Tijdschrift voor Mensenrechten

TvMR

bpost
PB-PP | B-00000
BELGIE(N) - BELGIQUE

twintigste jaargang • januari-februari-maart 2022 • nr. 1
driemaandelijkse uitgave
TvMR is een initiatief van de Liga voor Mensenrechten v.z.w.

Inhoud

Update **2**

- Nieuwe wet dataretentie in de maak
- Digitale dienstenwet als nieuwe wapen tegen haatspraak
- Europees parlement bespreekt het gebruik van spyware

Editoriaal **3**

- Digitalisering daagt mensenrechten uit: een themanummer in tijden van (cyber)oorlogsvoering
  Catherine Van De Heyning

Artikel **5**

- De digitale dimensie van seksuele zelfexpressie: een bevrijding of een nieuwe weg naar criminaliteit?
  Aurélie Gilen & Noa Vreven
- Het filmen en verspreiden van beelden van een politieoptreden. 'Part of the job', of is er een grens?
  Ronny Saelens
- Drones in EU-geïntegreerd grensbeheer: Mensenrechtelijke aansprakelijkheid en het gebruik van drones in terugkeeroperaties
  Joyce De Coninck
- De controle op het gebruik van algoritmische surveillance onder druk? Een exploratie door de lens van de relationele ethiek
  Rosamunde van Brakel

Interview **29**

- De AI-rechter: is artificiële intelligentie een bedreiging voor het recht op een eerlijk proces? Een kort gesprek met Nathalie Smuha
  Willem Debeuckelaere

Rechtspraak **31**

- "The world in my pocket." Het politioneel uitlezen van een smartphone, bekeken in het licht van artikel 8 EVRM
  Pieter Tersago
- De persvrijheid verhindert de vrijgave van gebruikersgegevens op discussiefora, of toch in bepaalde gevallen
  Laura Coeckelberghs

Afgiftekantoor: 9000 Gent Nieuwevaart
Bg TvMR PA3A9108
Afzendadres: Liga voor Mensenrechten
Gebroeders De Smetstraat 75
9000 Gent
V.U.: Kati Verstrepen
Gebroeders De Smetstraat 75
9000 Gent

LIGA VOOR MENSENRECHTEN
WWW.MENSENRECHTEN.BE

Colofon

TvMR
Tijdschrift voor Mensenrechten
Driemaandelijkse uitgave
Verschijnt vier keer per jaar
Aanbevolen citeerwijze: TvMR

ISSN 1379-0250

***Tijdschrift voor Mensenrechten* is een initiatief van de Liga voor Mensenrechten.**

Abonnement op TvMR? Bel 09 223 07 38

Redactiesecretariaat
Liga voor Mensenrechten vzw
Gebroeders De Smetstraat 75, 9000 Gent
tel: 09 223 07 38
e-mail: info@mensenrechten.be
website: https://mensenrechten.be

Jaarabonnementen tijdschriften
Abonnement op Tijdschrift voor Mensenrechten: €35
Abonnement op Fatik, tijdschrift voor Strafbeleid en Gevangeniswezen: €40
Abonnement op beide tijdschriften: €70
Steunabonnement op beide tijdschriften: €96

rek.nr. BE34 0011 2701 3290

Meer informatie bij Liga voor Mensenrechten.

TvMR online
Je kan TvMR online raadplegen.
Het meest recente nummer is beschikbaar voor abonnees.

Update

Nieuwe wet dataretentie in de maak

Minister van Justitie Van Quickenborne kondigde aan dat het nieuwe wetsontwerp voor het verplicht bewaren van communicatiegegevens kortelings in het parlement zal worden ingediend. In navolging van rechtspraak van het Hof van Justitie, vernietigde het Grondwettelijk Hof de vorige regelgeving in 2021. De nieuwe wetgeving voert opnieuw een verplichte bewaring van communicatiegegevens in, maar beperkt deze bewaring tot bepaalde zones. In tegenstelling tot België, besliste de Duitse regering al af te zien van een nieuwe bewaarplicht voor locatie- en verkeersgegevens.

Digitale dienstenwet als nieuwe wapen tegen haatspraak

Einde januari ging het voorstel van nieuwe digitale dienstenwet (Digital Services Act) van de EU de laatste rechte lijn in. Deze wetgeving moet digitale diensten, waaronder sociale media en andere platformen, transparanter en democratischer maken. Er komt meer controle op het beleid van de platformen, waarbij de bescherming van persvrijheid centraal staat. Ook zullen platformen aangemoedigd worden om meer te doen tegen schadelijke content zoals online haatspraak, bedreigingen, en kinder- en andere beeldmisbruikmateriaal. De Europese Commissie hoopt dat de finale tekst voor de zomer wordt goedgekeurd en in 2023 in werking treedt.

Europees parlement bespreekt het gebruik van spyware

Het schandaal rond het gebruik van de Israëlische technologie Pegasus voor spionage van staatshoofden, journalisten, dissidenten en mensenrechtenverdedigers krijgt een Europees staartje. Het Europese parlement heeft besloten het gebruik van deze technologie door de lidstaten van de Europese Unie verder te onderzoeken en aanbevelingen te formuleren. De Europese toezichthouder voor gegevensbescherming (EDPB) noemde deze technologie reeds een gevaar voor de democratie en rechtsstaat, en schaarde zich achter de oproep van NGO's om het gebruik van spyware in de EU te verbieden.

Digitalisering daagt mensenrechten uit: een themanummer in tijden van (cyber)oorlogsvoering

Terwijl dit editoriaal geschreven wordt, gaan de burgers in Kiev en andere Oekraïense steden opnieuw een bange nacht tegemoet, schuilend voor de artillerie van de Russische troepen. Meer dan eender welk voorgaand conflict, wordt deze oorlog niet enkel te land, ter zee en in de lucht gevoerd, maar ook in cyberspace, met digitale wapens. Zowel staatsgesteunde als losse cybergroepen vinden elkaar om via DDOS-aanvallen websites en digitale diensten langs beide kanten plat te leggen of met goed gerichte ransomware-aanvallen hele netwerken onbruikbaar te maken. De digitale arena is een constante *strike en counterstrike* aan cyberaanvallen van het pro-Russische en pro-Oekraïense kamp met een enorme impact op mensenlevens. Cyberaanvallen op ziekenhuizen betekenen immers dat operaties afgelast of verplaatst moeten worden, waardoor patiënten komen te overlijden. Het digitaal platleggen van militaire infrastructuur kan ook de fysieke verdediging van een land lam leggen. Het versleutelen van hulpdiensten betekent dat ambulances, brandweer of politie noodsignalen niet meer kunnen detecteren. Kortom, ook digitale oorlogsvoering kost levens. Dergelijke aanvallen op kritieke infrastructuur en communicatiekanalen zijn niet de enige wapens in het huidige wapenarsenaal van de moderne oorlogsvoering. Sociale media en andere platformen worden lustig gebruikt door de verschillende partijen om propaganda te voeren en de realiteit te verdraaien. Door het gebruik van internet kan desinformatie in luttele seconden over de hele wereld worden verspreid, zonder dat er enige controle bestaat op de waarheidsgetrouwheid. Door de creatie van fictieve profielen lijkt het alsof bepaalde boodschappen door een massa aan volgers gesteund wordt, terwijl het in werkelijkheid een volledig gestuurd mechanisme is dat wordt ingezet om een bepaalde visie op de realiteit door te drukken. De verwatering van waarheid en realiteit wordt nog verder versterkt door de geavanceerde technologieën om beelden te veranderen en zelfs levensechte beelden van personen te maken door het gebruik van deepfake-technologie.

Naast de aanvallen op infrastructuur en de waarheid, biedt digitalisering nog een derde wapen voor moderne oorlogsvoering, namelijk de dataficatie van de wereld. Telkens we klikken, zoeken of toetsen, laten we digitale kruimels van onszelf op het web achter, die autoriteiten en private spelers gretig verzamelen. Dit maakt een 24/7-controle op ons doen en laten mogelijk, en daardoor manipulatie van ons gedrag en gedachten. Kennis is macht, en dat geldt des te meer wanneer deze kennis door een onuitputtelijke hoeveelheid data van de eigen bevolking en de vijand gevoed wordt. Burgers worden niet gespaard in deze moderne digitale oorlogsvoering. The New York Times berichtte in 2021 dat Iraanse cybergroepen via hacking buitgemaakte gevoelige informatie van een Israëlische LGBTQ dating site online plaatsten (Fassihi en Bergman, 27 november 2021). Een cyberaanval op Iran zorgde er dan weer voor dat de 4300 tankstations van het land leeg kwamen te staan, met ellenlange files aan de stations tot gevolg.

Digitalisering daagt dus de bescherming van mensenrechten uit en dit in het bijzonder wanneer gedigitaliseerde beschavingen elkaar te lijf gaan. Deze speciale editie over de impact van digitalisering op mensenrechten komt dus geen dag te vroeg (ook al staat het nummer los van de oorlog in Oekraïne). Aurélie Gilen en Noa Vreven schrijven over de impact van digitalisering op seksueel geweld. Ook Ronny Staelens heeft het over het gebruik en misbruik van beeldmateriaal en dit keer bij politieacties. Joyce De Coninck verlegt het terrein naar het gebruik van digital surveillance in migratiepolitiek. Rosamunde Van Brakel gaat dan weer in op de ethische aspecten van het gebruik van algoritmes bij politionele surveillance. In een kort interview licht Nathalie Smuha vervolgens de impact van artificiële intelligentie in de rechtspraak toe. Pieter Tersago buigt zich over de digitale bewijsgaring in het strafrechtelijk onderzoek. En Laura Coeckelberghs besluit het themanummer door de focus te leggen op de aansprakelijkheid van platformen voor commentaren en de bescherming van de vrije meningsuiting. Deze goed gevulde editie gaat in op de uitdaging die digitalisering stelt voor de bescherming van mensenrechten. Naast de gevaren mogen we ook niet vergeten welke rijkdom digitalisering ons brengt: hoe we kunnen communiceren met de hele wereld en directe toegang hebben tot informatie voorbij de voormalige poorten van de censuur. Elke technologie en elke techniek brengt kansen en gevaren met zich mee. Niet de digitalisering op zich, maar wel onze omgang ermee bepaalt de impact op mensenrechten. Het gebrek aan statelijke samenwerking in cyberspace, controle- en handhavingsmechanismen, afwezigheid van doeltreffende regelgeving over ontwerp, productie, gebruik en export van digitale technologie, en de ongebreidelde macht van big Tech zijn ernstige risico's voor onze rechtstaat, democratie en de bescherming van mensenrechten. Het Russisch–Oekraïense conflict toont aan hoe broodnodig een herdenking van digitalisering is om de winsten van deze technologie te verzilveren en de risico's te beperken. De parafrasering van de bekende quote van de Amerikaanse historicus Melvin Kranzberg over technologie vat dit themanummer dan ook goed samen: "*Digitalisering is niet goed of slecht, maar evenmin is ze neutraal.*"

Catherine Van De Heyning*

* Docent UAntwerpen en redactielid TvMR.

De digitale dimensie van seksuele zelfexpressie: een bevrijding of een nieuwe weg naar criminaliteit?

Aurélie[1] Gilen & Noa Vreven[2]

Sociale media zijn een integraal onderdeel van het dagelijkse leven. Ze zijn een instrument voor informatievergaring, communicatie[3] en zelfontplooiing en -expressie.[4] De mogelijkheid om seksueel getinte berichten en foto's uit te wisselen, creëert een nieuwe dimensie in onze seksuele beleving.[5] Sociale media helpen om onze seksuele identiteit, hoe we over onszelf denken als seksueel wezen, verder te exploreren.[6] Het internet vormt een seksueel medium dat fungeert als een schakel tussen seksuele fantasieën of verlangens en het daadwerkelijk uitvoeren ervan. Dit faciliteert het seksuele experimenteren, maar legt eveneens de basis voor een nieuwe vorm van intimiteit. Bovendien verlaagt het ook bestaande seksuele drempels en zet het de deur open om met meerdere potentiële partners in contact te komen.

Dit komt gevoelens van vrijheid, zelfacceptatie en seksuele empowerment ten goede.[7] Of toch ten minste wanneer deze gedragingen in een consensuele context gebeuren. In het snelle, afstandelijke, korte en soms anonieme karakter van sociale media schuilt meteen ook de keerzijde van deze digitale medaille.[8] Hoewel velen de vruchten plukken van deze vooruitgang, ligt de kans dat seksueel getinte foto's doorgestuurd worden zonder toestemming van de persoon in kwestie, steeds op de loer.[9] Er is dus met andere woorden een nieuwe weg naar slachtoffer- en daderschap getimmerd.

Dit artikel illustreert op welke manier sociale media nieuwe uitdagingen creëren voor de bescherming van mensenrechten. Meer specifiek ligt de focus op de verspreiding van intieme foto's vanuit een sociaalpsychologisch en juridisch perspectief. Eerst nemen we de relevante terminologie, de prevalentiecijfers en de impact van het fenomeen onder de loep. Vervolgens bekijken we welk juridisch kader geldt voor de preventie en bestraffing van zulke daden. Tot slot gaan we dieper in op hoe dit fenomeen vanuit een gendergebonden perspectief benaderd wordt. Hierbij zetten we uiteen hoe deze tendens zich in de juridische en sociale normen reflecteert.

Het niet-consensueel verspreiden van seksueel getinte foto's

Terminologie

Het niet-consensueel verspreiden van intieme foto's, of NCII (*non-consensual dissemination of intimate images*), is vandaag een wijdverspreid fenomeen.[10] Waar het maken van de beelden initieel kan plaatsvinden met instemming van het slachtoffer, bv. bij *sexting*, heeft het gebrek aan toestemming betrekking op de latere verspreiding

1 BELSPO onderzoeker UAntwerpen, onderzoeksgroep MIOS.
2 Aspirant-onderzoeker UAntwerpen, onderzoeksgroep Overheid & Recht.
3 L. M. Cookingham en G.L. Ryan, "The Impact of Social Media on the Sexual and Social Wellness of Adolescents", *Journal of Pediatric and Adolescent Gynecology* 2015, 2-5.
4 N.M. Döring, "The internet's impact on sexuality: A critical review of 15 years of research", *Computers in Human Behaviour* 2009, 1089-1101.
5 M.W. Ross, "Typing, Doing and being: Sexuality and the internet", *Journal of Sex Research* 2005, 342-352.
6 M. Walrave, J. Van Ouytsel, E. Van Gool, K. Ponnet en E. Peeters, "Sexting: adolescents' perceptions of the applications used for, motivations for, and consequences of sexting", *Journal of Youth Studies* 2016, 446-470.
7 N.M. Döring, supra noot 4, 1089-1101; N.M. Ross, *supra* noot 5, 342-352.
8 A. Moore en P. Reynolds, *Childhood and Sexuality: Contemporary Issues and Debates* London, Macmillan Publishers, 2018, 225-246; N. M. Döring, *supra* noot 4, 1089-1101.
9 A. Powell, N. Henry, A. Flynn en A.J Scott, "Image-based sexual abuse: the extent, nature and predictors of perpetration in a community sample of Australian residents", *Computers in Human Behavior* 2018, 393-402.
10 J. Beyens en E. Lievens, "Niet-consensuele verspreiding van seksuele beelden: Analyse van wetgevende initiatieven in de Verenigde Staten, het Verenigd Koninkrijk en België", *NJW* 2016, nr. 348, 654.

van het beeldmateriaal.[11] NCII leidt bijgevolg tot een ernstige vertrouwensbreuk. Meer nog, de intentie van de dader bestaat er vaak in om het slachtoffer te vernederen, intimideren of chanteren. Het betekent daarom ook een ernstige aantasting van de privacy en seksuele integriteit van slachtoffers.[12]

In de literatuur wordt NCII onder verschillende noemers thuisgebracht. Wraakporno en non-consensuele pornografie worden tot op heden in de literatuur als referentiepunt voor dit fenomeen gebruikt.[13] Deze terminologieën impliceren dat NCII optreedt als gevolg van wraak of "intentioneel gecreëerd wordt voor consumptie door anderen".[14] Onderzoek toont echter aan dat de beweegredenen zich verder strekken: profijt, humor, seksuele bevrediging en het verhogen van de sociale status staan ook in het rijtje. Het gebruik van termen zoals "image-based sexual abuse (IBSA)"[15] en "technology-facilitated sexual violence" genieten dan ook de voorkeur van wetenschappers.[16] IBSA maakt een onderscheid tussen het dreigen met doorsturen, het effectief doorsturen en het maken van seksueel getinte foto's zonder toestemming.[17] Het gebrek aan homogeniteit in definiëring heeft evenwel tot gevolg dat de exacte prevalentie van dit fenomeen moeilijk vast te stellen is.[18] Wij consulteerden voor de prevalentiecijfers (onmiddellijk hieronder) literatuur die enkel focust op het doorsturen van seksueel getinte foto's.

Prevalentie

Een systematische review over NCII van Patel en Roesch was gebaseerd op 23 studies, daterend van 2015 tot en met 2019, waarin de prevalentie van NCII werd onderzocht. 3,34% tot 22,9% van de deelnemers gaf aan ooit al eens zelf seksueel getinte foto's te hebben doorgestuurd zonder toestemming van de betrokken partij. Het gemiddelde van de prevalentiecijfers in deze studies, toonde aan dat 8,78% al ooit dader was.[19] Een Belgisch onderzoek van Sensoa, waarbij 9% aangaf dader te zijn geweest, ligt in de lijn van dit resultaat.[20]

De systematische review van Patel en Roesch wijst erop dat het aantal slachtoffers tussen de 1,1% en de 24,09% ligt. Het gemiddelde van de prevalentiecijfers geeft ook aan dat van 12% van alle personen ooit al eens een seksueel getinte foto werd doorgestuurd zonder toestemming.[21] Een survey uit 2019 toonde aan dat 9,8% van de Vlaamse jongeren al ooit een seksueel getinte foto doorstuurde zonder toestemming van de afgebeelde persoon.[22] In België was maar liefst 21 % bezorgd over de verdere verspreiding van hun intieme foto's.[23] In de literatuur wordt vaak verwezen naar een mannelijke overhelling in daderschap en naar vrouwen die de overgrote meerderheid van de slachtoffers vormen.[24] Deze studies staan haaks op onderzoek dat aantoont dat evenveel, of zelfs meer, mannen dan vrouwen slachtoffer zijn van NCII.[25] Uit de cijfers blijkt dat de rol van gender bij het fenomeen geenszins eenduidig is.

De psychologische en sociale impact

Het medium dat zelfexpressie en -exploratie bewerkstelligt, kan bij slachtoffers van NCII pijnlijke en (soms) permanente herinneringen in zich sluiten.[26] Wanneer hogere instanties er niet in slagen

11 D. Ryan, "European remedial coherence in the regulation of non-consensual disclosure of sexual images", *Computer Law & Security Review* 2018, 1055.
12 M. Sepec, "Revenge pornography or non-consensual dissemination of sexually explicit material as a sexual offence or as a privacy violation offence", *International Journal of Cyber Criminology* 2019, 419.
13 A. Eaton en C. McGlynn, "The psychology of Nonconsensual Porn: Understanding and Addressing a Growing Form of Sexual Violence ", *Policy Insights from the Behavioral and Brain Sciences* 2020, 190-197; J. Beyens en E. Lievens, *supra* noot 10, 654.
14 U. Patel en R. Roesch, "The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Systematic Review", *Trauma, Violence & Abuse* 2020, 1-16.
15 C. McGlynn en E. Rackley, "Image-Based Sexual Abuse", *Oxford Journal of Legal Studies* 2017, 5; N. Henry, A. Flynn en A. Powell, "Image-based sexual abuse: Victims and perpetrators", *Trends & Issues in Crime and Criminal Justice* 2019, nr. 572, 1.
16 A. Powell, N. Henry, A. Flynn, A.J. Scott, *supra* noot 9, 393-402; A. Eaton en C. McGlynn, *supra* noot 13, 190-197; U. Patel en R. Roesch, *supra* noot 14, 1-16.
17 A. Powell, N. Henry, A. Flynn en A.J. Scott, supra noot 9, 393-402; U. Patel en R. Roesch, *supra* noot 14, 1-16.
18 U. Patel en R. Roesch, *supra* noot 14, 1-16.
19 *Ibid*.
20 Sensoa, sexting bij jongeren: feiten en cijfers, geraadpleegd op 10 februari 2022, https://www.sensoa.be/sexting-bij-jongeren-feiten-en-cijfers.
21 U. Patel en R. Roesch, *supra* noot 14, 1-16.
22 J. Van Ouytsel, M. Walrave, L. De Marez, B. Vanhaelewyn en K. Ponnet, "Sexting, pressured sexting and image-based sexual abuse among a weighted-sample of heterosexual and LGB-youth", *Computers in Human Behavior* 2021, 106630.
23 Apestaartjaren, de digitale leefwereld van jongeren, geraadpleegd op 14 februari 2022, https://www.apestaartjaren.be/index.php.
24 M.C. DiTullio en M.M. Sullivan, "A Feminist-Informed Narrative Approach: Treating Clients Who Have Experienced Image-based Sexual Abuse", *Journal of Feminist Family Therapy* 2019, 100-113; A. Powell, N. Henry, A. Flynn en A.J. Scott, *supra* noot 9, 393-402.
25 A. Flynn en N. Henry, The Palgrave Handbook of International Cybercrime and Cyberdeviance: Image-Based Sexual Abuse: A Feminist Criminological Approach, Switzerland, Palgrave Macmillan, 2020, 1109-1129.
26 J. Morahan-Martin, "Women and the Internet: Promise and Perils", *Journal of Cyberpsychology & Behavior* 2000, 683-691.

om het verspreiden van foto's te onderscheppen of stop te zetten, dan wordt in de literatuur ook wel verwezen naar de "digitale voetprint". Het internet vergemakkelijkt het verspreiden van deze seksueel getinte foto's. Deze worden niet alleen sneller, maar ook naar een breder publiek verspreid, en werken het permanente circuleren en bestaan van de foto's in de hand.[27] Onderzoek verwijst ook wel naar "de digitale laag van trauma" die aanwezig is in slachtoffers van NCII.[28] De psychologische en sociale gevolgen van NCII mogen niet worden onderschat. Het optreden van depressieve -, angst - en posttraumatische stress symptomen is eerder regel dan uitzondering bij deze groep van slachtoffers.[29] Slachtoffers ervaren vaak gevoelens van schaamte en schuld. Bovendien wordt het vertrouwen in de ander, wat fundamenteel is voor interpersoonlijke relaties, geschonden. Als gevolg hiervan treedt sociale isolatie op en een inherente angst om opnieuw een (digitale) connectie met de ander aan te gaan.[30] Wetenschappers merken dezelfde typen gevolgen op bij slachtoffers van fysiek seksueel geweld.[31] Zowel offline als online seksueel geweld kunnen hierdoor op het "continuüm van seksueel geweld" worden geplaatst.[32] Dit sluit aan bij de opvatting dat (de gevolgen van) online ervaringen niet te onderscheiden zijn van offline ervaringen en dat onze identiteit wortelt in beide werelden.[33]

NCII en de rol van mensenrechten

Meer dan een strafrechtelijk fenomeen

Doordat NCII een relatief recente vorm van seksueel geweld is, en bij gebrek aan toepasselijke supranationale normen[34], wordt dit fenomeen vaak gefragmenteerd aangepakt.[35] Zo wordt NCII niet overal bestraft als seksueel misdrijf of is er een gebrek aan geschikte bepalingen.[36] Sommige Europese landen hebben geopteerd om NCII te reguleren via gerichte strafrechtelijke sancties, waar andere landen een beroep doen op bestaande strafrechtelijke of civielrechtelijke maatregelen.[37] Door deze verschillende benaderingen, maar ook door het veelal grensoverschrijdende karakter van NCII (aangezien het zich in cyberspace afspeelt en gefaciliteerd wordt door grote *big tech* spelers), rijst de vraag of een supranationale of internationale benadering niet beter zou zijn om dit fenomeen aan te pakken. Deze vraagstelling is niet beperkt tot de nationale rechtshandhaving, maar heeft ook een belangrijke mensenrechtelijke component. Bij gebrek aan een supranationaal of internationaal mensenrechtelijk kader voor online en technologie-gefaciliteerd seksueel geweld, beschikken de nationale wetgevers vooralsnog over een grote beoordelingsruimte voor de aanpak van online seksueel geweld.[38] In de continentale rechtssystemen wordt NCII nog veelal beschouwd als een inbreuk op het privéleven en de waardigheid van een individu in plaats van een ernstig seksueel misdrijf dat de seksuele integriteit en identiteit schendt.[39] Er wordt beargumenteerd dat deze stijgende tendens in Europa uniforme normen vereist om de mensenrechten en vrijheden op seksueel vlak optimaal te beschermen.[40] De Raad van Europa heeft alvast getracht de bestaande fragmentatie te remediëren via het Verdrag van Istanboel. Dit Verdrag maakt het mogelijk om een zekere mate van harmonisatie te bereiken tussen de verdragspartijen (zie hierna).[41]

Internationaal en Europees juridisch kader

Op het internationale niveau wordt steeds meer aandacht besteed aan de impact van digitalisering op mensenrechten. Een eerste erkenning van cybergeweld zagen we in toepassing van het Verdrag van de Verenigde Naties inzake de uitbanning van alle vormen van discriminatie tegen

27 L.M. Cookingham en G.L. Ryan, supra noot 3, 2-5; A. Moore en R. Reynolds, *supra* noot 8, 225-246.
28 O. Marques, *The Emerald International Handbook of Technology-Facilitated Violence and Abuse: Intimate Image Dissemination and Consent in a Digital Age: Perspectives from the Front Line*, Bingley, Emerald Publishing Limited, 2021, 309-328.
29 U. Patel en R. Roesch, *supra* noot 14, 1-16; M.C. DiTullio en M.M. Sullivan, *supra* noot 24 , 100-113.
30 A. Eaton en C. McGlynn, *supra* noot 13, 190-197.
31 U. Patel en R. Roesch, *supra* noot 14, 1-16.
32 A. Eaton en C. McGlynn, *supra* noot 13, 190-197.
33 J. Morahan-Martin, *supra* noot 26 , 683-691.
34 In zover het gaat over online verspreiding van seksuele beelden van minderjarigen, overlappen zulke daden ten dele met de verspreiding van kindermisbruikmateriaal wat wel reeds in supranationale rechtelijke normen werd opgenomen. Zie Council of Europe Convention on Cybercrime (CETS No. 185), 23 november 2001, te raadplegen: https://rm.coe.int/1680081561 en zie ook Richtlijn 2011/93/EU, art. 383bis Strafwetboek, en Lanzarote declaration te raadplegen: https://www.coe.int/en/web/children/lanzarote-convention.
35 O. Jurasz en K. Barker, "Sexual violence in the digital age: A criminal law conundrum?", *German Law Journal* 2021, 792.
36 B. Burghardt en L. Steinl, "Sexual Violence and Criminal Justice in the 21st Century", *German Law Journal* 2021, 693.
37 D. Ryan, *supra* noot 11, 1066.
38 O. Jurasz en K. Barker, *supra* noot 35, 792.
39 M. Sepec, *supra* noot 12, 421-422.
40 O. Dudorov en Y. Pysmenskyy, "Sexual sphere: Thin line between freedom and crime", *International Journal for Legal Research* 2019, 317.
41 O. Jurasz en K. Barker, *supra* noot 35, 798.

vrouwen (CEDAW).[42] De focus lag hier op hoe nieuwe technologieën gender-gerelateerd geweld tegen vrouwen beïnvloeden en faciliteren. In 2017 verduidelijkte het CEDAW-Comité in zijn Algemene Aanbeveling nr. 35 dat het Verdrag ook in zijn geheel van toepassing is op door technologie bemiddelde omgevingen, zoals het internet.[43] Deze stap bevestigt de visie binnen de Verenigde Naties dat dezelfde rechten waarover men offline beschikt, ook online dienen te worden beschermd.[44]

In 2018 erkende de Speciale VN-Rapporteur betreffende geweld tegen vrouwen de uiteenlopende aard van zulk geweld online, inclusief geseksualiseerde vormen ervan.[45] In het bijhorende rapport wordt het zonder toestemming online publiceren van intieme foto's als een schending van het recht op privacy en waardigheid bestempeld. Staten horen online geweld tegen vrouwen te erkennen als een ernstige schending van de mensenrechten en een vorm van discriminatie en geweld tegen vrouwen, aldus de VN-Rapporteur. Bijgevolg moeten staten de internationale mensenrechteninstrumenten adequaat toepassen en voorzien in een nationaal rechtskader dat voldoende bescherming biedt aan vrouwen in een online context.[46] Meer nog, het rapport beveelt de volledige strafbaarstelling van geweld tegen vrouwen aan.[47]

Het groeiende probleem van de niet-consensuele verspreiding van seksuele beelden wordt ook erkend op Europees niveau door de Raad van Europa. Het Verdrag inzake het voorkomen en bestrijden van geweld tegen vrouwen en huiselijk geweld (Verdrag van Istanboel) was een belangrijke stap richting de uniformisering en standaardisering van het strafrechtelijk beleid van de verdragspartijen op het gebied van seksuele betrekkingen.[48] Recent publiceerde GREVIO, het onafhankelijke orgaan van experten dat toezicht houdt op de uitvoering van dit Verdrag, een aanbeveling betreffende de digitale dimensie van geweld tegen vrouwen. GREVIO erkent dat geweld in de digitale sfeer, waaronder '*non-consensual image or video sharing*', een van de centrale vormen uitmaakt van gender gerelateerd geweld tegen vrouwen. De verdragspartijen zijn verplicht deze digitale dimensie volledig te incorporeren in hun algemene aanpak ter preventie van geweld tegen vrouwen, ter ondersteuning en bescherming van de slachtoffers en tot slot, ter vervolging van de daders.[49]

Toepassing in de rechtspraak van het EHRM

Bij gebrek aan afdwingbare supranationale normen die de online inbreuk op de seksuele integriteit beschermen, wordt deze problematiek vanuit de klassieke mensenrechten benaderd. In de literatuur wordt beargumenteerd dat NCII raakt aan fundamentele rechten van het individu zoals het recht op privéleven, autonomie en menselijke waardigheid. Bijgevolg kan het Europees Verdrag voor de rechten van de mens (EVRM) een belangrijk instrument zijn in de bestrijding van het fenomeen. Bepaalde daden van cybergeweld, waaronder NCII, werden door het Europees Hof voor de Rechten van de Mens (EHRM) dan ook reeds beoordeeld als een onmenselijke of vernederende behandeling in de zin van Artikel 3 EVRM en als een inbreuk op het recht op privéleven in de zin van Artikel 8 EVRM.[50] In recente rechtspraak van het EHRM wordt duidelijk hoe digitalisering de visie op mensenrechten verandert en aanleiding geeft tot een nieuw perspectief op non-fysiek geweld. Zo erkende het Hof in de zaak *Buturuga t. Roemenië* [51] het veelzijdige karakter van huiselijk geweld en verwees het voor het eerst naar cybergeweld als een van de vormen waarin dit misbruik zich kan manifesteren.[52] Er werd geoordeeld dat nationale autoriteiten de digitale dimensie in rekening moeten brengen tijdens het onderzoek naar en de vervolging van huiselijk geweld.[53] In deze zaak ging het echter niet om NCII maar om het heimelijk lezen van online correspondentie door de partner, wat volgens het Hof een privacy inbreuk in

42 Verenigde Naties Verdrag inzake de Uitbanning van alle Vormen van Discriminatie van Vrouwen, 19 december 1979.
43 CEDAW-Committee General Recommendation No. 35 on gender-based violence, 14 July 2017, te raadplegen: https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf.
44 United Nations General Assembly [UNGA], 2018; United Nations Human Rights Council [UNHRC], 2016.
45 United Nations Human Rights Council, Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences on Online Violence Against Women and Girls from a Human Rights Perspective, U.N. Doc. A/HRC/38/47, 18 June 2018, parapara 27 & 31.
46 *Ibid*., p. 18-19.
47 *Ibid*., parapara 100-102.
48 Raad van Europa Verdrag van de Raad van Europa inzake het voorkomen en bestrijden van geweld tegen vrouwen en huiselijk geweld, 2011.; O. Dudorov en Y. Pysmenskyy, *supra* noot 40, 302.
49 GREVIO General recommendation no. 1 on the digital dimension of violence against women, aangenomen 20 oktober 2021, te raadplegen: www.coe.int/en/web/istanbul-convention/-/grevio-publishes-its-general-recommendation-no-1.
50 EHRM 9 juli 2019, nr. 41261/17, Volodina/Rusland (Nr. 1).
51 EHRM 11 februari 2020, nr. 56867/15, Buturuga/Roemenië.
52 F. Van Leeuwen, "Cyberviolence, domestic abuse and lack of a gender-sensitive approach – reflections on Buturuga versus Romania", Strasbourg Observers 2020, geraadpleegd op 9 februari 2022, https://strasbourgobservers.com/2020/03/11/cyberviolence-domestic-abuse-and-lack-of-a-gender-sensitive-approach-reflections-on-buturuga-versus-romania/; Buturuga/Roemenië, *supra* noot 51, para 74.
53 Buturuga/Roemenië, *supra* noot 51, para 78.

de zin van Artikel 8 EVRM uitmaakt.[54] Meer nog, de feiten gingen gepaard met bedreigingen, intimidatie en fysiek geweld in de zin van Artikel 3 EVRM.[55] Het Hof leek de samenhang tussen cybergeweld en fysiek geweld te benadrukken aangezien het oordeelde dat lidstaten de positieve verplichting hebben om aspecten van cybergeweld mee te nemen in de behandeling van huiselijk geweld. Desondanks behandelde het Hof Artikel 8 en Artikel 3 EVRM afzonderlijk in de beoordeling van deze zaak. Bijgevolg werden cybergeweld en fysiek huiselijk geweld als afzonderlijke kwesties naar voren geschoven. Zo gaf het Hof de indruk dat online surveillance niet als ernstig genoeg kan worden beschouwd om te kwalificeren als een onmenselijke behandeling.[56]

In de zaak *Volodina t. Rusland* (n°1) benadrukte het Hof dat ook ernstige vormen van non-fysiek geweld binnen de werkingssfeer van Artikel 3 EVRM kunnen vallen.[57] In de hierop volgende zaak, *Volodina t. Rusland* (n°2), kwalificeerde het Hof cybergeweld als een ernstige mensenrechtenschending dat als belangrijk onderdeel van huiselijk geweld moet worden beschouwd. Hierbij hebben de lidstaten onder Artikel 8 EVRM en in sommige gevallen onder Artikel 3 EVRM de verplichting om ook in een online context te voorzien in een adequaat wettelijk kader om slachtoffers te beschermen en de feiten effectief te onderzoeken en bestraffen.[58] In deze Russische zaak ging het om fysiek huiselijk geweld in combinatie met de online publicatie van intieme foto's en persoonlijke informatie zonder de toestemming van het slachtoffer. Het Hof oordeelde dat zulke feiten een vorm van cybergeweld uitmaken die de fysieke en psychologische integriteit van de persoon ernstig aantasten.[59] Ondanks dat de Russische autoriteiten beschikten over het juridisch kader om zulke daden van cybergeweld als inbreuk op het privéleven te onderzoeken en vervolgen, faalden ze om prompt en grondig strafrechtelijk gevolg te geven aan deze zaak.[60] Bijgevolg bleven de feiten onbestraft en besloot het Hof in *Volodina t. Rusland* (n°2) unaniem tot een schending van Artikel 8 EVRM.[61] Het arrest verduidelijkt in belangrijke mate de intrinsieke relatie tussen fysiek en online geweld. Het Hof benadrukte namelijk dat Artikel 8 EVRM de positieve verplichting inhoudt in hoofde van de staten om een systeem te voorzien dat alle vormen van huiselijk geweld aanpakt. Deze verplichting geldt ongeacht het geweld zich offline dan wel online of in beide contexten voordoet.[62]

Gender en haar rol in NCII

Gender en NCII: een seksuologisch perspectief

"Vrouwen zijn slachtoffers, mannen zijn daders". Die stelling wordt bijna automatisch voor waar aangenomen en vloeit voort uit onze genderstereotype attitudes, normen en gedragingen. We proberen een gendergelijke beleving van seksualiteit na te streven. Dit ideaalbeeld stelt dat zowel vrouwen als mannen dezelfde seksuele rechten en verlangens hebben, maar ook dat ze dezelfde seksuele gedragingen kunnen stellen.

Onderzoek naar attitudes toont aan dat vrouwen die naaktfoto's van zichzelf maken, automatisch ook meer risico lopen om slachtoffer te worden. In tegenstelling tot mannen die, wanneer ze naaktfoto's van zichzelf maken, net minder risico lopen om slachtoffer te worden omdat zij worden verwacht seksueel actief en dominant te zijn. Een vrouw daarentegen, aldus de verwachting, dient zich seksueel passief en onderdanig op te stellen.[63] Seksuele passiviteit en ondergeschiktheid zijn ook niet voor niets de kenmerken van "het ideale slachtoffer" in onderzoek naar verkrachting.[64] Wanneer vrouwen zichzelf uitdrukken door seksueel getinte foto's te nemen, voldoen ze niet meer aan deze passiviteit. Dit verklaart waarom vrouwen sneller een zogezegd "aandeel" hebben in hun slachtofferschap of worden gezien als "slet", ook wel "victim-blaming" en "slut-shaming" genoemd.[65] Deze attitudes ondersteunen de resultaten waarin vrouwen vaker slachtoffer van NCII worden. Tegelijkertijd wordt een wereld waarin seksualiteit

54 Ibid., para 73-78.
55 Ibid., para 65-72.
56 F. Van Leeuwen, *supra* noot 52.
57 R. McQuigg, "The European Court of Human Rights and Domestic Violence: Volodina v. Russia", *International Human Rights Law Review* 2021, 158.; Volodina/Rusland (Nr. 1), *supra* noot 50, para 81.
58 EHRM 14 september 2021, nr. 40419/19, Volodina/Rusland (Nr. 2), para 49.
59 Volodina/Rusland (Nr. 1), *supra* noot 50, para 48.
60 Volodina/Rusland (Nr. 2), *supra* noot 58, para 57-58, para67.
61 Volodina/Rusland (Nr. 2), *supra* noot 58, para 68.
62 R. Costello, "Voldina v Russia (no. 2): Intimate Images, Domestic Violence and the Positive Obligations of Member States under Article 8 ECHR", *European Data Protection Law Review* 2021, 614-620.
63 L. Zvi, "The Double Standard Toward Female and Male Victims of Non-consensual Dissemination of Intimate Images", *Journal of Interpersonal Violence* 2021, 1-22; A. Moore en P. Reynolds, supra noot 8, 225-246 ; O. Marques, *supra* noot 28, 309-328.
64 L. Zvi, *supra* noot 63, 1-22.
65 J. Morahan-Martin, *supra* noot 26 , 683-691; O. Marques, *supra* noot 28, 309-328 ; L. Zvi, *supra* noot 63, 1-22.

door alle genders op dezelfde manier wordt beleefd, louter een impressie.

Naast het meten van attitudes, proberen verscheidene theorieën ook te verklaren waarom mannen daders van NCII zijn. Enerzijds bestaat er de evolutionaire stroming die stelt dat mannelijke seksuele agressie, waar NCII een onderdeel van uitmaakt, een natuurlijk gevolg van de evolutie is. Anderzijds beweren feministische aanhangers dat NCII vloeit uit de mannelijke drang naar macht en sociale controle. Meer psychologische en individualistische strekkingen stellen dat beweegredenen zoals middelenverslaving en traumatische jeugdervaringen, determinanten zijn van seksuele agressie.[66] Deze problematieken komen echter zowel bij mannen als vrouwen voor. Hiermee wordt dan het onderzoek, waarin evenveel mannen als vrouwen slachtoffer zijn, ondersteund.[67] Er zijn dan ook verscheidene bevindingen die de gelijke genderverdeling in slachtofferschap ondersteunen. Ten eerste, onderzoek dat peilt naar de prevalentie van slachtoffers maakt vaak gebruik van zelfrapportage. Mannen vinden het enerzijds gemakkelijker dan vrouwen om aan te geven dat ze dader zijn. Anderzijds rapporteren mannen dat ze zowel mannelijke als vrouwelijke slachtoffers maken.[68]

Ten tweede focust het merendeel van de literatuur op vrouwelijke slachtoffers waardoor data over mannelijke slachtoffers gewoon ontbreekt. Het beeld waarin mannen niet als slachtoffers worden gezien, kan worden verklaard door onderrapportage – zoals bij fysiek seksueel geweld – en de attitudes ten opzichte van slachtoffers die onze maatschappij erop nahoudt. Dit laatste verwijst naar het idee waarin vrouwen NCII zouden uitlokken door het maken van seksueel getinte foto's, ook al is dit een inherent onderdeel van de seksuele beleving.[69]

Ten derde kunnen er geen genderpatronen worden gevonden in de studies van de hierboven vermelde review.[70] Studies naar slachtofferschap waarin meer vrouwen deelnemen leiden niet noodzakelijk tot hogere prevalentiecijfers, bv. 50,5% van de deelnemers is vrouwelijk met een prevalentie van 4,5%[71] versus 65,4% van de deelnemers is vrouwelijk met een prevalentie van 1,1%.[72] Hetzelfde principe geldt voor studies naar daderschap: minder vrouwelijke deelnemers in de studies leidt niet noodzakelijk tot minder daderschap, bv. 48% van de deelnemers is vrouwelijk met een prevalentie van 22,9%[73] versus 82% van de deelnemers is vrouwelijk met een prevalentie van 15%.[74] Tot slot is er ook bewijs dat meer neigt naar een genderneutrale benadering van dit fenomeen daar "same-gender targeting" ook gerapporteerd wordt.[75] Bij dit laatste denken we dan ook spontaan aan het optreden van NCII binnen een LGBTQIA+ gemeenschap.

Dit brengt ons bij de hamvraag of gender een cruciale rol speelt in slachtoffer- en daderschap van NCII. Hoewel zowel de wetenschap als de maatschappij neigen naar de aanname dat vrouwen slachtoffers zijn en mannen daders, is er weinig onderzoek dat de rol van gender in NCII ook echt bestudeerd heeft.[76] Het dieper ingaan op de studies waarin evenveel mannen als vrouwen slachtoffer zijn, kan misschien een antwoord bieden.[77] Toch geven de resultaten duidelijk weer dat genderongelijke opvattingen en attitudes wanneer het over seksuele beleving gaat, bestaan. De volgende alinea's beschrijven hoe dit ook terug te vinden is in de juridische benadering van dit fenomeen. Dat onze samenleving al is geëvolueerd naar een patroon waarin gendergelijk denken/gedragen de norm is, is allicht een illusie. Maar de assumptie dat vrouwen steeds slachtoffers zijn en mannen altijd daders, dient met enige voorzichtigheid te worden benaderd.

Gender in het juridisch kader

Het fenomeen NCII (en meer algemeen:

66 L. Zvi, *supra* noot 63, 1-22.
67 M. Gámez-Guadix, C. Almendros, E. Borrajo en E. Calvete, "Prevalence and association of sexting and online sexual victimization among Spanish adults", *Sexuality Research and Sexual Policy* 2015, 145-154; A. Powell, N. Henry en A. Flynn, *Handbook of Critical Criminology: Image-based sexual abuse*, London, Routledge, 2018, 305-315.
68 A. Powell, N. Henry en A. Flynn en A.J. Scott, *supra* noot 9, 393-402.
69 O. Marques, supra noot 28, 309-328; Zvi, L., *supra* noot 63, 1-22.
70 U. Patel en R. Roesch, *supra* noot 14, 1-16.
71 D. Fido, C.A. Harper, M.A. Davis, D. Petronzi en S. Worrall, "Intrasexual competition as a predictor of women's judgements of revenge pornography", *Sexual Abuse* 2019, 295-320.
72 M. Gámez-Guadix en C. Almendros, *supra* noot 67 , 145-154.
73 J. Garcia, A.N. Gesselman, S.A. Silliman, B.L. Perry, K. Coe en H.E. Fisher, "Sexting among singles in the USA: Prevalence of sending, receiving, and sharing sexual messages and images", *Sexual Health* 2016, 428-435.
74 K. Walker en E. Sleath, " A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexuality explicit media", *Aggression and Violent Behavior* 9-24.
75 A. Eaton en C. McGlynn, *supra* noot 13, 190-197.
76 A. Powell, N. Henry en A. Flynn en A.J. Scott, *supra* noot 9, 393-402.
77 De huidige bijdrage werd geschreven in het kader van het BELSPO @ntidote project waar onder andere gender als criterium voor cybergeweld wordt onderzocht.

technologie-gefaciliteerd seksueel geweld) wordt doorgaans in het juridisch kader benaderd als een fundamentele genderkwestie.[78] Dit zien we zowel in de literatuur als in het internationale en regionale kader voor mensenrechten. Academici bespreken NCII overwegend als een prevalente vorm van online geweld tegen vrouwen en benadrukken het belang van het gendergebonden karakter van zulke daden.[79] Er wordt beargumenteerd dat het risico om met online vormen van geweld, zoals NCII, geconfronteerd te worden en de impact daarvan het hoogst is bij vrouwen.[80] Bijgevolg horen deze fenomenen kennelijk begrepen te worden tegen de achtergrond van diepgewortelde genderstereotypen en ongelijke genderverhoudingen.[81] Zulke benadering sluit aan bij de eerder vermelde 'gendered' constructie van de mannelijke dader en het vrouwelijk slachtoffer. Ook het reeds besproken internationaal juridisch kader – kindermisbruikmateriaal uitgezonderd – vertrekt vanuit een genderperspectief. Hier zagen we hoe cybergeweld in het CEDAW in verband wordt gebracht met discriminatie tegen vrouwen. Verder wordt er op internationaal niveau ook aangemoedigd om online geweld tegen vrouwen universeel te erkennen als een obstakel voor gendergelijkheid en meer algemeen, voor de rechten van de vrouw.[82] Vervolgens wordt het gendergerelateerde karakter van NCII ook doorgetrokken op het regionaal niveau. Zo is de bestrijding van genderstereotypen diep verankerd in het taalgebruik van het Verdrag van Istanboel en de bijbehorende aanbeveling betreffende de digitale dimensie van geweld tegen vrouwen. Daarnaast is de toenemende tendens van online geweld tegen vrouwen een ernstige ondermijning van de principes van gelijkheid en niet-discriminatie ingebed in de regionale mensenrechteninstrumenten. De Raad van Europa benadrukt deze tendens via de '2018-2023 Gender Equality Strategy', waarin het actief aanpakken van geweld tegen vrouwen – zowel offline als online – door de bestrijding van seksisme en genderstereotypering centraal staat. Bovendien zagen we dat in de rechtspraak van het EHRM het probleem van NCII tot op heden enkel beoordeeld werd binnen de context van huiselijk geweld tegen vrouwen. In deze zaken hanteerde het Hof een "gender-sensitive approach" en gaf het bijzondere aandacht aan de link tussen cybergeweld en genderongelijkheid. Tot slot verwees het Hof telkens ook naar de eerder vermelde internationale en regionale instrumenten.

Conclusie

Het verspreiden van intieme beelden zonder toestemming of NCII is een fenomeen dat zich steeds frequenter voordoet. Studies wijzen uit dat zulke daden een grote psychologische en sociale impact hebben op het slachtoffer. Bovendien wordt NCII juridisch gekwalificeerd als een ernstige aantasting van de privacy en de seksuele integriteit van het individu. Bijgevolg werden op internationaal en regionaal niveau reeds belangrijke stappen gezet richting mensrechtelijke bescherming voor slachtoffers van dit fenomeen. Onderzoek toont duidelijk de invloed van genderstereotypen aan op hoe de maatschappij en het recht NCII benaderen. Zonder te miskennen dat vrouwen wellicht meer kans hebben om slachtoffer te worden van NCII, trekken de prevalentie en het maatschappelijk beeld de huidige gendered juridische aanpak in twijfel. In de internationale en regionale normen wordt het fenomeen immers enkel gekaderd binnen de notie van gender-gerelateerd geweld tegen vrouwen. De Belgische wetgever verkoos daarentegen een genderneutrale strafrechtelijke aanpak. Zo staat de bescherming van de seksuele integriteit centraal in de Wet niet-consensuele verspreiding van seksuele beelden, ongeacht het gender van het slachtoffer. Deze visie kan leiden tot een reducerend effect waarbij maatschappelijke en juridische normen minder worden beïnvloed door genderstereotypen. De juridische erkenning van online geweld tegen vrouwen is in de eerste plaats een positieve evolutie. Men moet echter in vraag stellen of deze benadering niet kan verrijkt worden door ook rekening te houden met de noden en gevoeligheden van alle genderidentiteiten. Dit zou meer overeenstemmen met onze realiteit en bovendien zou het de aanhoudende strijd tegen genderongelijkheid ondersteunen.

78 N. Henry en A. Powell, *Sexual Violence in a Digital Age*, Londen, Palgrave Macmillan, 2017, 261.
79 C. McGlynn en E. Rackley, *supra* noot 15, 9.; D. Ryan, *supra* noot 11, 1069-1070.
80 D. Ryan, *supra* noot 11, 1069; K. Barker en O. Jurasz, "Online violence against women as an obstacle to gender equality: a critical view from Europe", *European Equality Law Review* 2020, 3.
81 Ibid., 3.
82 Ibid., 2.
83 Artikel 14 Europees Verdrag voor de Rechten van de Mens; Artikel 20 en 21 Handvest van de Grondrechten van de Europese Unie.
84 O. Jurasz en K. Barker, supra noot 35, 798.; Council of Europe Gender Equality Strategy 2018-2023, COE, 2018, te raadplegen: https://rm.coe.int/prems-093618-gbr-gender- equality-strategy-2023-web-a5/16808b47e1.
85 Volodina/Rusland (Nr. 2), *supra* noot 58, para 43.
86 Volodina/Rusland (Nr. 2), *supra* noot 58, para 66; Buturuga/Roemenië, *supra* noot 51, para 78.
87 Volodina/Rusland (Nr. 2), *supra* noot 58, para 22-24; Buturuga/Roemenië, *supra* noot 51, para 37-40.

Het filmen en verspreiden van beelden van een politieoptreden. '*Part of the job*', of is er een grens?[1]

Ronny Saelens[2]

De digitalisering heeft een impact op de politiewerking. Een voorbeeld is het filmen van een politieoptreden door de burger met de smartphone gebruiksklaar in de hand, als een digitale versterking van het recht op vrije meningsuiting en informatie. Vooral om potentieel politiegeweld te kunnen aanklagen. Of gewoon omwille van de politiefunctie als zodanig, zonder meer. Velen zien dit als een gerechtvaardigd tegengewicht voor het geweldsmonopolie van de overheid, geïnstrumentaliseerd door middel van de politiebeambte. Die laatste is daarom het voorwerp van de kritische blik van de maatschappij. Een politieambtenaar moet dus maar principieel tolereren dat hij wordt gefilmd en dat de beelden worden verspreid.

Politie en privacy, een *contradictio in terminis*?

Moet de politiebeambte zich zonder meer laten filmen of fotograferen? Deze vraag raakt aan de draagwijdte van de bescherming van de fundamentele rechten en vrijheden, meer bepaald het recht op privacy. Maar als de politiebeambte tijdens de uitvoering van politionele opdrachten principieel geen bescherming van het recht op privacy of de bescherming van de persoonsgegevens geniet, stelt de vraag van het (on) wettig filmen of verspreiden van beelden zich toch niet? Integendeel, ook in dat geval vraagt dit om een democratische verantwoording. Nationale rechters lijken veel moeite te hebben met de beantwoording van deze vraag.[3] Ook in de rechtsleer en binnen de politiewereld zijn diverse stromingen merkbaar.[4]

Om een objectief inzicht te krijgen, lijkt het aangewezen een en ander in perspectief te plaatsen. We doen dit aan de hand van een bloemlezing van de Europese en nationale rechtspraak over de draagwijdte van de bescherming van het recht op de privacy en de bescherming van de persoonsgegevens in situaties waarbij het politieoptreden direct dan wel indirect in beeld wordt gebracht.

Wat zegt de Europese rechtspraak?

We weten dat het Europees Hof voor de Rechten van de Mens (EHRM) een ruim privacybegrip hanteert. Artikel 8 EVRM[5] laat zich, kort samengevat, lezen als een dynamisch concept waarbij de persoon, in functie van wat op een bepaalde plaats en tijd als maatschappelijk aanvaardbaar wordt geacht, ongestoord en vrij moet kunnen participeren in een complexe samenleving.

Dat impliceert ook de vrijheid om zichzelf te zijn en, omgekeerd, de vrijheid om net anders te zijn dan anderen, los van enige overheidsbemoeienis of van derden.[6] Deze dynamische invulling van het privacybegrip brengt met zich mee dat het EHRM ook de professionele activiteit of de publieke plaats niet uitsluit van bescherming onder artikel 8 EVRM.[7] Immers, ook deze activiteiten en plaatsen dragen bij tot

1 Zie uitgebreid: R. Saelens, "Opgepast, U wordt gefilmd". De politiebeambte en zijn zoektocht naar anonimiteit: een blinde vlek in de uitoefening van de politiefunctie", in F. Goossens, K. De Pauw, F. Verspeelt (eds.), *De sluier rond anonimiteit opgelicht... Identiteits-, privacy- en persoonsgegevensafscherming in het strafprocesrecht en politierecht, Brugge*, die Keure, 2022, te verschijnen.

2 Ronny Saelens is expert en commissaris-onderzoeker bij het Controleorgaan op de politionele informatie en vrijwillig wetenschappelijk medewerker bij de onderzoeksgroep Law, Science, Technology and Society van de Vrije Universiteit Brussel. Deze bijdrage is ten persoonlijke titel geschreven.

3 R. Saelens, "Het filmen van politiebeambten tijdens de taakuitoefening. Soms een misdrijf, soms een burgerrecht", *Vigiles* 2014, 211-217.

4 Zie voor enkele visies: E. De Raedt, P. Rosseel, B. Van Tienen (eds.), *De Wet op het politieambt. Handboek van de politiefunctie en politieorganisatie*, Brussel, Politeia, 2019, 447; D. Voorhoof, "Geen verbod op filmen van politieagenten", *De Juristenkrant* 2018, afl. 380, 1-2; K. Lemmens, "De politie gefilmd: l'arroseur arrosé?", *RW* 2014-15, 162; R. Saelens, "Ook politieambtenaren genieten tijdens het uitvoeren van hun opdrachten bescherming van hun persoonsgegevens en privacy" (noot onder HvJ 14 februari 2019, C-345/17, Sergejs Buivids), *P&R* 2019, 137-143.

5 Europees Verdrag voor de Rechten van de Mens.

6 Zie voor een algemene bespreking van de toepassing van artikel 8 EVRM: P. De Hert Artikel 8. "Recht op privacy" in J. Vande Lanotte en Y. Haeck (ed.), *Handboek EVRM. Deel 2. Artikelsgewijze commentaar*, I, Antwerpen, Intersentia, 2004, 705-788. S. Gutwirth, *Privacy and the information age*, Lanham/Boulder/New York/Oxford, Rowman & Littefield Publ., 2002, 158p.

7 EHRM 12 januari 2010, nr. 4158/05, Gillan en Quinton/Verenigd Koninkrijk; EHRM 28 januari 2003, nr. 44647/98, Peck/Verenigd Koninkrijk.

de sociale ontplooiing van het individu.[8] Werknemers en overheidsambtenaren, zoals een politieambtenaar, kunnen dus privacybescherming inroepen.[9]

Daarnaast ziet ook het Europees Hof van Justitie, dat toezicht houdt op de toepassing van het Unierecht, geen reden om principieel aan professionele activiteiten de bescherming van de persoonsgegevens en, desgevallend, de privacy te ontzeggen.[10] Op Unierechtelijk niveau wordt in de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (EU-Handvest), respectievelijk, het recht op privacy en de bescherming van de persoonsgegevens gewaarborgd.

De politie is geen publieke figuur zonder meer

De politiebeambte oefent evenwel een opdracht van algemeen belang uit: hij of zij handhaaft de openbare orde en voert daarbij politionele interventies uit.[11] Is de politiebeambte *daardoor* principieel uitgesloten van de privacybescherming? Het EHRM kiest voor een genuanceerd antwoord. Het loutere feit dat een persoon een opdracht van algemeen belang uitoefent betekent niet dat deze zonder meer buiten de bescherming van artikel 8 EVRM valt.[12] Het EHRM vereist namelijk dat de nationale rechter onderzoekt *waarom de politiebeambte in casu* minder privacybescherming zou moeten tolereren, maar niet "*door het enkele feit*"[13] dat hij politiebeambte is, "*en bovendien niet bekend was bij het publiek*".[14] Het Straatsburgse Mensrechtenhof lijkt dus niet te willen meegaan in de perceptie dat de politieambtenaar *ab initio* als een 'publiek figuur' te beschouwen is. Ook het feit dat de politiefunctie een opdracht van algemeen belang is, is geen doorslaggevend element.

Maar dit betekent niet dat de politieambtenaar in geen enkele omstandigheid kan gefilmd worden. Het recht op privacy is immers niet absoluut. Een inbreuk op de privacybescherming is toegestaan op basis van de exhaustief opgesomde legitieme gronden uit artikel 8, tweede lid, EVRM, zoals de vaststelling van strafbare feiten, waaronder buitensporig politiegeweld, en de rechten en belangen van derden, zoals het recht op vrije meningsuiting en informatie, en voor zover de inbreuk noodzakelijk en proportioneel is.

Niet elk politieoptreden is van publiek belang

Wanneer het recht op vrije meningsuiting en informatie wordt ingeroepen, moet het gaan om feiten of een gebeurtenis die bijdraagt aan een "*debat van publiek belang*".[15] Het moet gaan om nieuwswaardige feiten. Niet elke gebeurtenis in de publieke ruimte is een kwestie van maatschappelijk debat. Dat zou overigens enige privacybeleving in de openbare ruimte *de facto* onmogelijk maken.

Het louter filmen om de publieke nieuwsgierigheid te bevredigen, valt dus niet onder de noemer van '*public interest*', of maakt van de beelden geen nieuwswaardige feit (*debate of public interest*).[16] De proportionaliteitvereiste van de beeldverwerking brengt bovendien met zich mee dat de afbeelding van de gefilmde persoon moet worden gemaskeerd (*geblurd*) wanneer deze geen bijdrage levert aan de nieuwswaardigheid van het maatschappelijk debat.[17] Dit is een voorzorgsmaatregel, ook als de kwestie een debat van algemeen belang zou kunnen zijn.[18]

Het moet wel worden gezegd dat de hiervoor besproken rechtspraak vooral in verband staat met het politioneel optreden naar aanleiding van feiten of gebeurtenissen die meestal al op zichzelf een onderwerp van maatschappelijk debat waren en dus nieuwswaardig.

De bescherming van persoonsgegevens is niet per se gelijk aan privacy

In het EU-Handvest wordt de bescherming van de persoonsgegevens losgekoppeld van het recht op privacy. Het zijn twee afzonderlijke grondrechten. Dit betekent dat de beoordeling van de rechtmatigheid van de verwerking van persoonsgegevens buiten het privacyvraagstuk *kan* worden gehouden. Opdat een verwerking van persoonsgegevens als onrechtmatig kan worden beschouwd, is dus niet vereist dat de verwerking de bescherming van privacy schendt,

8 P. De Hert, J. Van Caeneghem, "Duidelijkheid over de grenzen aan collectieve, preventieve fouilleringen en 'crime control policing' in de publieke ruimte" (noot onder 28 januari 2003), *Vigiles* 2012, 377-384).
9 EHRM 28 november 2017, nr. 77838/13, Antovic en Mirkovic/Montenegro, met verwijzingen; EHRM 26 juli 2007, nr. 64209/01, Peev/Bulgarije; EHRM 27 juni 1997, nr. 20605/92, Halford/Verenigd Koninkrijk.
10 HvJ 14 februari 2019, C-345/17, Sergejs Buivids.
11 K. Lemmens, "De politie gefilmd: l'arroseur arrosé?", *RW* 2014-15, 162.
12 EHRM 26 mei 2020, nr. 50469/14, Marina/Roemenië.
13 Vrije vertaling van de auteur.
14 EHRM 26 mei 2020, nr. 50469/14, Marina/Roemenië, paras. 76-77 (vrije vertaling van de auteur).
15 Ibid, para. 75 (vrije vertaling van de auteur).
16 EHRM 20 maart 2021, nr. 1864/18, Matalas/Griekenland; EHRM 13 oktober 2015, nr. 37428/06, Bremner/Turkije.
17 EHRM 13 oktober 2015, nr. 37428/06, Bremner/Turkije.
18 Ibid.

maar het kan. Desalniettemin worden onrechtmatige verwerkingen (waardoor de privacy wordt geschonden) met administratieve of strafrechtelijke sancties bedreigd.[19] En inbeslagneming van de beelden lijkt daarbij niet uitgesloten.[20]

Het juridische kader voor de verwerking van persoonsgegevens is vastgelegd in de Algemene Vordering Gegevensbescherming[21], nader uitgewerkt in de Wet Gegevensbescherming (WGB).[22] Beide wettelijke kaders geven *tools* waarmee een evenwicht wordt gezocht tussen de verwerking van persoonsgegevens, die al dan niet de bescherming van de privacy raakt, en andere fundamentele rechten en belangen, zoals de uitingsvrijheid.

Niet elke verwerking van een mening heeft een journalistiek doeleinde

In dat verband moet worden aangestipt dat uitzonderingen op bepaalde basisrechten van de gefilmde persoon mogelijk zijn. In de eerste plaats door artikel 24 WGB, maar beperkt tot journalistieke doeleinden. Uit de omschrijving van dit artikel in de WGB valt af te leiden dat niet elke mening onder het begrip 'journalistieke doeleinden' valt. Met andere woorden, niet elke verwerking van mening of informatie is zonder meer een feit of gebeurtenis van maatschappelijk debat. In zo'n geval draagt het filmen en/of het verspreiden van de beelden zonder de voorafgaande toestemming van de gefilmde persoon – of bij gebrek aan een andere rechtsgrond – het risico van onwettigheid van de verwerking met zich. Een 'andere rechtsgrond' zou kunnen zijn, en waarbij dus de toestemming van de persoon niet nodig is, wanneer het filmen de aangifte van buitensporig geweld door de politie of van strafbare feiten in het algemeen beoogt.[23]

Sergejs Buivids: Valentijnsarrest of pilootarrest?

In dat verband heeft het Hof van Justitie op 14 februari 2019 voor het eerst geoordeeld dat ook politiebeambten tijdens de uitoefening van politionele opdrachten de bescherming van persoonsgegevens kunnen inroepen.[24] De uitspraak van het Hof van Justitie bevestigt het standpunt dat hoger al werd naar voor geschoven, namelijk dat in principe ook politiebeambten tijdens de uitvoering van hun opdrachten bescherming van hun persoonsgegevens genieten.[25] Het Hof sluit evenmin uit dat de politiebeambte tijdens het uitvoeren van een interventie ook de bescherming van de privacy zou kunnen genieten. Maar net zoals dat het geval is voor artikel 8 EVRM, is ook het recht op bescherming van de persoonsgegevens (en de privacy) geen absoluut grondrecht en moet deze afgewogen worden tegen andere in het spel zijnde fundamentele rechten en vrijheden of belangen van derden. Wat de uitingsvrijheid betreft, stelt het Hof van Justitie als voorwaarde dat het filmen én verspreiden betrekking heeft op een debat van maatschappelijk belang.[26] Ook de zogenaamde 'burgerjournalist' kan en mag een rol spelen in het ruimer spel van de *checks and balances*. Maar het Hof van Justitie gaat niet mee in de redenering dat iedere politionele opdracht zonder meer 'uitsluitend journalistieke' doeleinden dient, noch een potentieel ongeoorloofde politionele interventie in zich draagt. Het Hof aanvaardt evenmin dat *in casu* het filmen als een zuiver persoonlijke doeleinde kan worden beschouwd.[27]

De nationale rechtspraak volgt

We zien de criteria van de hiervoor besproken Europese rechtspraak ondertussen ook in de nationale rechtspraak doorsijpelen. De conclusie lijkt te zijn dat niet elke politionele interventie preventief zomaar kan worden gefilmd. Hoewel het filmen van het politieoptreden als zodanig niet uitdrukkelijk door een wet wordt verboden, is dat geen vrijgeleide om standaard elk politieoptreden preventief te filmen vanuit de veronderstelling dat de politie zijn bevoegdheden buitensporig zou kunnen gebruiken. Naar gelang de omstandigheden kan de

19 Artikel 221 en 230 WGB.
20 Artikel 39bis Wetboek van Strafvordering (Sv). Controleorgaan op de politionele informatie, Advies uit eigen beweging van 21 november 2021 *met betrekking tot het filmen door burgers van politie-interventies en betreffende de bescherming van de persoonsgegevens en de privacy van politieambtenaren tegenover derden tijdens de uitvoering van hun politionele opdrachten* (DD200025), www.controleorgaan.be/publicaties/adviezen-aanbevelingen.
21 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 het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad, *Pb.L.* 119, 4 mei 2016, 89-131.
22 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018.
23 Artikel. 6, 1. c) WGB en artikel 30 Sv.
24 HvJ 14 februari 2019, C-345/17, Sergejs Buivids.
25 Zie: R. Saelens, "Het filmen van politiebeambten tijdens de taakuitoefening. Soms een misdrijf, soms een burgerrecht", *Vigiles* 2014, 211-217.
26 Artikel 52.3 Handvest.
27 In welk geval anderszins het wettelijk kader van het gegevensbeschermingsrecht niet van toepassing is.

onrechtmatige verspreiding zelfs resulteren in een strafrechtelijke veroordeling voor belaging, laster en eerroof.[28] Dit zijn strafbare handelingen die een (ernstige) impact kunnen hebben op bescherming van de privacy van de politiebeambte: het risico dat de politiebeambte door de verspreiding van de beelden in zijn dagdagelijkse leven negatief wordt beoordeeld.

Conclusie: op zoek naar een evenwicht

Uit voorgaande blijkt dat het filmen van een politieoptreden niet zonder meer is toegelaten, ook al is het niet expliciet door de wet verboden. Het gaat om concurrende grondrechten, zonder een principieel voorangsrecht van het ene noch het andere. Het zoeken naar een aanvaardbaar en werkbaar evenwicht is dan ook noodzakelijk. Dat kan op twee manieren: op basis van vaststaande rechtspraak of door een wetgevend initiatief.

Op basis van de rechspraak, zijn er drie situaties denkbaar waarbij de politieambtenaar wettig kan worden gefilmd , mits daarbij rekening wordt gehouden met de proportionaliteit van de beeldverwerking:

1. bij het filmen van **een nieuwswaardige gebeurtenis** waarbij de aanwezigheid van een politieambtenaar bijkomstig en toevallig in beeld komt;
2. wanneer de gebeurtenis **een maatschappelijk debat** betreft dat onvermijdelijk samenvalt met een politieoptreden, maar de politiebeambte als zodanig niet geviseerd wordt;
3. met het oog op aangifte bij de bevoegde autoriteiten wanneer de politieambtenaar zijn bevoegdheid **op onwettige (disproportionele) wijze** uitvoert.

Slechts in de eerste twee gevallen lijkt de rechtspraak het *verspreiden* van de beelden voorwaardelijk te accepteren. Hier valt de rechtsgrond voor (1) het filmen en (2) het verspreiden van de beelden samen. Een bijkomend aandachtspunt is dat de Belgische rechtspraak voor een burger niet duidelijk en voorzienbaar is, des te meer in andere situaties waarbij wordt gefilmd. En het blijft hoe dan ook casuïstiek. Dit draagt niet bij tot de rechtszekerheid. De geïdentificeerde gevallen zijn in die zin beperkend dat *preventief* filmen, – in de zin dat de beelden *misschien* voor een legitiem doeleinde zouden kunnen worden gebruikt – niet de goedkeuring van de rechtspraak draagt. Wil het preventief filmen toelaatbaar zijn, lijkt een wetgevend initiatief aangewezen. Dit verdient ook de voorkeur in het belang van de rechtszekerheid.

Bij wijze van aanzet, en zonder volledig te willen zijn, lijken daarbij minstens de volgende aspecten het overwegen waard.

Een eerste mogelijkheid bestaat erin dat de hiervoor besproken gevallen en voorwaarden die door de rechtspraak worden ontwikkeld in een wet worden vastgelegd. Het is daarbij, als tweede mogelijkheid, niet uitgesloten dat de wetgever alleen het filmen op zichzelf toelaat, of omgekeerd, het verspreiden van beelden, uitdrukkelijk verbiedt, behalve voor de toepassing van artikel 24 WGB. Maar wat is dan de rechtvaardiging voor het louter filmen op zich? Daarbij kan de aard van de plaats waar mag worden gefilmd het aanknopingspunt zijn: (alleen) de openbare ruime of ook in publiek toegankelijk besloten plaatsen (winkel, trainstation, evenement). Een element daarbij is de redelijke privacyverwachting van de persoon die gefilmd kan worden. Daarbij moet nagedacht worden of deze verwerkingsbevoegdheid gerechtvaardigd wordt door het enkele feit dat 'men', en dus niet alleen de politiebeambte, zich in een openbare ruimte of publiek toegankelijk plaats bevindt. Of wordt aangenomen dat het *preventief* filmen gerechtvaardigd is omwille van legitieme gronden van algemeen belang, zoals ten behoeve van het opsporen en vervolgen van strafbare feiten? De laatste lijkt op gespannen voet te staan met de Camerawet van 21 maart 2007 waarvoor specifieke voorwaarden en modaliteiten gelden. Deze wet laat wel het filmen preventief toe. Maar dan verwordt de smartphone tot een bewakingscamera. Willen we dat, en zo ja in welke gevallen en onder welke voorwaarden? Het preventief filmen (van politieoptreden) zal hoe dan ook de evenredigheidstoets moeten kunnen doorstaan.

28 Corr. Brussel 28 januari 2021, onuitgegeven; Gent, 4e Kamer, 22 december 2020, inzake C.C., arrest nummer C/1527/2020, niet gepubliceerd; Corr. Gent 18 mei 2020, niet gepubliceerd; Antwerpen 19 februari 2020, *Limburgs Rechtsleven* 2020, afl. 4, 324; Gent 19 september 2018, *P&R* 2019, 37, noot R. SAELENS ("Filmen van politiebeambten en de bescherming van persoonsgegevens. Niet verboden wil niet zeggen zonder meer toegelaten"); Brussel, 10 januari 2018, niet gepubliceerd; Corr. Brugge 8 november 2016, niet gepubliceerd. Voor de casuïstiek aan de basis van deze uitspraak en later aan het in voetnoot 65 aangestipte Gentse arrest, zie: R. SAELENS, "Het filmen van politiebeambten tijdens de taakuitoefening. Soms een misdrijf, soms een burgerrecht", Vigiles 2014, 211-217. A contrario rechtbank Brussel 24 oktober 2019 (civiele zaak), randnummer 57. Zie ook het Controleorgaan op de politionele informatie, Advies uit eigen beweging van 21 november 2021 *met betrekking tot het filmen door burgers van politie-interventies en betreffende de bescherming van de persoonsgegevens en de privacy van politieambtenaren tegenover derden tijdens de uitvoering van hun politionele opdrachten* (DD200025), www.controleorgaan.be/publicaties/adviezen-aanbevelingen.

Drones in EU-geïntegreerd grensbeheer: Mensenrechtelijke aansprakelijkheid en het gebruik van drones in terugkeeroperaties

Joyce De Coninck[1]

Begin 2022 rapporteren internationale media dat de Libische overheid zich schuldig maakt aan collectieve uitzetting van derdelanders[2] **in de woestijn, zonder enige basisvoorzieningen.**[3] **Daarenboven staat het al jaren vast dat Libische autoriteiten zich reeds ruime tijd schuldig maken aan (onder meer) het folteren, seksueel misbruiken en opsluiten van derdelanders in ronduit abominabele en mensonwaardige omstandigheden.**[4]

Toch blijft de Europese Unie (EU) – in samenspraak met de EU-lidstaten – samenwerking met Libië nastreven in het implementeren van het EU-geïntegreerd grensbeheer.[5] Sterker nog, de Unie zet alsmaar meer in op het gebruik van geavanceerde technologieën en ambieert toenemend gebruik te maken van artificiële intelligentie om de maritieme buitengrens van de Unie te bewaken en te versterken.[6] Zo worden er door de Unie momenteel drones ingezet in het Middellandse Zeegebied, om derdelanders op te sporen en de coördinaten van hun locatie door te geven aan de Libische kustwacht, die de derdelanders vervolgens terugtrekken naar de Libische kustlijn met alle gevolgen van dien.[7] In de volle wetenschap van de omstandigheden waarin derdelanders bij hun aankomst in Libië terecht dreigen te komen, werken de Unie en de EU-lidstaten actief mee aan het terugsturen van individuen naar een land waar hun veiligheid op geen enkele wijze kan worden gegarandeerd.

Los van de institutionele hypocrisie inherent aan deze problematiek[8], doet dit een zeer pertinente vraag rijzen over wie de juridische verantwoordelijkheid draagt voor medeplichtigheid aan mensenrechtenschendingen. De Unie en de EU-lidstaten zijn immers niet *direct* verantwoordelijk voor het begaan van mensenrechtenschendingen zoals foltering en seksueel misbruik van derdelanders in Libië – maar ze werken wel actief en bewust mee aan het faciliteren van dergelijke schendingen door het communiceren van locatiedata van derdelanders aan de Libische kustwacht. De vraag stelt zich bijgevolg of onder het heersend Europees regime van mensenrechtelijke aansprakelijkheid, de Unie en/of de EU-lidstaten verantwoordelijk kunnen worden gehouden voor deze medeplichtigheid.

De vraag naar juridische verantwoordelijkheid wordt bemoeilijkt door het gebruik van (onbemande) technologieën zoals drones, die ingezet worden om een virtuele grens te creëren, waardoor derdelanders

1 Joyce De Coninck is postdoctoraal onderzoeker aan de UGent en Emile Noël Global Fellow aan het Jean Monnet Center van New York University.
2 De term 'derdelanders' poogt op een neutrale wijze het geheel van individuen aan te duiden, die internationale bescherming trachten te bekomen in de Europese Unie, ongeacht de rechtmatigheid van deze aanvragen.
3 N. Nielsen, "Libya 'abandoning migrants without water' in deserts", *EU Observer*, 28 januari 2022, https://euobserver.com/migration/154222.
4 Marion Macgregor, "International court asked to investigate possible war crimes against migrants", *Infomigrants*, 21 januari 2022, https://www.infomigrants.net/en/post/38046/international-court-asked-to-investigate-possible-war-crimes-against-migrants; *Human Rights Watch*, "No Escape From Hell – EU Policies Contribute to Abuse of Migrants in Libya", Human Rights Watch, 21 januari 2019, https://www.hrw.org/report/2019/01/21/no-escape-hell/eu-policies-contribute-abuse-migrants-libya#.
5 O. Shatz en J. Branco, "Communication to the Office of the Prosecutor of the International Criminal Court - EU Migration Policies in the Central Mediterranean and Libya", *Statewatch* 2019, https://www.statewatch.org/news/2019/jun/eu-icc-case-EU-Migration-Policies.pdf. Zie ook: European External Action Service (EEAS) and Political and Security Committee (CFSP), *Libyan Coast Guard and Navy Monitoring – Four Monthly Report*, Communication 5029/22; R. Jordans en L.Cook, "Migrant abuses continue in Libya. So does EU border training", *AP News*, 25 januari 2022, https://apnews.com/article/coronavirus-pandemic-business-health-libya-migration-a30dd342513aeeede5a7558de4c3089d?utm_source=dailybrief&utm_medium=email&utm_campaign=DailyBrief2022Jan25&utm_term=DailyNewsBrief.
6 Zie onder meer: C. Dumbrava, "Artificial Intelligence at EU Borders – Overview of Applications and Key Issues", *European Parliament*, 7 juli 2021, https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)690706.
7 L. Laursen, "Europe Expands Virtual Borders to Thwart Migrants", *IEEE Spectrum*, 4 februari 2022, https://spectrum.ieee.org/remote-sensing-of-migrants.
8 De uitspraken van het Hof van Justitie van de Europese Unie bij de bepaling of Servië een veilig derde land is n.a.v. automatische terugkeerprocedures van derdelanders uit Hongarije, vallen moeilijk te rijmen met de (terugkeer) samenwerking tussen Libië en de EU voortvloeiend uit militaire operaties Sophia en Irini, waarvan het alom geweten is dat Libië niet als veilig derde land kan beschouwd worden. Zie onder meer: EHRM (Grote Kamer) 23 februari 2012, nr. 27765/09, Hirsi Jamaa e.a./Italië.

weggehouden worden van de fysieke EU-buitengrens.[9] Er ontstaat geen fysiek contact tussen de derdelanders en de autoriteiten van de Unie of de EU-lidstaten.[10] Maar als deze technologisch gedreven aanpak werkbaar en legitiem zou zijn onder heersende mensenrechtenstandaarden, dan zou er geen nood zijn aan dergelijke geavanceerde technologieën. In plaats daarvan, zou men enkel gebruik maken van maritieme operaties – zoals oorspronkelijk vooropgesteld door militaire Operatie Sophia[11] en huidige Operatie Irini[12] – en zouden derdelanders door autoriteiten van de Unie en de EU-lidstaten simpelweg teruggebracht worden naar Libië. Net omwille van de onrechtmatigheid van dergelijke praktijken[13], wordt er in toenemende mate gebruik gemaakt van geavanceerde en onbemande technologieën om het vaststellen van rechtsmacht *vis-a-vis* derdelanders in de Middellandse Zee, en bijgevolg de toepassing van mensenrechten, te vermijden.

Met andere woorden: hoewel het duidelijk is dat het gebruik van drones als gevolg heeft dat derdelanders teruggetrokken worden naar een *onveilig* derde land, is het onduidelijk onder het huidig juridisch kader, wie hiervoor verantwoordelijk dient te worden gehouden: de Unie, de EU-lidstaten, beiden of geen van beide. Meer nog, in zoverre het mogelijk zou zijn om een of meerdere verantwoordelijke partijen aan te duiden, blijft het alsnog onduidelijk *hoe* en *voor welke schending* deze partijen juridische verantwoordelijkheid dragen, gezien de afwezigheid van fysiek contact met de desbetreffende derdelanders en het feit dit alles plaatsvindt buiten de *territoriale* rechtsmacht van de EU en de EU-lidstaten.

Mensenrechtelijke aansprakelijkheid onder Europees recht

Onder Europees recht geeft een mensenrechtenschending aanleiding tot juridische aansprakelijkheid (en eventuele genoegdoening) wanneer een handeling of nalatigheid toerekenbaar is (1) aan een partij gebonden door een (positieve of negatieve) mensenrechtelijke verplichting die deze niet naleeft (2). Daarenboven, zal er causaliteit (3) aangetoond moeten worden en moet het desbetreffende mensenrechteninstrument van toepassing zijn op de feiten – de zgn. vereiste rechtsmacht (4).[14] Deze ogenschijnlijke simpele vereisten werden traditioneel ontwikkeld om de verantwoordelijkheid van een staat vast te stellen voor het begaan van een mensenrechtenschending *vis-a-vis* individuen binnen de territoriale jurisdictie van de staat en werden geïnspireerd door het traditionele aansprakelijkheidsrecht. Echter, wanneer deze vereisten toegepast worden op hybride samenwerkingsvormen waarbij meerdere statelijke en niet-statelijke partijen betrokken zijn, en waar gebruik gemaakt wordt van geautomatiseerde en onbemande technologie, wordt het snel duidelijk dat deze voorwaarden juridische verantwoordelijkheid bemoeilijken in plaats van faciliteren.

Toerekenbaarheid

Om mensenrechtelijke aansprakelijkheid vast te stellen, moet de mensenrechtenschending toerekenbaar zijn aan de EU (als entiteit verantwoordelijk voor het ontwikkelen van het beleid), de lidstaten (die uitvoering geven aan dit beleid) of aan een combinatie van de beide. Volgens heersend Europees (Unie) recht zal toerekenbaarheid worden vastgesteld aan de hand van drie potentiële testen[15], die afwisselend en (enigszins) willekeurig door verschillende rechtbanken toegepast worden.

Volgens de eerste test zal (het nalaten van) een bepaalde handeling toerekenbaar zijn aan ofwel de staat, ofwel de EU, wanneer de handeling voortvloeit uit een orgaan van de staat, of van de EU. Er bestaat

9 L. Laursen, "Europe Expands Virtual Borders to Thwart Migrants", *IEEE Spectrum*, 4 februari 2022, https://spectrum.ieee.org/remote-sensing-of-migrants.

10 Zie algemeen: M. Giuffré en V. Moreno-Lax "The Rise of Consensual Containment: From 'Contactless Control' to 'Contactless Responsibility' for Forced Migration Flows", in S. Singh Juss (ed.), *Research Handbook on International Refugee Law*, Edward Elgar Publishing, 2019, 82-108.

11 Operatie Sophia is onlangs in haar geheel beëindigd. De taken ervan werden opgenomen in de GBVB-missie EUNAVFOR MED Operatie Irini (Operatie Irini). Deze nieuwe missie heeft tot doel het VN-wapenembargo tegen Libië uit te voeren. Voorts neemt deze operatie de taken over van voormalige operatie Sophia, namelijk het verzamelen van informatie en het uitoefenen van toezicht vanuit de lucht om illegale migratiestromen te controleren en mensensmokkel en mensenhandel in het gebied tegen te gaan. De overwegingen betreffende bewaking vanuit de lucht en de daaruit vloeiende de facto *push-* en *pull-backs* gelden daarom evenzeer voor operatie Irini. Besluit (GBVB) 2020/472 van de Raad van de Europese Unie van 31 maart 2020 inzake een militaire operatie van de Europese Unie in het Middellandse Zeegebied (EUNAVFOR Med Irini) [2020] PB L101/4.

12 *Ibid*.

13 EHRM (Grote Kamer) 23 februari 2012, nr. 27765/09, Hirsi Jamaa e.a./Italië.

14 J. De Coninck, *Catch-22 in the Law of Responsibility of International Organizations: systemic deficiencies in the EU responsibility paradigm for unlawful human rights conduct in integrated border management*, Doctoraal Proefschrift Ugent, 2021, https://lib.ugent.be/en/catalog/pug01:8721431 (hierna: De Coninck, 2021).

15 Hiernaast kunnen betrokken partijen ook op eigen initiatief aansprakelijkheid aannemen. Dit komt weliswaar niet vaak voor. Zie onder meer: International Law Commission, "Articles on the Responsibility of International Organizations with Commentaries - A/66/10", *ILC*, 2011, https://legal.un.org/ilc/texts/instruments/english/commentaries/9_11_2011.pdf (*hierna* ARIO).

een brede en een strenge interpretatie van deze test.[16] Het is weliswaar niet duidelijk onder welke modaliteiten de strengere of bredere toets van deze orgaantheorie wordt toegepast, waardoor rechtbanken op nationaal, regionaal en internationaal niveau, vrijblijvend kunnen kiezen. Hoewel deze keuzevrijheid enige flexibiliteit biedt, is het ook zo dat precies deze flexibiliteit rechtsonzekerheid in de hand werkt en ertoe kan leiden dat er helemaal geen toerekenbaarheid wordt vastgesteld, ten nadele van het slachtoffer van de vermeende schending (*zie infra*). Bovendien is het momenteel onduidelijk of de toerekenbaarheid van een mensenrechtenschending aan een enkele partij automatisch de toerekenbaarheid van dezelfde schending aan een andere partij uitsluit.

Hiernaast werd een bijkomende test ontwikkeld om tegemoet te komen aan de bijzonderheden van de bevoegdheidsverdeling van de EU.[17] Volgens deze *bevoegdheidsverdelingstest* zal een handeling of het nalaten van een handeling, toegerekend worden aan de partij (lidstaat of de EU) die bevoegdheid geniet onder EU-recht. Ook hier lijkt deze test in eerste instantie gemakkelijk toepasbaar, maar bestaan er twee versies van de test, die willekeurig toegepast kunnen worden door verschillende rechtbanken.[18] Het gebrek aan duidelijkheid over welke test dient toegepast te worden, zorgt alweer voor enige rechtsonzekerheid bij mogelijke slachtoffers. Bovendien is deze test moeilijk toepasbaar in de praktijk, daar de bevoegdheidsverdeling tussen de EU en de lidstaten niet statisch is en deze test geen pasklaar antwoord kan bieden op de vraag van toerekenbaarheid bij gedeelde bevoegdheden tussen de EU en de lidstaten – zoals het geval is bij EU-geïntegreerd grensbeheer. Ook hier zien we opnieuw dat het niet duidelijk is of toerekenbaarheid van een handeling/nalaten aan een partij, automatisch impliceert dat diezelfde handeling niet langer toerekenbaar is aan een andere partij.

Als laatste bestaat er een specifieke test om toerekenbaarheid te bepalen in *operationele situaties* waarvoor organen of functionarissen gedetacheerd worden bij de lidstaat/lidstaten of bij de EU.[19] Maar ook hier zien we weer dat toerekenbaarheid bepaald zal worden aan de hand van twee varianten van deze test, die willekeurig toegepast worden.[20] Volgens een variant van deze test zal er nagegaan worden in welke mate een lidstaat of de EU 'effectieve controle' heeft over de handeling of het nalaten, die aanleiding gaf tot de potentiële schending. De andere variant van deze test stelt dat er dient gekeken te worden naar welke partij de overkoepelende/overheersende controle heeft over de feiten die aanleiding gaven tot de schending. Bij deze laatste test heerst het vermoeden dat de toerekenbaarheid van het gedrag aan een partij, de overige partijen ontlast van enige verantwoordelijkheid. Bij de overige twee testen (*orgaantheorie en de bevoegdheidstest*) is dit echter onduidelijk.

Samenvattend bestaan er zes verschillende testen – waarvan geen enkele dwingend is – om te bepalen hoe handelingen (of het nalaten van handelen) dienen toegerekend te worden in multilaterale, hybride operaties waarin zowel de EU als de lidstaten betrokken zijn. Het bestaan van verschillende testen om toerekenbaarheid vast te stellen, heeft als gevolg dat er geen eenduidig juridisch criterium bestaat waarop een potentieel slachtoffer zich kan beroepen teneinde toerekenbaarheid aan te tonen. Het gebrek aan eenduidige standaarden zorgt ervoor dat het aantonen van toerekenbaarheid – een van de cumulatieve voorwaarden om mensenrechtelijke aansprakelijkheid vast te stellen – een zeer precaire oefening wordt.

Wanneer we toerekenbaarheid pogen vast te stellen voor het gebruik van drones binnen het kader van EU-operaties Sophia en Irini, is het belangrijk om te benadrukken dat dit militaire EU-operaties betreft, uitgevoerd door de lidstaten binnen het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) van de EU. Als we de orgaantheorie toepassen, stelt zich de vraag of de lidstaten organen van de EU zijn. Afhankelijk van de interpretatie van de orgaantheorie (breed of streng) zal dit al dan niet het geval zijn. Ditzelfde probleem stelt zich ook bij de toepassing van de test van bevoegdheid. Handelingen gesteld binnen het kader van EU-operaties Sophia en Irini worden bepaald door een confidentieel Operationeel Plan[21], waarbij (onder meer) de Raad van de Europese Unie betrokken is, alsook de verschillende

16 Volgens de bredere test zullen ook handelingen van entiteiten die nog enige discretionaire marge hebben, als handelingen van organen van de staat of internationale organisatie beschouwd worden. Volgens de strengere test, zullen enkel entiteiten die formeel deel uitmaken van de staat of de internationale organisatie, als dusdanig worden beschouwd en hun handelingen bijgevolg toegerekend worden aan de staat.

17 De Coninck, 2021, p. 151 - 174.

18 De eerste bredere bevoegdheidstest, stelt dat handelingen toerekenbaar zullen zijn aan de Unie of de lidstaten afhankelijk van wie de bevoegdheid geniet in theorie. De strengere bevoegdheidstest zal handelingen enkel toerekenen aan een partij, wanneer deze partij de bevoegdheid daadwerkelijk uitoefent.

19 *Ibid*, p. 152 – 167.

20 Waar een variant van deze test 'effectieve controle' over handelingen van de gedetacheerde functionarissen vereist, stelt de tweede variant van deze test dat handelingen enkel toerekenbaar zullen zijn, wanneer een partij 'algemene/overkoepelende (normatieve) controle' uitoefent over de desbetreffende handelingen. Zie bespreking van toerekenbaarheid in de Mukeshimana zaak voor verschillende Belgische rechtbanken: T. Ruys, "Mukeshimana-Ngulinzira and others v. Belgium and others", *American Journal of International Law* 2020, nr. 114, 272 – 274.

21 De Coninck, 2021, p. 289.

participerende lidstaten, voor een materie waarvoor de bevoegdheid gedeeld is tussen de lidstaten en de Unie. De modaliteiten van samenwerking zoals vastgesteld in het Operationeel Plan, alsook de toepassing van de test van bevoegdheid, zullen bepalend zijn bij het vaststellen van toerekenbaarheid. Bovendien is het onwaarschijnlijk dat onder de (derde) operationele test van toerekenbaarheid, er voldoende direct en fysiek contact is tussen de EU en/of de lidstaten en de derdelanders om effectieve controle te kunnen vaststellen.

Deze testen hebben bovendien gemeen dat ze niet definitief aangeven in welke mate toerekenbaarheid aan één partij, toerekenbaarheid van hetzelfde gedrag aan een andere partij uitsluit. Zonder normatieve en *ex ante* verduidelijking over hoe toerekenbaarheid vastgesteld dient te worden, kunnen verschillende rechtbanken verschillende testen doorvoeren, met als risico dat er uiteindelijk geen toerekenbaarheid wordt vastgesteld.[22]

Een (voldoende ernstige) schending

Naast toerekenbaarheid, moet er een (voldoende ernstige) schending van een mensenrechtenverplichting vastgesteld worden in hoofde van de partij aan wie de handeling of het nalaten toegerekend werd. Hoewel internationaal recht niet vereist dat de schending als voldoende ernstig gekwalificeerd wordt, is dit wel vereist onder EU-recht voor eventuele schendingen begaan door de Unie.[23]

Hierbij dient onmiddellijk opgemerkt te worden dat er een onderscheid dient gemaakt te worden tussen mensenrechtenverplichtingen in abstracto en daaruit vloeiende de facto verplichtingen. Om mensenrechtenverplichtingen te respecteren dienen er immers concrete positieve en negatieve verplichtingen nageleefd te worden. Maar deze verplichtingen werden traditioneel ontwikkeld voor, en toegepast op staten. Hoewel de EU en overige niet-statelijke partijen in bepaalde gradaties ook gebonden zijn door mensenrechtenstandaarden *in abstracto*, is het niet duidelijk of deze door dezelfde concrete (positieve en negatieve) verplichtingen gebonden zijn als de lidstaten. Staten, de EU en overige niet-statelijke actoren, zijn immers volledig verschillende (juridische) entiteiten en worden gekenmerkt door wezenlijke verschillen betreffende (o.a.) macht, bevoegdheden en beschikbare middelen. Rekening houdend met de functionele specialisatie van niet-statelijke actoren, stelt de vraag zich of het zonder meer mogelijk is om concrete verplichtingen die thans gelden voor staten, zomaar toe te passen op de EU en overige niet-statelijke entiteiten, gezien ze niet over hetzelfde apparatuur beschikken om de desbetreffende concrete verplichtingen na te komen. Is het niet wenselijker om met gemeenschappelijke maar gedifferentieerde verantwoordelijkheden[24] te werken, waarbij rekening gehouden wordt met de wezenlijke verschillen tussen statelijke en niet-statelijke partijen betrokken bij eenzelfde mensenrechtenschending?

Deze vragen werden tot op heden nog niet volwaardig beantwoord – althans niet voor entiteiten zoals de EU. Hoewel de EU *in abstracto* gebonden is door mensenrechtenstandaarden, is het niet mogelijk om hieruit af te leiden wat de concrete (negatieve en positieve) verplichtingen zijn waardoor de Unie gebonden is. Deze normatieve onduidelijkheid verhindert de vaststelling van een *voldoende ernstige* mensenrechtenschending. Indien het niet duidelijk is wat de concrete primaire verplichtingen zijn waardoor de Unie en overige niet-statelijke partijen gebonden zijn, zal het evenmin duidelijk zijn wanneer er een voldoende ernstige schending heeft plaatsgevonden in hoofde van deze partijen. Het komt dan toe aan de betrokken rechter om op discretionaire – *ex post facto* – wijze te beslechten wanneer er wel degelijk een schending heeft plaatsgevonden – alweer ten nadele van de rechtszekerheid voor potentiële slachtoffers.

Toegepast op het gebruik van drones in de Middellandse Zee, is het zo dat de drones an sich niet te vereenzelvigen zijn met verboden *push-* en *pull-backs* onder het *non-refoulement* principe. Echter, het gebruik van de drones faciliteert deze handelingen door de Libische kustwacht wel. Onder heersende mensenrechtenstandaarden kan er geopperd worden dat de lidstaten gebonden zijn door een (indirecte) *due diligence*-verplichting in het voorkomen van mensenrechtenschendingen. Het is weliswaar niet duidelijk of dergelijke verplichting ook toegepast kan worden op de EU en/of overige niet-statelijke partijen. Hoewel het een logisch gevolg lijkt van de *abstracto* verplichting om mensenrechten na te leven, werd dit tot op heden niet vertaald in concrete, *ex ante* vastgestelde verplichtingen. De afwezigheid van dergelijke concrete normen impliceert dat het volledig

22 Zo kan een eerste (nationale) rechtbank bijvoorbeeld stellen dat er een test van overheersende operationele controle dient te zijn om toerekenbaarheid vast te stellen. Dit zou impliceren dat de EU uitsluitend dergelijke controle uitoefent door de rol die de Raad speelt, en de lidstaten verantwoordelijkheid vermijden. Echter, gelet op het GBVB-karakter van militaire missies van de EU, geniet het Hof van Justitie van de EU geen rechtsmacht in de materie, met als gevolg dat een individu het recht op een effectief rechtsmiddel niet zal kunnen uitoefenen.

23 HvJ 16 juli 2009, nr. C-440/07, ECLI:EU:C:2009:459, *Commission of the European Communities v Schneider Electric* SA, para. 160.

24 Een gelijkaardig vorm van dergelijke verplichting is terug te vinden in Artikel 2 van het Internationaal Verdrag inzake Economische, Sociale en Culturele Rechten.

aan de rechter toekomt om op discretionaire wijze te bepalen wanneer er sprake is van een voldoende ernstige schending van (o.m.) het *non-refoulement* beginsel. Dit komt ten nadele van rechtszekerheid, rechtmatige verwachtingen en het beginsel van effectiviteit van mensenrechtenbescherming *vis-a-vis* betrokken derdelanders.

Causaliteit

Naast toerekenbaarheid en het aantonen van een voldoende ernstige schending, zal er ook causaliteit moeten aangetoond worden tussen de toerekenbare handeling en de geleden schade (althans onder EU-recht) om aansprakelijkheid voor een mensenrechtenschending vast te stellen. De test die hiervoor gehanteerd wordt onder Unierecht, stelt dat de Unie als partij enkel verantwoordelijkheid zal dragen in zoverre het *direct en exclusief verantwoordelijk* is voor de handeling of het nalaten.[25] Met andere woorden, in zoverre er een interveniërende handeling is van de lidstaten en/of overige niet-statelijke entiteiten in het begaan van de schending, zal de Unie als partij geen verantwoordelijkheid dragen voor het bijdragen aan de schending.[26] Wanneer deze test wordt toegepast op het gebruik van drones binnen het kader van Operatie Sophia of Operatie Irini, zien we dat het onmogelijk is voor de Unie om enige verantwoordelijkheid te dragen, daar het altijd aan de lidstaten zal toekomen om het beleid van de Unie uit te voeren – er zal dus altijd een interveniërende handeling zijn van de lidstaten en/of overige niet-statelijke actoren. Kortom, de test van causaliteit is dermate streng onder het Unierecht, dat hooguit de lidstaten verantwoordelijkheid kunnen dragen voor hun bijdragen in mensenrechtenschending, terwijl het haast onmogelijk is (onder deze test) om de EU als partij verantwoordelijk te houden voor haar eigen bijdrage hierin.

Rechtsmacht

Het gebruik van drones binnen het kader van Operaties Sophia en Irini in de Middellandse Zee impliceert automatisch dat de detectie van de locatie van derdelanders en het communiceren van deze data naar de Libische kustwacht *buiten* het territorium van de EU-lidstaten plaatsvindt. Dit is relevant aangezien heersende mensenrechtenverplichtingen traditioneel enkel van toepassing zijn *binnen* het fysieke territorium van de verdragspartijen. Hierop werden – onder meer door het EHRM – een aantal uitzonderingen geformuleerd, al worden deze uitzonderingen traditioneel zeer eng geïnterpreteerd.[27] Opdat mensenrechtenverplichtingen van toepassing zijn buiten het territorium van de lidstaten, zal er enige vorm van ofwel effectieve controle over een grondgebied dienen te zijn, of is het vereist dat de autoriteiten van een lidstaat een bepaalde vorm van controle uitoefenen over een individu. Zoals aangegeven, worden deze testen voor extraterritoriale jurisdictie zeer streng geïnterpreteerd en moet dergelijke controle invloed hebben op de rechtspositie van de geraakte individuen – zo niet, is er geen sprake van extraterritoriale rechtsmacht.

Wanneer de Unie gebruik maakt van drones om het Middellandse Zeegebied te surveilleren binnen het kader van Operatie Sophia en Irini, is het betwijfelbaar of dergelijke controle deze strenge drempel bereikt. Hoewel dit tot op heden nog niet werd uitgeklaard door het EHRM en/of het EU Hof van Justitie, is het onwaarschijnlijk dat het louter communiceren van locatiecoördinaten naar andere partijen (de Libische kustwacht) in het Middellandse Zeegebied deze grens bereikt. Wellicht zal er hierdoor geen extraterritoriale rechtsmacht vastgesteld worden, en zullen Europese mensenrechtenverplichtingen in eerste instantie niet eens toepasselijk geacht worden.

Gebruik van artificiële intelligentie aan de buitengrens: opzettelijk omzeilen van verantwoordelijkheid?

Het gebruik van drones in het Middellandse Zeegebied zorgt voor een toenemende automatisering en door technologie aangedreven aanpak, in het uitvoeren van het geïntegreerd grensbeleid van de EU. Door het louter surveilleren van de Middellandse Zee zorgen de Unie en de lidstaten ervoor dat er geen fysiek en direct contact ontstaat met derdelanders die op doortocht zijn naar de externe grens van de EU. Hoewel het argument dus gemaakt kan worden dat de Unie en

25 Zie (en alle overige verwijzingen hierin vervat): HvJ 12 december 2007, nr. T-113/04, ECLI:EU:T: 2007:377, *Atlantic Container Line and Others v Commission*, para. 31. Zie ook omtrent *exclusieve causaliteit*: P. Craig en G. de Búrca, EU *Law – Text, Cases and Materials*, Oxford University Press, 2020, 631-632.

26 HvJ 31 maart 2011, nr. C-433/10P, ECLI:EU:C:2011:204, *Volker Mauerhofer v European Commission*, para. 131 - 132; K. Lenaerts, I. Maselis, K. Gutman en J. Tomasz Nowak (eds.) *EU Procedural Law*, Oxford University Press, 2014, para. 11.81.

27 M. Milanovic, "Extraterritorial Investigations in Hanan v. Germany; Extraterritorial Assassinations in New Interstate Claim Filed by Ukraine against Russia", *EJIL:Talk*, 26 February 2021, https://www.ejiltalk.org/extraterritorial-investigations-in-hanan-v-germany-extraterritorial-assassinations-in-new-interstate-claim-filed-by-ukraine-against-russia/; M. Milanovic, E*xtraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*, Oxford University Press, 2011.

de lidstaten geen directe handelingen stellen die strijdig zijn met hun mensenrechtenverplichtingen, blijft het *gevolg* van het indirect surveilleren wel dat de desbetreffende individuen alsnog in mensonwaardige situaties terecht komen. De vraag stelt zich bijgevolg, of het gebruik van geautomatiseerde systemen bedoeld is om dergelijke directe inmenging van de Unie en de lidstaten – alsook de toepasselijkheid van mensenrechtenstandaarden – te ontwijken.

Wanneer we het juridisch kader toepassen op het gebruik van drones om locatie-data te communiceren aan de Libische kustwacht, wordt het onmiddellijk duidelijk dat het traditioneel Europees aansprakelijkheidsregime voor mensenrechtenschendingen niet langer volstaat. Door de samenwerking van statelijke en niet-statelijke entiteiten en het gebruik van geavanceerde technologieën, wordt de verantwoordelijkheid voor het uitvoeren van dit beleid verdeeld tussen de lidstaten en de Unie: de lidstaten werken immers mee aan de praktische uitvoering van het beleid vanuit het territorium van de Unie, terwijl de Unie (deels) verantwoordelijk is voor het conceptualiseren van het beleid en de opvolging ervan.

Als men zou kunnen vaststellen welke test van toerekenbaarheid zou moeten worden toegepast, dan nog blijft het onduidelijk *welke variant* van de verschillende testen dat zou zijn – de brede of de strenge variant? Bovendien beantwoordt dit evenmin de vraag of toerekenbaarheid aan een partij (*een lidstaat bv.*) toerekenbaarheid van hetzelfde gedrag (*samenwerking aan de operationalisering van de drone*) aan een andere partij (*de EU bv.*) uitsluit. *In casu* hebben we te maken met een situatie van operationele uitwerking van het EU-geïntegreerd grensbeleid in de Middellandse Zee – wellicht is de derde test van toerekenbaarheid op basis van 'effectieve controle' bijgevolg het meest passend. Maar omdat de modaliteiten van het gebruik van de drones binnen het kader van militaire operatie Sophia en Irini worden vastgelegd in het confidentieel Operationeel Plan, is het praktisch niet mogelijk om vast te stellen of de Unie of de lidstaten effectieve controle uitoefenen over de derdelanders wiens locatiedata worden gecommuniceerd aan de Libische kustwacht. Daarenboven lijkt het onwaarschijnlijk – gelet op de heersende interpretatie van de 'effectieve controle' test – dat het louter communiceren van locatiedata volstaat om tot een vaststelling van toerekenbaarheid te komen.

Indien men voorbij deze eerste van de cumulatieve voorwaarden geraakt om aansprakelijkheid vast te stellen, dan nog stelt zich de vraag of dezelfde concrete (positieve en negatieve) verplichtingen van toepassing zijn op niet-statelijke actoren die betrokken zijn bij de uitvoering van het beleid. Zo niet, zal het zeer moeilijk zijn (gezien de afwezigheid van ex ante verduidelijkingen over de concrete en bindende verplichtingen van niet-statelijke actoren in dergelijke hybride verhoudingen) om vast te stellen of de Unie wel degelijk een voldoende ernstige (mensenrechten-) schending heeft begaan door het ontwikkelen en sturen van dit beleid. En zelfs dan blijft de vraag of de Unie überhaupt enige verantwoordelijkheid kan dragen, gelet op de zeer strenge test van causaliteit en extraterritoriale rechtsmacht om aansprakelijkheid vast te stellen.

Gezien de vele obstakels die opduiken om aansprakelijkheid vast te stellen vis-a-vis de Unie, zal een individu zich eerder moeten richten op (lid-)staataansprakelijkheid. Maar door de hybride samenwerking met de Unie en overige niet-statelijke actoren, door het gebruik van (semi-)onbemande technologieën, en door de afwezigheid van een fysieke band tussen de lidstaten en de derdelanders, zal het ook dan haast onmogelijk zijn om toerekenbarheid op volwaardige wijze vast te stellen. Het zal bovendien ook moeilijk zijn om causaliteit op voldoende wijze vast te stellen, aangaande het meewerken aan door technologie gedreven grensbeheer en de uiteindelijke schade ondervonden door de betrokkenen, waardoor ook staatsaansprakelijkheid onwaarschijnlijk wordt.

Gedeelde en dynamische aansprakelijkheid?

De Unie en de lidstaten werken bewust mee – door het gebruik van drones in extraterritoriaal grensbeheer – aan een beleid dat ertoe leidt dat derdelanders worden teruggetrokken naar een onveilig derde land. Echter, onder het huidig aansprakelijkheidsregime, is het onaannemelijk dat deze bijdragen zullen leiden tot enige juridische repercussies voor de Unie en/of lidstaten. Hoe valt dit dan te rijmen met het rechtstaatbeginsel waarop de Unie gestoeld is, alsook het recht op een effectief rechtsmiddel dat hieruit voortvloeit?

Twee onoverkomelijke gebreken tekenen het traditioneel Europees aansprakelijkheidsregime voor mensenrechtenschendingen: enerzijds is het huidige regime gestoeld op een verouderde juridische fictie waarbij staten exclusief verantwoordelijk zijn voor naleven van mensenrechtenverplichtingen. Er wordt met andere woorden onvoldoende rekening gehouden met de hybride verhoudingen waarbij statelijke en niet-statelijke actoren samenwerken (*toerekenbaarheid, causaliteit*). Dit zorgt ervoor dat enige verantwoordelijkheid voor niet-statelijke actoren op (mogelijks) arbitraire wijze en voornamelijk *ex post facto* zal worden beslecht. Dit komt de principes van rechtszekerheid en legitieme verwachtingen, en de effectiviteit van mensenrechtenbescherming geenszins

ten goede.

Anderzijds wordt er onvoldoende rekening gehouden met de functionele specialiteit van niet-statelijke actoren zoals de EU (*voldoende ernstige schending, extraterritoriale rechtsmacht*). De Europese Unie is als supranationale organisatie op allerhande manieren beperkt in haar handelen door de toegewezen bevoegdheden die ze geniet (*e.g. financieel, operationeel*). Het valt dus moeilijk te beargumenteren dat de Unie door identieke concrete positieve en negatieve verplichtingen gebonden zou moeten zijn als de lidstaten, gezien het niet op dezelfde manier kan voldoen aan dergelijke (lidstatelijke) verplichtingen.

De vraag stelt zich vervolgens of *relationele en dynamische* aansprakelijkheid geen oplossing kan bieden voor hybride samenwerkingsvormen die aanleiding geven tot (bijdragen in) mensenrechtenschendingen. In eerste instantie – en als antwoord op het eerste vraagstuk – zou het wenselijk zijn om te werken met een combinatie van *prescriptieve* en *reactieve* aansprakelijkheid. Dit impliceert dat concrete positieve en negatieve verplichtingen van niet-statelijke actoren verankerd worden in (secundaire EU) wetgeving waarbij rekening wordt gehouden met de functionele specialiteit van deze niet-statelijke actoren. Deze tendens is reeds merkbaar in de secundaire wetgeving die van toepassing is op de Europese grens- en kustwacht, waarin *prescriptieve* verplichtingen verduidelijkt worden die van toepassing zijn op Frontex tijdens het uitvoeren van haar operaties.[28] Dergelijke prescriptieve verduidelijkingen zijn weliswaar betekenisloos wanneer ze niet gekoppeld worden aan reactieve aansprakelijkheid, waarmee verduidelijkt wordt hoe en wanneer niet-statelijke actoren aansprakelijkheid kunnen oplopen voor bijdragen in mensenrechtenschendingen. Met andere woorden, het volstaat niet om mensenrechtelijke verplichtingen prescriptief op te nemen en te verduidelijken in wetgeving – dit dient gekoppeld te worden aan duidelijke afspraken over hoe toerekenbaarheid, causaliteit en extraterritoriale rechtsmacht in hybride (operationele) samenwerkingsvormen zal geregeld worden.

Om tegemoet te komen aan de functionele specialiteit van niet-statelijke actoren, maar evenzeer aan het toenemend gebruik van geavanceerde (en vaak onbemande) technologieën in EU-geïntegreerd grensbeheer, kan een onderscheid gemaakt worden tussen de *primaire* mensenrechtenverplichtingen die rusten op de lidstaten en andere (secundaire) gradaties van dergelijke verplichtingen die rusten op niet-statelijke actoren (in verhouding met hun bevoegdheden). Dergelijke *secundaire* verplichtingen, impliceren geenszins dat niet-statelijke actoren in mindere mate gebonden zouden zijn door de toepasselijke mensenrechtenverplichtingen *in abstracto*. Integendeel, het betekent eerder dat de vertaling van de verplichtingen *in abstracto* naar concrete verplichtingen in verhouding blijft met hun daadwerkelijke bevoegdheden en capaciteiten.

Zoals recent ontwikkeld in de '*Guiding Principles of Shared Responsibility in International Law*', zou de EU volgens dit model verantwoordelijk gehouden worden voor het verlenen van leiding en controle over een bepaalde handeling, of voor het verlenen van hulp en bijstand bij het uitvoeren van een bepaalde militaire operatie. Met andere woorden, de Unie zou niet verantwoordelijk gehouden voor de eigenlijke – primaire – schending, maar wel voor een secundaire (inhoudelijke of procedurele) *bijdrage* aan de schending. Deze relationele vorm van aansprakelijkheid biedt een meer correcte weergave van de dynamiek tussen de Unie en de lidstaten in het uitvoeren van het geïntegreerd grensbeheer, waarbij de lidstaten nog altijd de primaire verantwoordelijkheid dragen voor de uitvoering van het grensbeheer, maar aangestuurd worden (of verplicht) door de Unie om dit beleid ten uitvoer te brengen.

Toegepast op het gebruik van drones in militaire operaties Sophia en Irini, zouden de lidstaten vervolgens aansprakelijk kunnen worden gehouden voor het bewust faciliteren van push- en pullbacks van derdelanders door de Libische kustwacht, in strijd met het *non-refoulement beginsel*. De Unie daarentegen, zou aansprakelijk kunnen worden gehouden voor diens leiding en controle over de operatie of het verlenen van hulp en bijstand aan dergelijke operaties. Het feit dat er gebruik gemaakt wordt van onbemande en geavanceerde technologieën zou dan geen belemmering vormen in het garanderen van het recht op een effectief rechtsmiddel, daar betrokken individuen twee mogelijke pistes behouden om aansprakelijkheid aan te kaarten.

Conclusie

Zonder deze verduidelijkingen blijft het recht op een effectief rechtsmiddel een lege doos, gezien het traditionele aansprakelijkheidsmechanisme niet voldoende ontwikkeld is om soelaas te bieden voor hybride samenwerkingsvormen waar gebruik gemaakt wordt van geavanceerde technologieën. Het belang van dit vraagstuk wordt des te meer benadrukt door

28 Zie bv. artikel 46 Verordening (EU) 2019/1896 van het Europees Parlement en de Raad van 13 november 2019 betreffende de Europese grens- en kustwacht en tot intrekking van Verordening (EU) nr. 1052/2013 en Verordening (EU) 2016/1624.

het recent voorstel van de Europese Commissie voor een verordening tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en het vooropgesteld toenemend gebruik van artificiële intelligentie in grensbeheer. Hoewel de voorstellen mensenrechtenbescherming in abstracto beogen, werd er tot op heden nog geen werk gemaakt van het concretiseren van aansprakelijkheid wanneer het gebruik van artificiële intelligentie alsnog tot een schending aanleiding geeft. Bij het uitblijven van concrete prescriptieve en reactieve relationele bepalingen, bestaat het risico dat het recht op een effectief rechtsmiddel en effectieve rechtsbescherming in nog mindere mate zal gerespecteerd worden, wat ontegensprekelijk indruist tegen het rechtstaatbeginsel waarop de Unie is gestoeld.

De controle op het gebruik van algoritmische surveillance onder druk? Een exploratie door de lens van de relationele ethiek

Rosamunde van Brakel[1]

Sinds het einde van de 20ste eeuw zijn er als gevolg van technologische ontwikkelingen nieuwe mogelijkheden ontstaan om data te verzamelen en te analyseren. De opkomst van 'big data' en de toegenomen mogelijkheden van artificiële intelligentie (AI) in de 21ste eeuw zijn met veel interesse omarmd door de politie. Het gebruik van deze technologieën door de politie kan worden beschreven als algoritmische surveillance.

Dit zijn algoritmische systemen die

1. gebruik maken van op regels gebaseerde algoritmen om gestructureerde en ongestructureerde gegevens te classificeren, op te slaan, te combineren en te doorzoeken, om vastgelegde gegevens te vergelijken met andere gegevens en overeenkomsten te vinden;

   en

2. gebruik maken van machine-lerende algoritmes om patronen en bruikbare kennis in big data sets trachten te voorspellen op basis van de patronen die in de vastgelegde gegevens zijn gevonden.[2]

Ondanks de toegenomen regelgeving[3], die als doel heeft de democratische waarborgen te garanderen van algoritmische surveillance, lijkt dit het gebruik ervan eerder te stimuleren.[4] Denk bijvoorbeeld aan de significante toename van het gebruik van 'intelligent' cameratoezicht in België, maar ook elders in Europa.[5] Dit roept de vraag op of de huidige controlemechanismen voldoende zijn om alle burgers te beschermen tegen de mogelijke gevolgen van het gebruik van algoritmische surveillance door de politie.

Het doel van deze bijdrage is om na te denken over de vraag of huidige controle en handhavingsmechanismen voor het gebruik van algoritmische surveillance door de politie herdacht zouden moeten worden. Om tot een (voorlopig) antwoord op die vraag te komen zal ik in het eerste deel van het artikel drie socio-technische ontwikkelingen bespreken die het huidig kader onder druk zetten. In het tweede deel zal ik huidige controle- en handhavingsmechanismen bekijken door de bril van de relationele ethiek om te exploreren hoe we hieruit kunnen leren om controlemechanismen te herdenken.

Controle- en handhavings-mechanismen onder druk: socio-technische ontwikkelingen

Als gevolg van de opkomst van algoritmische surveillance in het politiewerk kunnen drie socio-technische ontwikkelingen geïdentificeerd worden die het traditionele controle- en handhavingskader onder druk zetten: 1) de fragmentatie en privatisering van politiewerk, 2) de democratisering van surveillance, en 3) de toename van collectieve schade en sociale gevolgen. Deze ontwikkelingen zijn overlappend en verstrengeld en moeten niet als losstaande ontwikkelingen worden gezien.

Ten eerste, fragmentatie en privatisering van politiewerk is niet nieuw. Sinds het einde van 20ste eeuw is er in het Westen een stijging van de samenwerking met de private sector en spelen private

1 Rosamunde van Brakel is hoofddocent, TILT, Tilburg University en docent LSTS, Vrije Universiteit Brussel.
2 R. Van Brakel, "How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium", *Surveillance & Society* 2021, 19(2), 228-240.
3 Zoals de Europese politie- en justitie richtlijn die vertaald is in de Belgische wetgeving en ook de voorgestelde Europese wet op de artificiële intelligentie.
4 Hier werd al eerder voor gewaarschuwd zie: R.V. Ericson en K.D. Haggerty, *Policing the Risk Society*, Oxford, Oxford University Press, 1997.
5 Algorithm Watch, *Automating Society Report 2020*, AW AlgorithmWatch gGmbH, 2020, beschikbaar: https://automatingsociety.algorithmwatch.org.

spelers een steeds grotere rol in politiewerk. Dit is in belangrijke mate het gevolg van de toegenomen macht en groei van de private sector en bezuinigingen in de publieke sector.[6] De technologische ontwikkelingen van big data en AI in het begin van de 21ste eeuw hebben geleid tot de toenemende macht van technologiebedrijven door onder meer 'surveillance kapitalisme', waarbij gegevensverzameling een economische drijfveer wordt voor bedrijven.[7] Politiewerk wordt in toenemende mate *platform policing*, waarbij de politie gebruikt maakt van digitale platformen en digitale opsporingstechnologie.[8] Dit heeft als gevolg dat de politie steeds afhankelijker wordt van infrastructuur van technologiebedrijven[9] en leidt tot verschuivende machtsverhoudingen van de publieke naar de private sector, wat een negatieve invloed heeft op transparantie en controle.[10]

Ten tweede, kan er een 'democratisering' van surveillance worden herkend door een verschuiving van aandacht voor gerichte surveillance naar grootschalige surveillance.[11] Hierdoor staat nu een veel groter deel van de bevolking onder surveillance waardoor het risico op toename van de macht van de staat maar ook van private actoren steeds groter wordt. Waarbij grootschalige surveillancepraktijken vroeger vooral werden uitgevoerd door intelligentiediensten[12] of binnen een bepaalde context zoals op het vliegveld, spelen politiediensten maar ook technologiebedrijven hierin een steeds grotere rol.

Denk bijvoorbeeld in België aan de significante uitbreiding van het gebruik van 'intelligent' cameratoezicht voor allerlei doeleinden[13], wat nog meer werd aangewakkerd door de coronapandemie.[14] Andere voorbeelden zijn de infiltratie van het versleutelde Encrochat-netwerk[15], de gezichtsherkenningssoftware van Clearview AI dat ook uitgeprobeerd is door de federale politie in België[16], of de dataverzamelingspraktijken van Europol[17] die door sommige vergeleken worden met surveillance praktijken van de Amerikaanse NSA.[18] Denk ten slotte aan het gebruik van de spionagesoftware Pegasus om data te verzamelen van mobiele telefoons van activisten, politici en journalisten over de hele wereld.[19]

Ten derde is er steeds meer sprake van collectieve en sociale schade naast individuele schade. Een belangrijk kenmerk van big data-analyses is dat ze op geaggregeerd niveau plaatsvinden. Er worden dus op het eerste gezicht geen persoonsgegevens verwerkt.[20] Een van de gevolgen is een toename van sociale

6 I. Loader, "Consumer culture and the commodification of policing", *Sociology* 1999, 33 (2), 373–392.
7 S. Zuboff, *The age of surveillance capitalism. The Fight for a human future at the new frontier of power*, Londen, Profile Books, 2018.
8 R. Van Brakel "Een reflectie over het huidig toezicht van het gebruik van surveillanctechnologie door de lokale politie in België", *Cahiers Politiestudies* 2020, 55, 139-160; D. Wilson, "Platform policing and the real-time cop", *Surveillance & Society* 2019, 17 (1/2), 69–75.
9 Dit is een algemene ontwikkeling in de maatschappij. De Coronalert-app is hier een mooi voorbeeld van waarbij Europese landen afhankelijk zijn van Google en Apple's infrastructuur om de app te verspreiden. Zie https://www.esat.kuleuven.be/cosic/sites/corona-app/nl/.
10 R. Van Brakel "Een reflectie over het huidig toezicht van het gebruik van surveillanctechnologie door de lokale politie in België", *Cahiers Politiestudies* 2020, 55, 139-160.
11 K. D. Haggerty en R.V Ericson, "Surveillant assemblage", *The British Journal of Sociology* 2000, 51(4): 605-622.
12 Zie de onthullingen van Edward Snowden over NSA-surveillance praktijken, E. Macaskill en G. Dance, "NSA-files Decoded. What the revelations mean for you", *The Guardian* 1 november, 2013, beschikbaar: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.
13 P. Fussey en D. Murray, "Independent report on the London Metropolitan Police service's trial of live facial recognition technology", *Human Rights and Big Data Project University of Essex*, 2019, beschikbaar: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf; Algorithm Watch (2020). *Automating Society Report 2020*. AW AlgorithmWatch gGmbH, Beschikbaar: https://automatingsociety.algorithmwatch.org.
14 R. Van Brakel, "How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium", *Surveillance & Society* 2021, 19(2), 228-240.
15 Waarbij meer dan 100 miljoen berichten onderschept werden en een algoritmisch model ontwikkeld werd om levensbedreigende berichten te filteren. Tellemachus, "Dutch police used deep learning model to predict threats to life", 2021, beschikbaar: https://tellemachus.com/dutch-police-used-deep-learning-model-to-predict-threats-to-life/; C. Berthélémy, "How Europol's reform enables 'NSA-style' surveillance operation", *Euractiv* 18 juni 2021, beschikbaar : https://www.euractiv.com/section/data-protection/opinion/how-europols-reform-enables-nsa-style-surveillance-operations/.
16 P. Van Leemputten "Minister Verlinden (CD&V): Federale politie gebruikte toch ClearView AI-software voor gezichtsherkenning", *Knack Data News* 8 oktober 2021, beschikbaar: https://datanews.knack.be/ict/nieuws/minister-verlinden-cd-v-federale-politie-gebruikte-toch-clearview-ai-software-voor-gezichtsherkenning/article-news-1787557.html.
17 Op 3 januari 2022 heeft de Europese Toezichtshouder Gegevensbescherming (EDPS) Europol gevraagd om uit zijn gegevensbanken de data te verwijderen van individuen die geen duidelijke band hebben met criminele activiteiten, zie: https://edps.europa.eu/system/files/2022-01/EDPS-2022-01-EDPS-Order%20to%20Europol_EN.pdf., https://www.ianbrown.tech/2022/01/17/the-eus-own-snowden-scandal/.
18 D. Korff, "The EU's own Snowden scandal: Illegal mass surveillance and bulk data mining by Europol and the EU member states, Blog Data Proteciton and Digital Competition", 2022, beschikbaar: https://www.ianbrown.tech/2022/01/17/the-eus-own-snowden-scandal/.
19 Knack, "Het Pegasus Project over cyberspionage: alles wat u moet weten", 2021, beschikbaar: https://www.knack.be/nieuws/wereld/het-pegasus-project-over-cyberspionage-alles-wat-u-moet-weten/groupement-normal-1758429.html.
20 Er moet hier een kanttekening worden gemaakt. Afhankelijk van hoe breed persoonsgegevens geïnterpreteerd worden kan je zeker ook bij geaggregeerde analyses spreken over de verwerking van persoonsgegevens. Zie voor een goede bespreking hierover in het kader van *predictive policing* O. Lynskey, "Criminal justice profiling and EU data protection law: precarious protection from predictive policing", *International Journal of Law in Context* 2019, 15(2), 162-176.

stratificatie, met een ongelijke verhouding tussen maatschappelijke groepen als gevolg.

Doordat big data onregelmatigheden en afwijkingen in datasets reproduceert kan dit leiden tot uitkomsten die een onevenredige impact hebben voor bepaalde groepen of gemeenschappen. Dit kan dan tot een cumulatief nadeel (discriminatie en oneerlijke behandeling) leiden voor bepaalde groepen in de maatschappij, omdat deze, vaak kwetsbare, groepen bovengemiddeld het doelwit zijn van deze technologieën.[21] Dit komt bijvoorbeeld duidelijk tot uiting bij *predictive policing*. Als gevolg van *feedback loops*, die ontstaan door steekproefbias, wordt politie herhaaldelijk teruggestuurd naar dezelfde wijken ongeacht het werkelijke misdaadcijfer.[22] Dit leidt tot *overpolicing* en stigmatisering van bepaalde al geviseerde wijken en gemeenschappen.[23]

Deze risico's op discriminatie en stigmatisering door het gebruik van big data-analyses worden ook bevestigd in de uitspraak in Nederland over het gebruik van SyRI, een algoritmisch systeem om sociale fraude op te sporen. Daarnaast toont de uitspraak ook aan hoe big data-technologie sociale gevolgen heeft en naast discriminatie en stigmatisering ook bijdraagt tot het criminaliseren van armoede en kansarmoede en aan de toename van ongelijkheid in de samenleving.[24]

Hierboven heb ik drie socio-technische ontwikkelingen beschreven die huidige controlemechanismen onder druk zetten. In het verdere verloop van deze bijdrage reflecteer ik over de vraag of huidige controlemechanismen om kunnen gaan met deze ontwikkelingen. Ik doe dit vanuit de lens van relationele ethiek.

Het huidige juridisch kader

Zoals deze bijdrage duidelijk maakt, zetten socio-technische ontwikkelingen traditionele controle- en handhavingsmechanismen onder druk. De vraag stelt zich of het huidige juridisch kader voldoende is om met deze drie ontwikkelingen om te gaan en effectieve democratische waarborgen te voorzien.

Het juridisch kader wordt vandaag gevormd door de regels aangaande de gegevensbescherming. De controle-instrumenten die daarbij momenteel ingezet worden voor de verwerking van gegevens door middel van AI, zoals toezichtsorganen, functionarissen voor gegevensbescherming en gegevensbeschermingseffectbeoordelingen (*Data Protection Impact Assessments* of DPIA's), zijn vaak beperkt in hun reikwijdte. De focus ligt grotendeels op informatieveiligheid en de formele naleving van het wettelijk kader. Er wordt daarentegen te weinig nadruk gelegd op de bescherming van fundamentele rechten, en meer specifiek vanuit artikel 8 van het EVRM.[25] De manier waarop deze instrumenten werken in België is bovendien weinig democratisch, omdat burgers en het middenveld niet worden betrokken. Daarnaast is de politie niet verplicht DPIA's te publiceren volgens de politie en justitierichtlijn. Hierdoor wordt publieke controle bemoeilijkt. Er bestaan ook geen standaarden waaraan DPIA's moeten voldoen. Noch zijn er standaardprofielen voor functionarissen voor gegevensbescherming. Het huidige wettelijke kader betreft enkel toepassingen van algoritmische surveillance die 'persoonsgegevens' verzamelen en verwerken.[26]

De EU publiceerde intussen een voorstel van AI-wet dat een tweevoudig doel heeft: de bescherming van de grondrechten van het individu tegen de nadelige gevolgen van AI, en daarnaast de harmonisatie van de regelgeving van lidstaten om mogelijke handelsbelemmeringen op de interne markt weg te nemen. De nadelige gevolgen van AI worden opgesplitst in risico-categorieën van laag naar hoog en er wordt in de verordening naast risico's voor het individu ook gesproken over risico's voor de samenleving. De verordening maakt echter niet duidelijk wat deze risico's juist zijn.[27]

21 WRR, Big Data in een Vrije en Veilige Samenleving, WRR-rapport 95, 2016, beschikbaar: https://www.wrr.nl/publicaties/rapporten/2016/04/28/big-data-in-een-vrije-en-veilige-samenleving; R. Van Brakel, "Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing", in B. Van der Sloot, E. Schrijvers en D. Broeders (eds.), *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, 117-141.

22 K. Lum en W. Isaac "To predict and serve?", Significance 2016 13(5), 14-18; D. Ensign, S.A. Friedler, S. Neville, C. Scheidegger en S. Venkatasubramanian, "Runaway Feedback Loops in Predictive Policing", *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR 81, 2018, 160-171q.

23 R. Van Brakel, "Pre-Emptive Big Data Surveillance and its (Dis)Empowering Consequences: The Case of Predictive Policing", in B. Van der Sloot, E. Schrijvers en D. Broeders (eds.), *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, 117-141.

24 R. Van Brakel, Noot: Nederlandse SyRI-wetgeving inzake fraudebestrijdding schendt mensenrechten, *Tijdschrift Privacy en Persoonsgegevens*, 2020, 2, 31-39.

25 *Ibid*;

26 Zie artikel 2 Richtlijn politie en justitie, https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.NLD.

27 Voorstel tot Verordening van het Europees parlement en de raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandeling van de Unie, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0206&from=EN; N.A. Smuha, "Beyond the Individual: Governing AI's Societal Harm", *Internet Policy Review*, 2021, 10(3).

Wat betreft controle- en handhavingsmechanismen is de voorgestelde verordening hoopvol. Het geeft aan dat lidstaten één of meer nationale bevoegde autoriteiten moeten aanwijzen om toezicht te houden op de toepassing en uitvoering van AI en als officieel contactpunt voor het publiek en andere actoren moeten fungeren. Ook wordt benadrukt dat de handhavingsmechanismen versterkt kunnen worden "door de invoering van een Europees coördinatiemechanisme dat in de passende capaciteit voorziet en audits van de AI-systemen vergemakkelijkt met nieuwe eisen inzake documentatie, traceerbaarheid en transparantie".[28]

De verordening geeft ook aan dat er een systeem zal opgezet worden om autonome AI-toepassingen met een hoog risico te registreren in een openbare databank voor de hele EU en dat deze enkel toegelaten zullen worden op de Europese markt indien zij voldoen aan "bepaalde dwingende voorschriften en vooraf een conformiteitsbeoordeling ondergaan."[29] De manier waarop deze beoordelingen concreet in de praktijk toegepast en gehandhaafd zullen worden blijft echter vaag. Het is onduidelijk hoe de conformiteitsmechanismen eruit zullen zien. Ook schiet de verordening tekort op democratisch vlak, omdat burgers of het middenveld niet betrokken worden bij deze mechanismen. Bovendien zouden burgers ook geen klacht kunnen indienen bij de nationale toezichthoudende autoriteit, indien zij menen dat de wet niet wordt nageleefd.[30]

Herdenken van algoritmische surveillance-controle mechanismen door de lens van relationele ethiek

Hieronder reflecteer ik over wat we kunnen leren uit de relationele ethiek, geïnspireerd door Ubuntufilosofie, om op een andere manier over controle in de algoritmische politiepraktijk na te denken, rekening houdend met de drie besproken socio-technische ontwikkelingen. Ubuntufilosofie heeft zijn oorsprong in Afrikaanse filosofie uit landen ten zuiden van de Sahara.[31] Ubuntufilosofie verschilt van traditionele rationele ethiek in de zin dat in tegenstelling tot rationele Kantiaanse ethiek, waarbij personen menselijke waardigheid hebben door hun vermogen tot autonomie, personen die menselijke waardigheid hebben omdat ze de capaciteit hebben om zich tot de andere te verhouden op een gezamenlijke manier.[32] Vanuit deze visie zijn mensenrechtenschendingen erop gericht om het vermogen van mensen tot gemeenschappelijke betrekkingen, opgevat als identiteit en solidariteit, ernstig te schaden; en moet menselijke waardigheid gezien worden als het menselijk vermogen om zich op een gemeenschappelijke manier tot anderen te verhouden.

Verschillende computerwetenschappers, die zich inspireren op Ubuntufilosofie, stellen een fundamentele verschuiving voor in het denken over algoritmische onrechtvaardigheid en bestuur van AI, van rationele ethiek naar relationele ethiek.[33] Volgens Birhane is relationele ethiek "een kader dat ons ertoe dwingt onze onderliggende werkhypothesen opnieuw te onderzoeken, ons ertoe dwingt hiërarchische machtsasymmetrieën te ondervragen, en ons ertoe aanzet de bredere, contingente en onderling verbonden achtergrond te beschouwen waar algoritmische systemen uit voortkomen (en worden ingezet) in het proces van bescherming van het welzijn van de meest kwetsbaren".[34] Deze visie veronderstelt dat de schade en onrechtvaardigheid die door algoritmische systemen wordt toegebracht, niet los kan worden gezien van de filosofische beginselen van de technologie en de economische, politieke en sociale structuren die het mee vormgeven.[35]

28 Achtergrond 3.4 Voorstel tot Verordening van het Europees parlement en de raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (Wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandeling van de Unie, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

29 Achtergrond 5.2.3.AI-*Systemen met een hoog risico (title III)* en artikel 43 *Ibid*.

30 N.A. Smuha, "Beyond the Individual: Governing AI's Societal Harm", *Internet Policy Review*, 2021, 10(3).

31 S. Mhlambi, "From rationality to relationality. Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance", *Carr Center Discussion Paper*, 2020, beschikbaar: https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial.

32 T. Metz, "Ubuntu as a moral theory and human rights in South Africa", *African Human Rights Law Journal* 2011, 11(2), 532–559; V. Dignum, "Relational Artificial Intelligence", *Position paper Arvix Computers & Society* 2022, beschikbaar: https://arxiv.org/abs/2202.07446.

33 A. Birhane, "Algorithmic injustice: a relational ethics approach", Patterns, 2021, 2(2). Beschikbaar: https://www.sciencedirect.com/science/article/pii/S2666389921000155#bib11; S. Mhlambi, "From rationality to relationality. Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance", *Carr Center Discussion Paper*, 2020, beschikbaar: https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial; V. Dignum, "Relational Artificial Intelligence", *Position paper Arvix Computers & Society* 2022, beschikbaar: https://arxiv.org/abs/2202.07446.

34 A. Birhane, "Algorithmic injustice: a relational ethics approach", *Patterns*, 2021, 2(2). Beschikbaar: https://www.sciencedirect.com/science/article/pii/S2666389921000155#bib11.

35 S. Mhlambi, "From rationality to relationality. Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance", Carr Center Discussion Paper, 2020, beschikbaar: https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial.

Hoe kan deze visie verzoend worden met de visie van een politie- en justitie-apparaat dat vraagt naar steeds grootschaligere surveillance en samenwerken met de private sector?[36] Dit zou impliceren dat ook politiewerk vanuit dezelfde ethiek zou moeten vertrekken. Het zou betekenen dat de politieopdracht herdacht zou moeten worden op een relationele manier, als het beschermen van collectieve veiligheid. In het huidig beleid wordt veiligheid echter op een enge manier geïnterpreteerd als bescherming tegen criminaliteit en handhaving van de publieke orde. Vaak gaat het zelfs niet meer over veiligheid, maar om politieke drijfveren, om te laten zien dat er hard opgetreden wordt tegen criminaliteit. Het is een vorm van 'surveillance theater'.[37]

Vanuit een collectieve visie op veiligheid die als doel heeft om de veiligheid van alle burgers te vrijwaren, moet er meer aandacht besteed worden aan andere oorzaken van onveiligheid. Veiligheid is meer dan bescherming tegen criminaliteit alleen: gezond eten, proper water, huisvesting, basisinkomen, gezondheidszorg, onderwijs en werk, maar ook bijvoorbeeld niet het voorwerp zijn van discriminatie, pesterijen, haat, geweld en disproportionele controle van de overheid. Vaak worden deze sociale en economische rechten niet opgenomen in het veiligheidsbeleid.[38]

Wanneer men vanuit deze visie vertrekt, wordt het bijvoorbeeld duidelijk dat encryptie cruciaal is om mensenrechten en de meest kwetsbaren in de maatschappij te beschermen omdat door achterdeuren in te bouwen in de technologie, de veiligheid van bijvoorbeeld activisten en journalisten om democratische controle uit te oefenen wordt belemmerd.[39] Aangezien het zeker in het huidig politieke klimaat onwaarschijnlijk is dat veiligheid als sociale veiligheid gezien wordt, moet de vraag gesteld worden hoe de mazen van het net verfijnd zouden kunnen worden zodat controlemechanismen ervoor zorgen dat de meest kwetsbaren in de maatschappij beschermd worden.

Als we vanuit de relationele ethiek gaan kijken naar controle- en handhavingsmechanismen voor algoritmische surveillance dan impliceert dit dat het 'rationele' controle-kader, geconstrueerd vanuit het paradigma van gegevensbescherming, tekortschiet, zeker in de manier waarop dit in de praktijk en nationale politiewetgeving vertaald wordt. Het rationele kader gaat uit van mondige betrokkenen die individueel hun rechten kunnen beschermen door middel van informatieverzoeken, waarbij geen rekening wordt gehouden met kwetsbare groepen. Niet alle betrokkenen zijn gelijk. Ze hebben verschillende inzichten, niveaus van kennis, besluitvaardigheid, neiging om hun gegevens bekend te maken, en individuele kwetsbare eigenschappen. Factoren als leeftijd, geestelijk vermogen, kansarmoede, geletterdheid of geslacht kunnen van invloed zijn op het genot en de uitoefening van individuele rechten over gegevensbescherming.[40]

Controle moet daarom verder gaan dan enkel statische technische oplossingen en formele naleving van de wet, naar een praktijk die rekening houdt met de dynamische historische context en sociaal-technische praktijken waarin de technologie ingebed is, aandacht heeft voor machtsrelaties van de verschillende betrokken actoren, en waarin de bescherming van de meest kwetsbaren in de maatschappij voorop staat. Deze relationele controle impliceert het betrekken van de (belangen van) de meest kwetsbaren en hun vertegenwoordigers in het beleid alsook in controlemechanismen die het sociaal-technisch proces van algoritmische surveillance als uitgangspunt nemen.[41] Daarnaast is transparantie cruciaal om te vermijden dat vooroordelen en fouten leiden tot schendingen van de mensenrechten, zoals het Federaal Instituut voor de bescherming en bevordering van de rechten van de mens (FIRM) aangeeft. Volgens het FIRM weten mensen in België momenteel vaak niet voor welke beslissingen de overheid algoritmen gebruikt. Daarnaast is het ook niet altijd duidelijk hoe een algoritme persoonsgegevens verwerkt.[42]

36 Zie C. De Bolle en C.R. Vance, "The last refuge of the criminal: Encrypted smartphones", Politico 2021, beschikbaar: https://www.politico.eu/article/the-last-refuge-of-the-criminal-encrypted-smartphones-data-privacy/. Zie ook: M.Verbergt, "Speurders bibberen voor arrest Grondwettelijk Hof", *De Standaard,* 19 maart 2021. Beschikbaar op: https://www.standaard.be/cnt/dmf20210318_98028590.

37 L. Melgaço en R. Van Brakel, "Smart cities as surveillance theatre", *Surveillance & Society* 2021, 19(2), 244-249.

38 R. Van Brakel, "Slaapwandelend stappen we controlemaatschappij in: beschermen we iedereen met de huidige technologie?", *VRTNWS*, 26 maart 2021, beschikbaar: https://www.vrt.be/vrtnws/nl/2021/03/25/opinie-privacy/.

39 W. Schultz en J. van Hoboken, *Human Rights and encryption*, UNESCO 2016, beschikbaar: https://apo.org.au/sites/default/files/resource-files/2016-12/apo-nid71867.pdf.

40 J. Breuer, R. van Brakel, R., Heyman en J. Pierson, "From Data Protection as a Privilege to Data Protection as Entitlement - An Identification of Factors that increase use of GDPR in Vulnerable groups", *Frontiers Research Topic Interrogating the Design of Smart, Sustainable, and Socially Just Urban Spaces: A Look at Institutions, Places, and Values*, te verschijnen.

41 Uit de literatuur over DPIA's komt naar voor dat veel methoden te weinig aandacht besteden aan het proces. Zie bijvoorbeeld het comparatief onderzoek door T. Bisztray en N. Gruscka, "Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality", in A. Askarov, R. Hansen en W. Rafnsson (eds.), *Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science*, Springer, 2019.

42 FIRM, "FIRM vraagt meer transparantie bij gebruik van algoritmen door de overheid", 7 oktober 2021, beschikbaar: https://www.federaalinstituutmensenrechten.be/nieuws/2021/10/07/federaal-instituut-voor-de-rechten-van-de-mens-vraagt-meer-transparantie-bij-gebruik-van-algoritmen-door-de-overheid.

Concrete stappen

Concreet houdt dit in dat er nagedacht moet worden over hoe controlemechanismen herdacht kunnen worden om met bovenstaande rekening te houden. Hoe kunnen ze rekening houden met asymmetrische machtsrelaties en de toenemende macht van technologiebedrijven? Hoe kunnen ze collectieve en sociale schade voorkomen? Vooraleer er besloten wordt om te investeren in (het ontwerpen van) een bepaalde technologie door de politie, moet er een democratische evidence-based proportionaliteitstoets uitgevoerd worden. Deze toets betrekt burgers bij de beslissingen. Bovendien heeft deze toets aandacht voor de toenemende macht van de staat en private partners alsook aandacht voor collectieve en sociale schade. Deze toets moet gebeuren op basis van wetenschappelijke en objectieve analyse. Hier zou bijvoorbeeld een orgaan zoals de Nederlandse onafhankelijke Raad voor Regeringsbeleid (WRR)[43] een rol kunnen spelen door beleidsgericht onderzoek te verrichten in nauwe samenwerking met universiteiten en het middenveld. Dit orgaan zou dan bijvoorbeeld ook onderzoek kunnen doen naar de collectieve en sociale schade van algoritmische surveillance en naar innovatieve controle en handhavingsmechanismen. Daarnaast zou men meer specifiek kunnen denken aan een AI-coördinatiecentrum, zoals het recente WRR AI rapport voorstelt, dat aan beleidsdirecties, toezichthouders en uitvoeringsorganisaties een structuur biedt om regelmatig en rond uiteenlopende kwesties met elkaar in contact te treden en van elkaar te leren. Dit centrum zou politiek verankerd moeten zijn, zodat er snel beleid kan worden gemaakt als dat nodig is.[44]

Zeker wanneer het gaat over grootschalige surveillance door politiediensten zou de bevolking betrokken moeten worden bij beslissingen om hun legitimiteit te bewaren.[45] Volgens het recente WRR-rapport over AI zal steeds vaker debat nodig zijn over de doelen die de samenleving wil nastreven en de vraag waar, waarvoor en onder welke condities de samenleving AI wil gebruiken. Methoden die hiervoor gebruikt kunnen worden, zijn bijvoorbeeld het organiseren van publieke debatten, openbare raadplegingen[46], burgerjury's, maar ook bijvoorbeeld de ondersteuning van citizen-science initiatieven.[47] Door het publiek te betrekken als actieve deelnemers aan het proces, kan de overheid leren van de expertise van burgers.[48]

Vanuit de relationele ethiek is het dan wel van essentieel belang dat kwetsbare groepen en gemeenschappen een significante stem krijgen in beslissingsmakingsprocessen en dat dit niet enkel 'voor de show' is. Samenvattend biedt relationele controle interessante pistes aan om huidige controlemechanismen te herdenken, op een manier die rekening houdt met de sociaal-technische ontwikkelingen beschreven in de aanvang van deze bijdrage.

Conclusie

In deze bijdrage heb ik gereflecteerd over de vraag of huidige controle- en handhavingsmechanismen voor algoritmische surveillance herdacht zouden moeten worden. Eerst heb ik drie socio-technische ontwikkelingen besproken die huidige controlemechanismen onder druk zetten. Nadien heb ik gekeken naar welke lessen we kunnen trekken als we controle- en handhavingsmechanismen voor algoritmische surveillance bekijken vanuit de relationele ethiek. Een voorlopig antwoord op de vraag is dat de drie socio-technische ontwikkelingen aangeven dat het huidig kader niet volstaat om deze ontwikkelingen op te vangen. Deze eerste exploratie van relationele ethiek om op een andere manier na te denken over controle en handhaving van gebruik van algoritmische surveillance door de politie, geeft aan dat 'rationele' controlemechanismen tekortschieten. Het relationele kader biedt interessante pistes om verder over de vooropgestelde vraag na te denken. Het antwoord in deze bijdrage blijft evenwel voorlopig, omdat verder (empirisch) onderzoek noodzakelijk zal zijn om hier beter inzicht in te krijgen.

43 Dit is een onafhankelijk instituut dat beleidsgericht onderzoek verricht in alle overheidsdomeinen, www.wrr.nl.
44 WRR, Opgave AI De nieuwe systeemtechnologie, *WRR-rapport* 105 2021. Beschikbaar op: https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie.
45 Natuurlijk is het in het kader van het geheim van het onderzoek niet altijd evident om dit te doen. Maar momenteel wordt dit niet eens overwogen in het beleid.
46 Uitzonderlijk is er voor de Coronalert-app een openbare raadpleging georganiseerd door de experten werkgroep die succesvol was: https://www.esat.kuleuven.be/cosic/sites/corona-app/nl/
47 Zie bijvoorbeeld het Amai project in Vlaanderen: https://amai.vlaanderen.
48 T. Schillemans, M. Van Twist en I. Vanhommerig, "Innovations in Accountability. Learning Through Interactive, Dynamic, and Citizen-Initiated Forms of Accountability", *Public Performance and Management Review* 2013, 36(3), 407-435.

De AI-rechter: is artificiële intelligentie een bedreiging voor het recht op een eerlijk proces? Een kort gesprek met Nathalie Smuha

Willem Debeuckelaere*

Beslist kunstmatige intelligentie binnenkort over onze rechtszaken? Uit een onderzoek van 2016 bleek dat AI tot 79% de uitkomst van zaken voor het Europees Hof voor de Rechten van de Mens correct kan voorspellen. De nieuwe technologie is dus niet alleen efficiënt, maar ook accuraat. Maar wat zijn de grote uitdagingen vanuit mensenrechtelijke hoek? Niemand beter om dit aan te vragen dan Nathalie Smuha, onderzoeker aan de KU Leuven, waar ze ethische en juridische vragen rond Kunstmatige Intelligentie en andere nieuwe technologieën onderzoekt. Ook de Europese Commissie weet haar geregeld te vinden voor input over de juridische en ethische dimensies van AI.

TvMR: Welke risico's van AI voor mensenrechten zou jij aanstippen vanuit je onderzoek?

Nathalie Smuha: Mijn onderzoek spitst zich toe op het gebruik van AI-applicaties voor besluitvormingsprocessen binnen de overheid, en de impact hiervan op mensenrechten, democratie en de rechtsstaat. Hoewel deze technologie opportuniteiten creëert – bijvoorbeeld voor interne efficiëntie en vlottere dienstverlening – zijn er ook risico's aan verbonden. Denk aan de impact op privacy, gezien AI-systemen vaak grote hoeveelheden persoonsgegevens verwerken. Of denk aan het risico op discriminatie, omdat AI-systemen soms getraind worden op datasets die vooroordelen kunnen bevatten.

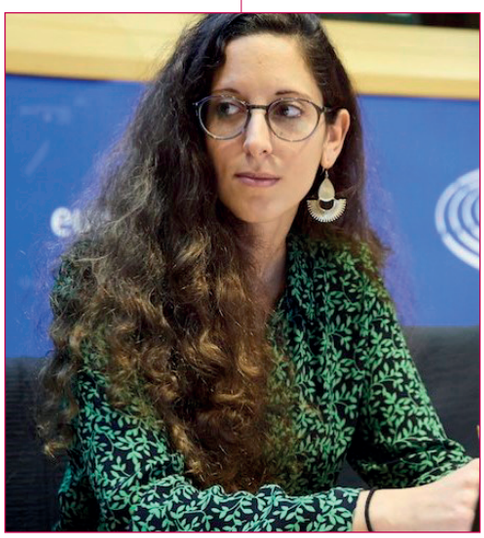

Foto: KU Leuven

TvMR: Hoe zie je die risico's voor het gebruik van AI in de rechtbank?

Nathalie Smuha: Het gebruik van AI kan een invloed hebben op beginselen van de rechtsstaat. Als rechtbanken zich laten leiden door de output van systemen die werden ontwikkeld door de uitvoerende macht of door privébedrijven, kan immers ook hun onafhankelijkheid en onpartijdigheid in het gedrang komen, aangezien de output volledig wordt bepaald door de keuzes van de AI-ontwerpers. Welke dataset wordt gebruikt of net niet gebruikt? Hoe worden data gecategoriseerd? Wat zijn de onderliggende vooronderstellingen? Hoe wordt de output van het systeem gepresenteerd? In mijn onderzoek bekijk ik hoe deze risico's zich kunnen manifesteren en hoe ze kunnen worden aangepakt.

TvMR: Hoe denk je dat AI het werk van rechters zal veranderen?

Nathalie Smuha: Magistraten zullen in de toekomst steeds vaker gebruik maken van AI-systemen om hun dagelijkse taken te faciliteren. Met mijn onderzoek wil ik nagaan aan welke voorwaarden het ontwerp, de ontwikkeling en het gebruik van deze systemen moeten voldoen om beginselen zoals de onafhankelijkheid van de rechterlijke macht, de scheiding der machten, legaliteit en rechtszekerheid, en respect voor mensenrechten te verzekeren. Het gebruik van AI-systemen binnen de magistratuur zal binnenkort ook onderworpen worden aan Europese regelgeving, omdat dit beschouwd wordt als een 'hoog-risico-domein'. Bovendien moeten rechters hun autonomie kunnen bewaren wanneer ze gebruik maken van AI, wat enkel kan indien ze voldoende kennis hebben van zowel de capaciteiten

* Willem Debeuckelaere is redactielid van TvMR.

als de beperkingen en risico's ervan – iets wat mijn onderzoek eveneens tracht te bewerkstelligen.

TvMR: Zullen we dergelijke AI-toepassingen al op korte termijn in de rechtbank zien?

Nathalie Smuha: Er bestaat een grote waaier aan AI-systemen die magistraten zouden kunnen toepassen om hun taken te faciliteren – van applicaties die hen in staat stellen om voorgaande rechtspraak over een juridische materie snel te analyseren, om de toekenning en de omvang van schadevergoedingen in verschillende jurisdicties te vergelijken, om het risico van recidive te helpen voorspellen, of zelfs om een eerste ontwerp van vonnissen te schrijven. De timing voor het gebruik van zo'n tools zal in België echter grotendeels afhangen van de digitalisering van justitie meer in het algemeen, want zonder hoogwaardige datasets kan men deze applicaties niet ontwikkelen. Verder zal het ook afhangen van de beschikbaarheid van opleidingen voor magistraten om met deze systemen om te gaan en tegelijk hun autonomie te behouden. Tot slot kan deze technologie ook pas toegepast worden als er een beter begrip is van de risico's die met het inzetten van deze systemen gepaard gaan.

TvMR: Tot besluit, voor we het toepassen, is er nog denkwerk nodig?

Nathalie Smuha: Hoe gevoeliger de applicatie, hoe belangrijker het is dat men eerst een maatschappelijk debat voert over de grenzen van het gebruik van deze systemen in de magistratuur, om ervoor te zorgen dat de activiteit van het 'recht spreken' mens-centraal blijft.

"The world in my pocket." Het politioneel uitlezen van een smartphone, bekeken in het licht van artikel 8 EVRM

Pieter Tersago[1]

Strafrechtelijke onderzoeken teren op informatie, inclusief (gevoelige) persoonsgegevens. Waar iemand op een bepaald ogenblik is, met wie hij wanneer contact heeft (dataretentie van telefoniegegevens) en wat er wordt gecommuniceerd (heimelijke informaticazoeking), welke reizen een persoon maakt (…) en welke bancaire transacties hij verricht (bankonderzoek),… Al deze informatie kan belangrijk zijn om de betrokkenheid van een persoon bij een bepaald misdrijf te onderzoeken of, eerder à décharge, om zijn strafrechtelijke betrokkenheid uit te sluiten. Hoe meer informatie men verzamelt over het doen en laten van een persoon, hoe meer men een beeld van zijn persoon en privéleven kan schetsen: zijn sociale en professionele contacten, zijn bestedings- en reispatroon,…

Desalniettemin dragen we tegenwoordig al deze gegevens panklaar mee in onze broekzak. De talloze applicaties op een smartphone of tablet bevatten ontzettend veel persoonsgegevens: chatapplicaties, datingapps, banking apps, fitness apps,… bevatten dezelfde of zelfs meer informatie dan een telefonie- of bankonderzoek kan opleveren. Google verwerkt met angstwekkende precisie onze locaties en verplaatsingen, de foto's op een modale smartphone en sociale media-profielen kunnen een kast vol fotoboeken vullen en tags kunnen andere personen op die foto's ook naadloos in kaart brengen.[2]

In de 21e eeuw is surveillance ook niet louter een externe activiteit vanuit de overheid, maar participeren burgers meer en meer actief in "kijken en bekeken worden". In deze *surveillance culture* worden persoonsgegevens actief gedeeld en bekijken burgers gretig hun eigen data (selftracking) én die van anderen (via sociale media bijvoorbeeld).[3] Deze data zijn niet alleen voor commerciële partijen van goudwaarde[4] (bijvoorbeeld voor gerichte advertenties) of voor politieke doeleinden (cf. het Cambridge analytica-schandaal). Ze kunnen ook in een strafrechtelijk onderzoek van groot belang zijn.

Het hoeft echter geen betoog dat ook het uitlezen van een smartphone (of eender welk informaticasysteem[5]) een inmenging in het recht op persoonlijke levenssfeer uitmaakt en dus moet voldoen aan de voorwaarden van artikel 8, lid 2, EVRM om zulke informaticazoeking te rechtvaardigen.[6] Het uitlezen van een informaticasysteem had nochtans lange tijd geen rechtsgrond in het Belgische strafprocesrecht. Op 11 februari 2015 oordeelde het Hof van Cassatie dat de politie een in beslag genomen informaticasysteem steeds mag uitlezen, zonder rechterlijke machtiging.[7] Deze rechtspraak werd door de wet van 25 december 2016[8] uiteindelijk opgenomen in het Wetboek van

1 Dr. Pieter Tersago is jurist en praktijkassistent aan de KU Leuven, LINC.
2 C. Conings, "Wetgever maakt digitaal speurwerk makkelijker", *Juristenkrant* 2017, afl.344, 3.
3 D. Lyon, *Surveillance culture. Watching as a way of life*, Cambrigde, Polity Press, 2018, 172p.
4 Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Londen, Profile Books Ltd, 2019.
5 Elk systeem voor de opslag, verwerking of overdracht van data. Hierbij wordt door de wetgever vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan (Memorie van toelichting bij de wet digitale recherche, Parl.St. Kamer 2015-16, 54-1966/001, 14-15). Ook een USB-stick of tegenwoordig steeds meer 'slimme' huishoudapparaten vallen onder deze definitie. Het Hof van Cassatie beschouwt ook een databank met een historiek van aan- en verkopen en klanten van een bedrijf als een informaticasysteem in de zin van artikel 39bis Sv. (Cass. 5 november 2019, P.19.0426.N).
6 Zie bijvoorbeeld EHRM 17 december 2020, nr. 459/18, Saber/Noorwegen, §48.
7 Cass. 11 februari 2015, P.14.1739.N.
8 Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, BS 17 januari 2017. Zie hierover uitgebreid C. Conings en S. Royer, "Verzamelen en vastleggen van digitaal bewijs in strafzaken", NC 2017, 311-338; C. FORGET, "Les nouvelles méthodes d'enquête dans un contexte informatique: vers un encadrement (plus) strict?", RTDI 2017, 25-52; S. Royer, F. Verbruggen en W. Yperman, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", NC 2019, 5, 389-416.

Strafvordering. Het Grondwettelijk Hof vernietigde deze wet deels, doch kan niet iedereen volledig overtuigen en lost zeker niet alle juridische vraagstukken op.[9] Enkele juridische pijnpunten worden hier opgelijst.

Het uitlezen van informaticasystemen: een trapsgewijze bevoegdheids-regeling die niet overtuigt

De wet maakt een onderscheid tussen *openlijke* (artikel 39 bis Sv. en 88ter Sv.) en *heimelijke* (artikel 90 ter Sv.) informaticazoekingen. Heimelijke informaticazoekingen zijn de moderne versie van de 'telefoontap', waarbij het op bevel van de onderzoeksrechter is toegelaten communicatie of gegevens van een informaticasysteem dat niet voor het publiek toegankelijk is, met technische hulpmiddelen te onderscheppen, ervan kennis te nemen, te doorzoeken of op te nemen. Dit omvat niet alleen het afluisteren van telecommunicatie, maar laat eveneens het heimelijk binnendringen (hacken) van bijvoorbeeld smartphones of laptops toe om zowel de opgeslagen inhoud te doorzoeken als in real-time mee te volgen (bv. communicatie via chatapplicaties e.d., die met een telefoontap als dusdanig niet kunnen worden geïntercepteerd).

Hoewel de mogelijkheden van artikel 90 ter Sv. danig zijn verruimd en het mogelijk wordt heimelijk kennis te nemen van alle gegevens op een informaticasysteem én live mee te kijken met alles wat een persoon op zijn smartphone of laptop doet – wat véél meer is dan enkel privé-communicaties voeren – maakt de wetgever geen onderscheid wat betreft de voorwaarden tussen een 'simpele' telefoontap en de veel ruimere 'informaticatap'. Voor alle misdrijven op de steeds langere 'taplijst', is een informaticatap dus ook mogelijk. Dit euvel werd niet voorgelegd aan het Grondwettelijk Hof. Het Europees Hof voor de Rechten van de Mens lijkt evenwel striktere voorwaarden voor een informaticatap te verlangen.[10]

Heimelijke informaticazoekingen kunnen enkel worden uitgevoerd tijdens een gerechtelijk onderzoek. Maar ook tijdens een opsporingsonderzoek zijn informaticazoekingen mogelijk, zelfs zonder enige rechterlijke tussenkomst. De politie en procureur des Konings hebben immers de bevoegdheid om in beslag genomen, respectievelijk beslagbare[11] informaticasystemen van een advocaat te doorzoeken (artikel 39bis §2 Sv.). Hoewel een smartphone een schat aan persoonlijke informatie kan bevatten, en daarmee eerder aanleunt bij een huiszoeking dan bij een zoeking in een aktentas die de verdachte meedraagt[12], werd het gebrek aan een rechterlijke machtigingsvereiste aanvaard door het Grondwettelijk Hof.[13] Volgens het Grondwettelijk Hof is zulke informaticazoeking met name aan de orde na een rechtmatige inbeslagname in een heterdaadsituatie of na een huiszoeking. Aangezien het toestel is losgekoppeld van elke externe verbinding, heeft de speurder enkel toegang tot de inhoud die de eigenaar of de bezitter van het toestel erin heeft opgeslagen of bewaard. Zodoende onderscheidt de zoeking zich volgens het Hof niet van de exploitatie van de inhoud van documenten die het voorwerp uitmaken van een inbeslagneming (overweging B.8.4 en 6).

Bovendien maakt de notificatieplicht aan de verantwoordelijke van het informaticasysteem het volgens het Hof mogelijk dat die persoon een strafrechtelijk kortgeding (artikel 28 sexies Sv. / 61 quater Sv.) inleidt om de opheffing van de informaticazoeking te verzoeken (overweging B.8.5). Om die reden interpreteert het Grondwettelijk Hof de verantwoordelijke van het informaticasysteem ruim, in die zin dat het ook de verdachte betreft wiens daarin opgeslagen gegevens het voorwerp uitmaken van die zoeking, wanneer die verdachte zelf niet de effectieve controle heeft over het onderzochte informaticasysteem (overweging B.15.2). Volgens het Grondwettelijk Hof zijn er dan ook voldoende juridische waarborgen die een openlijke informaticazoeking rechtvaardigen.

In de rechtsleer wordt het arrest van het Grondwettelijk Hof terecht bekritiseerd. De vergelijking met een notitieboekje of agenda loopt uiteraard volkomen

9 GwH 6 december 2018, nr. 174/2018. Zie over dit arrest H. Berkmoes, " Saints in space...': het Sinterklaasarrest van 6 december 2018 van het Grondwettelijk Hof over de Kerstmis(cyber)wet van 25 december 2016", *P&R 2019*, 29-36; C. Conings, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr*. 2019, 257-261; P. Monville, M. Giacometti en L. Grisard, "La collecte des preuves numériques en droit belge après l' arrêt de la Cour constitutionnelle du 5 décembre 2018", *Rév.dr.pén*. 2019, 993-1032. Naar aanleiding van dit arrest werd de wet aangepast door Wet van 5 mei 2019 houdende diverse bepalingen in strafzaken en inzake erediensten, en tot wijziging van de wet van 28 mei 2002 betreffende de euthanasie en van het Sociaal Strafwetboek, *BS* 24 mei 2019.

10 EHRM 12 januari 2016, nr. 37138/14, Szabo en Vissy/Hongarije. Zie uitgebreid C. Conings en S. Royer, "Verzamelen en vastleggen van digitaal bewijs in strafzaken", *NC* 2017, 4, 311-338.

11 Wanneer een informaticasysteem in aanmerking komt voor beslag maar dit niet aangewezen (bijvoorbeeld een pc in een cybercafé) of moeilijk is (bv. een grote server van een bedrijf).

12 Cf. de rechtspraak van het Amerikaanse US Supreme Court, Riley v. California, 573 U.S. (2014); US Supreme Court, Carpenter v. United States, 585 U.S. (2018); alsook in Nederland, HR 4 april 2017.

13 GwH 25 december 2018, nr. 174/2018.

mank. Op een gemiddeld informaticasysteem staan doorgaans veel meer en veel meer privacy-intrusieve gegevens dan in eender welk boekje of aktentas. Hoe een strafrechtelijk kortgeding de inmenging in het privéleven a posteriori ongedaan kan maken, is en blijft een groot vraagteken.[14]

Het wereldvreemde karakter van deze redenering van het Grondwettelijk Hof wordt nog frappanter, aangezien het Hof zelf ook erkent dat die 'waarborgen' niet volstaan om de uitbreiding van de informaticazoeking naar andere verbonden informaticasystemen toe te vertrouwen aan de procureur des Konings in plaats van aan de onderzoeksrechter. Om die reden werd artikel 39§3 Sv. vernietigd en werd de netwerkzoeking door de wet van 5 mei 2019 opnieuw toevertrouwd aan de onderzoeksrechter (artikel 88 ter Sv.).

Wanneer de politie dus een informaticasysteem kan doorzoeken, moet het zich beperken tot de gegevens die op het informaticasysteem zelf zijn opgeslagen. Elke externe verbinding moet worden verbroken. Willen ze toegang tot andere informaticasystemen waartoe de eigenaar rechtmatig toegang heeft én waarmee er een gewoonlijke, niet-occasionele verbinding connectie bestaat[15] vanop het initieel doorzochte toestel (bijvoorbeeld de mailbox of de banking applicatie), dan hebben ze hiervoor de machtiging van de onderzoeksrechter nodig, wat evenwel ook via een mini-instructie tijdens het opsporingsonderzoek kan (artikel 28septies Sv.).[16]

Het is hierbij van belang dat die externe verbinding wordt verbroken op het ogenblik van de inbeslagname. Laten speurders een smartphone nog dagenlang verbonden met het internet, dan kunnen er berichten binnen blijven komen en is er sprake van een netwerkzoeking, wat een machtiging van de onderzoeksrechter verlangt.[17]

Vergrendeling en versleuteling

De mogelijkheden voor politie om een informaticasysteem autonoom uit te lezen, is ook beperkt wanneer het toestel is vergrendeld of de inhoud is versleuteld. De procureur des Konings of de onderzoeksrechter kan bevelen "*elke beveiliging van de betrokken informaticasystemen tijdelijk op te heffen, desgevallend met behulp van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheden*" of "*technische middelen in de betrokken informaticasystemen aan te brengen teneinde de door dat systeem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen*" (artikel 39bis §5).

In een strikte lezing van deze wetsbepaling is er dus steeds een machtiging van een magistraat nodig wanneer er een paswoord of pincode moet worden ingegeven om het toestel (of een onderdeel/app ervan) te ontgrendelen. Men kan evenwel oordelen dat de vrijwillige ontgrendeling door de verdachte of het vrijwillig prijsgeven van een wachtwoord, kan gelden als toestemming en afstand van de procedurele voorwaarden. Dit geldt alleen indien die toestemming vrijwillig en met kennis van zaken wordt gegeven[18] en de zoeking niet stiekem wordt uitgebreid tot andere verbonden informaticasystemen.

De vraag rijst of de verdachte ook kan worden gedwongen zijn wachtwoord prijs te geven. De verdachte dwingen het toestel zelf te bedienen of gegevens op te zoeken, is wettelijk uit den boze (artikel *88 quater* §2 Sv.) Op grond van artikel 88quater §1 Sv. kan de onderzoeksrechter evenwel *eenieder* van wie hij vermoedt dat hij over een bijzondere kennis van computersystemen beschikt, verplichten inlichtingen te verstrekken over de werking van het informaticasysteem en over de wijze om er toegang toe te verkrijgen. De medewerking is verplicht en het niet-verlenen van medewerking wordt strafrechtelijk gesanctioneerd.

Zowel het Grondwettelijk Hof[19] als het Hof van Cassatie[20] oordelen dat het decryptiebevel geen inbreuk vormt op het recht om zichzelf niet te beschuldigen omdat het betrekking heeft op "materiaal dat onafhankelijk van de wil van de verdachte bestaat" en op zichzelf niet incriminerend is. Ook de verdachte kan dus worden bevolen zijn wachtwoord prijs te

14 H. Berkmoes, " Saints in space...': het Sinterklaasarrest van 6 december 2018 van het Grondwettelijk Hof over de Kerstmis(cyber)wet van 25 december 2016", *P&R* 2019, 29-36; C. Conings, "Grondwettelijk Hof buigt zich over de wet digitale recherche", *T.Strafr.* 2019, 257-261; P. Monville, M. Giacometti en L. Grisard, "La collecte des preuves numériques en droit belge après l'arrêt de la Cour constitutionnelle du 5 décembre 2018", *Rév. dr.pén*. 2019, 993-1032.

15 Zie uitgebreid hierover S. Royer, F. Verbruggen en W. Yperman, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, afl. 5, 389-416.

16 Dit is ook het geval indien ze niet vanuit het in beslag genomen toestel (openlijk) toegang willen tot de mailbox (artikel 39bis §4 Sv.).

17 Antwerpen 3 juni 2020, C/798/2020, onuitg. Het hof van beroep liet het onrechtmatig verkregen bewijs (i.e. de berichten die 16 dagen na de inbeslagname binnenkwamen op het toestel) evenwel alsnog toe op basis van artikel 32 V.T.Sv.

18 Zie uitgebreid over deze thematiek (zonder de informaticazoeking hierin te betrekken): A. Bailleux, *Afstand van recht in de strafprocedure*, Mortsel, Intersentia, 2019, 1030 p.

19 GwH 20 februari 2020, nr. 28/2020.

20 Cass. 4 februari 2020, A.R. P.19.1086.N.

geven. Deze jurisprudentie wordt echter opnieuw fel bekritiseerd in de Belgische rechtsleer. Het EHRM laat weliswaar toe dat er onder bepaalde voorwaarden materiaal dat "onafhankelijk van de wil van de verdachte" – zoals een haarstaal of welbepaalde[21] documenten – kan worden verzameld zonder dat het recht zichzelf niet te moeten beschuldigen, wordt geschonden.[22]

Of deze stelregel kan worden doorgetrokken naar het moeten prijsgeven van een wachtwoord onder druk van een mogelijke bestraffing, kan ten zeerste worden betwist. Nog los van de vraag of een wachtwoord wel degelijk "onafhankelijk van de wil van de verdachte" bestaat (tenzij er met een vingerafdruk of gezichtsherkenning[23] wordt gewerkt, vergt een wachtwoord immers nog steeds een creatief denkproces), wordt de verdachte immers gedwongen de sleutel tot de in het toestel opgeslagen gegevens te verstrekken en de onderzoekers mogelijk incriminerende informatie op een presenteerblaadje aan te bieden.[24]

Besluit

De digitalisering van ons dagelijks leven leidt ertoe dat we meer en meer (gevoelige) persoonsgegevens zelf verzamelen op een toestel dat gemakkelijk in onze broekzak past. De massa aan informatie die we zo zelf verzamelen, kan van goudwaarde zijn in een strafrechtelijk onderzoek. Een informaticazoeking is derhalve een belangrijke onderzoekshandeling, maar botst evident met het recht op bescherming van het privéleven. Een wettelijke grondslag en effectieve waarborgen tegen willekeur en misbruik zijn derhalve noodzakelijk (artikel 8, lid 2, EVRM). Het Belgisch strafprocesrecht kent sinds enkele jaren wel degelijk een wettelijke bevoegdheid informaticasystemen uit te lezen. Niettemin moet worden vastgesteld dat deze wettelijke regeling op menig vlak lijkt te botsen met de Straatsburgse vereisten inzake artikel 6 en 8 EVRM. Of het huidige rechtskader, zelfs na toetsing door het Grondwettelijk Hof en het Hof van Cassatie, overeind zal blijven in een eventuele procedure voor het EHRM blijft dus af te wachten.

21 Zonder te vervallen in een *fishing expedition* waarbij geen concrete, specifieke documenten worden opgevraagd: EHRM 3 mei 2001, nr. 31827/96, J.B./Zwitserland.

22 EHRM 17 december 1996, nr. 19187/91, Saunders/Verenigd Koninkrijk.

23 Of een verdachte kan worden gedwongen zijn vinger op het scherm te leggen of om in de camera te kijken, is nog niet beslecht door een Belgisch strafgerecht. In Nederland meende de Hoge Raad alvast dat dit geen bovenmatige dwang inhoudt en dat het recht niet te worden gedwongen zichzelf te beschuldigen niet werd geschonden: HR 9 februari 2021, ECLI:NL:HR:2021:202.

24 F. Koning, "Droit au silence et à ne pas s'incriminer: *Quo vadis*?", JT 2020, 204-206; J. Meese, "Recht om te zwijgen maar toch verplicht om te spreken?", *RW* 2019-2020, 1322; S. Royer en W. Yperman, "Wankele argumenten van hoogste Belgische hoven in uitspraken over decryptiebevel (noot onder Cass. 4 februari 2020 en GwH 20 februari 2020)", *NC* 2020, 441-445. Zie ook C. Conings en J. Kerkhofs, "U hebt het recht te zwijgen. Uw login kan en zal tegen u worden gebruikt? Over ontsleutelplicht, zwijgrecht en *nemo tenetur*", *NC* 2018, 457-472; W. Yperman, S. Royer en F. Verbruggen, "Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering", *NC* 2019, 389-416.

De persvrijheid verhindert de vrijgave van gebruikersgegevens op discussiefora, of toch in bepaalde gevallen

Laura Coeckelberghs[1]

In de arresten *Delfi t. Estlandi*[2] en *Magyar t. Hongarije*[3] gaf het Europees Hof voor de Rechten van de Mens ('EHRM') reeds aan dat een online nieuwsportaal aansprakelijk kan zijn voor haar lezersreacties. De vraag of deze online dienstverleners – los van enige aansprakelijkheid – verplicht zouden zijn om gegevens van gebruikers vrij te geven indien vermeende slachtoffers van lasterlijke commentaren de daders wensen te vervolgen, gaat nog een stap verder. In het verleden hamerde het Hof reeds op de nood aan een effectief rechtsmiddel voor slachtoffers, zeker in tijden van digitalisering waar de identificatie en opsporing van daders moeilijk is.[4]

Hoewel de discussie doorgaans verloopt op grond van het recht op eerbiediging van het privéleven (artikel 8 van het Europees Verdrag voor de Rechten van de Mens; 'EVRM'), bekijkt het Hof in *Standard Verlagsgesellschaft Mbh t. Oostenrijk*[5] de problematiek vanuit een andere hoek, namelijk die van artikel 10 EVRM omtrent het recht op vrije meningsuiting. In dit arrest oordeelt het Hof dat de persvrijheid zich kan verzetten tegen het verplicht vrijgeven door een online nieuwsportaal van de gegevens van haar gebruikers.

Het arrest van het EHRM

Feiten

Aan de basis van het arrest liggen een drietal commentaren van gebruikers op het online platform van de krant *Der Standard*. De commentaren werden geplaatst onder artikels die de redactie selecteerde uit haar papieren krant en opnam op haar online forum. Aan het einde van elk artikel worden gebruikers via de banner "*Uw mening telt*" uitgenodigd om een reactie te plaatsen. Om dat te kunnen doen, dienen zij zich voorafgaand te registreren en zijn ze verplicht hun volledige naam en hun e-mailadres door te geven, optioneel ook een adres. Gebruikers worden er op dat ogenblik op gewezen dat hun gegevens niet openbaar zullen worden weergegeven.

Daarnaast voorzien de algemene voorwaarden in een aantal gebruikersrichtlijnen. Op basis hiervan zijn gebruikers zelf verantwoordelijk voor de commentaren die ze plaatsen en waarschuwt de krant dat ze het recht voorbehoudt om commentaren die strijdig zijn met de richtlijnen, te verwijderen. Hiertoe voorziet de krant in een aantal controlemechanismen, waaronder een voorafgaand geautomatiseerd systeem dat kernwoorden screent en een *notice and takedown*-systeem dat werkt via een rapporteringsfunctie onder elke opmerking. Volgens de richtlijnen is een navolgende vrijgave van de gebruikersgegevens slechts mogelijk indien de krant hiertoe wettelijk verplicht zou zijn.

De mogelijkheid dan wel verplichting tot vrijgave van gegevens vormt de kern van de discussie in het geannoteerde arrest. Toen *Der Standard* in 2012 en 2013 de vraag kreeg om vermeende lasterlijke en

1 Advocate bij ARTES Advocaten.
2 EHRM 16 juni 2015, nr. 64569/09, Delfi AS/Estland.
3 EHRM 2 februari 2016, nr. 22947/13, Magyar Tartalomszolgaltatok Egyesülere and Index.hu Zrt/Hongarije.
4 EHRM 2 december 2008, nr. 2872/02, K.U./Finland, §49: "*The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.*". Op lidstaten rusten ook positieve verplichtingen ter bescherming van het recht op privéleven onder artikel 8 EVRM (C.J. FORDER e.a., "Art. 8 EVRM" in *Sdu Commentaar EVRM*, Den Haag, Sdu Uitgevers bv, 2020, 845). Lidstaten dienen daarom de nodige maatregelen te treffen opdat daders geïdentificeerd kunnen worden en vervolging mogelijk is.
5 EHRM 7 december 2021, nr. 39378/15, Standard Verlagsgesellschaft MBH/Oostenrijk (No. 3).

beledigende commentaren te verwijderen en de accountgegevens van de betreffende gebruikers over te maken, weigerde het blad dit te doen. Het ging om een aantal commentaren die enerzijds betrekking hadden op de regionale politieke partij FPK (*Freiheitlichen in Kärnten*[6]) en haar leider, en anderzijds op een lid van het lagerhuis van het Oostenrijkse parlement en algemeen secretaris van de politieke partij FPÖ (*Freiheitliche Partei Österreichs*). De krant verwijderde de commentaren, maar weigerde resoluut om de gegevens te delen.

De geviseerde partijen trokken hierop naar de rechtbanken in Oostenrijk waar ze in eerste aanleg ongelijk kregen nu de rechtbank oordeelde dat de weigering geoorloofd was. Reden was dat voor politici de grenzen van aanvaardbare kritiek verder liggen en dat aldus de voorwaarden voor een wettelijke verplichting tot vrijgave onder de Oostenrijke e-Commercewet niet vervuld waren. De zaak kwam vervolgens met succes in hoger beroep, waar het hof oordeelde dat de bewuste commentaren wel degelijk lasterlijk waren en een vrijgave van gegevens aan de orde was. De krant trachtte zich nog te beroepen op haar bronnengeheim, maar volgens het hof kon niet worden vastgesteld dat zij de commentaren voorafgaand controleerde zodat er geen sprake kon zijn van een verband met haar journalistieke activiteiten. Het Oostenrijkse Hooggerechtshof hield deze beslissingen in stand zodat er voor Der Standard niets anders opzat dan de zaak voor te leggen aan het EHRM.

Beoordeling door het EHRM

Het EHRM benadrukt in haar arrest vooreerst dat de aansprakelijkheid van de krant voor commentaren van haar gebruikers niet ter discussie stond, wel de vraag of de krant als 'host' verplicht was om de data van haar gebruikers al dan niet vrij te geven (§ 68). Het EHRM ging vervolgens over tot de kern van de zaak, namelijk: (i) is er door een verplichting tot vrijgave sprake van een inmenging met de persvrijheid en (ii) zo ja, voldoet deze verplichting aan de beperkingsvoorwaarden uit artikel 10, lid 2, EVRM op basis waarvan een inbreuk op de vrijheid van meningsuiting toelaatbaar is indien de inbreuk bij wet voorzien is, een legitiem doel dient en noodzakelijk is in een democratische samenleving.

(i) Inmenging met de persvrijheid? Het Hof aanvaardt vooreerst niet dat de krant zich kan beroepen op haar bronnengeheim om een vrijgave te beletten. Het Hof bevestigt weliswaar dat de persvrijheid ook de bescherming van 'journalistieke bronnen' dekt, maar dan zouden de commentaren op het nieuwsportaal gericht dienen te zijn aan een journalist, niet aan het publiek (§ 70-71). Desalniettemin benadrukt het Hof dat een inmenging in de persvrijheid ook nog op andere manieren tot uiting kan komen.

Los van de vraag of *Der Standard* als uitgever of 'host' gekwalificeerd kon worden, stelt het Hof vast dat de publicatie van de commentaren slechts een deel van de activiteiten van de krant vormt, aangezien ze daarnaast ook een dagelijkse papieren krant uitgeeft en een nieuwsportaal onderhoudt waar ze lezers actief uitnodigt om commentaren te plaatsen die ze al dan niet controleert.

Volgens het Hof zijn al deze activiteiten onderling met elkaar verbonden en bestaat de algemene rol van de krant in het bevorderen van een open discussie en de uitwisseling van ideeën met betrekking tot onderwerpen van publiek belang. Een rol die naast het bronnengeheim eveneens beschermd wordt onder de persvrijheid (§ 73). Het Hof aanvaardt in lijn hiermee dat de mogelijke verplichting tot vrijgave van gegevens ertoe kan leiden dat gebruikers minder snel geneigd zijn om nog gebruik te maken van het nieuwsportaal en dat dit aldus een '*chilling effect*' kan hebben op het achterlaten van commentaren. Volgens het Hof beïnvloedt dit indirect de persvrijheid van de krant (§ 74).

Het Hof houdt evenwel rekening met de eigenheid van het internet – waar onwettige meningen zich wijd en snel kunnen verspreiden – en stelt dat er op het internet geen absoluut recht op anonimiteit bestaat (§ 75). Toch aanvaardt het Hof dat de krant haar gebruikers een mogelijkheid van anonimiteit toekent, niet alleen in het licht van de eigen persvrijheid, maar ook op grond van het recht op privéleven en de vrijheid van meningsuiting van haar gebruikers – een anonimiteit die volgens het Hof niet effectief zou zijn indien de krant niet zelf deze bescherming zou kunnen afdwingen (§ 78). Het Hof oordeelt op basis hiervan dat het bevel om de gegevens van gebruikers vrij te geven een inmenging vormt op de persvrijheid zoals beschermd door artikel 10 EVRM.

(ii) Voorzien bij wet, legitiem doel en noodzakelijk in een democratische samenleving? Dat de beperking op de persvrijheid via de verplichting tot vrijgave voorzien was bij wet en een legitiem doel had, werd niet betwist. De hoofdvraag was of de inmenging noodzakelijk was in een democratische samenleving. Het Hof brengt hiervoor haar welgekende criteria in herinnering en benadrukt dat er weinig ruimte is voor een beperking van de persvrijheid indien het

6 De partij maakt deel uit van de federale Freiheitliche Partei Österreichs (FPÖ).

gaat om publieke personen zoals politici (§ 85-87). De commentaren in kwestie waren misschien wel aanvallend of getuigden van weinig respect, het ging vooralsnog niet om *hate speech* of het aanzetten tot geweld, noch waren de commentaren kennelijk onwettig (§ 89-90).

Het Hof erkent dat slachtoffers van lasterlijke uitlatingen recht hebben op een effectieve toegang tot de rechter, maar ook dat nationale rechtbanken in dat geval nog altijd de verschillende belangen correct dienen af te wegen. Volgens het Hof gaat het bij deze belangenafweging niet alleen om het recht op bescherming van reputatie onder artikel 8 EVRM en de persvrijheid onder artikel 10 EVRM, maar ook om de rol van de krant in de bescherming van de gegevens van haar gebruikers en hun vrijheid om publiekelijk commentaren te formuleren (§ 93).

Het Oostenrijkse Hooggerechtshof meende dat deze belangenafweging slechts plaats hoorde te vinden in een procedure tegen de auteur van de opmerking, maar dit kan volgens het Hof niet volstaan. De belangenafweging is vereist, al is dit in het kader van een prima facie onderzoek. Het Hof meent hierdoor dat er onterecht geen rekening werd gehouden met de rol van de anonimiteit in het promoten van het openlijk delen van meningen, ideeën en informatie door gebruikers van een platform, in het bijzonder wanneer het gaat om politieke uitingen die niet haatdragend of anderszins duidelijk onwettig waren (§ 95). Het EHRM komt tot het besluit dat de nationale rechtbanken faalden in een correcte afweging van het recht op privéleven met het recht op bescherming van de persvrijheid, met een schending van artikel 10 EVRM tot gevolg (§ 96-97).

Commentaar: implicaties in de praktijk

Het arrest van het EHRM is opmerkelijk te noemen, nu het de bescherming door artikel 10 EVRM aanzienlijk uitbreidt voor online dienstverleners die – ondanks hun passieve rol – in het algemeen gekenmerkt worden door hun journalistieke activiteiten. Bovendien worden vermeende slachtoffers met dit arrest enigszins beperkt in de uitoefening van hun rechten. Niet enkel de persvrijheid in de strikte zin van het woord dient immers mee in rekening worden genomen, maar ook de rol van het platform in de bescherming van de anonimiteit van haar gebruikers. Als het ware wordt hiermee het recht op bescherming van het privéleven onder artikel 8 EVRM van de gebruikers mee in de beoordeling genomen bij de vraag of er sprake is van een inmenging met de persvrijheid onder artikel 10 EVRM. Een discussie die overigens in *Delfi en Magyar* niet aan bod kwam, aangezien partijen het in beide gevallen eens waren over een inmenging met artikel 10 EVRM.[7]

Verrassend is ook dat *Der Standard* haar rol als beschermer van de anonimiteit en vrijheid van meningsuiting van haar gebruikers zelf niet aanreikte als argument om een vrijgave te beletten, maar zich louter beriep op haar bronnengeheim. Aldus is het Hof zelf op zoek gegaan naar een verantwoording om een inmenging met de persvrijheid te weerhouden en een evenwicht te vinden tussen de verschillende belangen.

Dat het arrest ver gaat in de toepassing van artikel 10 EVRM is ook rechter Eicke, die een gedeeltelijke *dissenting opinion* neerpende, niet ontgaan. Hij is het niet eens met de meerderheid in diens oordeel dat er sprake was van een inmenging met de persvrijheid. Dat de toepassing van artikel 10 EVRM in het spel komt indien een online nieuwsportaal aansprakelijk is voor de verwijdering van geplaatste commentaren of wanneer die verplicht wordt eigen onderzoeksmateriaal over te dragen, kan rechter Eicke begrijpen aangezien er dan een duidelijke link is met de journalistieke activiteiten. Maar hij vraagt zich af of dit nog altijd het geval is wanneer deze dienstverleners gevraagd worden gegevens van gebruikers over te maken m.b.t. commentaren waar ze zelf niet bij betrokken waren en die – zoals het Hof zelf aangeeft – geen enkele link met journalistieke activiteiten vertonen.

Waar het '*chilling effect*' duidelijk aanwezig is bij aansprakelijkheid voor het plaatsen of verwijderen van commentaren, is dit volgens rechter Eicke niet of minder het geval bij overmaking van accountgegevens. Hij wijst hiervoor ook op het feit dat de algemene voorwaarden van de krant uitdrukkelijk stelden dat *Der Standard* gegevens zou delen indien zij hiertoe wettelijk verplicht zou zijn. Gebruikers waren bijgevolg verwittigd dat hun anonimiteit grenzen kende. Bovendien bleek nergens uit dat de gebruikers er iets op tegen hadden dat hun gegevens gedeeld zouden worden en/of ze verlangden dat het platform in hun naam optrad. Eicke meende dan ook dat er in het licht van de concrete omstandigheden geen grond was om de toepassing van artikel 10 EVRM uit te breiden naar passieve dienstverleners onder de e-Commercerichtlijn.[8]

7 EHRM 16 juni 2015, nr. 64569/09, Delfi AS/Estland, §118-119; EHRM 2 februari 2016, nr. 22947/13, Magyar Tartalomszolgaltatok Egyesülere and Index.hu Zrt/Hongarije, §45.

8 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *Pub.* 17 juli 2000, L-178/1.

Het is voer voor een zeer interessante discussie, al is de draagwijdte van het arrest ook wel beperkter dan op het eerste zicht lijkt. De concrete feiten zijn en blijven belangrijk en zorgen ervoor dat de uitkomst van dit arrest niet zomaar toegepast kan worden op andere gevallen. Het Hof stelt immers duidelijk dat de noodzaak om de rol van anonimiteit mee in rekening te nemen in de belangenafweging of de proportionaliteitstoets in het bijzonder geldt wanneer het gaat om politieke uitingen die niet haatdragend of anderszins duidelijk onwettelijk zijn.[9] Wat indien het dus niet gaat om politieke uitingen of indien het gaat om commentaren die wél kennelijk onwettig zijn?

Ook de aard van de dienstverlener speelt een rol en niet elke blog of elk forum zal in de toekomst een beroep kunnen doen op artikel 10 EVRM om een vrijgave van gegevens te weigeren. Het arrest heeft betrekking op een als het ware hybride dienstverlener die naast een forum ook een krant met bijhorende website uitgeeft over onderwerpen van publiek belang. Indien de journalistieke link ontbreekt en het zou gaan om zuivere blogs of andere sociale mediakanalen waar geen enkele actieve rol is voor het platform, is het maar de vraag of het Hof dezelfde mening zou zijn toegedaan. Het toont aan dat het Hof heeft getracht te zoeken naar een juist evenwicht tussen de verschillende belangen in het licht van de concrete omstandigheden.

Evenmin lijkt het dat we met dit arrest opnieuw in een situatie terechtkomen waarbij de mening van het Hof niet strookt met de bepalingen van de e-Commercerichtlijn zoals dit met *Delfi* het geval was.[10] Indien de commentaren niet kennelijk onwettig zijn, zijn host-dienstverleners immers niet verplicht om reacties te verwijderen en te voldoen aan hun meld- en medewerkingsplichten. In België kan hiervoor verwezen worden naar artikel XII.20 §2 lid 2 Wetboek Economisch Recht, dat voorziet in een verplichting voor dienstverleners om bij onwettige activiteiten of informatie op verzoek van de autoriteiten alle informatie te verschaffen waarover ze beschikken en die nuttig is voor de opsporing en de vaststelling van inbreuken door hun tussenkomst, zoals gebruikersgegevens.[11] Het is dus slechts wanneer het Hof zou menen dat een vrijgave van gebruikersgegevens evenzeer niet mogelijk is bij (kennelijk) onwettige commentaren, dat online dienstverleners zich in een positie kunnen bevinden waarin ze wettelijk gezien verplicht zouden zijn om informatie te delen op grond van de e-Commercerichtlijn, maar zich tegelijk ook kunnen beroepen op artikel 10 EVRM om dit te verhinderen.

In die lijn valt er tot slot nog iets te zeggen over de inperking door het arrest van de effectiviteit voor slachtoffers om daders aansprakelijk te stellen. Zoals hoger opgemerkt, is het identificeren van daders essentieel om tot een vervolging te komen, iets wat door de anonimiteit op het internet vaak onmogelijk wordt gemaakt. Zelfs indien het gaat om politieke uitingen die niet haatdragend zijn of commentaren die niet kennelijk onwettig zijn, is toegang tot de rechter een fundamenteel recht. Indien slachtoffers zich niet kunnen richten tot het platform, tot wie dan wel?

De opmerking van rechter Eicke dat gebruikers die de algemene voorwaarden van het platform aanvaarden, op de hoogte zijn van het feit dat hun gegevens gedeeld kunnen worden indien de wet dit vereist (en dus bij onwettige activiteiten), zou er eigenlijk toe moeten leiden dat platformen zich niet achter de persvrijheid kunnen en zelfs hoeven te verschuilen, iets wat de nodige effectiviteit van het recht tot toegang tot de rechter alleen maar ten goede zou komen. Een vrijgave impliceert overigens niet per definitie een veroordeling. Het besproken arrest geeft daarmee opnieuw een mooi voorbeeld van hoe de digitalisering de mensenrechten wel eens kan uitdagen.

9 *"In the instant case, the lack of any balancing between the opposing interests (see paragraph 94 above) overlooks the function of anonymity as a means of avoiding reprisals or unwanted attention and thus the role of anonymity in promoting the free flow of opinions, ideas and information, in particular if political speech is concerned which is not hate speech or otherwise clearly unlawful. In view of the fact that no visible weight was given to these aspects, the Court cannot agree with the Government's submission that the Supreme Court struck a fair balance between opposing interests in respect of the question of fundamental rights (see paragraph 60 above)."* (eigen nadruk)

10 Zie hierover: K. Janssens en T. De Meese, "De aansprakelijkheid van nieuwswebsites na de Delfi- en Magyar-arresten van het EHRM: Much Ado About Nothing?", *Computerrecht* 2016, 2, 101-112.

11 Artikel 15 (2) van de e-Commercerichtlijn voorziet in dit kader het volgende: "*De lidstaten kunnen voorschrijven dat dienstverleners de bevoegde autoriteiten onverwijld in kennis dienen te stellen van vermeende onwettige activiteiten of informatie door afnemers van hun dienst, alsook dat zij de bevoegde autoriteiten op hun verzoek informatie dienen te verstrekken waarmee de afnemers van hun dienst met wie zijn opslagovereenkomsten hebben gesloten, kunnen worden geïdentificeerd*" (eigen nadruk).

12 K. De Schepper en C. Van De Heyning, "De strafrechtelijke aansprakelijkheid van een internetnieuwsportaal voor zijn lezersreacties: het arrest Delfi in de Belgische strafrechtelijke context", *T.Strafr*. 2016, 4, 282, 286.