieleden.[312]

Opmerkelijk is het feit dat het hier om een niet-limitatieve opsomming gaat.[313] In tegenstelling tot wat in de Kwalificatierichtlijn[314] te lezen staat, kunnen volgens de Belgische vreemdelingenwet nog andere dan de hierboven opgesomde documenten/verklaringen worden vereist van de verzoeker OIB.[315] De relevantie hiervan zit in de gevolgen die worden verbonden aan het niet kunnen of willen aanvoeren van de elementen van de medewerkingsplicht. Dit vormt volgens de Vreemdelingenwet namelijk een negatieve indicatie ten aanzien van de gehele geloofwaardigheid van het asielrelaas, tenzij een rechtvaardiging kan worden gegeven voor het ontbreken van deze gegevens.[316] Ook deze bepaling komt niet voor in de Kwalificatierichtlijn. Aangezien de Kwalificatierichtlijn minimumnormen voor de erkenning als vluchteling of de toekenning van subsidiaire bescherming bevat, staat het aan de lidstaten niet vrij om bijkomende normen of voorwaarden voor het bekomen van internationale bescherming in te voeren en is deze bepaling hier dan ook mee in strijd.[317] Meer nog, het invoeren van een medewerkingsverplichting, zoals geformuleerd in de Kwalificatierichtlijn als onderdeel van de verzoekprocedure OIB, vormt eerder een optionele dan een verplichte maatregel.[318] De eerste zin van artikel 4, lid 1 Kwalificatierichtlijn (de medewerkingsplicht) is namelijk facultatief, terwijl de tweede zin (de samenwerkingsplicht) verplicht is.[319]

5.1.2. Onevenwichtige benadrukking van de medewerkingsplicht

Zowel de medewerkingsplicht, de samenwerkingsplicht als de gedeelde bewijslast zijn concepten waarbij discussie bestaat over de reikwijdte en betekenis ervan.[320] Dit blijkt alleen al uit de opmerkingen tijdens de voorbereidingen van het wetsontwerp in het advies van het UNHCR en de replieken hierop in het tweede verslag over het wetsontwerp (na het advies van het UNHCR).

Het UNHCR stelt in zijn advies dat de samenwerkingsplicht in het wetsontwerp onvoldoende wordt benadrukt. Het voert aan dat artikel 48/6, §1, lid 4 van de Vreemdelingenwet niet voldoende expliciteert

---

[312] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 527.
[313] Artikel 48/6, §1, lid 2 Vreemdelingenwet bevat de woorden 'onder meer'.
[314] Artikel 4, lid 2 Kwalificatierichtlijn
[315] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 527.
[316] Artikel 48/6, §1, lid 3 en 4 Vreemdelingenwet
[317] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 528.
[318] VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 86.; European Asylum Support Office (EASO). "Judicial analysis: Evidence and credibility assessment in the context of the Common European Asylum System." EASO Professional Development Series for members of courts and tribunals (2018). https://easo.europa.eu/sites/default/files/EASO%20Evidence%20and%20Credibility%20Assesment_JA_EN_0.pdf. P.43.
[319] European Asylum Support Office (EASO). "Judicial analysis: Evidence and credibility assessment in the context of the Common European Asylum System." EASO Professional Development Series for members of courts and tribunals (2018). https://easo.europa.eu/sites/default/files/EASO%20Evidence%20and%20Credibility%20Assesment_JA_EN_0.pdf. P 47.
[320] Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 526.

dat de bewijslast binnen de verzoekprocedure niet alleen op de verzoeker OIB weegt en dat er een gedeelde bewijslast geldt.[321] Het verwijst hierbij naar het UNHCR-handboek dat stelt dat, hoewel de bewijslast in beginsel bij de verzoeker ligt, de verzoeker en de asielinstantie gezamenlijk alle relevante feiten moeten vaststellen en beoordelen.[322] Ook wordt in het tweede verslag over het wetsontwerp aangehaald dat het feit dat het ontbreken van bewijsmateriaal een negatieve indicatie vormt voor de beoordeling van het verzoek OIB, indruist tegen de samenwerkingsplicht en het voordeel van de twijfel.[323]

In dit tweede verslag wordt echter door de toenmalige Staatssecretaris voor Asiel en Migratie de indruk gewekt dat de medewerkingsplicht de prioritaire plicht zou zijn en dat de samenwerkingsplicht van het CGVS pas, als ondergeschikte plicht, zou beginnen spelen wanneer de verzoeker heeft voldaan aan diens medewerkingsplicht en er ernstige aanwijzingen zijn dat het verzoek gegrond zou kunnen zijn.[324] Ook wordt beweerd dat er in de door het UNHCR aangehaalde rechtspraak van het EHRM en het HvJ nergens sprake blijkt te zijn van een gedeelde bewijslast. Integendeel, ook het EHRM zou volgens de Staatssecetaris de bewijslast in de eerste plaats op de schouders van de verzoeker leggen.[325]

Wat de bewering betreft dat de door het UNHCR aangehaalde rechtspraak niet getuigt van het bestaan van een gedeelde bewijslast, worden een aantal relevante passages uit de geciteerde zaken hieronder verklaard. Reeds in 1991 zette het EHRM het principe van de samenwerkingsplicht (en dus ook de gedeelde bewijslast) uiteen in de zaak Vilvarajah e.a. t. VK[326]. Het Hof benadrukte daarin dat het bestaan van het risico op een schending van artikel 3 EVRM door een verwijderingsmaatregel in de eerste plaats moet worden beoordeeld aan de hand van de feiten die ten tijde van de verwijdering bekend waren of bekend 'hadden moeten zijn' bij de lidstaat. Dit citaat wijst op het feit dat de lidstaten wel degelijk de plicht hebben om zelf onderzoek te verrichten naar de omstandigheden binnen de staten waarnaar ze verzoekers OIB zouden terugsturen. Vervolgens zette het Hof in 2007 uiteen wat precies onder deze samenwerkingsplicht moet worden begrepen in de zaak Salah Sheekh t. Nederland[327]. De beoordeling, die door de autoriteiten van de lidstaten wordt gemaakt in het kader van mogelijke schendingen van artikel 3 EVRM, dient adequaat en voldoende ondersteund te zijn. Deze ondersteuning moet zowel bestaan uit binnenlandse bronnen, als door andere objectieve en betrouwbare bronnen, bijvoorbeeld afkomstig van andere verdragsluitende of niet-verdragsluitende staten, organisaties van de Verenigde Naties en gerenommeerde ngo's. Ook is voor het evalueren van een vermeend risico op een behandeling in strijd met artikel 3 EVRM door een verwijderingsmaatregel, een volledige en *ex nunc*-beoordeling nodig, aangezien de situatie in een land van bestemming in de loop van de tijd kan veranderen. Hierop volgend bevestigde het EHRM het 'slechts principiële' karakter van de medewerkingsplicht in de zaken NA t. VK (2008)[328] en F.H. t. Zweden (2009)[329]. Het Hof stelt daarin dat het 'in beginsel' aan de verzoeker is om het bewijs te leveren voor het risico op een schending van artikel 3 EVRM, bij uitvoering van de aangevochten maatregel. Daarop volgt echter onmiddellijk de vereiste samenwerkingsplicht van de lidstaat, die inhoudt dat wanneer dergelijke bewijzen worden aangevoerd, het aan de lidstaat is om elke twijfel daarover weg te nemen. Daar waar verzoekers vaak niet in staat zijn om verder bewijs te leveren tegen de opgekomen twijfels over de geloofwaardigheid van de door

[321] Advies UNHCR P. 5.
[322] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Guide des procédures et critères à appliquer pour déterminer le statut de réfugié." (december 2011). https://www.refworld.org/docid/4fc5db782.html. § 196.
[323] Verslag 2 bij de wetswijziging P. 21.
[324] Ibid. P. 8.
[325] Ibid. P. 7.
[326] EHRM, Vilvarajah e.a. t. VK, nr. 45/1990/236/302-306, 26 september 1991. §107 (2).
[327] EHRM, Salah Sheekh t. Nederland, nr. 1948/04, 23 mei 2007. §136.
[328] EHRM, NA t. Verenigd Koninkrijk, nr. 25904/07, 17 juli 2008. §111.
[329] EHRM, F.H. t. Zweden, nr. 32621/06, 20 januari 2009. §95.

hen beweerde feiten, beschikken beslissingsautoriteiten namelijk wel over de nodige middelen en bronnen om bewijsmateriaal te verkrijgen dat niet toegankelijk is voor verzoekers.[330]

Ook het HvJ volgt de rechtspraak van het EHRM rond de samenwerkingsplicht en gedeelde bewijslast. In 2012 beantwoordde het Hof een principiële prejudiciële vraag hieromtrent in M.M. t. Ierland. Het Hof zet eerst de verhouding tussen de medewerkingsplicht en de samenwerkingsplicht uiteen: 'Volgens artikel 4, lid 1, van [de Kwalificatierichtlijn] dient normalerwijs de verzoeker alle elementen tot staving van zijn verzoek in te dienen, wat niet wegneemt dat de betrokken lidstaat voor de bepaling van de relevante elementen van dat verzoek met de verzoeker dient samen te werken'.[331] Deze samenwerkingsplicht wordt inhoudelijk verder uiteengezet: '[…] indien de door de verzoeker OIB aangevoerde elementen om welke reden ook niet volledig, actueel of relevant zijn, [moet] de betrokken lidstaat in deze fase van de procedure actief met de verzoeker samenwerken om alle elementen te verzamelen die het verzoek kunnen staven'.[332]

De door het UNHCR aangehaalde rechtspraak in het advies omtrent de besproken wetswijziging bevestigt dus wel degelijk het bestaan van een samenwerkingsplicht en gedeelde bewijslast. Echter, de discussie omtrent de reikwijdte en betekenis van deze begrippen, lijkt zijn oorsprong eerder in een tekstuele, dan in een inhoudelijke onenigheid te vinden. Waar het UNHCR, het EHRM en het Hof van Justitie, blijkend uit hun vaststaande leer en rechtspraak, de uitdrukking 'in principe' gebruiken met de betekenis 'normaalgezien geldt een bepaalde regel, maar in dit geval geldt hierop een uitzondering of sterke nuance', verschuift de toenmalige Belgische Staatssecretaris deze betekenis in het tweede verslag omtrent de besproken wetswijziging naar 'in de eerste plaats'. Deze tekstuele verwarring heeft een enorm gevolg voor de interpretatie en reikwijdte van de begrippen 'medewerkingsplicht, samenwerkingsplicht en gedeelde bewijslast'. Men mag echter niet uit het oog verliezen dat in het monistisch Belgisch rechtssysteem (de interpretatie door internationale hoven en rechtbanken van) internationale en supranationale verdragen zich op absolute wijze boven de tekstuele interpretatie ervan door een nationale staatssecretaris positioneert.[333] Dit indachtig, wordt voor dit onderzoek de verhouding gehanteerd, die door de internationale rechtspraak tussen de concepten 'medewerkingsplicht, samenwerkingsplicht en gedeelde bewijslast' werd ingesteld. Dit leidt tot de conclusie dat de medewerkingsplicht geenszins op de eerste plaats komt, dat er simpelweg geen hiërarchie bestaat tussen de medewerkings- en samenwerkingsplicht, dat het gaat om een 'gedeelde' bewijslast en dat deze plichten ook op die manier moeten worden weerspiegeld in nationale wetgeving, in nationale rechtspraak en in de praktijk van nationale asielautoriteiten.

Deze weerspiegeling kent echter een aantal onrustwekkende hiaten in het geval van België. In Belgische nationale rechtspraak stond reeds meerdere malen te lezen dat de bewijslast, zonder voorbehoud, bij de verzoeker zou liggen en/of dat het niet de taak van het CGVS zou zijn om zelf de lacunes in de bewijsvoering van de vreemdeling op te vullen.[334] Tegenstrijdig met deze rechtspraak, bevestigde de RvV echter zelf dat het CGVS tegelijkertijd verplicht is om ervoor te zorgen dat zijn beslissingen gebaseerd zijn op correcte feiten en dat dit in bepaalde omstandigheden een actief optreden vereist van

[330] VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 132.

[331] HvJ, C-277/11, M.M. t. Ierland, 2012. §65.

[332] Ibid. §66.

[333] Vande Lanotte, J., Goedertier, G. en Haeck, Y. Belgisch Publiekrecht. Brugge: Die Keure, 2015. P. 93-96.

[334] RvSt nr. 139.515 van 19 januari 2005. § 2.1.2.2.; RvSt nr. 190.508 van 16 februari 2009. § 2.4.3.; RvV nr. 69.017 van 21 oktober 2011. § 2.3.; RvV nr. 67.749 van 30 september 2011. § 2.7.; RvV nr. 69.519 van 28 oktober 2011. § 2.4.; RvV nr. 73.834 van 24 januari 2012. § 2.2.1.; RvV nr. 70.439 van 22 november 2011. § 3.6.; RvV nr. 73.798 van 23 januari 2012. § 2.3.; RvV nr. 74.347 van 31 januari 2012. § 2.1.1.; RvV nr. 72.597 van 23 december 2011. § 4.1.; Raad voor Vreemdelingenbetwistingen (RvV). "Jaarverslag 2009-2010." (2011). https://www.rvv-cce.be/sites/default/files/jaarverslag0910.pdf. P. 71.; VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 87.

het Commissariaat om voldoende informatie te verkrijgen alvorens een beslissing te nemen.[335] Bovendien werd België in 2012 veroordeeld door het EHRM voor het incorrect omgaan met bewijsmateriaal dat door verzoekers OIB werd aangebracht in het kader van hun medewerkingsplicht. Concreet ging het om het afwijzen van relevant bewijsmateriaal dat door een verzoeker werd aangebracht, zonder de authenticiteit ervan te verifiëren.[336]

In dezelfde lijn, wordt ook in de voorbereidende werken van het besproken wetsvoorstel beweerd dat het niet zozeer om een 'gedeelde bewijslast' zou gaan, maar hoogstens om 'een nuancering van de bewijslast'. De samenwerkingsplicht zou in hoofde van het CGVS geen verplichting doen ontstaan om de lacunes in de bewijsvoering van de verzoeker op te vullen.[337] Dit uitgangspunt wordt niet alleen doorgetrokken in de wettekst zelf, maar ook in de manier waarop het CGVS zijn eigen plichten presenteert. Het Commissariaat erkent op de officiële website dat er een samenwerkingsplicht rust op de beslissingsautoriteit. Desondanks wordt niets vermeld over de gedeelde bewijslast, die onlosmakelijk met deze samenwerkingsplicht is verbonden. De website stelt beknopt: 'De bewijslast ligt bij de asielzoeker'. Het feit dat de bewijslast verschuift in gevallen waar een verzoeker het risico op een schending van artikel 3 EVRM door een verwijderingsmaatregel *prima facie* heeft aangetoond, wordt enkel erkend in het geval dat de verzoeker in het verleden reeds werd blootgesteld aan vervolging of ernstige schade.[338] Dit ligt in lijn met de tekst van de Belgische Vreemdelingenwet[339], maar druist in tegen de vaststaande rechtspraak van het EHRM.[340]

Wat in de voorbereidende werken van de besproken wetswijziging wordt gesteld, namelijk dat de samenwerkingsplicht in hoofde van het CGVS geen afbreuk doet aan de verplichting van de verzoeker om in de eerste plaats zelf te voldoen aan zijn medewerkingsplicht[341], klopt. Deze vaststelling wordt ook geëxpliciteerd in de term 'gedeelde' bewijslast. Het rechtvaardigt echter niet dat de medewerkingsplicht van de verzoeker OIB onevenwichtig sterk wordt benadrukt, ten opzichte van de samenwerkingsplicht van het CGVS, zowel in de wettekst zelf, als in de praktijk van het CGVS.

5.2. Niet-gerespecteerde beginselen voor gegevensverwerking in de Algemene Verordening Gegevensbescherming

5.2.1. Behoorlijke en transparante verwerking niet gegarandeerd

De behoorlijke en transparante verwerking vereist een eerlijk en loyaal proces, waarbij tijdig en in duidelijke en begrijpelijke taal de regels, de risico's en de rechten die aan de gegevensverwerking verbonden zijn, aan de betrokkene worden meegedeeld.[342] De behoorlijkheids- en transparantievereiste

[335] RvV nr. 61.581 van 16 mei 2011.§ 2.3.
[336] EHRM, Singh e.a. t. België, nr. 33210/11, 2 oktober 2012.
[337] Verslag 2 bij de wetswijziging P. 7-9.
[338] "De beoordeling van de asielaanvraag". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/de-beoordeling-van-de-asielaanvraag.
[339] Artikel 48/7 Vreemdelingenwet
[340] EHRM, R.C. t. Zweden, nr. 41827/07, 9 maart 2010. §5.
Council of Europe/ European Court of Human Rights. "Article 3 The Court's approach to burden of proof in asylum cases." Research Division (2016).
https://www.echr.coe.int/Documents/Research_report_Art3_burden_proof_asylum_cases_ENG.pdf. P. 5 en 8.; Reneman, A.M. "EU Asylum Procedures and the Right to an Effective Remedy." VU Amsterdan (2014).
https://openaccess.leidenuniv.nl/bitstream/handle/1887/20403/Reneman.Thesis%20def.pdf?sequence=26. P. 204.; Spijkerboer, T. "Subsidiarity and 'Arguability': the European Court of Human Rights' Case Law on Judicial Review in Asylum Cases." 21 International Journal of Refugee Law (2009). http://thomasspijkerboer.eu/wp-content/uploads/2015/01/Subsidiarity-and-Arguability-The-European-Court-of-Human-Rights-Case-Law-on-Judicial-Review-in-Asylum-Cases.pdf. P. 61-62.
[341] Verslag 2 bij de wetswijziging P. 8.
[342] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 118-122.

bevatten dus enerzijds eisen over de manier waarop betrokkenen moeten worden geïnformeerd over de gegevensverwerking en anderzijds eisen over de inhoud van deze communicatie. Er zijn in de wetswijziging geen expliciete bepalingen voorzien die een dergelijke informatieverplichting aan het CGVS opleggen. Strikt gezien is het Commissariaat dus niet gehouden om de verzoeker OIB voorafgaand aan de verwerking van gegevens op diens sociale mediaprofiel of smartphone in te lichten over de regels, risico's en rechten die hieraan verbonden zijn.

Het informeren van de betrokkenen in duidelijke taal en op begrijpelijke wijze blijkt in migratiecontext echter geen vanzelfsprekendheid. Uit onderzoek van het European Union Agency for Fundamental Rights (FRA) is gebleken dat autoriteiten, die persoonsgegevens van verzoekers OIB, visumaanvragers en irreguliere migranten verzamelen en vervolgens opslaan in IT-systemen, het een uitdaging vinden om op begrijpelijke manier informatie te verstrekken. Zo zijn betrokkenen vaak niet volledig op de hoogte van alle aspecten van de gegevensverwerking en hebben ze moeite om de informatie die zij ontvangen te begrijpen.[343] Ook het UNHCR erkent deze problematiek, daar waar de nodige informatie niet mondeling (wel bijvoorbeeld in de vorm van een brochure) of niet volledig wordt meegedeeld. Verzoekers kunnen dergelijke brochures vaak niet lezen vóór het interview met het CGVS omdat zij analfabeet zijn, niet vertrouwd zijn met de bureaucratische behandeling van administratieve zaken en papieren, de brochure niet beschikbaar is in een taal die zij begrijpen of gewoonweg omdat er onvoldoende tijd is voor het begin van het interview.[344]

Inhoudelijk vereist de transparantieverplichting dat de verwerkingsverantwoordelijke de betrokkene op volledige wijze inlicht over de gegevensverwerking. De meest substantiële aspecten van dit inhoudelijk luik zijn de plichten tot informeren over 'de categorieën en bronnen van persoonsgegevens' en 'de manier waarop de persoonsgegevens zullen worden verwerkt'. Dit zijn echter twee aspecten waar in de besproken wetswijziging weinig of geen duidelijkheid over bestaat. Het ontbreken van verduidelijking rond de manier waarop toegang wordt verstrekt tot de digitale gegevensdrager, wordt tevens bevestigd in het advies over de wetswijziging van de CBPL.[345] Op die manier vervaagt de grens van de mate waarin en de wijze waarop een administratieve instantie, zonder strikte gerechtelijke onderzoeksbevoegdheden, zoals een asielautoriteit, dergelijke gegevensverwerkingen kan toepassen bij het beoordelen van een verzoek OIB.[346] Er is namelijk geen beperking voorzien op de soorten digitale informatie die kunnen worden verwerkt, noch regelt de wetswijziging precies hoe de gegevens zullen of moeten worden behandeld.[347]

Het is in de eerste plaats dus onduidelijk of het CGVS van plan is om effectief de inhoud van communicatie op smartphones te raadplegen, of slechts de locatiegegevens (geodata) en/of

Necessary & Proportionate. "International Principles on the Application of Human Rights to Communications Surveillance." Necessary & Proportionate (mei 2014). https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. P. 10.

[343] European Union Agency for Fundamental Rights (FRA). "Under watchful eyes: biometrics, EU IT systems and fundamental rights." (april 2018). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf. P. 9.

[344] VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 105.

[345] Advies CBPL P. 9.

[346] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 84.

[347] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 45.

metagegevens van deze communicatie (zoals informatie over hoe lang, waar, wanneer, door wie en met wie werd gecommuniceerd).[348] In Duitsland bijvoorbeeld, waar de praktijk van het doorlichten van smartphones al sinds 2017 in voege is[349], is ondertussen duidelijk dat de asielautoriteiten geen inhoudelijke screening van de communicatie van verzoekers OIB uitvoeren.[350] Het gaat daar vooral over informatie met betrekking tot het gebruik van de gegevensdrager, maar geen communicatie-inhoud (met uitzondering van logingegevens die in apps worden gebruikt).[351] In de voorbereidende fase van een gelijkaardige wetswijziging als de Belgische in Oostenrijk, beloofde de Minister van Binnenlandse Zaken dat 'het niet zal gaan om het lezen van gesprekken of sms'en, we weten dat dit problematisch is onder het grondwettelijk recht en zijn natuurlijk enkel geïnteresseerd in geodata'.[352] Desondanks bevat de uiteindelijk doorgevoerde wetswijziging deze beperking niet.[353] Zoals het CGVS de gegevensverzameling in verzoekprocedures OIB momenteel kadert, zal het om meer dan alleen meta- en/of geodata gaan. Op de privacypagina van de officiële website van het Commissariaat staat immers het volgende te lezen: 'gelet op het ingediende verzoek OIB, kan het gaan om de volgende categorieën van gegevens: identificatiegegevens, contactgegevens, persoonlijke kenmerken, leefgewoonten, samenstelling van het gezin, studie en opleiding, beroep en betrekking, rijksregisternummer, financiële situatie, gerechtelijke gegevens, raciale of etnische gegevens, politieke opvattingen/lidmaatschap van een vakvereniging, filosofische en religieuze overtuigingen, gegevens met betrekking tot het seksueel gedrag of seksuele gerichtheid en gegevens betreffende de gezondheid'.[354]

Over de categorieën of de bronnen van gegevens die vanop afstand op sociale mediaprofielen zullen worden geraadpleegd bestaat evenmin uitsluitsel. Welke sociale netwerken zullen worden gescreend en vanuit welke doelstellingen de relevante informatie zal worden geselecteerd is evenmin duidelijk. In de VS worden sociale mediaprofielen van buitenlandse reizigers al langer gescreend.[355] Sociale netwerken die deel uitmaken van deze grootschalige screenings zijn onder andere Facebook, Twitter, Instagram, YouTube en algemene zoekmachines (vb. Google). De screenings zijn bedoeld om publieke informatie in (mededelingen op) sociale mediaprofielen van verzoekers te identificeren, die relevant kunnen zijn voor de verwerking van hun migratiedossier. Het kan gaan om informatie met betrekking tot hun verzoek OIB, informatie die kan wijzen op fraude (zoals identiteitsfraude of valsheid in geschrifte) of informatie

[348] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 326.

[349] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 4.

[350] De Duitse asielautoriteiten verzamelen de volgende gegevens: landnummers van contactpersonen in het contactenbestand, landnummers en duur van inkomende en uitgaande gesprekken, landnummers van inkomende en uitgaande sms'en en andere berichten, taalgebruik in inkomende en uitgaande sms'en en andere berichten, landcodes van bezochte websites in de browsegeschiedenis, logingegevens en e-mailadressen gebruikt in apps, locatiegegevens van foto's en eventueel van apps.
Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 18.

[351] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 37.

[352] Hagen, L. "Kickl will Flüchtlinge "konzentriert" an einem Ort halten". www.derstandard.at. Der Standard, 11 januari 2018. https://www.derstandard.at/story/2000071880249/asyl-fpoe-kickl-will-fluechtlinge-konzentriert-an-einem-ort-halten.

[353] Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.

[354] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[355] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 3.

met betrekking tot criminele activiteiten of mogelijke problemen op het gebied van nationale veiligheid.[356] Hoewel hier de doelstellingen voor het screenen van sociale mediaprofielen vastliggen en als richtsnoer kunnen worden gebruikt, bestaat onder de personeelsleden die deze screenings uitvoeren in de VS nog steeds onzekerheid over welke informatie op een nationaal veiligheidsrisico zou kunnen wijzen en welke niet.[357] De specifieke, maar nog steeds ruim omschreven doelstellingen voor de grensonderzoeken en de beperkte maten waarin in openbare documenten wordt aangegeven welke soort data medewerkers precies moeten zoeken, draagt bij tot deze onzekerheid.[358] Waar de focus van dergelijke screenings door het CGVS ligt, is dus sterk afhankelijk van de doelstellingen die met de gegevensverwerking trachten te worden bereikt en vereist zeer strikte en duidelijke richtlijnen voor de personen die het onderzoek van sociale mediaprofielen uitvoeren.

Over de manier waarop gegevens door het CGVS in de verzoekprocedure OIB zullen worden verwerkt is evenmin duidelijkheid. In landen waar het doorzoeken van digitale gegevensdragers reeds een vaststaande praktijk is, wordt bijvoorbeeld een onderscheid gemaakt tussen het 'manueel of basisonderzoek'[359] en het 'geavanceerd of forensisch onderzoek'[360] in digitale gegevensdragers.[361] In Noorwegen en Nederland hanteren of hanteerden asielautoriteiten de techniek van de manuele of basisonderzoeken (*manual 'quick scans'* genoemd)[362]. In Noorwegen werd hier echter snel van afgestapt door twijfels omtrent de wettigheid van manuele onderzoeken en de eventuele negatieve juridische gevolgen ervan op lange termijn. Door het manueel doorbladeren van een digitale gegevensdrager worden bijvoorbeeld foto's geopend, waardoor de *time stamps* van de foto's worden gewijzigd. Hierna kan niet meer worden vastgesteld wanneer de foto voor het laatst door de verzoeker werd geopend, wat ernstige gevolgen kan hebben in eventuele toekomstige strafprocedures. Nu worden in Noorwegen teams van forensisch experten ingeschakeld voor 'geavanceerd of forensisich onderzoek'.[363] Het al dan niet handmatig doorzoeken van digitale gegevensdragers brengt ook gevolgen met zich mee voor het ingrijpende karakter van de onderzoeksmaatregel. In Amerikaanse rechtspraak werd het forensisch onderzoek van digitale gegevensdragers bijvoorbeeld als drastischer beschouwd dan het manueel of basisonderzoek.[364] In de zaak 'Verenigde Staten t. Kolsuz' werd geoordeeld dat een forensisch onderzoek van een digitale telefoon (tegenover een manueel onderzoek) moet worden behandeld als een 'niet-routinematige grenscontrole', waarvoor een vorm van 'geïndividualiseerde verdenking' nodig

[356] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for Refugee Case Processing and Security Vetting DHS/USCIS/PIA-068." (juli 2017). https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf. P. 7.

[357] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 7.

[358] Ibid. P. 14.

[359] omschreven als 'elke controle van een digitale gegevensdrager dat geen geavanceerde zoekactie is'

[360] gedefinieerd als 'elke zoekopdracht waarbij externe apparatuur via een bekabelde of draadloze connectie met een digitale gegevensdrager wordt verbonden, niet alleen om toegang te krijgen tot het apparaat, maar ook om de inhoud ervan te bekijken, te kopiëren en/of te analyseren'

[361] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 5-7.

[362] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 85 en 138.

[363] Ibid. P. 89.

[364] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 26.; Donohue, L. K. "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches." The Yale Law Journal Forum (april 2019). https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3174&context=facpub. P. 1001.

is.[365] In Noorwegen[366], Nederland[367] en Duitsland[368] daarentegen, wordt de omgekeerde redenering gemaakt en worden manuele onderzoeken als ingrijpender gezien dan geavanceerde onderzoeken op eerder geautomatiseerde wijze en/of door gespecialiseerde, van de asielautoriteiten gescheiden, forensische teams.

Er kan dus worden besloten dat de behoorlijke en transparante verwerking van de persoonsgegevens van verzoekers OIB niet wordt gegarandeerd in de huidige formulering van artikel 48/6, §1, lid 4 en artikel 57/7, §2 van de Vreemdelingenwet. De wetsartikelen bevatten geen verplichting om de verzoekers (in duidelijke en begrijpelijke taal) te informeren omtrent de regels, de risico's en de rechten die aan de gegevensverwerking verbonden zijn. Tevens is er, zoals de onderzoeksbevoegdheid van het CGVS momenteel in de Vreemdelingenwet wordt omschreven, omtrent substantiële aspecten van deze informatieplicht nog geen duidelijkheid. Er bestaat dus een zeer reëel risico dat verzoekers, zonder bijkomende maatregelen, op ontoereikende wijze door het CGVS worden geïnformeerd met betrekking tot de verwerking van hun gegevens op sociale mediaprofielen en smartphones.[369]

5.2.2. Doelbindingsprincipe niet onbetwistbaar nageleefd

Door asielautoriteiten worden tal van doeleinden voor het verwerken van persoonsgegevens (in het bijzonder gegevens uit smartphones en sociale mediaprofielen) aangevoerd, de een al verregaander dan de ander. Enerzijds wordt de verwerking vaak gekaderd binnen de identiteitscontrole of het herkomstonderzoek en zo ook de volledige beoordeling van het verzoek OIB.[370] De Belgische wettekst bevindt zich, strikt tekstueel gezien, binnen deze categorie: het CGVS kan gegevens verwerken '(die essentieel zijn) voor (een correcte) beoordeling van het verzoek'[371]. Ook in Duitsland is dit bijvoorbeeld het geval, waar asielautoriteiten enkel informatie van gegevensdragers kunnen extraheren om de

[365] United States Court of Appeals, Fourth Circuit, Verenigde Staten t. Kolsuz, nr. 16-4687, 9 mei 2018.
Hierop volgend werd in 2019, in de zaak Alasaad t. Nielsen, door een (lager geplaatste) rechtbank in Massachusetts geoordeeld dat zowel basis- als geavanceerde onderzoeken in elektronische apparaten een enorme hoeveelheid aan persoonlijke informatie kunnen onthullen en daarom beiden een redelijke verdenking vereisen. (United States District Court of Massachusetts, Alasaad t. Nielsen, nr. 17-cv-11730-DJC, 12 november 2019.)

[366] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 85 en 89.

[367] Bolhuis, M. en van Wijk, J. "Practices in establishing the identity and screening on national security and exclusion aspects in Syrian asylum cases in five European countries." Migration Policy Practice (april-juni 2019). https://publications.iom.int/system/files/pdf/mpp_38.pdf. P. 14.

[368] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 12-13.

[369] Tevens door het US Department of Homeland Security erkend in een gegevensbeschermingseffectbeoordeling U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 13.

[370] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 2.; International Committee of the Red Cross (ICRC) en Privacy International. "The Humanitarian Metadata Problem: Doing no harm in the digital era." (oktober 2018). https://reliefweb.int/sites/reliefweb.int/files/resources/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf. P. 27.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 81.

[371] Artikel 48/6, §1, lid 4 Vreemdelingenwet; Artikel 57/7, §2 Vreemdelingenwet

identiteit van verzoekers vast te stellen, maar niet voor andere doeleinden (zoals het reconstrueren van de reisroute).[372] Anderzijds worden gegevens op smartphones en sociale mediaprofielen ook om redenen van veiligheid en criminaliteit[373] verwerkt, bijvoorbeeld in de strijd tegen terrorisme[374] (hoewel de link tussen migratie en terrorisme op zich al een fel bediscussieerd gegeven vormt[375]), de strijd tegen identiteitsfraude[376] of om te controleren of iemand een bedreiging voor de openbare veiligheid kan vormen.[377] Deze tweede categorie is bijvoorbeeld van toepassing in de VS[378] en in Zweden (enkel voor het screenen van sociale mediaprofielen vanop afstand)[379].

Het doelbindingsprincipe houdt in dat gegevensverwerking enkel kan plaatsvinden voor een specifiek, uitdrukkelijk en gerechtvaardigd doel en enkel voor bijkomende doeleinden, indien deze verenigbaar zijn met het initieel afgebakende en geëxpliciteerde doel.[380] In de voorbereidende werken van de wetswijziging vooral de strijd tegen misbruik van verzoekprocedures OIB benadrukt.[381] De in de wet specifiek afgebakende doelen bestaan uit identiteitscontrole of herkomstonderzoek en de beoordeling van verzoeken OIB in het algemeen. Het zich verschaffen van toegang tot smartphones en sociale

---

[372] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 86.

[373] Latonero, M. en Kift, P. "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control." Social Media + Society (2018). https://journals.sagepub.com/doi/pdf/10.1177/2056305118764432. P. 5.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 81 en 135.; Fremstad, M. "Regjeringen mener asylsøkernes obile bør sjekkes". www.abcnyheter.no. Abv Nyheter, 2 maart 2017. https://www.abcnyheter.no/nyheter/politikk/2017/03/02/195282321/regjeringen-mener-asylsokernes-mobiler-bor-sjekkes.

[374] International Committee of the Red Cross (ICRC) en Privacy International. "The Humanitarian Metadata Problem: Doing no harm in the digital era." (oktober 2018). https://reliefweb.int/sites/reliefweb.int/files/resources/the_humanitarian_metadata_problem_-_icrc_and_privacy_international.pdf. P. 27.; Oltermann, P. en Henley, J. "German proposals could see refugees' phones searched by police". www.theguardian.com. The Guardian, 11 augustus 2016. https://www.theguardian.com/world/2016/aug/11/germany-security-proposals-refugees-phones-searched-suspicious-posts-social-media.; Gillespie, M. et al. "Mapping Refugee Media Journeys: Smartphones and Social Media Networks. Research Paper." The Open University en France Médias Monde (mei 2016). https://www.researchgate.net/profile/Dimitris_Skleparis/publication/310416833_Mapping_Refugee_Media_Journeys_Smartphones_and_Social_Media_Networks/links/582c77b008ae102f0729e9a1.pdf. P. 29.

[375] Tilovska-Kechedji, E. "Migrants and terrorism: A link or misconception." Journal of Advanced Research in Social Sciences and Humanities vol. 3, no. 2 (2018). https://pdfs.semanticscholar.org/af90/0d7d70ef0b1b01062da941b9d48de6f54971.pdf. P. 59-67.

[376] La Fors-Owczynik, K. "Monitoring migrants or making migrants 'misfit'? Data protection and human rights perspectives on Dutch identity management practices regarding migrants." Computer Law & Security Review (2016). https://www.sciencedirect.com/science/article/pii/S0267364916300243. Abstract.

[377] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 2.

[378] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 3.

[379] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 83 en 136.

[380] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 122-123.

[381] Memorie van toelichting bij de wetswijziging P. 6 en 7.; Verslag 2 bij de wetswijziging P. 22.; Verslag 1 bij de wetswijziging P. 5.

mediaprofielen in Belgische verzoekprocedures OIB wordt dus algemeen gecategoriseerd als 'praktijken voor het vaststellen van de identiteit van verzoekers om internationale bescherming'.[382]

De kwestie of deze doelstelling voldoende uitdrukkelijk en expliciet is overgebracht aan de betrokkenen zelf, is een vraag met betrekking tot de transparantie van de verwerking, zoals in '5.2.1.' werd uiteengezet. Of het door het CGVS vooropgestelde doel (het vaststellen van de identiteit van verzoekers OIB) ook een 'gerechtvaardigd doel' uitmaakt, wordt behandeld onder '5.2.7.'.

Als laatste schrijft het doelbindingsprincipe voor dat verzamelde gegevens niet mogen worden verwerkt voor andere doeleinden, die onverenigbaar zijn met het oorspronkelijk aangegeven doel. Het CGVS bevestigt op zijn officiële website dat persoonsgegevens worden verwerkt met (onder andere) het doeleinde om 'beslissingen te nemen inzake de verzoeken OIB'. Doeleinden die zich situeren binnen het gebied van de strafrechtspleging komen daarnaast niet aan bod. Ook verbindt het CGVS zich ertoe om persoonsgegevens niet verder te gebruiken op een wijze die onverenigbaar is met de zelf aangehaalde doeleinden.[383] Strikt genomen beoogt het CGVS met de gegevensverwerking dus niet de verwezenlijking van een doelstelling gerelateerd aan misdaadbestrijding. De CBPL stelde in haar advies omtrent het wetsontwerp ook dat medewerkers van het CGVS niet opgeleid zijn om taken uit te voeren in verband met de bestrijding van criminaliteit.[384]

Echter, als bij het onderzoek van een verzoek OIB op aanwijzingen van strafbare feiten wordt gestuit, wordt hiervan aangifte gedaan bij (o.a.) de Procureur des Konings.[385] Daarnaast wordt sinds augustus 2016 een opleiding over het screenen van sociale mediaprofielen van verzoekers OIB gegeven aan de medewerkers van het CGVS. Deze screenings worden niet alleen gebruikt in geval van twijfel over de geloofwaardigheid van de asielmotieven of het land van herkomst. Ook gebruikt het CGVS ze om potentiële gevallen, die voor uitsluiting van de vluchtelingenstatus of subsidiaire beschermingsstatus in aanmerking komen, te identificeren.[386] Een van deze uitsluitingsgronden bestaat erin dat een verzoek OIB als kennelijk ongegrond kan worden beschouwd bij ernstige vermoedens dat de verzoeker een gevaar vormt voor de nationale veiligheid of de openbare orde.[387] Het CGVS bevestigt op zijn officiële website tevens dat de door het Commissariaat verwerkte persoonsgegevens (kunnen) worden gedeeld met (o.a.) inlichtingen- en veiligheidsdiensten, politiediensten, de procureur des konings, de federale procureur, de onderzoeksrechters en, in bepaalde gevallen, met Europese of internationale rechtbanken.[388] Ook geldt een uitzondering op het beroepsgeheim van het CGVS, voor gegevens die worden gedeeld met diezelfde instanties.[389] Daarnaast bestaat binnen deze structuur geen uitsluitsel over de vraag of politiediensten deze gegevens op hun beurt niet zullen delen met instanties als bijvoorbeeld Interpol en Europol, wat binnen hun takenpakket in de criminele sfeer ligt.[390]

---

[382] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017).
https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 45 e.v.

[383] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen.
https://www.cgvs.be/nl/privacy-persoonsgegevens.

[384] Advies CBPL P. 7.

[385] Artikel 29 Wetboek van Strafvordering
Advies CBPL P. 7.

[386] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017).
https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 47.

[387] Artikel 57/6, §1, 2° jo. artikel 57/6/1, §2 jo. artikel 57/6/1, §1, j) Vreemdelingenwet

[388] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen.
https://www.cgvs.be/nl/privacy-persoonsgegevens.

[389] Artikel 57/27, lid 2 Vreemdelingenwet

[390] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017).
https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 61.

Het doorgeven en verwerken van verzamelde gegevens voor een doel dat onverenigbaar is met het initiële doel van de verwerking heeft niet alleen een inbreuk op het doelbindingsprincipe tot gevolg. Ook de nauwkeurigheid (zie '5.2.4.') van de persoonsgegevens kan bijvoorbeeld ernstig in het gedrang komen. Sociale mediaprofielen worden initieel op geïndividualiseerde wijze gescreend door asielautoriteiten, die daarnaast ook over contextuele en biografische informatie beschikken en de verzoeker eventueel kunnen vragen om de verzamelde data te becommentariëren. Wanneer deze informatie uit zijn context wordt gehaald en wordt doorgespeeld aan andere instanties om er secundaire analyses op uit te voeren, neemt het risico op verkeerde interpretaties echter toe. Gegevensuitwisseling tussen verschillende overheidsinstanties zou, onder strikte voorwaarden en controles, eventueel interessante opties openen. Het ongecontroleerd delen van informatie over de politieke en religieuze opvattingen van mensen bijvoorbeeld, vooral als die informatie afkomstig is uit de ambigue sfeer van de sociale media, vergroot enkel de kans op misbruik en onjuiste interpretatie.[391]

De onduidelijkheid omtrent de doeleinden waarvoor persoonsgegevens van verzoekers OIB worden gebruikt in de Belgische Vreemdelingenwet bevindt zich tussen twee uitersten in de internationale praktijk, die het doelbindingsprincipe wel strikt in acht nemen. Enerzijds perken landen als Duitsland de bevoegdheden van hun asielautoriteiten omtrent de besproken gegevensverwerking sterk in. De Duitse regelgeving bepaalt dat het verwerken van persoonsgegevens op sociale media en smartphones enkel mag worden gebruikt voor het herkomstonderzoek van verzoekers. Het gebruik van de gegevens voor de beoordeling van uitsluitingsgronden of potentiële problemen voor de nationale veiligheid, is uitgesloten.[392] Zelfs het inzetten van de verzamelde gegevens om vluchtroutes en asielmotieven te achterhalen betekent in het Duitse wettelijk kader een inbreuk op de basisrechten van de verzoekers.[393] Anderzijds hanteren landen als de VS een zeer ruime bevoegdheidsomschrijving voor het screenen van sociale mediaprofielen en smartphones van vreemdelingen. De Amerikaanse grensautoriteiten kunnen smartphones doorzoeken met het doeleinde om een verzoek OIB te beoordelen, maar ook om bewijzen van wetsovertredingen te identificeren, waaronder bijvoorbeeld de invoer van obsceen materiaal, drugssmokkel, andere douaneschendingen of terrorisme.[394]

Het is dus geen vanzelfsprekendheid dat de verwerking van gegevens op smartphones en sociale media van verzoekers volledig los staat van doelstellingen in verband met criminaliteit, hoewel dit nergens in de besproken wetswijziging wordt vermeld. Bijgevolg bestaat het risico dat de persoonsgegevens op smartphones en sociale mediaprofielen van verzoekers OIB, zonder bijkomende maatregelen, voor bijkomende doeleinden zullen worden verwerkt, die eventueel onverenigbaar zijn met het initieel afgebakende doel. Dit risico wordt erkend door de Europees Toezichthouder voor Gegevensbescherming in een advies over het screenen van sociale mediaprofielen door EASO (European Asylum Support Office).[395] Ook het US Department of Homeland Security heeft, in een gegevensbeschermingseffectbeoordeling over het screenen van sociale mediaprofielen van vreemdelingen die de VS binnenkomen, het bestaan van dit risico bevestigd en wijst op het bijkomend

[391] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 8.

[392] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 136.

[393] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 51.

[394] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 15.

[395] European Data Protection Supervisor (EDPS). "Formal consultation on EASO's social media monitoring reports (case 2018-1083)." (2019). https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf. P. 3.

risico dat de met externe partners gedeelde gegevens buiten het oorspronkelijke verwerkingsdoel zullen worden gebruikt.[396]

5.2.3. Dataminimalisatie niet gegarandeerd

Het beginsel van de dataminimalisatie[397] schrijft voor dat de verzamelde persoonsgegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Op de officiële website van het CGVS, verbindt het Commissariaat zich ertoe 'enkel persoonsgegevens te verwerken die toereikend zijn, ter zake dienend en niet buitensporig in verhouding tot de doeleinden waarvoor ze zijn verzameld'.[398] Het laatste onderdeel van deze verbintenis komt echter eerder overeen met de omschrijving van het beginsel van dataminimalisatie in de Richtlijn Gegevensbescherming[399] (de voorganger van de AVG), dan die van de huidige Algemene Verordening Gegevensbescherming. De voormalige omschrijving bevatte namelijk de verwoording 'toereikend, ter zake dienend en niet bovenmatig, uitgaande van de doeleinden'[400]. Het huidige artikel 5 (1) c) AVG legt de lat om aan het beginsel van de dataminimalisatie te voldoen echter hoger.[401] De verzamelde gegevens moeten niet alleen 'niet buitensporig' zijn, maar moeten zelfs 'noodzakelijk' zijn om de vooropgestelde verwerkingsdoeleinden te bereiken. Op deze noodzakelijkheidsvereist wordt hieronder in '5.3.2.1.' verder ingegaan.

Daarnaast vereist het beginsel van dataminimalisatie dat de gegevens die worden verzameld voor de verwerking kwantitatief 'toereikend' zijn. De hoeveelheid verzamelde gegevens mag de grens van wat nodig is voor het vooropgestelde verwerkingsdoel niet overschrijden. De intrinsieke aard van sociale media en smartphones, maakt het naleven van deze kwantitatieve vereiste echter moeilijk.[402] Voor smartphones gaat het hierbij niet enkel om gegevens die op het toestel zelf worden opgeslagen. Daarnaast geven 'cloud-gebaseerde applicaties' op elektronische toestellen ook toegang tot online opslagruimtes[403], die het mogelijk maken om nog grotere hoeveelheden informatie op te slaan dan op een individueel en offline apparaat mogelijk zou zijn.[404] Wat het doorzoeken van deze online

[396] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for Refugee Case Processing and Security Vetting DHS/USCIS/PIA-068." (juli 2017). https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf. P. 19 en 25.

[397] Artikel 5 (1) c) AVG

[398] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[399] Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

[400] Artikel 6 (1) c) Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

[401] European Union Agency for Fundamental Rights (FRA). "Fundamental rights and the interoperability of EU information systems: borders and security." (2017). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf. P. 21.

[402] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 2 en 16.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 9.; U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 2.

[403] Donohue, L. K. "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches." The Yale Law Journal Forum (april 2019). https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3174&context=facpub. P.964 en 999.

[404] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 4.

opslagruimtes betreft, oordeelde het Belgisch GWH reeds dat 'netwerkzoekingen'[405] in digitale gegevensdragers in strafrechterlijke onderzoeken zonder tussenkomst van de onderzoeksrechter ongrondwettig zijn. Het Hof argumenteerde dat rekening moet worden gehouden met 'de aanzienlijke ontwikkeling van de netwerken die toegankelijk zijn vanaf informaticasystemen en met het intensieve gebruik ervan door de overgrote meerderheid van de burgers, zowel om er documenten en gegevens op te slaan die tot hun privéleven behoren, met inbegrip van heel persoonlijke zaken, als om met elkaar te communiceren'. Bijgevolg vormt een onderzoeksmaatregel, die toegang geeft tot alle gegevens en communicatie die zich op de netwerken bevinden, verbonden aan een gegevensdrager, volgens het GWH een inmenging in het recht op privacy, die op zijn minst vergelijkbaar is met een huiszoeking in een woonplaats of een private plaats.[406]

Daarnaast moeten de verzamelde gegevens ook kwalitatief 'ter zake dienend' of relevant zijn. Ook hier creëert het medium van de sociale mediaprofielen en smartphones moeilijkheden voor het voldoen aan de vereiste. Smartphones en sociale mediaprofielen bevatten een enorme verscheidenheid aan gegevens, zoals medische gegevens, locatiegegevens, relatiegegevens, politieke of religieuze overtuigingen[407], sms-berichten naar familieleden, contactgegevens (waaronder bijvoorbeeld informatie over advocaten), betalingsgegevens, toegangsgegevens tot e-mailaccounts, geschiedenis van zoekmachines, verblijfsgegevens, intieme foto's[408] … Het is binnen deze verscheidenheid vaak niet mogelijk om op voorhand te weten welke informatie relevant kan blijken voor een onderzoek.[409] Daarnaast is het onvermijdelijk dat bij het screenen van sociale mediaprofielen en smartphones ook persoonsgegevens worden verwerkt van andere personen dan de verzoeker OIB zelf.[410] Dit laatste risico wordt in een arrest van de RvV ook uitdrukkelijk bevestigd door de toenmalige Staatssecretaris voor Asiel en Migratie en de RvV.[411] Zo vergroot de kans dat asielautoriteiten stuiten op allerhande informatie, die niet relevant is voor de verzoekprocedure OIB, aanzienlijk.[412]

Er is geen beperking voorzien op de hoeveelheid of soorten digitale informatie die kunnen worden verwerkt in de Belgische Vreemdelingenwet.[413] Zelfs in Duitsland, waar de wettekst rond het

[405] De uitbreiding van de informaticazoeking naar andere informaticasystemen die zich op een afstand bevinden en waarmee het oorspronkelijk doorzochte systeem is verbonden (bijvoorbeeld verbinding maken met de Facebookapp op een smartphone) wordt de netwerkzoeking genoemd.
Royer, S. en Oerlemans, J.J. "Naar een nieuwe regeling voor beslag op gegevensdragers." Computerrecht 2017/200 (2017). https://www.law.kuleuven.be/strafrecht/BijlagenNEDL/Sroyer_Computerrecht_2017_20.pdf. P. 278.
[406] GWH nr. 174/2018 van 6 december 2018. § B.14.1.
[407] Donohue, L. K. "Customs, Immigration, and Rights: Constitutional Limits on Electronic Border Searches." The Yale Law Journal Forum (april 2019). https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3174&context=facpub. P.999.
[408] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 22.
[409] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for the Immigration and Customs Enforcement Forensic Analysis of Electronic Media DHS/ICE/PIA-042." (mei 2015). https://www.dhs.gov/sites/default/files/publications/privacy-pia-forensicanalysisofelectronicmedia-may2015.pdf. P. 6.
[410] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 6 en 14.; Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.; EHRM, Szabo & Vissy t. Hongarije, nr. 37138/14, 12 januari 2016. §89.
[411] RvV nr. 175 324 van 26 september 2016. § 1, 3.2.2. en 3.2.3.
[412] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 197.
[413] Artikel 48/6, §1, lid 4 Vreemdelingenwet en artikel 57/7, §2 Vreemdelingenwet; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 45.

doorzoeken van sociale media en smartphones heel wat strikter is begrensd dan de Belgische[414], gaan stemmen op tegen de slecht afgebakende reikwijdte van de methode.[415] Zoals hierboven (zie '5.2.2.') reeds werd aangehaald, leidt een onvoldoende afbakening van de onderzoeksbevoegdheid van asielautoriteiten ook tot onzekerheid in de praktijk omtrent welke categorieën gegevens precies kunnen worden verzameld. Over het omschrijven van dergelijke bevoegdheden in niet-afgebakende bewoordingen, velde het HvJ een oordeel in de 'Digital Rights Ireland-zaak'. De algemene omschrijving van het toepassingsgebied van een bepaalde gegevensverwerking als 'alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder onderscheid, beperking of uitzondering in het licht van de doelstelling […]' werd door het Hof als problematisch bevonden.[416]

De aanzienlijke ontwikkeling van de netwerken die toegankelijk zijn vanaf informaticasystemen, het intensieve gebruik ervan door de overgrote meerderheid van de burgers voor opslag van gegevens en communicatie, de hoeveelheid gegevens, de combinatie van verschillende soorten gegevens en het feit dat de gegevens jaren kunnen teruggaan[417] verantwoorden een verhoogd risico op serieuze inbreuken op het recht op privacy. Zo erkent ook het US Department of Homeland Security, in hun gegevensbeschermingseffectbeoordelingen over sociale mediascreenings en grensonderzoeken van elektronische apparaten, het bestaan van de volgende risico's: dat te veel informatie wordt verzameld[418], dat toegang wordt verschaft tot informatie in bepaalde *clouds* (zoals informatie van sociale netwerksites, online e-maildiensten, online bankieren en andere zeer gevoelige informatie)[419] of dat te veel informatie extern zal worden gedeeld (onder andere met rechtshandhavingspartners)[420]. Het is door de gemakkelijk toegankelijke aard en de grote hoeveelheid en variëteit die kenmerkend is voor digitale persoonsgegevens dus geen vanzelfsprekendheid om de raadpleging ervan te beperken in functie van het beginsel van dataminimalisatie. Hieromtrent worden ook geen waarborgen voorzien in de Belgische wettekst.

5.2.4. Nauwkeurigheid niet gegarandeerd

Volgens het nauwkeurigheidsbeginsel in de AVG[421] mag een verwerkingsverantwoordelijke verzamelde persoonsgegevens niet gebruiken zonder stappen te ondernemen om met redelijke zekerheid te garanderen dat de gegevens accuraat en actueel zijn. Hiervoor moeten gegevens zo nauwkeurig mogelijk worden geregistreerd, moeten onjuiste gegevens onmiddellijk worden gewist of gecorrigeerd en moeten gegevens regelmatig worden gecontroleerd om ze actueel te houden. De juistheid van persoonsgegevens

[414] Artikel 15, (2), 6 jo. 15a Asylgesetz (Duitse Vreemdelingenwet); Artikel 48, 3 en 3a, 2-7 jo. artikel 48a Aufenthaltsgesetz (Duitse Verblijfswet)

[415] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 89.

[416] HvJ, C-293/12 en C-594/12, Digital Rights Ireland Ltd t. Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a., 2014. § 44 en 57.

[417] GWH nr. 174/2018 van 6 december 2018. § B.14.1.; Supreme Court of the United States (SCOTUS), Riley t. Californië, nr. 13–132, 25 juni 2014. https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf. P. 17-21.

[418] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for Refugee Case Processing and Security Vetting DHS/USCIS/PIA-068." (juli 2017). https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf. P. 17.

[419] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 16.

[420] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for the Immigration and Customs Enforcement Forensic Analysis of Electronic Media DHS/ICE/PIA-042." (mei 2015).
https://www.dhs.gov/sites/default/files/publications/privacy-pia-forensicanalysisofelectronicmedia-may2015.pdf. P. 10.

[421] Artikel 5 (1) d) AVG

op digitale dragers en platformen garanderen is niet evident, aangezien deze gegevens vaak een gelimiteerde betrouwbaarheid of accuraatheid hebben en gemakkelijk kunnen worden aangepast.[422]

Een eerste reden voor de beperkte betrouwbaarheid van digitale persoonsgegevens bestaat erin dat smartphones en/of sociale mediaprofielen vaak door meerdere personen achtereenvolgens of tegelijkertijd worden gebruikt.[423] Het is bijvoorbeeld gebruikelijk in Afrika en Azië om mobiele telefoons te delen, meestal om economische redenen.[424] Daarnaast worden smartphones ook gebruikt door of doorgegeven aan mensensmokkelaars en -handelaars, wat het moeilijk maakt om de gegevens op een bepaald apparaat te linken aan een specifiek individu.[425] Ook sociale mediaprofielen worden gedeeld, zoals in het voorbeeld van een verzoeker OIB, wiens verzoek werd afgewezen nadat de Deense autoriteiten vaststelden dat zijn Facebookaccount actief was geweest tijdens een periode waarin hij naar eigen zeggen in de gevangenis verbleef. De verklaring dat zijn broer ook toegang had tot zijn account werd door de asielautoriteiten terzijde geschoven.[426]

Ten tweede bevatten smartphones en sociale mediaprofielen soms ook onjuiste informatie, die bewust door de verzoekers OIB is gecreëerd. Het is bijvoorbeeld reeds bekend dat Facebookwachtwoorden worden opgevraagd bij controleposten in Syrië, zowel door overheids- als door IS-troepen[427], om de positie van individuen in het conflict te identificeren of de loyaliteit aan het regime te onderzoeken.[428] Gevonden data wijzen dus niet noodzakelijkerwijs op lidmaatschap van of affiniteit met een terroristische organisatie.[429] De betrokkene kan bijvoorbeeld gedwongen zijn om dergelijke gegevens op te slaan op het apparaat of profiel om ongewenste aandacht af te leiden en te kunnen vluchten uit de regio.[430] Ook leeftijdsonderzoek kan worden vertroebeld, wanneer het doorzoeken van sociale mediaprofielen hiervoor wordt ingezet. Het is namelijk niet ongewoon dat jonge gebruikers van sociale

[422] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2.
[423] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.; Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 29.
[424] Toor, A. "Germany Moves to Seize Phone and Laptop Data from People Seeking Asylum". www.theverge.com. The Verge, 3 maart 2017. https://www.theverge.com/2017/3/3/14803852/germany-refugee-phone-data-law-privacy.
[425] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2.
[426] Meaker, M. "Europe Is Using Smartphone Data as a Weapon to Deport Refugees". www.wired.co.uk. Wired, 2 juli 2018. https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations.
[427] Brunwasser, M. "A 21st-Century Migrant's Essentials: Food, Shelter, Smartphone". www.nytimes.com. The New York Times, 25 augustus 2015. https://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=1.
[428] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.
[429] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 136-137.
[430] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 50. (voetnoot 51)

media zich online registreren met een andere leeftijd, omdat het anders soms niet mogelijk is om een account aan te maken.[431]

Naast de kans op het aantreffen van onjuiste gegevens of gegevens die niet aan de betrokkene te linken zijn, schuilt ook een risico op incorrecte gegevensverzameling in de interpretatie van data op sociale mediaprofielen en smartphones. De betekenis van deze data spreekt namelijk alles behalve voor zich[432] en is moeilijk te interpreteren[433]. Dit is des te meer het geval wanneer de taal op sociale mediaprofielen en smartphones niet dezelfde is als die van de asielautoriteiten die ze doorzoeken of wanneer de culturele context hen minder bekend of helemaal onbekend is.[434] Bovendien toonde een recente studie bijvoorbeeld aan dat het determineren van iemands politieke overtuiging op basis van Twitterberichten slechts in 27% van de gevallen tot een accuraat besluit leidt, door de moeilijke en genuanceerde aard van informatie op sociale media.[435] Smartphones bieden toegang tot een enorme hoeveelheid gegevens en wekken vaak de veronderstelling dat ze daardoor ook meer accurate informatie opleveren. De vraag of het doorzoeken van sociale mediaprofielen en smartphones effectief bruikbare resultaten oplevert, is echter eerder afhankelijk van de soort informatie die wordt verzameld en hoe deze informatie wordt geïnterpreteerd.[436]

Tot slot is de massa aan verzamelde informatie van sociale mediaprofielen en smartphones meestal niet voorzien van tekst of uitleg. Het is ook niet gegarandeerd dat de betrokken verzoeker OIB deze uitleg of context aan de onderzoekende autoriteit zal kunnen verschaffen tijdens of na het raadplegen ervan. Artikel 17, §2 van het KB omtrent de werking van het CGVS bepaalt: 'indien de ambtenaar tijdens het gehoor tegenstrijdigheden vaststelt in de verklaringen van de [verzoeker] […], stelt hij de [verzoeker] in de loop van het gehoor in de gelegenheid om hier uitleg over te geven'[437]. Deze bepaling biedt echter

---

[431] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 83.

[432] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.

[433] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 4.
Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 136-137.

[434] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 4-5.

[435] Preotiuc-Pietro, D., Liu, Y., Hopkins, D. J. en Ungar, L. "Beyond Binary Labels: Political Ideology Prediction of Twitter Users." Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (2017). https://www.aclweb.org/anthology/P17-1068.pdf. P. 736-737.; Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 5.

[436] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.

[437] Artikel 17, §2 Koninklijk besluit tot regeling van de werking van en de rechtspleging voor het Commissariaat-generaal voor de Vluchtelingen en de Staatlozen, 11 juli 2003. Hierna: KB Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen

geen garantie dat verzoekers, indien hun smartphone of sociale mediaprofiel pas na het interview wordt doorzocht, hieromtrent nog verduidelijking kunnen verschaffen. In de memorie van toelichting wordt ook bevestigd dat, indien de informatie later (na het persoonlijk gehoor van de verzoeker) aan het licht zou komen, er geen verplichting is om de verzoeker andermaal op te roepen voor een gehoor teneinde hem te confronteren met de informatie die door de verzoeker via elektronische weg werd verstuurd of ontvangen. Er is immers geen enkele bepaling die de Commissaris-Generaal zou verhinderen om gebruik te maken van de informatie waarmee de verzoeker niet geconfronteerd werd.[438]

In tegenstelling tot deze realiteit, wordt in een studie van het Belgisch contactpunt van het European Migration Network (EMN) van 2017 bevestigd dat, voor herkomstonderzoek door het CGVS, de resultaten uit de interviews met de verzoeker OIB nog steeds de belangrijkste invloed hebben op de uiteindelijke beslissing. Ook wordt hierin erkend dat er 'in principe' consistentie moet bestaan tussen de door de verzoeker verstrekte verklaringen, de ingediende documenten en de persoonsgegevens die via andere methoden zijn verkregen (VIS, Eurodac, sociale media...). Bij gebrek aan een dergelijke consistentie, worden verzoekers hier 'in principe' mee geconfronteerd en krijgen zij de kans om uitleg en verheldering aan te brengen.[439] Duits expert migratierecht Prof. Thym stelde zelfs de grondwettelijkheid van het doorzoeken van sociale mediaprofielen en smartphones afhankelijk van het voorzien van een mogelijkheid voor de verzoekers om toelichting te geven bij de over hen verzamelde digitale gegevens.[440] Ook het UNHCR stelt dat asielautoriteiten de plicht hebben om verzoekers de kans te geven om uitleg te verschaffen bij verzamelde gegevens die een negatieve invloed kunnen hebben op hun geloofwaardigheid, opdat verzoekers hun medewerkingsplicht ten volle kunnen vervullen.[441] Een lidstaat die een geloofwaardigheidsbeoordeling van de elementen in een verzoekprocedure uitvoert, zonder de verzoeker toe te staan aan dit deel van het proces deel te nemen, schendt artikel 4, lid 1 Kwalificatierichtlijn (de medewerkingsplicht en de samenwerkingsplicht).[442] Ook het EHRM bevestigde reeds deze plicht van de asielautoriteiten om de verzoeker de beoordeling van het verzoek OIB mee te delen alvorens een definitieve beslissing te nemen, zodat laatstgenoemde de mogelijkheid heeft te antwoorden op de elementen die een negatief antwoord in het vooruitzicht stellen.[443]

Door de grote kans op het aantreffen van onjuiste informatie of het inaccuraat interpreteren van de informatie, is de bewijswaarde van gegevens op sociale mediaprofielen en smartphones tot een minimum te herleiden. De veronderstelling dat het verkrijgen van gegevens uit digitale apparaten en platformen leidt tot betrouwbaar bewijs, is onjuist.[444] Inconsistentie tussen de mondelinge beweringen tijdens een interview van verzoekers en de informatie die later over hen op sociale media of smartphones wordt gevonden, vormt geen bewijs dat een persoon liegt.[445] Gegevens op sociale media en smartphones

[438] Memorie van toelichting bij de wetswijziging P. 137.
[439] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 54 en 56.
[440] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 51.
[441] VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 105.
[442] Noll, G. "Evidentiary assessment and the EU qualification directive, New Issues in Refugee Research, Working Paper no. 117." VN- Hoog Commissariaat voor de Vluchtelingen (UNHCR) (juni 2005). https://www.refworld.org/pdfid/4ff165bf2.pdf. P. 4.
[443] HvJ, C-277/11, M.M. t. Ierland, 2012. §50.
[444] European Data Protection Supervisor (EDPS). "Formal consultation on EASO's social media monitoring reports (case 2018-1083)." (2019). https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf. P. 7.
[445] "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers". www.privacyinternational.org. Privacy International. https://privacyinternational.org/node/2776.

zijn behept met een inherente onbetrouwbaarheid, waardoor ze zelden een solide basis vormen om een oordeel te vellen over verzoeken OIB. Daarbij komt nog dat er geen garantie blijkt te bestaan dat asielautoriteiten het juiste sociale mediaprofiel bij de verzoeker OIB in kwestie zullen plaatsen. Zelfs wanneer dit wel het geval is, blijft het moeilijk om met enig niveau van zekerheid de authenticiteit en sociale context van de gegevens vast te stellen.[446] Ook de RvV erkent de nood aan een zekere voorzichtigheid bij het beoordelen van materiaal dat is gepubliceerd op sociale netwerken in zijn rechtspraak. De redenen hiervoor zijn onder andere dat dergelijke informatie geen absolute tijdsaanduidingen bevat, dat een sociale mediaprofiel door iemand anders dan de verzoeker kan zijn opgesteld of dat het verklaringen kan bevatten die niet overeenkomen met de werkelijkheid. Uit de gevonden gegevens op sociale mediaprofielen mogen dus enkel conclusies worden getrokken indien ze voldoende betrouwbaar zijn.[447]

Samenvattend moet met verzamelde persoonsgegevens uit sociale mediaprofielen en smartphones van verzoekers OIB uitermate zorgvuldig worden omgesprongen, gezien hun inherent onnauwkeurig karakter. De minimale bewijswaarde die aan dergelijke persoonsgegevens moet worden gehecht, wordt gerechtvaardigd door het feit dat toestellen en/of profielen worden gedeeld en doorgegeven, dat ze soms (bewust gecreëerde) onjuiste informatie bevatten, dat de gegevens erop substantiële interpretatieproblemen met zich meebrengen en dat verzoekers niet gegarandeerd de mogelijkheid krijgen om toelichting te verschaffen bij de verzamelde gegevens. Er bestaat dus een onmiskenbaar risico dat het CGVS zich, bij het doorzoeken van sociale mediaprofielen en smartphones van verzoekers, zal baseren op foutieve informatie om beslissingen te nemen in verzoekprocedures OIB. Zoals het doorzoeken van sociale mediaprofielen en smartphones momenteel in de Vreemdelingenwet wordt omkaderd, voorziet het CGVS onvoldoende maatregelen om met redelijke zekerheid te garanderen dat de verzamelde gegevens accuraat en actueel zijn, in het licht van de gedefinieerde verwerkingsdoelstellingen. De CBPL bevestigt dit hiaat in de wettekst in haar advies, door te stellen dat niet is gespecifieerd door wie de verstrekte informatie vertaald en geïnterpreteerd zal worden en op welke manier de authenticiteit ervan zal gewaarborgd worden.[448] Volgens het nauwkeurigheidsbeginsel in de AVG, mag het Commissariaat deze gegevens dan ook niet gebruiken zonder hieromtrent verdere waarborgen in te bouwen.

5.2.5. Opslagbeperking niet gegarandeerd

De opslagbeperking[449] gebiedt dat persoonsgegevens worden gewist of geanonimiseerd zodra ze niet langer nodig zijn voor de doeleinden waarvoor ze zijn verzameld. De AVG voorziet een uitzondering op deze regel voor de opslag van persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. De wetswijziging bevat geen specifieke bepalingen omtrent de manier waarop gegevens, verzameld bij het doorzoeken van sociale mediaprofielen en smartphones, worden geregistreerd en opgeslagen. Het ontbreken van elke verduidelijking hieromtrent, wordt tevens bevestigd in het advies van de CBPL.[450] Ervan uitgaande dat er over de doorzoekingen van sociale mediaprofielen en smartphones wel degelijk gegevens worden bijgehouden in het dossier van de verzoeker OIB, geldt de volgende regeling.

---

[446] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 4 en 6.
[447] RvV nr. 95 844 van 25 januari 2013. § 4.6.; RvV nr. 119 575 van 26 februari 2014. § 5.3.4.; RvV nr. 152 234 van 10 september 2015. § 3.8.
[448] Advies CBPL P. 9.
[449] Artikel 5 (1) e) AVG
[450] Advies CBPL P. 9.

De officiële website van het CGVS vermeldt algemeen dat alle door hen verwerkte persoonsgegevens worden opgeslagen 'volgens de behoeften van de dienst en zolang het dossier open is'. Hierna worden de dossiers van verzoekprocedures OIB overgedragen aan het Rijksarchief.[451] De door het CGVS aangegeven onbepaalde bewaartermijn, wordt in de archiefselectielijst[452] voor het CGVS van het Rijksarchief verder gespecifieerd. Voor niet-ingewilligde verzoeken gaat het om een bewaartermijn bij het CGVS van 75 jaar na de geboorte of 5 jaar na het overlijden van de verzoeker OIB. Voor dossiers van verzoekers bij wie de vluchtelingenstatus is erkend of subsidiaire beschermingsstatus is toegekend, wordt het dossier bij het CGVS enkel bijgehouden 'zo lang het dossier van de verzoeker open staat'.[453] De ratio achter deze bewaartermijnen is de volgende: zolang de verzoeker OIB leeft, kan een volgend verzoek OIB ingediend worden, op voorwaarde dat men voor elk nieuw verzoek over nieuwe elementen beschikt. Dit heeft tot gevolg dat het dossier te allen tijde heropend moet kunnen worden door de betrokken verzoeker of door diens vertegenwoordiger.[454]

Voor beide van de bovenstaande gevallen wordt als 'finale bestemming' voor de dossiers aangegeven dat ze moeten worden overgebracht naar het Rijksarchief.[455] De bewaartermijn van het Rijksarchief is onbeperkt voor documenten die volgens de archiefselectielijsten bestemd zijn voor overbrenging naar het Rijksarchief en dus voor 'permanente bewaring'. De persoonsgegevens die in deze documenten voorkomen, worden bewaard 'met het oog op archivering in het algemeen belang'.[456] Hierdoor vallen dossiers van verzoeken OIB onder de uitzondering op de opslagbeperking, zoals gedefinieerd in artikel 5 (1) e) AVG. Gegevens mogen volgens die uitzondering langer worden opgeslagen, indien passende technische en organisatorische maatregelen worden genomen om de rechten en vrijheden van de betrokkenen te beschermen. In de archiefselectielijst voor het CGVS worden echter geen dergelijke passende technische en organisatorische maatregelen vermeld.

Er wordt vooralsnog niet gespecifieerd hoe en of persoonsgegevens door het CGVS verzameld van smartphones en sociale mediaprofielen deel uitmaken van deze dossiers en in welke mate de verzoeker het recht heeft de verwijdering van deze gegevens te vragen. Ook is er geen duidelijkheid omtrent het lot van verzamelde gegevens die achteraf irrelevant bleken voor het beoordelen van het verzoek. De CBPL vraagt zich in het advies omtrent de wetswijziging terecht af: 'Wordt enkel de relevante informatie opgeslagen dan wel overgeschreven in een verslag, of alle informatie die door de medewerker van de CGVS wordt gelezen?'.[457] Met betrekking tot informaticazoekingen, die in België kunnen worden uitgevoerd in het kader van de strafrechtspleging[458], werd reeds kritiek geuit op het feit dat de wetgever niet heeft voorzien in een uitdrukkelijke plicht tot verwijdering van gegevens die geen verband

[451] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.
[452] Het gaat om een lijst, opgesteld door het Rijksarchief, voor het efficiënt laten verlopen van de selectie van archieven, die een systematisch overzicht biedt van alle papieren en digitale reeksen van een administratie met vermelding van de bewaartermijn en de definitieve bestemming ervan.
[453] Soyez, S. "Tableaux de tri: Archives du Commissariat général aux Réfugiés et aux Apatrides et Archives de la Délégation belge du Haut-Commissariat des Nations Unies pour les Réfugiés." Algemeen Rijksarchief en Rijksarchief in de Provinciën Publ. 5314 (2012). http://arch.arch.be/pdf/fs_web_pub/P5314/EP5314.pdf#viewer.action=download. P. 31-32.
[454] Soyez, S. "Dossier d'étude et de préparation du tableau de tri: Archives du Commissariat général aux Réfugiés et aux Apatrides et Archives de la Délégation belge du Haut-Commissariat des Nations Unies pour les Réfugiés." Algemeen Rijksarchief en Rijksarchief in de Provinciën Publ. 5313 (2012). http://arch.arch.be/ViewerJS/?startpage=0#../pdf/fs_web_pub/P5313/EP5313.pdf. P. 28.
[455] Soyez, S. "Tableaux de tri: Archives du Commissariat général aux Réfugiés et aux Apatrides et Archives de la Délégation belge du Haut-Commissariat des Nations Unies pour les Réfugiés." Algemeen Rijksarchief en Rijksarchief in de Provinciën Publ. 5314 (2012). http://arch.arch.be/pdf/fs_web_pub/P5314/EP5314.pdf#viewer.action=download. P. 31-32.
[456] "Bescherming van persoonsgegevens: Bewaartermijn". www.arch.be. Rijksarchief België. http://arch.arch.be/index.php?l=nl&m=praktische-info&r=bescherming-van-persoonsgegevens#6.
[457] Advies CBPL P. 9.
[458] Artikel 39bis Wetboek van Strafvordering

houden met het onderzochte misdrijf.[459] Ook in Oostenrijk gingen reeds kritische stemmen op tegen het feit dat politiediensten volledige reservekopieën kunnen maken van alle soorten gegevensdragers, zonder vervolgens gegevens te hoeven verwijderen die irrelevant bleken voor de beoogde verwerkingsdoeleinden.[460] In Duitsland geldt dan weer de regel dat verzamelde gegevens, die achteraf deel blijken uit te maken van 'het kerngebied van iemands privacy', niet mogen worden gebruikt en onmiddellijk moeten worden gewist. Het feit dat dergelijke gegevens zijn verzameld en achtereenvolgens gewist, moet ook worden geregistreerd.[461]

In de praktijk komt dit neer op de vaststelling dat dossiers van verzoeken OIB nooit volledig worden vernietigd, zonder bijkomende waarborgen. Dit houdt niet alleen een risico op schending van het beginsel van opslagbeperking in, maar ook van het beginsel van nauwkeurigheid. Lange bewaartermijnen voor informatie van sociale mediaprofielen bijvoorbeeld vergroten het risico op foutieve interpretatie ervan nog verder. Zo kan een bericht op een sociale mediaprofiel uit 2007 tegen 2022 (of later) een geheel nieuwe betekenis krijgen.[462] Tevens wordt nog niet in rekening gebracht in welke mate verzamelde gegevens door het CGVS eventueel worden doorgespeeld aan andere entiteiten (zoals reeds vermeld in '5.2.2.') en hoe de gegevens daar worden opgeslagen.

De grootschalige en langdurige bewaring van grote hoeveelheden persoonlijke informatie door het CGVS en het Rijksarchief kan aanleiding geven tot ernstige bezorgdheid over de risico's voor de privacy van de betrokkene en de opslagbeperking in het bijzonder. De wetswijziging bevat bijvoorbeeld geen waarborgen omtrent het bewaren van irrelevante, uiterst privacygevoelige of niet langer actuele gegevens. Daarnaast werden geen waarborgen ingebouwd, zoals anonimisering of pseudonimisering, eens de dossiers naar het Rijksarchief worden overgebracht, om de rechten en vrijheden van de betrokkenen te beschermen.

5.2.6. Vertrouwelijkheid en integriteit niet gegarandeerd

Volgens het beginsel van vertrouwelijkheid en integriteit, zijn verwerkingsverantwoordelijken verplicht om de beveiliging en vertrouwelijkheid van de gegevensverwerking te garanderen. Hiervoor dienen zij technische of organisatorische maatregelen te nemen om de gegevens te beschermen, ten eerste tegen ongeoorloofde toegang en gebruik en ten tweede tegen onopzettelijk verlies, vernietiging of beschadiging ervan. Bij het uitvoeren van deze maatregelen moet onder andere rekening gehouden worden met de risico's voor de rechten en vrijheden van de betrokkenen.[463]

Volgens het UNHCR is het beginsel van vertrouwelijkheid en integriteit van uitzonderlijk belang voor verzoekers OIB, gezien de stijgende hoeveelheid gegevensverzameling, het stijgende gebruik van (draagbare) digitale verwerkingsapparatuur, de stijgende opslag in elektronische databanken, het stijgend aantal digitale datatransfers naar derde verwerkers en, in het bijzonder, het stijgend aantal bedreigingen voor de gegevensbeveiliging[464], zoals cybercriminaliteit.[465] Informaticasystemen, die

[459] Kerkhofs, J. en van Linthout, P. Cybercrime. Brussel: Politeia 2013. P. 137-171.
[460] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 46.
[461] Artikel 48, 3a, 5-7 Aufenthaltsgesetz (Duitse Verblijfswet)
[462] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 9.
[463] Artikel 5 (1) e) jo. Artikel 32 jo. Overweging 39 AVG
[464] European Union Agency for Fundamental Rights (FRA). "Fundamental rights and the interoperability of EU information systems: borders and security." (2017). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-interoperability-eu-information-systems_en-1.pdf. P. 9 en 42.
[465] VN- Hoog Commissariaat voor de Vluchtelingen. "Guidance on the Protection of Personal Data of Persons of Concern to UNHCR." (augustus 2018). https://www.refworld.org/docid/5b360f4d4.html. P. 36.

gegevens over verzoekers OIB bevatten, kunnen namelijk bijzonder aantrekkelijk zijn voor hacking door onderdrukkende regimes of personen die hen vervolgen.[466] Tegen deze achtergrond, mogen overheidsactoren, die belang hebben bij de toegang tot vertrouwelijke informatie over onder andere verzoekers OIB, het belang en de uitdaging van gegevensbeveiliging niet onderschatten. De bijzonder kwetsbare positie van deze verzoekers OIB en de over het algemeen gevoelige aard van hun persoonsgegevens vraagt een uiterst zorgvuldige behandeling ervan.[467] Het beginsel van de vertrouwelijkheid en integriteit vormt dus een van de meest prominente aandachtsgebieden met betrekking tot de gegevensverwerking in verzoekprocedures OIB.[468]

Met betrekking tot de vertrouwelijkheid tijdens het interview met de verzoeker OIB, bepaalt het KB omtrent de werking van het CGVS dat het plaatsvindt in 'omstandigheden die een passende geheimhouding waarborgen'.[469] Los van dit interview[470], is op het CGVS het beroepsgeheim van toepassing.[471] De Vreemdelingenwet bevat echter een aantal uitzonderingen op dit beroepsgeheim, vooral in het kader van de strafrechtspleging[472], maar ook bijvoorbeeld 'met betrekking tot gegevens over de identiteit die ter kennis worden gebracht van de Dienst Vreemdelingenzaken'[473]. Voor de Dienst Vreemdelingenzaken bestaat echter geen gelijkaardig algemeen beroepsgeheim. Er is in de wet enkel sprake van een geheimhoudingsplicht met betrekking tot medische gegevens[474] en van het feit dat het gehoor plaats moet vinden in 'omstandigheden die een passende geheimhouding waarborgen'[475]. Bovendien gebeurt de gegevensuitwisseling tussen het CGVS en de Dienst Vreemdelingenzaken niet volledig digitaal, aangezien de informaticasystemen waarin hun gegevens worden opgeslagen (respectievelijk 'Actio' en 'Evibel') niet compatibel zijn.[476] De toenmalige Staatssecretaris voor Asiel en Migratie stelde daarenboven dat de informatie-uitwisseling van het CGVS aan de Dienst Vreemdelingenzaken bestaat uit de identiteitsgegevens die nodig zijn voor de identificatie van de vreemdeling en dat er dus geen sprake zou zijn van een inbreuk op de Privacywet.[477] Ten slotte wordt in de wet uitdrukkelijk vermeld dat noch informatie betreffende het verzoek, noch het feit dat het verzoek

[466] European Union Agency for Fundamental Rights (FRA). "Under watchful eyes: biometrics, EU IT systems and fundamental rights." (april 2018). https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf. P. 13 en 80.

[467] VN- Hoog Commissariaat voor de Vluchtelingen. "Guidance on the Protection of Personal Data of Persons of Concern to UNHCR." (augustus 2018). https://www.refworld.org/docid/5b360f4d4.html. P. 36.

[468] Latonero, M., Hiatt, K., Napolitano, A., Clericetti, G. en Penagos, M. "Digital Identity in the Migration & Refugee Context: Italy case study." Data & Society (2019). https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf. P. 2.

[469] Artikel 13/1 en 14 KB Commissariaat-generaal voor de Vluchtelingen en de Staatlozen

[470] Hiervoor werd namelijk reeds aangehaald dat, indien de informatie later (na het persoonlijk interview van de verzoeker) aan het licht zou komen, er geen verplichting is om de verzoeker andermaal op te roepen voor een gehoor teneinde hem te confronteren met de informatie die door de verzoeker via elektronisch weg werd verstuurd of ontvangen.

[471] Artikel 57/27, lid 1 Vreemdelingenwet jo. Artikel 458 Strafwetboek

[472] Het gaat om informatie die wordt overgebracht aan de inlichtingen- en veiligheidsdiensten, de politiediensten, de procureur des Konings, de federale procureur, de onderzoeksrechter en Europese of internationale rechtbanken. Artikel 57/27, lid 2 Vreemdelingenwet

[473] Artikel 57/27, lid 2, 5) Vreemdelingenwet

[474] Artikel 48/9, §2, lid 2 Vreemdelingenwet

[475] Artikel 8, §1, lid 3 Koninklijk besluit van 11 juli 2003 houdende vaststelling van bepaalde elementen van de procedure die dienen gevolgd te worden door de dienst van de Dienst Vreemdelingenzaken die belast is met het onderzoek van de asielaanvragen op basis van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen

[476] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 63-64.

[477] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 72.

werd ingediend, mag worden meegedeeld aan de vermeende actoren van vervolging of ernstige schade (noch door het CGVS, noch door de Dienst Vreemdelingenzaken).[478]

Er wordt in de Vreemdelingenwet vooralsnog niet gespecifieerd hoe en of persoonsgegevens, door het CGVS verzameld van smartphones en sociale mediaprofielen, deel uitmaken van de dossiers van verzoekers OIB. Noch wordt duidelijkheid verschaft rond de manier waarop deze gegevens worden gedeeld en/of beveiligd, indien ze effectief worden opgenomen in de dossiers. Wel vermeldt de officiële website van het CGVS algemeen dat de nodige stappen worden ondernomen voor de beveiliging van de verwerkte persoonsgegevens. Het CGVS maakt gebruik van verschillende technische en organisatorische maatregelen om ervoor te zorgen dat de gegevens worden beschermd tegen onder meer ongeoorloofde toegang, onrechtmatig gebruik, verlies of ongeoorloofde wijzigingen.[479] Er doen zich echter een aantal specifieke complicaties voor in de context van het beveiligen van gegevens, verzameld via doorzoekingen van smartphones en sociale mediaprofielen, die niet door deze algemene verklaring bevat worden.

Een onvoorzichtige of ad-hoc analyse van sociale mediaprofielen kan ernstige gevolgen hebben voor de vertrouwelijkheid van de verzoekprocedure OIB. Wanneer bijvoorbeeld zoekacties naar sociale mediaprofielen vanop afstand worden uitgevoerd, kunnen deze traceerbaar zijn door overheden van herkomstlanden of andere actoren van vervolging of ernstige schade.[480] In Nederland wordt speciale software gebruikt door asielautoriteiten, om aan dit risico tegemoet te komen. Onderzoek op sociale mediaprofielen wordt enkel en alleen uitgevoerd op '*stand-alone* computers' met speciale accounts. Op deze manier zijn de zoekactiviteiten van de asielautoriteiten niet traceerbaar en zijn medewerkers die sociale mediaonderzoek uitvoeren niet verplicht om te zoeken via een eigen persoonlijk profiel of via het opzetten van een nepprofielen, zoals in andere landen reeds is gebeurd. De ontwikkeling van een dergelijk systeem vereist een investering en het personeel moet worden opgeleid om dergelijke beveiligde zoekacties uit te voeren.[481] Ook het onzorgvuldig doorzoeken van smartphones houdt risico's in voor de vertrouwelijkheid en integriteit van de verzoekprocedure, meer bepaald creëert het een risico dat gegevens gewijzigd of zelfs beschadigd worden. Zoals hierboven in '5.2.1.' reeds vermeld, kunnen door het manueel doorbladeren van een digitale gegevensdrager bijvoorbeeld de *time stamps* van foto's worden gewijzigd, met mogelijke gevolgen voor toekomstige strafprocedures.[482]

Artikel 32 AVG vermeldt bovendien dat adequate maatregelen ter beveiliging van de gegevens bijvoorbeeld kunnen bestaan uit het pseudonimiseren en versleutelen van persoonsgegevens en/of het regelmatig testen en evalueren van de effectiviteit van de maatregelen om ervoor te zorgen dat de

[478] Artikel 57/27, lid 3 Vreemdelingenwet
Artikel 10, §3 Koninklijk besluit van 11 juli 2003 houdende vaststelling van bepaalde elementen van de procedure die dienen gevolgd te worden door de dienst van de Dienst Vreemdelingenzaken die belast is met het onderzoek van de asielaanvragen op basis van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen

[479] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[480] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 84.

[481] Bolhuis, M. en van Wijk, J. "Practices in establishing the identity and screening on national security and exclusion aspects in Syrian asylum cases in five European countries." Migration Policy Practice (april-juni 2019). https://publications.iom.int/system/files/pdf/mpp_38.pdf. P. 14.

[482] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 89.

gegevensverwerking veilig is.[483] Ook bepaalt de wet dat bij het uitvoeren van deze maatregelen moet rekening gehouden worden met de risico's voor de rechten en vrijheden van de betrokkenen, vooral als gevolg van (onder andere) de wijziging of ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de gegevens, hetzij per ongeluk hetzij onrechtmatig.[484] Er zijn vooralsnog geen dergelijke waarborgen ter bescherming van de betrokkenen, zoals pseudonimisering, ingebouwd in de verzoekprocedure OIB. Rekening houdend met de specifieke situatie van verzoekers OIB (bijvoorbeeld wanneer zij opgespoord en/of vervolgd worden door autoriteiten in hun herkomstland), waardoor eventuele datalekken of misbruik van gegevens enorme gevolgen kunnen hebben voor hun veiligheid[485], worden in de huidige wettekst onvoldoende waarborgen ingebouwd om de veiligheid, vertrouwelijkheid en integriteit van het verwerkingsproces te garanderen. Deze tekortkoming in de wettekst werd tevens door de CBPL bevestigd in het advies omtrent de wetswijziging. Daarin stelt de Commissie namelijk dat het wetsontwerp geen uitsluitsel geeft over de vraag op welke manier de verstrekte digitale informatie wordt beveiligd.[486]

5.2.7. Onrechtmatigheid van de verwerking: drempel (zwaarwegend) algemeen belang niet bereikt

5.2.7.1. Publieke (gevoelige) persoonsgegevens: uitdrukkelijke openbaarmaking en algemeen belang

Wat de uitzondering van de 'uitdrukkelijke openbaarmaking'[487] betreft, kan worden aangenomen dat deze van toepassing is op gegevens op sociale mediaprofielen of andere online fora die door de betrokkene bewust voor iedereen publiek toegankelijk zijn gemaakt (artikel 57/7, §2 en artikel 48/6, §1, lid 4 van de Vreemdelingenwet).

Naast het voldoen aan de uitzondering op het principiële verbod op verwerking van gevoelige persoonsgegevens, moet de gegevensverwerking van publieke informatie echter ook kunnen worden gecategoriseerd onder de verwerkingsgrond 'taak van algemeen belang', om rechtmatig te zijn. Zoals uiteengezet in '5.2.2.', wordt het doorzoeken van sociale mediaprofielen en smartphones gekaderd binnen het algemeen belang van 'het vaststellen van de identiteit van verzoekers OIB'[488] of ruimer gesteld 'het beheer van en de controle op migratie'[489]. De voorbereidende werken van de wetswijziging bepalen daarnaast dat de nieuwe onderzoeksbevoegdheden van het CGVS moeten worden geplaatst binnen 'de strijd tegen misbruik van verzoekprocedures OIB'.[490] Het CGVS zelf stelt op de officiële website dat persoonsgegevens worden verwerkt 'in het kader van wettelijke verplichtingen, voor de

[483] Artikel 32 (1) AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 131.
[484] Artikel 32, lid 2 AVG
[485] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.
[486] Advies CBPL P. 9.
[487] Artikel 9 (2) e) AVG
[488] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 45 e.v.
[489] Latonero, M. en Kift, P. "On Digital Passages and Borders: Refugees and the New Infrastructure for Movement and Control." Social Media + Society (2018). https://journals.sagepub.com/doi/pdf/10.1177/2056305118764432. P. 7.
[490] Memorie van toelichting bij de wetswijziging P. 6 en 7.; Verslag 2 bij de wetswijziging P. 22.; Verslag 1 bij de wetswijziging P. 5.

vervulling van een taak van algemeen belang [en] voor de uitoefening van het openbaar gezag dat aan het CGVS is verleend'.[491]

Het feit dat het UNHCR en de Europese Toezichthouder voor Gegevensbescherming op algemene wijze erkennen dat voor bepaalde verwerkingsactiviteiten in het kader van verzoeken OIB een 'taak van algemeen belang' een voldoende verwerkingsgrond grond is[492], wil echter niet zeggen dat dit ook voor de specifieke doorzoekingen van sociale mediaprofielen en smartphones door het CGVS het geval is. Noch kan hieruit worden geconcludeerd dat de andere voorwaarden in artikel 6 (1) e) AVG zijn vervuld. Er werd reeds benadrukt dat, om onder de verwerkingsgrond van 'de taak van algemeen belang' te vallen, de gegevensverwerking effectief noodzakelijk moet zijn voor de uitoefening van het openbaar gezag.[493] Daarnaast moet de gegevensverwerking die wordt gerechtvaardigd door 'een taak van algemeen belang' een wettelijke grondslag hebben, die aan dezelfde voorwaarden voldoet als bij de verwerkingsgrond 'unie- of lidstaatrechtelijke wettelijke verplichting'.[494] Bijgevolg moet de wetsbepaling onder andere evenredig zijn met het nagestreefde gerechtvaardigde doel.[495] Ook beslaat deze verwerkingsgrond een zeer ruim toepassingsgebied, waardoor een strikte interpretatie en een duidelijke 'geval per geval' beoordeling moet plaatsvinden van het algemeen belang in kwestie.[496]

Naast de context van verzoekprocedures OIB, worden smartphones en sociale mediaprofielen ook door overheidsinstanties onderzocht onder het algemeen belang van 'de strafrechtspleging'.[497] Zo vormen in België de inbeslagname van digitale gegevensdragers en de zoekingen daarin een gangbare praktijk in het strafrechtelijk kader.[498] Dit vooropgesteld algemeen belang werd in de rechtspraak van het EHRM en het HvJ reeds als legitiem doel aanvaard.[499] Zelfs in het kader van de strafrechtspleging, worden dergelijke informaticazoekingen als zeer invasief beschouwd. De Belgische wetgever identificeert (digitale) zoekingen als een verregaande inbreuk op het privéleven van de betrokkene, waarvan de toepassing slechts in specifieke gevallen gerechtvaardigd is, mits inachtneming van wettelijke waarborgen.[500] Wat het doorzoeken van sociale mediaprofielen in het bijzonder betreft, oordeelde het Belgisch GWH, zoals reeds eerder vermeld, dat 'netwerkzoekingen'[501] in digitale gegevensdragers de tussenkomst van de onderzoeksrechter vereisen. Artikel 39bis, §3 van het Wetboek van Strafvordering,

---

[491] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[492] Zoals hierboven uiteengezet in '4.2.1.3.'; VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 1.; European Data Protection Supervisor (EDPS). "EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations) nr. 07/2016." (september 2016). https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf.. P. 17.

[493] Werkgroep gegevensbescherming artikel 29. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. P. 21-22.

[494] Artikel 6 (3) jo. overwegingen 41 en 45 AVG

[495] Artikel 6 (3) jo. overweging 45 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 152.

[496] Werkgroep gegevensbescherming artikel 29. "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC 844/14/EN WP 217." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. P. 22.

[497] Royer, S. en Oerlemans, J.J. "Naar een nieuwe regeling voor beslag op gegevensdragers." Computerrecht 2017/200 (2017). https://www.law.kuleuven.be/strafrecht/BijlagenNEDL/Sroyer_Computerrecht_2017_20.pdf. P. 280.

[498] Artikel 39bis Wetboek van Strafvordering

[499] EHRM, Saint-Paul Luxembourg S.A. t. Luxemburg, nr. 26419/10, 18 april 2013. § 42.; EHRM, Sérvulo en Associado-Sociedade de Advogados, RL e.a. t. Portugal, nr. 27013/10, 3 september 2015. § 97.; EHRM Posevini t. Bulgarije, nr. 63638/14, 19 januari 2017. § 68.; EHRM, Cacuci en S.C. Virra & Cont Pad S.R.L. t. Roemenië, nr. 27153/07, 17 januari 2017. § 91.; HvJ, C-293/12 en C-594/12, Digital Rights Ireland Ltd t. Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a., 2014. § 42 en 44.

[500] Advies CBPL P. 7.

[501] Royer, S. en Oerlemans, J.J. "Naar een nieuwe regeling voor beslag op gegevensdragers." Computerrecht 2017/200 (2017). https://www.law.kuleuven.be/strafrecht/BijlagenNEDL/Sroyer_Computerrecht_2017_20.pdf. P. 278.

dat geen dergelijk bevel van de onderzoekrechter voorziet, werd ongrondwettig bevonden, aangezien deze vorm van zoeking volgens het Hof een even grote impact heeft op het privéleven als een huiszoeking.[502] In dezelfde lijn werd, tijdens de voorbereidingen van de wetswijziging, het doorzoeken van digitale informatie over de verzoeker OIB omschreven als 'een digitale huiszoeking'.[503] Ook in het baanbrekende Amerikaanse arrest 'Riley t. Californië' werd uitgelicht dat gegevens op een mobiele telefoon niet immuun zijn voor een digitale zoeking, maar dat er over het algemeen wel een bevelschrift voor nodig is, zelfs in het geval van een officiële arrestatie.[504]

De verwerking van gegevens op sociale mediaprofielen en smartphones van verzoekers OIB door het CGVS kan echter niet worden gestoeld op een redelijke verdenking van het plegen van een strafbaar feit. De gegevensverwerking wordt uitsluitend in het algemeen belang van 'het beheer van en de controle op migratie' uitgevoerd en de onderzoeksbevoegdheid van het CGVS heeft het loutere doel om het onrechtmatig toekennen van internationale bescherming te voorkomen. Dat dit vooropgestelde algemeen belang evenveel rechtvaardiging zou bieden voor een dermate ingrijpende praktijk als het algemeen belang van 'de strafrechtspleging', is sterk te betwijfelen. Het is namelijk niet te vergelijken met een maatregel die is genomen om ernstige strafbare feiten te voorkomen op basis van concrete verdenkingen.[505] Het doorzoeken van sociale mediaprofielen en smartphones kan zinvol zijn bij het vervolgen van misdrijven, maar het toepassen van deze praktijk op vreemdelingen, die in kwetsbare omstandigheden op zoek zijn naar internationale bescherming, opent de deur voor vrijelijk 'datagraaien' naar informatie die erg gevoelig is voor misinterpretatie.[506] Het is moeilijk om zich een maatschappelijke groep voor de geest te halen, wiens gegevensbeschermings- en privacyrechten op dermate indringende wijze worden beperkt, zonder aanwezigheid van enige strafrechtelijke verdenking of rechterlijke controle.[507] Het Duitse GWH oordeelde hieromtrent reeds dat de toegang tot digitale gegevensdragers door overheidsinstanties niet is toegestaan om eender welk algemeen belang te dienen, maar alleen voor de bescherming van 'bijzonder belangrijke juridische belangen'. Het algemeen belang van 'het beheer van en de controle op migratie' kan niet op overtuigende wijze op hetzelfde niveau worden geplaatst als de preventie of vervolging van ernstigste misdrijven.[508]

Los van de inhoudelijke zwaarwichtigheid van het vooropgestelde algemeen belang van 'het beheer van en de controle op migratie', moet de maatregel dit algemeen belang logischerwijze ook effectief dienen. Er moet namelijk een redelijk en reëel verband bestaan tussen de aangevoerde taak van algemeen belang

---

[502] GWH nr. 174/2018 van 6 december 2018. § B.14.1.

[503] Amendement 1 bij de wetswijziging P. 2.; Verslag 2 bij de wetswijziging P. 19.

[504] Supreme Court of the United States (SCOTUS), Riley t. Californië, nr. 13–132, 25 juni 2014. https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf. P. 2-3.

[505] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 25.; VN- Hoog Commissariaat voor de Vluchtelingen. "Note on Burden and Standard of Proof in Refugee Claims." (december 1998). https://www.refworld.org/docid/3ae6b3338.html. P. 5.

[506] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 6.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 89.

[507] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 6.; Necessary & Proportionate. "International Principles on the Application of Human Rights to Communications Surveillance." Necessary & Proportionate (mei 2014). https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. P. 8.

[508] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 9.

en de maatregelen van gegevensverwerking om deze taak als legitiem te kunnen beschouwen.[509] Analyses van de doorzoekingen van smartphones door de Duitse asielautoriteit brachten echter aan het licht dat dergelijke doorzoekingen in de praktijk slechts zeer zelden ten dienste staan van dit algemeen belang en van de doelstelling om misbruik van de verzoekprocedure OIB te voorkomen.[510] Men stelde vast dat ongeveer een vierde van de rapporten met geëxtraheerde digitale gegevens van smartphones technisch onbruikbaar was. Van de overgebleven technisch bruikbare rapporten was de inhoud maar in minder dan de helft van de gevallen functioneel bruikbaar. Van de zowel technisch als inhoudelijk bruikbare rapporten, resulteerde de evaluatie ervan slechts in 1 à 2% van de gevallen in een tegenstrijdigheid met de door de verzoeker zelf verstrekte informatie. In alle andere gevallen bevestigde het gegevensrapport de verklaringen van de verzoeker.[511] De aanname, dat verzoekers OIB op grote schaal zouden misbruik maken van de verzoekprocedures of zich schuldig zouden maken aan documentvervalsing, kan dus niet worden bevestigd.[512] Bijgevolg ontkrachten bovenstaande cijfers niet alleen deze misvatting, maar ook de door de wetswijziging vooropgestelde 'taak van algemeen belang' om 'misbruik van verzoekprocedures OIB te bestrijden'[513], die op deze misvatting is gebaseerd. In tegenstelling tot deze vaststelling, vereist de Europese Toezichthouder voor Gegevensbescherming nochtans dat het vooropgestelde 'probleem', dat met de maatregel tracht te worden aangepakt, concreet is en niet slechts hypothetisch. Om deze reden moet het bestaan van het probleem objectief worden aangetoond met bewijsmateriaal dat kan bestaan uit feiten of statistische gegevens, dat wetenschappelijke verificatie mogelijk maakt en dat het bestaan van het probleem op overtuigende wijze ondersteunt.[514]

Een andere vaststelling, die de effectiviteit van het doorzoeken van smartphones substantieel kan verhinderen, is dat technologieën die bedoeld zijn om migratie te controleren, uiteindelijk het gedrag van migranten gaat beïnvloeden doordat zij zich aan de maatregelen aanpassen.[515] Er werd namelijk reeds vastgesteld dat verzoekers OIB, eens zij zich bewust zijn van de onderzoeksstrategieën van nationale asielautoriteiten, op een interview verschijnen zonder een smartphone of andere digitale gegevensdragers bij zich.[516] Het omzeilen van de maatregel kan eenvoudigweg door het ontkennen van het bezit van een smartphone (of andere gegevensdragers).[517] Door het hoge percentage onbruikbare gegevensrapporten en de lage bewijswaarde voor misbruik van de bruikbare resultaten enerzijds, en de makkelijke omzeilbaarheid van de maatregel anderzijds, is de mate waarin het doorzoeken van smartphones effectief ten dienste staat van het vooropgestelde algemeen belang uiterst minimaal.

---

[509] EHRM, Rotaru t. Roemenië, nr. 28341/95, 4 mei 2000. Concurring Opinion of Judge Wildhaber.

[510] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 31.

[511] Ibid. P. 5-6 en 28-30.

[512] Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.

[513] Memorie van toelichting bij de wetswijziging P. 6 en 7.; Verslag 2 bij de wetswijziging P. 22.; Verslag 1 bij de wetswijziging P. 5.

[514] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 8 en 15.

[515] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.

[516] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 83 en 87.

[517] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 28-29.

Uit het bovenstaande kan dus worden geconcludeerd dat 'het beheer van en de controle op migratie' als voldoende 'taak van algemeen belang', in het licht van artikel 6 (1) e) AVG, sterk in twijfel moet worden getrokken. Zelfs indien dit algemeen belang in overweging wordt genomen, moet worden vastgesteld dat de mate waarin doorzoekingen van smartphones en sociale mediaprofielen dit algemeen belang ook effectief dienen, verwaarloosbaar is. Daarnaast bevat artikel 6 (1) e) AVG nog andere vereisten. Het moet namelijk ook gaan om een maatregel die effectief noodzakelijk is voor de vervulling van de taak van algemeen belang en die daarmee evenredig is. Deze vereisten worden verder besproken onder '5.3.2.1.' en '5.3.2.2.'.

5.2.7.2. Private (gevoelige) persoonsgegevens: zwaarwegend algemeen belang

Wat de private gegevens op smartphones en sociale mediaprofielen betreft, is de uitzonderingsgrond van 'het zwaarwegend algemeen belang'[518] van toepassing. De grens om van 'redenen van zwaarwegend algemeen belang' te kunnen spreken ligt vanzelfsprekend hoger dan bij de algemene verwerkingsrond van 'het algemeen belang'. Hierboven, in '5.2.7.1.', werd reeds vastgesteld dat *in casu* niet op overtuigende wijze kan gesproken worden van een 'taak van algemeen belang'. Bijgevolg moet worden geconcludeerd dat ook de hogere grens van het 'zwaarwichtig algemeen belang' niet wordt bereikt.

5.3. Niet-gerespecteerde voorwaarden voor beperkingen op het recht op privacy en gegevensbescherming

5.3.1. Ontbreken van een gerechtvaardigd doel

Voor de beoordeling of het doorzoeken van smartphones en sociale mediaprofielen van verzoekers OIB door het CGVS een gerechtvaardigd doel nastreeft, wordt verwezen naar de uiteenzetting onder '5.2.7.1.'. De analyse of de gegevensverwerking door het CGVS al dan niet een 'taak van algemeen belang' vormt in de zin van de AVG kan namelijk in nauw verband worden gebracht met de beoordeling van het 'gerechtvaardigd doel', in de zin van het EU-Handvest en het EVRM[519]. Deze verwantschap werd reeds bevestigd door de WGA29[520] en de Europese Toezichthouder voor Gegevensbescherming[521]. In lijn met de analyse rond de 'taak van algemeen belang', moet worden geconcludeerd dat 'het beheer van en de controle op migratie' ook niet als voldoende 'gerechtvaardigd doel' kan worden beschouwd.

5.3.2. Noodzaak en proportionaliteit in een democratische samenleving

5.3.2.1. Niet-noodzakelijkheid in een democratische samenleving

De noodzakelijkheidstoets, zowel vermeld in het EU-Handvest als in het EVRM[522], vereist ten eerste dat de gegevensverwerking werd voorzien om tegemoet te komen aan een 'dringende maatschappelijke behoefte'[523], die het functioneren van de samenleving op problematische wijze verhindert.[524] Tevens moet de maatregel relevant en geschikt zijn om bij te dragen tot de dringende maatschappelijke behoefte

[518] Artikel 9 (2) g) AVG
[519] artikel 52 (1) en (3) EU-Handvest; artikel 8 (2) EVRM
[520] Werkgroep gegevensbescherming artikel 29. "Advice paper on special categories of data ("sensitive data") Ref. Ares(2011)444105." (2011). https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. P. 11.
[521] European Data Protection Supervisor (EDPS). "A Preliminary Opinion on data protection and scientific research." (2019). https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf. P. 23.
[522] artikel 52 (1) en (3) EU-Handvest; artikel 8 (2) EVRM
[523] EHRM, Leander t. Zweden, nr. 9248/81, 26 maart 1987. §58.
[524] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 15

en het nagestreefde doel.[525] Ten tweede moet, in het licht van de individuele verwerkingsactiviteiten, telkens worden vastgesteld dat het vooropgestelde doel niet kan worden bereikt met minder ingrijpende maatregelen.[526]

Wat het bewijsmateriaal betreft voor het aantonen van het bestaan van een 'dringende maatschappelijke behoefte'[527], wordt verwezen naar de eerdere uiteenzetting onder '5.2.7.1.'. Hier werd reeds verduidelijkt hoe de aanname dat verzoekers OIB op grote schaal zouden misbruik maken van de verzoekprocedures of zich schuldig zouden maken aan documentvervalsing niet kan worden bevestigd.[528] Nochtans verduidelijkt de WGA29 het begrip 'dringende maatschappelijke behoefte' als volgt. Bij het evalueren van de noodzakelijkheid van een maatregel, moeten volgende vragen affirmatief kunnen worden beantwoord: 'Is de maatregel bedoeld om aan een probleem tegemoet te komen dat, als het niet wordt aangepakt, kan leiden tot schade of tot een of ander negatief effect op de samenleving of een deel van de samenleving?' en 'Is er enig bewijs dat de maatregel dergelijke schade kan beperken?'.[529] Er moet worden vastgesteld dat, voor doorzoekingen in sociale mediaprofielen en smartphones van verzoekers OIB, niet op beide vragen positief kan worden geantwoord. Daarnaast zijn ook nergens in de parlementaire voorbereidingen van de wetswijziging sporen te vinden van een beoordeling van de strikte noodzakelijkheid van de onderzoeksbevoegdheid van het CGVS, wat in de rechtspraak van het EHRM reeds werd beschouwd als een hindernis voor het vervullen van de noodzakelijkheidsvereiste.[530]

Daarnaast moet ook worden besloten dat het doorzoeken van sociale mediaprofielen en smartphones van verzoekers OIB een ongeschikte maatregel is ten aanzien van de vooropgestelde doelstelling. Opnieuw zoals uiteengezet in '5.2.7.1.', werd vastgesteld dat heel wat rapporten met geëxtraheerde digitale gegevens van smartphones technisch onbruikbaar zijn en dat van de overgebleven technisch bruikbare rapporten, de inhoud maar in minder dan de helft van de gevallen functioneel bruikbaar is.[531] Daarnaast werd in de praktijk reeds geobserveerd hoe verzoekers OIB, eens zij zich bewust zijn van de onderzoeksstrategieën van nationale asielautoriteiten, op een interview verschijnen zonder een smartphone of andere digitale gegevensdragers bij zich.[532] Het is dus sterk te betwijfelen of deze

[525] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 40.
[526] Ibid. P. 46
[527] Werkgroep gegevensbescherming artikel 29. "Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 536/14/EN WP 211." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. P. 8.
[528] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 5-6 en 28-30.; Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.
[529] Werkgroep gegevensbescherming artikel 29. "Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 536/14/EN WP 211." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. P. 8.
[530] EHRM, Szabo & Vissy t. Hongarije, nr. 37138/14, 12 januari 2016. §89.
[531] De inhoudelijke bruikbaarheid van dergelijke rapporten kan bijvoorbeeld worden verhinderd doordat de database te klein is (als een mobiele telefoon lange tijd niet is gebruikt), doordat de gegevens tegenstrijdig zijn (als de mobiele telefoon door meerdere personen tegelijk of na elkaar is gebruikt, zonder dat alle inhoud is gewist bij het doorgeven van het apparaat) of doordat de verzoeker de smartphone pas in het land van bestemming heeft aangekocht (in dat geval zijn de geodata uiteraard waardeloos omdat geen enkele locatie buiten dat land kan worden bepaald).
Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 5-6 en 28-30.
[532] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 83 en 87.

maatregel effectief geschikt is om betrouwbare aanwijzingen te verzamelen over de identiteit en de herkomst van verzoekers OIB. Daarnaast bekritiseerde de WGA29 reeds hoe bepaalde maatregelen van digitale controle op migratie wel het vooropgestelde misbruik in migratieprocedures opsporen, maar geen van de onderliggende oorzaken ervan op holistische wijze aanpakken. Los van het eventueel licht afschrikkend effect van de maatregel, wordt het beweerde aantal misbruiken zelf er niet door verminderd.[533] In dezelfde lijn kan worden gesteld dat de onderzoeksbevoegdheid van het CGVS in de Belgische Vreemdelingenwet ongeschikt is ten aanzien van het vooropgestelde doel om misbruik van verzoekprocedures OIB te bestrijden[534].

In het licht van de individuele verwerkingsactiviteiten, moet telkens worden vastgesteld dat het vooropgestelde doel niet kan worden bereikt met minder ingrijpende maatregelen.[535] Hierover is de wetswijziging beknopt. Artikel 57/7, §2 van de Vreemdelingenwet vermeldt enkel dat de maatregel zal gebruikt worden 'voor de beoordeling van het verzoek om internationale bescherming'. Artikel 48/6, §1, lid 4 van de Vreemdelingenwet vermeldt dat de maatregel kan worden aangewend 'indien de met het onderzoek van het verzoek belaste instanties goede redenen hebben om aan te nemen dat de verzoeker […] elementen achterhoudt die essentieel zijn voor een correcte beoordeling van het verzoek'. Wat met deze 'goede redenen' precies wordt bedoeld, is een gegeven dat aan het vrije oordeel van het CGVS is onderworpen en dus voorwerp blijft van speculatie.[536] In het tweede verslag omtrent de wetswijziging wordt verduidelijkt dat het in elk geval niet de bedoeling is om een systematische controle van de digitale apparatuur van verzoekers in te voeren[537], wat wijst op de intentie om de noodzaak van de maatregel geval per geval te beoordelen.[538]

De noodzakelijkheid van de toegang tot de privégegevens en communicatie van de verzoeker OIB is dus enkel gebaseerd op de subjectieve en moeilijk te evalueren beoordelingsbevoegdheid van het CGVS.[539] In Duitsland wordt bijvoorbeeld wel expliciet vermeld in de wettekst dat de doorzoeking enkel is toegestaan indien 'het doel van de maatregel niet met mildere middelen kan worden bereikt'[540]. Desalniettemin werd ook in de praktijk van de Duitse asielautoriteit reeds vastgesteld dat de gegevens vanop digitale gegevensdragers niet alleen worden gelezen en gekopieerd wanneer andere middelen zijn uitgeput, maar routinematig al bij het eerste contact met een verzoeker OIB.[541] De informatie nodig 'om verzoeken OIB correct te kunnen beoordelen', kan echter wel degelijk op minder ingrijpende wijze worden verkregen. Het onderzoeken van smartphones van verzoekers brengt namelijk gegarandeerd meer informatie aan het licht dan nodig is voor het beoordelingsproces.[542] De meer gebruikelijke technieken, zoals een interview in verband met de herkomst en het asielrelaas van de verzoeker OIB, blijven minder verregaande maatregelen. De informatie die tijdens deze interviews wordt verstrekt, kan

[533] Werkgroep gegevensbescherming artikel 29. "Opinion 05/2013 on Smart Borders 00952/13/EN WP206." (2013). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf. P. 10.
[534] Memorie van toelichting bij de wetswijziging P. 6 en 7.; Verslag 2 bij de wetswijziging P. 22.; Verslag 1 bij de wetswijziging P. 5.
[535] Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 46
[536] Verslag 1 bij de wetswijziging P. 54.
[537] Verslag 2 bij de wetswijziging P. 4 en 9.
[538] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 81.
[539] Advies CBPL P. 7.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 22.
[540] Artikel 15a (1) Asylgesetz (Duitse Vreemdelingenwet)
[541] Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.
[542] Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.

op nauwkeurige wijze worden gecontroleerd aan de hand van specifieke vragen.[543] Een inperking van het recht op gegevensbescherming of privacy kan alleen legitiem zijn als laatste redmiddel en kan dus alleen worden goedgekeurd als alle andere maatregelen hebben gefaald. Bijgevolg zou het doorzoeken van sociale mediaprofielen en smartphones slechts te rechtvaardigen zijn, indien het interview met de verzoeker tot geen enkel (waarheidsgetrouw) resultaat zou leiden omtrent diens herkomst, identiteit en asielrelaas.

Hieruit kan ten eerste worden geconcludeerd dat de noodzakelijkheid van de maatregel ten opzichte van het vooropgestelde doel om misbruik van verzoekprocedures OIB te bestrijden niet kan worden bewezen of aangetoond en ook niet voldoet aan de drempel van 'een dringende maatschappelijke behoefte'. Ten tweede zijn doorzoekingen in sociale mediaprofielen en smartphones niet geschikt ten aanzien van dit beweerd gerechtvaardigd doel. Ten derde voorziet de wettekst ook voor de individuele gegevensverwerkingen onvoldoende toetsingsplicht van de vraag of het vooropgestelde doel niet kan worden bereikt met minder ingrijpende maatregelen. De noodzakelijkheidsvereiste in het EU-Handvest en het EVRM is dus op onvoldoende wijze vervuld.

5.3.2.2. Disproportionaliteit in een democratische samenleving

Om proportioneel te zijn, moet een maatregel 'een redelijk of eerlijk evenwicht' bewerkstelligen tussen de belangen en/of rechten van de partijen die bij de uitvoering ervan betrokken zijn.[544] De voordelen die voortvloeien uit de inperking van het fundamenteel recht moeten opwegen tegen de nadelen die deze inperking met zich meebrengt voor de uitoefening van het recht door de betrokkene.[545] Ten eerste moeten dus de nadelen of beperkingen van de betrokkene, met betrekking tot de uitoefening van diens recht op gegevensbescherming en privacy, worden beoordeeld. De gevolgen van onnauwkeurige beoordelingen of interpretaties van gegevens op sociale mediaprofielen en smartphones kunnen fataal zijn[546], aangezien deze kunnen leiden tot de ongeloofwaardigheid van de verklaringen van verzoekers en dus tot het in gevaar brengen van hun verzoek OIB.[547] De Belgische Vreemdelingenwet bepaalt namelijk dat een verzoek OIB als kennelijk ongegrond kan worden beschouwd op grond van 'het feit dat de verzoeker kennelijk incoherente en tegenstrijdige, kennelijk valse of duidelijk onwaarschijnlijke verklaringen heeft afgelegd […]'.[548] Bijgevolg lopen verzoekers OIB het risico op bijvoorbeeld een uitzetting in strijd met het non-refoulementbeginsel[549].[550] Daarbovenop zorgt de specifieke situatie van verzoekers OIB (bijvoorbeeld wanneer zij opgespoord en/of vervolgd worden door autoriteiten in hun herkomstland) ervoor dat eventuele datalekken of misbruik van gegevens enorme gevolgen kunnen hebben voor hun veiligheid.[551]

---

[543] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 25.

[544] White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl. P. 36.

[545] European Data Protection Supervisor (EDPS). "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit." (april 2017). P. 5.

[546] De waarschijnlijkheid hiervan werd uiteengezet in '5.2.4.'.

[547] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 6 en 33.

[548] Artikel 57/6, §1, 2° jo. artikel 57/6/1, §2 jo. artikel 57/6/1, §1, e) Vreemdelingenwet

[549] Zie voetnoot 116

[550] White, M. "Immigration Exemption and the European Convention on Human Rights." European Data Protection Law Review (EDPL) vol. 5, no. 1 (2019). https://heinonline.org/HOL/Page?handle=hein.journals/edpl5&id=32&collection=journals&index=journals/edpl. P. 30.

[551] Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018).

Daarnaast wordt de rechtspositie van de betrokken verzoekers substantieel ingeperkt door de grote hoeveelheid informatie die terug te vinden is op elektronische dragers. Hieronder bevinden zich data die geen directe relevantie hebben voor het beoordelen van het verzoek[552], waardoor ongelimiteerde toegang tot digitale informatie van verzoekers als een onevenredige inmenging in het privéleven van de verzoeker wordt beschouwd.[553] De gemakkelijke toegang tot elektronische gegevens rechtvaardigt volgens de het UNHCR geen ongeconcentreerd, ongedifferentieerd of speculatief zoeken naar informatie.[554] Ook in Duitsland werd de maatregel als disproportioneel beoordeeld, gezien deze kan leiden tot het doorzoeken van het uiterst persoonlijke domein van de betrokken personen en er derden bij zouden kunnen worden betrokken die met deze personen in contact stonden.[555] Voorts moet bij de evenredigheidstoets rekening worden gehouden met factoren als de omvang van de inperking (vb. het aantal betrokken personen) en de waarborgen die zijn ingebouwd om de impact ervan te beperken of de schadelijke gevolgen voor de rechten van personen te beperken.[556] Hieromtrent kan worden vastgesteld dat het aantal betrokkenen enorm is, aangezien de maatregel theoretisch gezien op elke verzoeker OIB kan worden toegepast. Daarenboven worden bij het screenen van sociale mediaprofielen en smartphones ook de persoonsgegevens verwerkt van alle personen, met wie de verzoeker (al dan niet gewenst) in contact staat.[557] Ook zijn weinig of geen waarborgen ingebouwd om de impact op het recht op gegevensbescherming te minimaliseren, zoals uiteengezet in '5.2.'.

Ten tweede moeten de voordelen die voortvloeien uit de inperking van het fundamenteel recht worden geanalyseerd. Hierboven, in '5.2.7.1.', werd reeds uiteengezet hoe, in de praktijk van de Duitse asielautoriteiten, van de bruikbare gegevensrapporten slechts 1 à 2% van de gevallen in een tegenstrijdigheid met de door de verzoeker zelf gegeven verklaringen resulteerde.[558] Bijna twee derde van de gegevensrapporten identificeerde geen relevante inhoud met betrekking tot identiteit en herkomst.[559] Ook in de VS concludeerde men dat de informatie op sociale media in de overgrote meerderheid van de gevallen weinig tot geen nut of effect heeft voor de procedure.[560] De waarde van sociale mediagegevens in het bijzonder vormt ook vaak een bron van discussie en is slechts van beperkt nut wanneer niet-gespecialiseerde medewerkers dataverzamelingen op sociale media uitvoeren.[561] De

https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 3.

[552] Hierover werd uitgeweid onder '5.2.3.'.

[553] Amendement 1 bij de wetswijziging P. 2.; Verslag 2 bij de wetswijziging P. 25.

[554] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2.

[555] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 51.

[556] Werkgroep gegevensbescherming artikel 29. "Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 536/14/EN WP 211." (2014). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf. P. 9-11.

[557] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 6 en 14. Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.; EHRM, Szabo & Vissy t. Hongarije, nr. 37138/14, 12 januari 2016. §89.

[558] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 5-6 en 28-30.

[559] Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.

[560] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 31 en 34.

[561] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-

gegevens die van sociale mediaprofielen en smartphones worden geëxtraheerd vormen dus zwak bewijsmateriaal. Dit lage 'succespercentage'[562] en het feit dat de maatregel in het beste geval slechts een indicatie geeft van de identiteit of de herkomst van de verzoeker[563], roepen terecht vragen op over de waarde van het concentreren van middelen op het verzamelen en analyseren van dit soort gegevens. In verhouding tot het beperkte voordeel van het doorzoeken van smartphones, zijn de kosten voor het systeem namelijk onevenredig hoog. In februari 2017 verklaarde het Duitse Ministerie van Binnenlandse Zaken bijvoorbeeld dat er eenmalige installatiekosten van 3,2 miljoen euro te verwachten waren voor de uitleesapparatuur, wat de oorspronkelijke verwachtingen bij het opstellen van wetsvoorstel duidelijk overtrof.[564]

Uit bovenstaande vaststellingen kan dus worden geconcludeerd dat de verhouding tussen de aantasting van de grondrechten van de betrokken verzoekers OIB en het nut van de doorzoekingen in hun smartphones en sociale mediaprofielen duidelijk onevenwichtig is. Hierbij wordt nog abstractie gemaakt van de inperking op het recht op gegevensbescherming van alle andere personen, van wie gegevens worden teruggevonden naar aanleiding van voormelde doorzoekingen. De ernstige nadelen voor de betrokkene bij een onnauwkeurige beoordeling van hun verzoek en de ongelimiteerde en verregaande raadpleging van hun persoonlijke gegevens en communicatie wegen onmogelijk op tegen de gegevensrapporten met minimale bewijswaarde, die het resultaat vormen van deze doorzoekingen. Op de officiële website van het CGVS verbindt het Commissariaat zich ertoe om enkel persoonsgegevens te verwerken die 'niet buitensporig zijn in verhouding tot de doeleinden waarvoor ze zijn verzameld'.[565] Deze verbintenis indachtig, moet dus de vraag worden gesteld of het extraheren van gegevens op sociale mediaprofielen en smartphones in het licht van de proportionaliteitstoets wel mogelijk is.

5.3.3. Disrespect voor de wezenlijke inhoud van de fundamentele rechten

De beperkingsclausules voor het recht op gegevensbescherming in artikel 52 (1) en (3) EU-Handvest en artikel 8 (2) EVRM bepalen dat inperkingen die zo ingrijpend zijn dat ze de kern of basisinhoud van het fundamenteel recht ontnemen, waardoor het individu het recht in essentie niet kan uitoefenen, niet te rechtvaardigen zijn. Het doorzoeken van smartphones en sociale mediaprofielen is een praktijk die zowel door de CBPL[566], het UNHCR[567], als door een platform van zeven Belgische ngo's[568] terecht als 'een praktijk met hoog risico tot schending van de rechten en vrijheden van natuurlijke personen' wordt gekwalificeerd. De wettekst van de Vreemdelingenwet hieromtrent voorziet echter geen garanties om de kern of basisinhoud van het fundamenteel recht op gegevensbescherming te waarborgen. Noch wordt

content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 83.

[562] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 31.

[563] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 51.

[564] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 34.

[565] "Privacy – Persoonsgegevens". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgvs.be/nl/privacy-persoonsgegevens.

[566] Advies CBPL P. 4.

[567] Advies UNHCR P. 6.; Verslag 2 bij de wetswijziging P. 3.

[568] 11.11.11, CNCD-11.11.11, Amnesty International Belgique Francophone, Amnesty International Vlaanderen, CIRÉ, Liga voor mensenrechten, Ligue des droits de l'Homme, Orbit, Platform kinderen op de vlucht - Plate-Forme Mineurs en Exil, Point d'Appui en Vluchtelingenwerk Vlaanderen
"Vandaag stemt de Kamer over wetsontwerpen die onze asielwetgeving ingrijpend wijzigen". www.vluchtelingenwerk.be. Vluchtelingenwerk Vlaanderen, 9 november 2017. https://www.vluchtelingenwerk.be/nieuws/vandaag-stemt-de-kamer-over-wetsontwerpen-die-onze-asielwetgeving-ingrijpend-wijzigen.

verduidelijkt in welke mate het CGVS bij het doorzoeken van sociale mediaprofielen en smartphones ook effectief de inhoud van de persoonlijke informatie en communicatie van de verzoeker zal raadplegen. De impact voor 'de wezenlijke inhoud' van het recht op gegevensbescherming wordt hieronder dus in beide gevallen beoordeeld, zowel in het geval van effectieve toegang tot de inhoud, als het geval waarbij geen inhoudelijke analyse wordt uitgevoerd.

In de rechtspraak van het HvJ, werd reeds geoordeeld dat wetgeving die de overheid in staat stelt om op algemene wijze toegang te krijgen tot de inhoud van elektronische communicatie moet worden beschouwd als een aantasting van de essentie van het grondrecht op privacy.[569] Omgekeerd stelde het Hof dat de essentie van het recht op privacy niet wordt aangetast, indien bepaalde wetgeving het niet mogelijk maakte kennis te verwerven over de inhoud van elektronische communicatie (maar alleen over 'metagegevens').[570] Deze rechtspraak indachtig, erkende ook de Oostenrijkse Minister van Binnenlandse Zaken bijvoorbeeld, tijdens de voorbereidende fase van een gelijkaardige wetswijziging als de Belgische, dat men niet van plan is om de inhoud van persoonlijke communicatie te raadplegen, aangezien dit problematisch zou zijn onder het grondwettelijk recht.[571] Desondanks bevat de uiteindelijk doorgevoerde wetswijziging in Oostenrijk deze beperking niet.[572] Ook de huidige Belgische wettekst bevat geen beperking op de soorten digitale informatie die kunnen worden verwerkt, noch regelt de wetswijziging precies hoe de gegevens zullen worden behandeld.[573]

Met betrekking tot het geval waarbij geen inhoudelijke analyses worden uitgevoerd, kan het doorzoekingssysteem van de Duitse asielautoriteit als voorbeeld dienen. Informatie op een digitale gegevensdrager wordt daar automatisch geanalyseerd, samengevoegd in een resultatenrapport en volgens de Duitse asielautoriteit worden de ruwe gegevens onmiddellijk na het aanmaken van het resultatenrapport gewist.[574] Daarnaast bevat de Duitse wettekst de bepaling 'als er concrete aanwijzingen zijn om te veronderstellen dat het doorzoeken van gegevensdragers enkel inzicht zou geven in het kerngebied van het privéleven, is de maatregel niet toegestaan'.[575] Deze waarborg is gebaseerd op een bepaling in de Duitse Grondwet[576], die voorschrijft dat 'een fundamenteel recht in geen geval in zijn essentie mag worden aangetast'. In een recente zaak voor het EHRM, herinnerde een van de raadsheren van het Hof er zelfs aan dat het concept van 'de kern of basisinhoud van een fundamenteel recht' zijn oorsprong vindt in de Duitse Grondwet.[577] De Duitse Federale Commissaris voor Gegevensbescherming en Vrijheid van Informatie stelt hieromtrent dat zelfs buitengewone openbare belangen geen rechtvaardiging kunnen vormen voor overheidsinmenging in dit absoluut beschermde gebied van het privéleven. De bescherming van dit kerngebied moet daarom zowel worden gewaarborgd op het niveau van het verzamelen van de gegevens, als op het niveau van het raadplegen van de inhoud ervan, door

[569] HvJ, C-362/14, Schrems, 2015. § 94.
[570] HvJ, C-293/12 en C-594/12, Digital Rights Ireland Ltd t. Minister for Communications, Marine and Natural Resources e.a. en Kärntner Landesregierung e.a., 2014. § 39.
[571] Hagen, L. "Kickl will Flüchtlinge "konzentriert" an einem Ort halten". www.derstandard.at. Der Standard, 11 januari 2018. https://www.derstandard.at/story/2000071880249/asyl-fpoe-kickl-will-fluechtlinge-konzentriert-an-einem-ort-halten.
[572] Thüer, L., Fanta, A. en Köver, C. "Asylum Procedure: Cell Phone Search Has No Benefits". www.unhcr.org/blogs. UNHCR Blogs, 16 juli 2018. https://www.unhcr.org/blogs/asylum-procedure-cell-phone-search-no-benefits/.
[573] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 45.
[574] Ibid. P. 12.
[575] Artikel 48, 3a, 2 Aufenthaltsgesetz (Duitse Verblijfswet)
[576] Artikel 19 (2) Grundgesetz für die Bundesrepublik Deutschland (Duitse Grondwet)
[577] EHRM, Naït-Liman t. Zwitserland, nr. 51357/07, 15 maart 2018. Partly dissenting opinion of Judge Wojtyczek.; Van Drooghenbroeck, S. en Rizcallah, C. "The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?" German Law Journal 20 (2019). https://www.cambridge.org/core/services/aop-cambridge-core/content/view/594CA9F2A83DF4B52A1FB6B638339FB4/S2071832219000683a.pdf/echr_and_the_essence_of_fundamental_rights_searching_for_sugar_in_hot_milk.pdf. P. 907.

middel van passende maatregelen.[578] Zelfs als de ruwe verzamelde gegevens worden verwijderd nadat het gegevensrapport is opgesteld, heeft de inperking op het recht op gegevensbescherming reeds plaatsgevonden, door de analyse ervan. Vanwege deze laatste vaststelling, bekritiseerde voormelde Commissaris de Duitse wettekst, die het kerngebied van het privéleven onvoldoende zou beschermen.[579] Voldoende waarborgen zouden bestaan in een 'upstreamcontrole' om te verzekeren dat het verzamelen van gegevens uit het kerngebied van het privéleven in ieder geval wordt uitgesloten. Wanneer absoluut niet kan worden vermeden dat dergelijke kerninformatie wordt verzameld, vereist de Duitse Commissaris een controle van de gegevens door een onafhankelijke instantie, waarbij de meest gevoelige en persoonlijke gegevens uitgefilterd worden. [580]

De Duitse wettekst bevat echter geen dergelijke waarborgen. Meer nog, de wettekst faalt in het beschermen van het kerngebied van het privéleven door de formulering dat de gegevensverwerking alleen dan verboden is wanneer 'enkel' gegevens uit dit kerngebied worden verzameld. Gevallen waarin 'uitsluitend' informatie uit het kerngebied van het privéleven zou worden verkregen, zijn namelijk moeilijk voor de geest te halen in de context van sociale mediaprofielen en smartphones. In de praktijk is deze waarborg dan ook uitgehold, aangezien geen bescherming wordt geboden tegen gegevensverzamelingen die, naast informatie uit het kerngebied van de privacy, ook minder privacygevoelige gegevens aan het licht brengen.[581] De Belgische wettekst bevat, in tegenstelling tot de Duitse, geen enkele waarborg omtrent het vermijden van de doorzoeking van persoonsgegevens uit het kerngebied van het privéleven, waardoor het respect voor de wezenlijke inhoud van het recht op gegevensbescherming in geen geval gegarandeerd wordt.

De besproken wetswijziging bevat geen beperkingen voor de manier waarop persoonsgegevens op sociale mediaprofielen en smartphones zullen worden geraadpleegd. Het is dus onduidelijk of het CGVS zal overgaan tot het inhoudelijk raadplegen van persoonlijke informatie en communicatie van verzoekers of niet. Desalniettemin kan voor beide scenario's, vanuit de rechtspraak van het HvJ en de invulling van het 'kerngebied van het privéleven' in Duitsland, worden vastgesteld dat het respect voor de wezenlijke inhoud van het recht op gegevensbescherming niet wordt gegarandeerd zonder bijkomende waarborgen. De Belgische wettekst bevat echter geen enkele waarborg hieromtrent, waardoor kan worden vastgesteld dat de onderzoeksbevoegdheid van het CGVS de basisinhoud van het fundamenteel recht op gegevensbescherming niet respecteert, zodat verzoekers OIB hun recht op gegevensbescherming in essentie niet kunnen uitoefenen.

[578] Voßhoff, A. "Betreff Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht 12282/2017." Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (maart 2017). http://docplayer.org/54764603-Andrea-vosshoff-bundesbeauftragte-fuer-den-datenschutz-und-die-informationsfreiheit.html. P. 7.

[579] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 51.

[580] Voßhoff, A. "Betreff Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht 12282/2017." Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (maart 2017). http://docplayer.org/54764603-Andrea-vosshoff-bundesbeauftragte-fuer-den-datenschutz-und-die-informationsfreiheit.html. P. 7.

[581] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 23.

6. Praktijk- en rechtspraakschets rond de toegang tot smartphones en sociale mediaprofielen in verzoekprocedures om internationale bescherming

6.1. Praktijkschets

6.1.1. Praktijkschets: toegang tot smartphones en onrechtstreeks tot sociale mediaprofielen

Tijdens de voorbereidingen van de besproken wetswijziging werden talloze privacygerelateerde bezorgdheden geuit door adviesverleners en ngo's. Hoewel het hun bedoeling was om de voorgestelde aanpassingen ingevoegd te zien in de gewijzigde wetsartikelen zelf, bestond het antwoord van de toenmalige Staatssecretaris voor Asiel en Migratie in de aankondiging van de uitvaardiging van een KB, dat aan de ongunstige adviezen tegemoet zou komen.[582] Dit KB werd tot op heden echter niet uitgevaardigd. Het CGVS heeft hierop besloten om zijn nieuwe onderzoeksbevoegdheid met betrekking tot (o.a.) smartphones voorlopig niet in de praktijk om te zetten.[583] De Commissaris-Generaal erkende omtrent deze beslissing dat er 'terechte opmerkingen met betrekking tot de privacy werden geformuleerd'.[584] Ook verklaarde het Commissariaat dat men 'nog niet had uitgezocht hoe de wetswijziging moest worden uitgevoerd en dat eerst zal worden onderzocht wat technisch gezien nodig is om de methode te gebruiken en vervolgens of het de moeite waard is om erin te investeren'.[585]

6.1.2. Praktijkschets: toegang vanop afstand tot publieke onderdelen van sociale mediaprofielen

In tegenstelling tot het doorzoeken van smartphones, is het screenen en analyseren van sociale mediaprofielen reeds langere tijd een standaardpraktijk van het CGVS.[586] Dit werd ook in de parlementaire stukken met betrekking tot de wetswijziging een aantal maal bevestigd. De wetswijziging zou een loutere verankering uitmaken van een praktijk die al lang gangbaar was bij het CGVS.[587] Deze

[582] Verslag 2 bij de wetswijziging P. 5.; European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 70.

[583] De Wilde, A. "Niet-begeleide minderjarige vreemdelingen in de praktijk van het Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen" in Desmet, E., Verhellen, J. en Bouckaert, S. Rechten Van Niet-begeleide Minderjarige Vreemdelingen In België. Brugge: Die Keure, 2019. P. 197.; European Migration Network (EMN). "Annual Report on Migration and Asylum in Belgium 2018." (juni 2019). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/02_belgium_arm_2018_part2_en_0.pdf. P. 62.; "Wetswijzigingen in de asielprocedure en opvang van asielzoekers". www.agii.be. Agentschap Integratie & Inburgering. https://www.agii.be/nieuws/wetswijzigingen-in-de-asielprocedure-en-opvang-van-asielzoekers#inzage.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 45-46.

[584] Commissaris-Generaal voor de Vluchtelingen en de Staatlozen (Van den Bulck, D.) "Wetswijzing november 2017: een stap vooruit in de realisatie van een Europees geharmoniseerd asielsysteem (powerpointpresentatie voor EMN conferentie)." Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen (december 2017). https://emnbelgium.be/sites/default/files/attachments/Session%201.2%20-%20Dirk%20Vanden%20Bulck%20-%20Procedure%20Internationale%20bescherming%20-%20FINAL.pdf. Slide 7.

[585] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 86.

[586] European Migration Network (EMN). "EMN Synthesis Report for the EMN Focussed Study 2017: Challenges and practices for establishing the identity of third-country nationals in migration procedures." (december 2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_identity_study_final_en.pdf. P. 32.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 81.

[587] Verslag 2 bij de wetswijziging P. 6, 8, 16 en 18.; Verslag 1 bij de wetswijziging P. 84.

sociale mediascreening gebeurt niet op systematische wijze, maar enkel in gevallen waar twijfels of indicaties opduiken die dergelijke screenings nuttig maken, aangezien ze erg tijdrovend zijn. Ook worden in deze context enkel de publieke delen van sociale mediaprofielen geraadpleegd.[588] In dit kader beschikt het CGVS over een gespecialiseerde eenheid voor onderzoek naar sociale media. De eenheid, de 'New Media Unit' (NMU), ressorteert onder 'Cedoca', het onderzoeksbureau van het CGVS dat informatie over de landen van herkomst verzamelt en analyseert.[589] Deze eenheid zorgt sinds augustus 2016 voor een continue opleiding van de medewerkers van het CGVS omtrent sociale mediascreening en helpt hen bij het uitvoeren ervan.[590]

6.2. Rechtspraakschets

6.2.1. Rechtspraakschets: toegang tot smartphones en onrechtstreeks tot sociale mediaprofielen

Gezien het feit dat doorzoekingen van smartphones, in afwachting van het aangekondigd KB, nog niet door het CGVS worden uitgevoerd (zie '6.1.1.'), bestaat vooralsnog geen specifieke rechtspraak over artikel 48/6, §1, lid 4 van de Vreemdelingenwet. Opvallend is wel, dat de RvV in 2016 een arrest velde dat bevestigt waarom de Belgische migratieautoriteiten net geen toegang zouden mogen krijgen tot de private onderdelen van iemands sociale mediaprofiel. De toenmalige Staatssecretaris voor Asiel en Migratie motiveert in deze zaak waarom men zich geen toegang kan verschaffen tot en dus geen rekening kan houden met de (voor het publiek afgeschermde) gegevens en communicatie op het facebookprofiel van de verzoekende partij in kwestie. De motivering luidt: 'De privacywet van 8 december 1992 laat niet zonder meer toe dat het bestuur zich toegang verschaft tot het facebookprofiel van betrokkene (zelf met zijn toestemming), onder meer omdat ook persoonsgegevens van andere personen dan betrokkene beschikbaar zijn op het facebookprofiel. Bovendien impliceert het zorgvuldigheidsbeginsel dat het aan betrokkene zelf toekomt om alle nuttige en relevante stukken die aantonen dat hij voldoet aan de verblijfsvoorwaarden, te selecteren en over te maken aan het bestuur'.[591] Deze redenering werd door de RvV beaamd en bevestigd. Op te merken valt, dat dit arrest in scherp contrast staat met de latere verklaringen van de Staatssecretaris voor Asiel en Migratie tijdens de voorbereidingen van de besproken wetsartikelen, namelijk dat de wetswijziging in het licht van de privacywetgeving 'geenszins problematisch' is.[592]

6.2.2. Rechtspraakschets: toegang vanop afstand tot publieke onderdelen van sociale mediaprofielen

Wat de toegang tot publieke onderdelen van sociale mediaprofielen vanop afstand betreft, bestaat wel een gangbare praktijk bij het CGVS en is bijgevolg rechtspraak van de RvV voorhanden.[593] Ten eerste

[588] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 81-82.

[589] "Cedoca". www.cgvs.be. Commissariaat-Generaal voor de Vluchtelingen en de Staatlozen. https://www.cgra.be/en/country-information/cedoca.

[590] European Migration Network (EMN). "Annual Report on Migration and Asylum in Belgium 2018." (juni 2019). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/02_belgium_arm_2018_part2_en_0.pdf. P. 62.; European Asylum Support Office (EASO). "Annual Report on the Situation of Asylum in the European Union 2018." (juni 2019). https://www.easo.europa.eu/sites/default/files/easo-annual-report-2018-web.pdf. P. 165.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 82.

[591] RvV nr. 175 324 van 26 september 2016. § 1, 3.2.2. en 3.2.3.

[592] Memorie van toelichting bij de wetswijziging P. 36 en 137.; Verslag 2 bij de wetswijziging P. 5 en 27.

[593] Adam, C. 10 Jaar Raad Voor Vreemdelingenbetwistingen / 10 Ans Du Conseil Du Contentieux Des Étrangers. Daadwerkelijke Rechtsbescherming / La Protection Juridictionnelle Effective. Brugge: Die Keure, 2017. P. 356-357.

erkent de Raad in zijn rechtspraak dat een zekere voorzichtigheid geboden is bij het beoordelen van materiaal dat is gepubliceerd op sociale netwerken zoals Facebook of Twitter. De redenen hiervoor zijn onder andere dat dergelijke informatie geen absolute tijdsaanduidingen bevat, dat een sociale mediaprofiel door iemand anders dan de verzoeker kan zijn opgesteld of dat het verklaringen kan bevatten die niet overeenkomen met de werkelijkheid. De gevonden informatie op sociale mediaprofielen moet dus voldoende betrouwbaar zijn om er conclusies uit te kunnen trekken.[594] Bijgevolg stelt de RvV ook vast dat een beslissing over de geloofwaardigheid van een verzoek OIB niet uitsluitend mag gebaseerd zijn op tegenstrijdigheden tussen de verklaringen van de verzoeker en de bevindingen op sociale mediaprofielen. Wel kunnen dergelijke bevindingen deel uitmaken van een geheel van elementen die gezamenlijk zouden duiden op een gebrek aan geloofwaardigheid.[595]

Daarnaast behandelen een aantal zaken voor de RvV de kwestie of het raadplegen van publieke onderdelen van sociale mediaprofielen al dan niet een schending van het recht op privacy uitmaakt. De Raad verwijst naar rechtspraak van het EHRM om te beoordelen of bepaalde informatie al dan niet onder het begrip 'privacy' valt. Volgens deze rechtspraak moet er sprake zijn van 'een redelijke verwachting dat bepaalde informatie tot het gebied van de privacy behoort' in hoofde van de betrokkene.[596] Op basis van dit criterium oordeelt de Raad stelselmatig dat 'een persoon die informatie over zichzelf verspreidt op sociale netwerken, die voor iedereen toegankelijk zijn, niet kan beweren dat men verwachtte dat die informatie beschermd zou worden op grond van het recht op privacy'.[597]

Op het meermaals aangehaalde argument door verzoekers OIB dat sociale mediaprofielen 'geen open bron' zijn en dat ze behoren 'tot de privacy van de burgers', antwoordt de Raad dus steevast dat de verzoekers in kwestie de gegevens op hun sociale mediaprofiel zelf openbaar hebben gemaakt en dat het gebruik ervan geen schending uitmaakt van het recht op privacy als bedoeld in artikel 8 EVRM. De rechtspraak van het EHRM eindigt echter niet bij de door de RvV aangehaalde arresten. In de zaak Satakunnan Markkinapörssi Oy and Satamedia Oy t. Finland, oordeelde het Hof namelijk dat 'wanneer gegevens over een bepaalde persoon zijn verzameld, verwerkt of gebruikt, of wanneer het betrokken materiaal is gepubliceerd op een wijze of in een mate die verder gaat dan normaal gesproken te verwachten is, worden overwegingen in verband met het privéleven relevant'.[598] Deze rechtspraak indachtig, is het zeer aannemelijk dat gebruikers bij het aanmaken van hun sociale mediaprofiel niet steeds de verwachting hebben dat deze informatie later zal gebruikt worden voor de beoordeling van hun verzoek OIB. Daarnaast stelt het EHRM en de Raad van Europa (o.a. in hun handboek over het Europees gegevensbeschermingsrecht) dat het feit dat informatie reeds deel uitmaakt van het publieke domein, niet betekent dat de bescherming van artikel 8 EVRM wegvalt, noch dat de verwerkingsverantwoordelijken van hun verplichtingen in de wetgeving inzake gegevensbescherming worden ontslaan.[599]

[594] RvV nr. 95 844 van 25 januari 2013. § 4.6.; RvV nr. 119 575 van 26 februari 2014. § 5.3.4.; RvV nr. 152 234 van 10 september 2015. § 3.8.
[595] RvV nr. 154 195 van 9 oktober 2015. § 6.5.1.
[596] EHRM, Peev t. Bulgarije, nr. 64209/01, 26 oktober 2007. § 38-39.; EHRM, Copland t. VK, nr. 62617/00, 3 april 2007. § 42.
[597] RvV nr. 156 935 van 24 november 2015. § 4.5.3.; RvV nr. 82 384 van 4 juni 2012. § 2.5.; RvV nr. 116 470 van 3 januari 2014. § 2.2.3.
[598] EHRM, Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland, nr. 931/13, 27 juni 2017. § 136.
[599] EHRM, Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland, nr. 931/13, 27 juni 2017. § 134.; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 162.; Council of Europe/European Court of Human Rights. "Guide on Article 8 of the European Convention on Human Rights." (augustus 2019). https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf. P. 40.

7. Voorgestelde waarborgen en voorwaarden voor conformiteit met het asiel-, privacy- en gegevensbeschermingsrechtelijk kader

7.1. Context van het invoeren van waarborgen en voorwaarden voor conformiteit

In het tweede verslag omtrent de wetswijziging, diende de toenmalige Staatssecretaris voor Asiel en Migratie de adviesverleners (de CBPL en het UNHCR) van antwoord door middel van de belofte om in een KB[600] tegemoet te komen aan hun opmerkingen. Met betrekking tot dat KB zou het advies van de CBPL opnieuw worden ingewonnen. In plaats van de opmerkingen en voorstellen van de adviesverleners meteen op te nemen in de voorgestelde wettekst, werd toen reeds beloofd om een aantal bijkomende waarborgen in het toekomstig KB te voorzien. Deze waarborgen zouden de volgende hiaten opvullen: de concrete manier waarop de toegang tot de elektronische informatiedragers of communicatiemiddelen wordt gegeven aan de medewerker van het CGVS, op welke (eventueel technische) manier de gegevens zullen bewaard worden, wat er precies bewaard moet worden en op welke manier deze gegevens beveiligd zullen worden. Concreet worden in het tweede verslag omtrent de wetswijziging de volgende waarborgen beloofd:

- dat de betrokkene voor het inkijken geïnformeerd wordt over de reden waarom inzage gevraagd wordt en over de mogelijkheid tot weigering (met een weergave van de eventuele consequentie)
- dat de betrokkene duidelijk zijn toestemming gegeven heeft
- dat men enkel inkijkt wat de betrokkene wenst dat wordt ingekeken
- dat enkel op het ogenblik van het gehoor een inkijken mogelijk is
- dat enkel ingekeken wordt wat relevant is voor de beoordeling van de asielaanvraag
- dat enkel in het dossier opgenomen wordt wat relevant is voor de beoordeling van de asielaanvraag

Het antwoord van de toenmalige Staatssecretaris voor Asiel en Migratie stemde echter niet overeen met de bedoeling van de adviesverleners om hun opmerkingen in de wettekst zelf te zien opgenomen worden. Ook een platform van zeven Belgische ngo's[601] sprak zich laatdunkend uit over de 'gemiste kans om de kritische bemerkingen op een transparante manier in de wetsontwerpen zelf te regelen'. KB's hoeven daarenboven niet aan het parlement te worden voorgelegd.[602] KB's zijn echer wel hiërarchisch ondergeschikt aan de Grondwet, de internationale normen met directe werking, de wetskrachtige normen en de algemene rechtsbeginselen en moeten hier dus mee in overeenstemming zijn. Deze hiërarchie is op twee wijzen afdwingbaar, ten eerste door de exceptie van onwettigheid in artikel 159 van de Grondwet, dat bepaalt dat rechters KB's die niet in overeenstemming zijn met bovenvermelde normen buiten toepassing moeten laten. Ten tweede is de afdeling bestuursrechtspraak van de RvSt bevoegd om de KB's te vernietigen, wanneer ze in strijd zijn met de hogere rechtsnormen.[603]

---

[600] Op basis van artikel 57/24 Vreemdelingenwet; Verslag 2 bij de wetswijziging P. 5.

[601] 11.11.11, CNCD-11.11.11, Amnesty International Belgique Francophone, Amnesty International Vlaanderen, CIRÉ, Liga voor mensenrechten, Ligue des droits de l'Homme, Orbit, Platform kinderen op de vlucht - Plate-Forme Mineurs en Exil, Point d'Appui en Vluchtelingenwerk Vlaanderen

[602] European Migration Network (EMN) National Contact Point Belgium. "Challenges and practices for establishing identity in the migration process in Belgium." (december 2017). https://emnbelgium.be/sites/default/files/publications/rapport%20spf%20web.pdf. P. 70.; "Vandaag stemt de Kamer over wetsontwerpen die onze asielwetgeving ingrijpend wijzigen". www.vluchtelingenwerk.be. Vluchtelingenwerk Vlaanderen, 9 november 2017. https://www.vluchtelingenwerk.be/nieuws/vandaag-stemt-de-kamer-over-wetsontwerpen-die-onze-asielwetgeving-ingrijpend-wijzigen.

[603] Vande Lanotte, J., Goedertier, G. en Haeck, Y. Belgisch Publiekrecht. Brugge: Die Keure, 2015. P. 130.

7.2. Voorgestelde waarborgen en voorwaarden voor conformiteit

7.2.1. Voorgestelde waarborgen per geïdentificeerd pijnpunt in de wetswijziging

Hieronder worden, per geïdentificeerd pijnpunt in '5.', waarborgen voorgesteld die de tekortkomingen in de wetswijziging (deels) kunnen remediëren.[604] Daarnaast worden een aantal mogelijke hindernissen geïdentificeerd. Enerzijds gaat het om hindernissen doordat het KB geen gepast medium vormt voor bepaalde voorgestelde waarborgen. Deze waarborgen hebben immers betrekking op de begrenzing van de onderzoeksbevoegdheid van het CGVS zelf, in tegenstelling tot de uitvoeringsmodaliteiten ervan, waarvoor het KB wel passend wordt geacht. Anderzijds worden mogelijke hindernissen aangehaald voor het implementeren van de voorgestelde waarborgen.

GEÏDENTIFICEERDE PIJNPUNTEN	VOORGESTELDE WAARBORGEN	HINDERNISSEN VOOR OPNAME IN HET KB EN IMPLEMENTERING
VERKEERDE OMZETTING EN ONEVENWICHTIGE BENADRUKKING MEDEWERKINGS-PLICHT	º Het verwijderen van volgende zin uit artikel 48/6, §1, lid 4 Vreemdelingenwet: "De weigering van de verzoeker om deze elementen voor te leggen zonder bevredigende verklaring kan een aanwijzing zijn van zijn weigering om te voldoen aan zijn medewerkingsplicht zoals bedoeld in het eerste lid."[605]	º Moet in de wet zelf worden aangepast
BEHOORLIJKE EN TRANSPARANTE VERWERKING NIET GEGARANDEERD	º Het garanderen van het voldoende en doeltreffend informeren van betrokkenen over alle aspecten van de gegevensverwerking[606] d.m.v. schriftelijke en mondelinge informatie, voldoende tijd om correct begrip te bewerkstelligen en de gegarandeerde mogelijkheid tot raadplegen van een advocaat[607] (o.a.) omtrent de bewijswaarde dat aan de gegevens zal worden gehecht[608], de beperkte doeleinden van de verwerking, hoe men rechtsmiddelen kan aanwenden indien men zich door een doorzoeking benadeeld voelt[609]…	
DOELBINDINGS-PRINCIPE NIET ONBETWISTBAAR NAGELEEFD	º Het toevoegen van volgende vermelding in artikel 48/6, §1, lid 4 en 57/7, §2 Vreemdelingenwet: "De gegevens mogen in geen geval voor andere dan de in dit artikel beschreven doeleinden worden gebruikt."[610]	º Moet in de wet zelf worden aangepast

[604] Omtrent de voorgestelde waarborgen, moet worden opgemerkt dat de aangehaalde voetnoten niet enkel kunnen duiden op het feit dat de waarborg reeds elders werd vermeld, maar ook dat de aangegeven bron louter als inspiratie voor de waarborg heeft gediend.

[605] Artikel 48/6, §1, lid 4 Vreemdelingenwet; Denys, L. Overzicht van het vreemdelingenrecht. 4e ed. Heule: INNI Publishers, 2019. P. 528.

[606] Advies UNHCR P. 8.

[607] VN- Hoog Commissariaat voor de Vluchtelingen. "Beyond Proof: Credibility Assessment in EU Asylum Systems." (mei 2013). https://www.unhcr.org/protection/operations/51a8a08a9/full-report-beyond-proof-credibility-assessment-eu-asylum-systems.html. P. 105

[608] European Migration Network (EMN). "EMN Synthesis Report for the EMN Focussed Study 2017: Challenges and practices for establishing the identity of third-country nationals in migration procedures." (december 2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_identity_study_final_en.pdf. P. 4.

[609] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 12.

[610] Artikel 15a (1) Asylgesetz (Duitse Vreemdelingenwet); Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit

	◦ Het opstellen van strikte regels i.v.m. de manier waarop en de mate waarin de gegevens kunnen worden doorgegeven aan andere entiteiten voor andere doeleinden[611] Indien er andere doeleinden dan 'beoordeling van het verzoek OIB' bestaan, moet dit worden vermeld in artikel 48/6, §1, lid 4 en 57/7, §2 Vreemdelingenwet en moeten betrokkenen hieromtrent worden geïnformeerd	◦ Moet in de wet zelf worden aangepast
DATAMINIMALISATIE EN RESPECT VOOR DE WEZENLIJKE INHOUD VAN DE FUNDAMENTELE RECHTEN NIET GEGARANDEERD	◦ Het toevoegen van volgende vermelding in artikel 48/6, §1, lid 4 en 57/7, §2 Vreemdelingenwet: "De onderzoeksbevoegdheid geldt niet indien er aanwijzingen zijn dat het analyseren van (digitale) gegevensdragers en (digitale) platformen 'tevens' inzicht zou geven in het kerngebied van het privéleven van de betrokkene. Als dergelijke inzichten worden verkregen, mogen ze niet worden gebruikt en moet eventuele registratie ervan onmiddellijk worden verwijderd."[612]	◦ Moet in de wet zelf worden aangepast
	◦ Het uitvoeren van een 'upstreamcontrole' zodat het verzamelen van gegevens uit 'het kerngebied van het privéleven' wordt uitgesloten[613]	
	◦ Controle van de geregistreerde informatie door een onafhankelijke instantie[614] om irrelevante gegevens, gegevens die buiten de bevoegdheid van het CGVS vallen[615] en gegevens uit 'het kerngebied van het privéleven' uit te filteren vooraleer ze worden gebruikt	
	◦ Het beperken van de soorten geraadpleegde gegevens tot: landnummers (en duur) van gesprekken/sms'en/ andere berichten/contactpersonen, taalgebruik in sms'en/andere berichten, landcodes van bezochte	◦ Geautomatiseerde taalanalyses hebben een grote foutmarge en leiden tot discriminatie van sprekers van vaker incorrect

Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 86-87.

[611] Necessary & Proportionate. "International Principles on the Application of Human Rights to Communications Surveillance." Necessary & Proportionate (mei 2014). https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. P. 8.

[612] Artikel 48, 3a, 2, 5 en 6 Aufenthaltsgesetz (Duitse Verblijfswet); Voßhoff, A. "Betreff Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht 12282/2017." Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (maart 2017). http://docplayer.org/54764603-Andrea-vosshoff-bundesbeauftragte-fuer-den-datenschutz-und-die-informationsfreiheit.html. P. 7.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 23.

[613] Voßhoff, A. "Betreff Entwurf eines Gesetzes zur besseren Durchsetzung der Ausreisepflicht 12282/2017." Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (maart 2017). http://docplayer.org/54764603-Andrea-vosshoff-bundesbeauftragte-fuer-den-datenschutz-und-die-informationsfreiheit.html. P. 7.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 88.

[614] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 85, 89 en 94.

[615] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3.; Advies CBPL P. 9.

	websites in de browsegeschiedenis, locatiegegevens van foto's en eventueel van apps[616]	geïdentificeerde talen[617]
	o Het vermijden dat gegevens in online opslagruimtes op cloud-gebaseerde applicaties worden geraadpleegd door de verbinding met een netwerk uit te schakelen (bijvoorbeeld door het apparaat in de vliegtuigmodus te plaatsen)[618]	
NAUWKEURIGHEID NIET GEGARANDEERD	o Het garanderen van de mogelijkheid voor de betrokkene om uitleg en verduidelijking te verschaffen omtrent de verzamelde en gebruikte persoonsgegevens[619]	
	o Het garanderen dat gegevens niet worden veranderd of verwijderd van de gegevensdrager om de authenticiteit ervan te waarborgen[620] In elk geval door manuele of basisonderzoeken (*manual 'quick scans'*) uit te sluiten[621]	
	o Het voorzien van training voor medewerkers om specifieke privacygevoelige interventies uit te voeren[622] door voldoende inzicht te bieden in de beperkingen van de gegevenskwaliteit van informatie op sociale media/smartphones[623] Het enkel toelaten van gespecialiseerde medewerkers om de gegevens te vertalen en te interpreteren[624]	
OPSLAGBEPERKING NIET GEGARANDEERD	o Het beperken van de gegevensopslag tot gegevens die relevant zijn voor het beoordelen van het verzoek OIB en onmiddellijk verwijderen van irrelevant gebleken gegevens[625]	

[616] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 18.
[617] Ibid. P. 20.
[618] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 8.
[619] Memorie van toelichting bij de wetswijziging P. 137.; Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 31.
[620] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3. Advies CBPL P. 9.
[621] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 89.
[622] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 45.
[623] U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for Refugee Case Processing and Security Vetting DHS/USCIS/PIA-068." (juli 2017). https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf. P. 18.
[624] Advies CBPL P. 9.
[625] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3. Advies CBPL P. 9.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 88.; U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018).

	⁰ Het pseudonimiseren of zelfs anonimiseren van de dossiers van verzoekers, eens ze naar het Rijksarchief worden overgebracht voor archivering in het algemeen belang[626]	
	⁰ Het bijhouden van een rapport met de audit trail van elk zoekproces toegepast op digitaal bewijsmateriaal, opdat een onafhankelijke derde partij deze processen kan onderzoeken en tot dezelfde conclusie kan komen[627]	
VERTROUWELIJKHEID EN INTEGRITEIT NIET GEGARANDEERD	⁰ Het beveiligen van de gegevens[628] opdat enkel de bevoegde en competente autoriteit de doorzoekingen kan uitvoeren en toegang heeft tot de gegevens, volgens diens bevoegdheid en de wettelijke waarborgen[629], d.m.v. bijvoorbeeld: pseudonimisering, garantie van vertrouwelijkheid/integriteit/ beschikbaarheid/veerkracht van de verwerkingssystemen en diensten, garantie van tijdig herstel van beschikbaarheid/toegang tot de persoonsgegevens bij fysiek/technisch incident, tijdig testen/beoordelen/evalueren van de doeltreffendheid van de beveiligingsmaatregelen, aansluiting bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme…[630]	
	⁰ Het opstellen van strikte regels i.v.m. de manier waarop en de mate waarin de gegevens kunnen worden doorgegeven aan andere entiteiten[631] Indien andere entiteiten dan het CGVS de gegevens raadplegen, moet dit worden vermeld in artikel 48/6, §1, lid 4 en 57/7, §2 Vreemdelingenwet en moeten betrokkenen hieromtrent worden geïnformeerd	⁰ Moet in de wet zelf worden aangepast
	⁰ Uitsluitend gebruik van 'stand-alone computers', met speciale accounts voor onderzoek op sociale media om de veiligheid van het personeel te waarborgen en om de niet-traceerbaarheid van de zoekopdrachten voor de overheid in een land van herkomst te garanderen[632]	

https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 17.

[626] Overweging 156 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 131.

[627] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3.
U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment Update for CBP Border Searches of Electronic Devices DHS/CBP/PIA-008(a)." (januari 2018). https://www.dhs.gov/sites/default/files/publications/PIA-CBP%20-%20Border-Searches-of-Electronic-Devices%20-January-2018%20-%20Compliant.pdf. P. 3, 6, 20 en 21.

[628] Advies CBPL P. 9.

[629] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3.

[630] Artikel 25 jo. 32 lid 1 en 3 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 131-132

[631] Necessary & Proportionate. "International Principles on the Application of Human Rights to Communications Surveillance." Necessary & Proportionate (mei 2014).
https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. P. 8.

[632] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 83.

	⁰ Het garanderen dat de gegevens niet worden gedeeld met de overheid in landen van herkomst, noch met derde landen waar de betrokkene moet vrezen voor vervolging of ernstige schade[633]	
ONRECHTMATIGHEID VAN DE VERWERKING	⁰ De onderzoeksbevoegdheid van het CGVS afhankelijk stellen van een vrije en geïnformeerde toestemming van de betrokkene[634] Beide besproken wetsartikels zouden moeten worden geherformuleerd als: "Indien de verzoeker in het kader van de medewerkingsplicht zelf het initiatief neemt om gegevens op een (digitale) gegevensdrager of (digitaal) platform aan te brengen ter staving van diens verzoek OIB, is het CGVS bevoegd om hier kennis van te nemen."[635]	⁰ Moet in de wet zelf worden aangepast ⁰ Het bereiken van een volledig vrije toestemming in de zin van de AVG is praktisch onmogelijk gezien de absolute machtsverhouding tussen het CGVS en de verzoeker[636] ⁰ Gegarandeerde verwerking van persoonsgegevens van andere personen dan de verzoeker zelf[637] zonder hun toestemming
NIET-NOODZAKELIJKHEID IN EEN DEMOCRATISCHE SAMENLEVING	⁰ Het toevoegen van volgende vermelding in artikel 48/6, §1, lid 4 en 57/7, §2 Vreemdelingenwet: "De onderzoeksbevoegdheid geldt enkel indien alle andere minder ingrijpende maatregelen om het doel te bereiken zonder enig resultaat zijn uitgeput[638] en indien de betrokkene geen geldige identiteitsdocumenten kan voorleggen[639]." Het hierdoor instellen van objectieve selectiecriteria voor het uitvoeren van de doorzoekingen, om te vermijden dat de maatregel op ad-hocbasis en op basis	⁰ Moet in de wet zelf worden aangepast ⁰ Het interview met de verzoeker vormt in de praktijk steeds een minder ingrijpende maatregel, tenzij hier geen enkele bruikbare informatie uit voorkomt[642]

[633] Tangermann, J. "Documenting and Establishing Identity in the Migration Process." German National Contact Point for the European Migration Network (EMN) (2017). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/11a_germany_identity_study_final_en.pdf. P. 24.
[634] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3.
[635] RvV nr. 175 324 van 26 september 2016. § 1, 3.2.2. en 3.2.3.
[636] Overweging 43 AVG; Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6.
[637] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 6 en 14.
Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.
EHRM, Szabo & Vissy t. Hongarije, nr. 37138/14, 12 januari 2016. §89.
[638] Artikel 15a (1) Asylgesetz (Duitse Vreemdelingenwet); VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3.
[639] Artikel 48, 3, 1 Aufenthaltsgesetz (Duitse Verblijfswet); Jumbert, M. G., Bellanova, R. en Gellert, R. "Smart Phones for Refugees: Tools for Survival, or Surveillance?" The Peace Research Institute Oslo (Prio) (2018). https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf. P. 4.
[642] Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020).

	van informele criteria wordt toegepast[640] en dat de de selectiecriteria geen onevenredig grote invloed hebben op bepaalde minderheden[641]	o Discriminatie van verzoekers uit landen waar moeilijk geldige identiteitsdocumenten te verkrijgen zijn, die hierdoor meer kans hebben om aan de maatregel te worden onderworpen
	o Het beperken van de doorzoekingen in de tijd en de onmiddellijke teruggave van de (digitale) gegevensdragers na het bereiken van het doel van de gegevensverzameling[643]	
DIS-PROPORTIONALITEIT IN EEN DEMOCRATISCHE SAMENLEVING	o Het toevoegen van volgende vermelding in artikel 48/6, §1, lid 4 en 57/7, §2 Vreemdelingenwet: "De beoordeling (van de geloofwaardigheid) van een verzoek OIB mag niet uitsluitend gebaseerd zijn op de bevindingen op (digitale) gegevensdragers en/of op (digitale) platformen.[644] Dergelijke bevindingen kunnen hoogstens een indicatie vormen van identiteit of nationaliteit[645]." Het hierdoor herleiden van de bewijswaarde van deze bevindingen tot het minimum[646], naar evenredigheid met de intrinsieke onnauwkeurigheid en inefficiëntie van de maatregel	o Moet in de wet zelf worden aangepast

https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 25.

[640] Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 85.

[641] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 7.

[643] VN-Hoog Commissariaat voor de Vluchtelingen. "UNHCR Preliminary Legal Observations on the Seizure and Search of Electronic Devices of Asylum-Seekers." (augustus 2017). https://www.refworld.org/docid/59a5231b4.html. P. 2-3.

[644] Adam, C. 10 Jaar Raad Voor Vreemdelingenbetwistingen / 10 Ans Du Conseil Du Contentieux Des Étrangers. Daadwerkelijke Rechtsbescherming / La Protection Juridictionnelle Effective. Brugge: Die Keure, 2017. P. 356-357.
RvV, nr. 154 195 van 9 oktober 2015. § 6.5.1.; U.S. Department of Homelands Security (DHS). "Privacy Impact Assessment for Refugee Case Processing and Security Vetting DHS/USCIS/PIA-068." (juli 2017).
https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-refugee-july2017.pdf. P. 18.; Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020).
https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 3 en 14.

[645] European Migration Network (EMN). "EMN Synthesis Report for the EMN Focussed Study 2017: Challenges and practices for establishing the identity of third-country nationals in migration procedures." (december 2017).
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_identity_study_final_en.pdf. P. 41.

[646] European Migration Network (EMN). "EMN Synthesis Report for the EMN Focussed Study 2017: Challenges and practices for establishing the identity of third-country nationals in migration procedures." (december 2017).
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/00_eu_synthesis_report_identity_study_final_en.pdf. P. 4.; Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020).
https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 31.; Bolhuis, M. en van Wijk, J. "Case management, identity controls and screening on national security and 1F exclusion." Center for International Criminal Justice (CICJ) (Vrije Universiteit Amsterdam) (2018). https://cicj.org/wp-content/uploads/2018/09/Bolhuis-Van-Wijk-2018-Case-management-identity-controls-and-screening-on-national-security-and-1F-exclusion.pdf. P. 137.; Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 42.

	◦ Het instellen van een leeftijdsgrens voor betrokkenen, wiens sociale mediaprofielen en smartphones kunnen worden geraadpleegd, naar evenredigheid met het verhoogde ingrijpende karakter van de maatregel voor minderjarige verzoekers OIB[647]	
ALGEMEEN	◦ De onderzoeksbevoegdheid van het CGVS afhankelijk stellen van een bevel of machtiging van een onafhankelijke en neutrale rechterlijke instantie (vergelijkbaar met het vereiste bevel van de onderzoeksrechter voor strafrechtelijke netwerkzoekingen) om de wettigheid, de noodzakelijkheid en de proportionaliteit van de maatregel te controleren[648]	◦ Moet in de wet zelf worden aangepast
	◦ Het uitvoeren van een gegevensbeschermingseffectbeoordeling[649]	

7.2.2. Bemerkingen omtrent de voorgestelde waarborgen

Ondanks het feit dat de voorgestelde waarborgen afzonderlijk bepaalde tekortkomingen in de besproken wetswijziging (kunnen) remediëren, zijn ze niet noodzakelijkerwijs 'in hun geheel' toepasbaar. Het is bijvoorbeeld niet mogelijk om aan dataminimalisatie te doen, door het uitvoeren van taalanalyses op de communicatie van de betrokkene in plaats van de inhoud ervan te raadplegen, en tegelijkertijd de nauwkeurigheid van de gegevensverwerking te garanderen. Geautomatiseerde taalanalyses hebben namelijk een niet weg te cijferen foutmarge en als een taal niet voorkomt in het systeem, koppelt het de communicatie simpelweg aan de meest 'vergelijkbare' geregistreerde taal.[650] Daarnaast kan de wet theoretisch gezien wel stellen dat 'gegevens op (digitale) gegevensdragers en/of op (digitale) platformen hoogstens een indicatie vormen van identiteit of nationaliteit' en dat de weigering van het laten doorzoeken van dergelijke gegevens geen invloed heeft op de medewerkingsplicht en de beoordeling van het verzoek van de betrokkene. De vraag is echter of deze 'opgelegde' percepties zich ook werkelijk in de beslissingen van het CGVS zullen laten voelen en hoe dit precies afdwingbaar is. Vervolgens zijn er voorgestelde waarborgen die het onwenselijke neveneffect van een 'risico op discriminatie' met zich meebrengen. Dit risico ligt bij sprekers van vaker incorrect geïdentificeerde talen door systemen voor geautomatiseerde taalanalyse[651] of bij verzoekers uit landen waar moeilijk geldige identiteitsdocumenten te verkrijgen zijn, die hierdoor meer kans hebben om aan de maatregel te worden onderworpen.

Daarbovenop is er geen enkele waarborg die het gebrek aan een overtuigend, empirisch onderbouwd en wettelijk vereist 'algemeen belang' of 'gerechtvaardigd doel' kan remediëren. Wetenschappelijk onderzoek hieromtrent zal naar alle waarschijnlijkheid namelijk leiden tot dezelfde conclusie als bij de

[647] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 12.
[648] Ibid. P. 13 en 23.
[649] Artikel 35 AVG; Council of Europe, European Court of Human Rights, European Data Protection Supervisor en European Union Agency for Fundamental Rights. Handbook on European data protection law. 3e ed. Luxemburg: Publications Office of the European Union, 2018. P. 135.; Advies CBPL P. 4.; Advies UNHCR P. 6.
[650] Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 20.
[651] Ibid. P. 20.

Duitse asielautoriteit.[652] Deze vaststelling indachtig, zou een 'onafhankelijke en neutrale rechterijke instantie' ook nooit tot het uitreiken van een zoekingsbevel komen, aangezien de controle van de 'wettigheid' van de maatregel nooit tot een positief resultaat kan leiden.

De alternatieve verwerkingsgrond van de 'vrije geïnformeerde toestemming' is amper toepasbaar in de absolute machtsverhouding tussen een verzoeker OIB en de beoordelende asielautoriteit.[653] De uiterst vrijblijvende voorgestelde herformulering[654], die de enige manier vormt waarop deze verwerkingsgrond enigszins in aanmerking kan worden genomen, beantwoordt waarschijnlijk niet aan de motieven die in de eerste plaats tot het indienen van het wetsvoorstel hebben geleid, namelijk het 'bestrijden van misbruik in verzoekprocedures OIB'. Daarnaast blijft het onvermijdelijk dat bij het screenen van sociale mediaprofielen en smartphones ook persoonsgegevens worden verwerkt van andere personen dan de verzoekers OIB zelf, met wie zij (al dan niet gewenst) in contact staan.[655] Hierdoor worden gegarandeerd persoonsgegevens verwerkt van personen die hier geen toestemming toe hebben gegeven.[656] Bovendien is het vragen van de toestemming van de betrokkene bij het raadplegen van sociale mediaprofielen vanop afstand ook niet aan de orde.

Tot slot moet de afweging worden gemaakt of de kostprijs en arbeidsintensiviteit om aan de vereisten in het gegevensbeschermingsrechtelijk kader te voldoen[657] wel opwegen tegen de minimale output van doorzoekingen van sociale mediaprofielen en smartphones.[658] Zowel de minimale bewijswaarde die aan het resultaat moet worden gehecht als het empirisch bewezen minimale 'succespercentage' van de resultaten, stellen deze evenwichtsoefening namelijk in een ongunstig kosten-batenanalytisch daglicht. Naast het feit dat er *de facto* geen combinatie van waarborgen mogelijk is die cumulatief aan alle gegevensbeschermingsrechtelijke eisen kan voldoen, leidt dit noodgedwongen tot de vraag of er überhaupt nog overtuigende bestaansredenen overblijven voor artikelen 48/6, §1, lid 4 en 57/7, §2 van de Belgische Vreemdelingenwet.

---

[652] Ibid. P. 5-6 en 28-30.

[653] Overweging 43 AVG; Werkgroep gegevensbescherming artikel 29. "Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679 WP 259." (2018).
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf. P. 6.

[654] "Indien de verzoeker in het kader van de medewerkingsplicht zelf het initiatief neemt om gegevens op een (digitale) gegevensdrager of (digitaal) platform aan te brengen ter staving van diens verzoek om internationale bescherming,is het CGVS bevoegd om hier kennis van te nemen."

[655] Patel, F., Levinson-Waldman, R., DenUyl, S. en Koreh, R. "Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security." Brennan Center for Justice at New York University School of Law (maart 2020). https://www.brennancenter.org/sites/default/files/2020-03/SocialMediaMonitoring.pdf. P. 6 en 14.;
Carpanelli, E. Use and Misuse of New Technologies: Contemporary Challenges in International and European Law. Springer International Publishing, 2019. P. 8.; EHRM, Szabo & Vissy t. Hongarije, nr. 37138/14, 12 januari 2016. §89.

[656] RvV nr. 175 324 van 26 september 2016. § 1, 3.2.2. en 3.2.3.

[657] o.a. technische middelen voor 'upstreamcontrole' van gegevensdragers/platformen en het voorzien van 'stand-alone computers' met speciale accounts, controle van de geregistreerde informatie op relevantie door een onafhankelijke instantie, het voorzien van training en het opleiden van gespecialiseerde medewerkers voor het vertalen en interpreteren van gegevens, het opstellen van rapporten met de audit trails van elk zoekproces, het aanvragen van een bevel of machtiging van een onafhankelijke en neutrale rechterlijke instantie voor elke gegevensverwerking…

[658] In februari 2017 verklaarde het Duitse Ministerie van Binnenlandse Zaken bijvoorbeeld dat er eenmalige installatiekosten van 3,2 miljoen euro te verwachten waren voor de uitleesapparatuur, wat de oorspronkelijke verwachtingen bij het opstellen van wetsvoorstel duidelijk overtrof.
Biselli, A. en Beckmann, L. "Invading Refugees' Phones: Digital Forms of Migration Control In Germany and Europe." Gesellschaft für Freiheitsrechte e.V. (februari 2020). https://freiheitsrechte.org/home/wp-content/uploads/2020/02/Study_Invading-Refugees-Phones_Digital-Forms-of-Migration-Control.pdf. P. 34-35.

8. Conclusie

Uit dit onderzoek moet worden geconcludeerd dat de wetswijziging van de Vreemdelingenwet op 21 november 2017, die de bevoegdheid voor het CGVS invoerde om smartphones en sociale mediaprofielen van verzoekers OIB te doorzoeken, niet in overeenstemming is met het toepasselijk (inter)nationaal asiel-, privacy- en gegevensbeschermingsrechtelijk kader. Voor de wettelijke vereisten in het asielrechtelijk kader (de Kwalificatierichtlijn) werd vastgesteld dat de wetswijziging een verkeerde omzetting ervan vormt en op onevenwichtige wijze de medewerkingsplicht van de verzoeker OIB benadrukt. Wat het privacy- en gegevensbeschermingsrechtelijk kader (de AVG, het EU-Handvest en het EVRM) betreft, vormen artikelen 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet een fundamentele beperking van het recht op gegevensbescherming van verzoekers OIB. De artikelen voldoen op zichzelf namelijk aan geen enkele van de in de AVG geformuleerde verwerkingsvereisten (behoorlijke en transparante verwerking, doelbinding, dataminimalisatie, nauwkeurigheid, opslagbeperking, vertrouwelijkheid/integriteit en rechtmatigheid van de verwerking). Tevens beantwoorden deze artikelen aan geen enkele van de voorwaarden voor een gerechtvaardigde beperking van het recht op privacy en gegevensbescherming (gerechtvaardigd doel, noodzaak en proportionaliteit in een democratische samenleving en respect voor de wezenlijke inhoud van de fundamentele rechten). De onderzoeksbevoegdheid van het CGVS met betrekking tot smartphones en sociale mediaprofielen in verzoekprocedures OIB vormt dus een onmiskenbare schending van het recht op privacy en gegevensbescherming van de verzoekers.

De voorgestelde waarborgen om conformiteit met het asiel-, privacy- en gegevensbeschermingsrechtelijk kader te garanderen zouden afzonderlijk bepaalde tekortkomingen in de besproken wetswijziging (kunnen) remediëren. Er bestaan echter substantiële hindernissen voor het implementeren ervan en het aangekondigde KB blijkt hiervoor geen geschikt instrument. De voorgestelde waarborgen kunnen ten eerste niet cumulatief worden toegepast. Ten tweede brengen bepaalde waarborgen discriminatoire gevolgen met zich mee. Ten derde kan het gebrek aan het wettelijk vereist ‘algemeen belang’ of ‘gerechtvaardigd doel’ door geen enkele waarborg worden geremedieerd. Tot slot moet worden vastgesteld dat de ‘nadelen’ van artikelen 48/6, §1, lid 4 en 57/7, §2 van de Vreemdelingenwet (zowel de flagrante schending van de fundamentele rechten van verzoekers OIB, als de effectieve ‘kosten’ van de besproken onderzoeksbevoegdheid) onmogelijk opwegen tegen de minimale bewijswaarde en het te verwaarlozen ‘succespercentage’ van het doorzoeken van sociale mediaprofielen en smartphones in verzoekprocedures OIB.

Nationale wetgevers en asielautoriteiten lijken blindelings aan te nemen dat de identiteit, de herkomst of het asielrelaas van verzoekers OIB kunnen worden gereconstrueerd en afgeleid uit hun digitale sporen op sociale media en smartphones. Zo verdwijnen verzoekers OIB, met hun persoonlijke vluchtgeschiedenis, naar de achtergrond en worden ze gereduceerd tot een pure ‘gegevensverzameling’. Deze onrustwekkende evolutie draagt bij tot een dehumaniserend discours, wat open dialoog vertroebelt en efficiënte oplossingen blokkeert. De vraag of er überhaupt nog overtuigende bestaansredenen overblijven voor artikelen 48/6, §1, lid 4 en 57/7, §2 van de Belgische Vreemdelingenwet, moet, als conclusie van dit onderzoek, resoluut negatief worden beantwoord.