UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content

Eindrapportage

van Hoboken, J.; Appelman, N.; van Duin, A.; Blom, T.; Zarouali, B.; Ó Fathaigh, R.; Seel, M.; Stringhi, E.; Helberger, N.

Publication date
2020

Document Version
Final published version

Link to publication

Citation for published version (APA):
van Hoboken, J., Appelman, N., van Duin, A., Blom, T., Zarouali, B., Ó Fathaigh, R., Seel, M., Stringhi, E., & Helberger, N. (2020). *WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content: Eindrapportage*. (WODC rapport; No. 3108). Instituut voor Informatierecht, Universiteit van Amsterdam.
https://repository.wodc.nl/handle/20.500.12832/2489

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:17 Nov 2026

Universiteit van Amsterdam

IViR (Instituut voor Informatierecht)

WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content

Eindrapport, 1 september 2020

Instituut voor Informatierecht (IViR),
Universiteit van Amsterdam, 2020

Een rapport voor het Wetenschappelijk
Onderzoek- en Documentatiecentrum

Instituut voor Informatierecht
Faculteit der Rechtsgeleerdheid
Universiteit van Amsterdam
Nieuwe Achtergracht 166
1018 WV Amsterdam

WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content

Eindrapportage

Joris van Hoboken, Naomi Appelman, Anna van Duin, Tom Blom, Brahim Zarouali,
Ronan Ó Fathaigh, Michelle Seel, Elisabetta Stringhi, Natali Helberger

Amsterdam, 1 september 2020

Inhoudsopgave

Samenvatting 11

1. Introductie 15
- **A. Algemene inleiding** 15
- **B. Onderzoeksvragen** 15
- **C. Opzet en methodologie** 17

2. De problematiek van onrechtmatige online content 19
- **A. Soorten onrechtmatigheid** 19
- **B. Type internetdienst** 23
- **C. Omvang maatschappelijk probleem** 28
- **D. Toegang tot recht** 30
- **E. Maatschappelijke behoefte** 34
- **F. Conclusie** 38

3. Grondrechtelijk kader en internationale context 39
- **A. Grondrechtelijke kader** 39
  - i. Artikel 8 EVRM (Recht op privéleven) 39
  - ii. Artikel 10 EVRM (Vrijheid van meningsuiting) 41
  - iii. Artikel 6 EVRM (eerlijk proces) 44
- **B. Europese context** 45
  - i. Digital Services Act 45
  - ii. Andere landen 47
- **C. Conclusie** 50

4. Bestaande juridisch kader voor verwijdering en knelpunten 51
- **A. Notice and Takedown-procedure** 51
  - i. Zelfregulering 52
  - ii. Beleid van internetdiensten en automatisering 53
  - iii. Gebruik en knelpunten 55
- **B. Civielrechtelijke routes** 58
  - i. Modaliteiten 58
  - ii. Bodemprocedure vs. kort geding 59
  - iii. Verzoekschriftprocedure en collectieve actie 60
  - iv. Ex parte-procedure op grond van art. 1019e Rv 61
  - v. Evaluatie en knelpunten 63
- **C. Bestuursrechtelijke route** 64
  - i. Klachtenprocedure Autoriteit Persoonsgegevens 64
  - ii. Individuele rechten uit de AVG 65
  - iii. Evaluatie en knelpunten 66
- **D. Raakpunten Strafrecht** 67
  - i. Verwijderen informatie via strafprocesrecht 67
  - ii. Samenloop met civiel recht 71
  - iii. Evaluatie en knelpunten 71
- **E. Conclusie** 71

5. Knelpuntenanalyse en oplossingsrichtingen 72
A. Knelpuntenanalyse 72
i. Analyse procedurele routes 72
ii. Koppeling maatschappelijke behoefte 75
B. Notice and Takedown 79
C. Civiele recht 82
i. Gefaseerde opbouw van procedurele mogelijkheden 82
ii. Tijdelijke Experimentenwet rechtspleging 85
D. Bestuursrecht 86
E. Strafrecht 88
i. Kan de strafrechtelijke procedure worden vereenvoudigd? 88
ii. De rol van de aangifte bij een vereenvoudigde procedure 89
F. Informatievoorziening 90
i. Routekaart 90
ii. Juridische informatie en rechtshulp 91
iii. Meldpunten 92
G. Toezichthouder 93
H. Conclusie 94

6. Conclusie 95

Literatuurlijst 100

Annex i – Begeleidingscommissie 117

Annex ii – Verkorte leidraad expert workshop 118
i. Probleemanalyse 118
ii. Specifieke knelpunten 118
iii. Mogelijke oplossingsrichtingen 119

Annex iii – Verkorte leidraad expert interviews 120

Annex iv – Deelnemers expert interviews en workshop 121
i. Overzicht deelnemers expertinterviews 121
ii. Overzicht deelnemers expertworkshops 121

Annex v – Survey 123

Annex vi – Resultaten survey 128
i. Algemene info 128
ii. Surveyresultaten 129
iii. Nadere analyse 142

Samenvatting

Dit onderzoek is uitgegeven als onderdeel van het speerpunt van de Minister voor Rechtsbescherming om de positie van slachtoffers van onrechtmatige uitingen op het internet te verbeteren. Aanleiding is dat het voor mensen als te moeilijk ervaren wordt om onrechtmatige online content snel verwijderd te krijgen.[1] Dit rapport biedt inzicht in de juridische en praktische haalbaarheid van een voorziening voor de verwijdering van onrechtmatige online content die mensen persoonlijk raakt. Onrechtmatige content is informatie, door mensen op het internet geplaatst, die in strijd is met het recht, vanwege de schadelijke gevolgen ervan en/of omdat de belangen van anderen daardoor op ernstige wijze worden aangetast. Hierbij moet, bijvoorbeeld, gedacht worden aan bedreigingen, privacy-inbreuken of wraakporno. Het doel van de onderzochte voorziening is om mensen in staat te stellen deze onrechtmatige online content zo snel mogelijk te verwijderen. Het onderzoek focust op onrechtmatige online content die mensen in hun persoon raakt en daarmee onder het recht op privéleven uit artikel 8 Europees Verdrag voor de Rechten van de Mens (**"EVRM"**) valt. Het onderzoek is uitgevoerd middels een combinatie van analyse van literatuur, jurisprudentie, wetgeving, en andere relevante documentatie, een representatieve survey onder de Nederlandse bevolking, een serie expertinterviews, en twee workshops met experts.

De problematiek van het verwijderen van onrechtmatige online content is complex en heterogeen. Uit de uitgevoerde survey is af te leiden dat 15% van de Nederlandse bevolking direct of indirect ervaring heeft met het soort van schadelijke, en mogelijk onrechtmatige, content waar deze studie zich op richt. Uit de survey en expertinterviews blijkt verder dat het moeilijk verwijderd krijgen van onrechtmatige online content breed gezien wordt als een maatschappelijk probleem. De heterogeniteit van de problematiek komt door de grote diversiteit aan typen onrechtmatige uitingen, de diversiteit aan internetdiensten die betrokken zijn, en de verschillende soorten schade die de content kan veroorzaken. De problematiek bevindt zich op het snijvlak van de bredere onderwerpen van de toegang tot recht en internetregulering.

De problemen die een individu tegen kan komen wanneer deze geconfronteerd wordt met onrechtmatige content en op zoek is naar een manier om deze te verwijderen, zijn samengevat in zeven struikelblokken, weergegeven in de tabel (Figuur i). Om daadwerkelijk zicht te krijgen op de maatschappelijke behoefte aan een nieuwe procedure, zijn de verschillende bestaande procedures geanalyseerd en is gekeken in hoeverre zij deze struikelblokken wegnemen.

Individuele struikelblokken
Bekendheid & bereikbaarheid dienst
Type onrechtmatige content
Type internetdienst
Mate van vereiste specialistische kennis
Terugkomende content
Persoonlijke omstandigheden
Toegang tot de rechter

Figuur i

Concreet zijn dit de volgende procedures. Ten eerste zijn er vier civielrechtelijke procedures onderzocht, waarin de civiele rechter een bevel gevraagd kan worden om de onrechtmatige content te verwijderen. De doorloopttijd van een civiele bodemprocedure is in de praktijk 6-9 maanden. In geval van spoed kan in kort geding op relatief korte termijn een voorlopige voorziening verkregen worden. In beide gevallen geldt verplichte procesvertegenwoordiging door een advocaat. In de verzoekschriftprocedure die nu al openstaat voor verzoeken op grond van de Algemene Verordening Gegevensbescherming (**"AVG"**) is geen advocaat vereist. Deze procedure wordt als flexibeler en informeler gezien en de rechtbank is

1 Zie de reactie van de regering op het burgerinitiatief «Internetpesters aangepakt», Tweede Kamer, vergaderjaar 2018–2019, 34 602, nr. 2.

verantwoordelijk voor de oproeping van betrokken partijen. De ex parte-procedure uit hoofde van artikel 1019e Wetboek van Burgerlijke Rechtsvordering (**"Rv"**), tot slot, bestaat momenteel alleen binnen het Intellectueel Eigendomsrecht (**"IE-recht"**) en houdt in dat, in zeer spoedeisende situaties, een voorlopige voorziening van de civiele rechter kan worden verkregen zonder dat de wederpartij eerst gehoord wordt. Geen van deze procedures neemt alle struikelblokken weg, maar er is wel ruimte om gericht te experimenteren met het (deels) verminderen van de geïdentificeerde procedurele obstakels.

Naast de civielrechtelijke route is de bestuursrechtelijke route via de Autoriteit Persoonsgegevens (**"AP"**) besproken. Bij schending van de AVG kan een individu een klacht indienen bij de AP. Het ligt binnen de discretionaire bevoegdheid van de AP om te besluiten of de klacht opgepakt wordt. Om specifieke onrechtmatige content verwijderd te krijgen heeft de AP de mogelijkheid boetes of dwangsommen op te leggen. Daarnaast kent de AVG ook individuele rechten die mensen zelf kunnen uitoefenen tegenover iemand die inbreuk maakt op zijn of haar rechten. Een individu moet zich dan eerst tot degene die de inbreuk maakt (de verwerker) wenden en wanneer deze weigert mee te werken is er de mogelijkheid dit af te dwingen via een civiele verzoekschriftprocedure.

De klachtenprocedure bij relevante internetdiensten (Notice and Takedown) is ook centraal betrokken in het onderzoek. Dit is geen juridische route tot verwijdering, maar in de praktijk wel belangrijk voor het verwijderen van onrechtmatige online content gezien het laagdrempelige karakter. Een individu volgt hierbij de klachtenprocedure die een internetdienst zelf aanbiedt en waar de internetdienst ook zelf de beslissing neemt of de content verwijderd wordt. Wanneer een Notice and Takedown-procedure niet tot resultaat leidt kan een individu zich alsnog wenden tot de civiele rechter. Tenslotte besteedt het rapport aandacht aan de waarde van de aangifte in het strafrecht en hoe politie en justitie een rol kunnen spelen bij de verwijdering van onrechtmatige online content.

De procedures zijn op een aantal criteria beoordeeld, ontleend aan de besproken problematiek rond de toegang tot recht, het grondrechtelijk kader van artikel 6, 8 en 10 EVRM en de ervaringen en belangen van betrokken personen. Het betreft de doorlooptijd, en de drempels om te procederen uitgesplitst in kosten en complexiteit, procedurele waarborgen, waarborgen voor de vrijheid van meningsuiting, doeltreffendheid en capaciteit/schaalbaarheid.

Uit de uitgevoerde analyse ontstaat het onderstaande beeld (Figuur ii). Wanneer de figuur in zijn geheel wordt bekeken, is zichtbaar waar bepaalde afwegingen moeten worden gemaakt. Er zijn enerzijds procedurele routes die snel, laagdrempelig en schaalbaar zijn, en anderzijds procedures die optimale rechtstatelijke waarborgen bieden. Een combinatie van al deze kwaliteiten in één procedure lijkt uitgesloten.

	Schaalbaarheid	Doorlooptijd	Drempelkosten	Drempel complexiteit	Proceswaarborg	VvMU* waarborg	Doeltreffendheid
Civielrecht							
Bodemprocedure							
Verzoekschrift							
Kort geding							
Ex parte							
Bestuursrecht							
Klacht AP							
AVG rechten							
Buiten juridisch							
Notice & Takedown							

Rood: de procedure scoort niet goed op het criterium.
Oranje: de procedure scoort niet goed maar ook niet slecht op het criterium.
Groen: de procedure scoort goed op het criterium.
* Vrijheid van Meningsuiting

Figuur ii

Door de heterogeniteit van de problematiek en de noodzakelijke afwegingen in het vormgeven van een procedure is er niet één alomvattende oplossing voor de onderzochte problematiek in de zin van één specifieke juridische procedure. Wel zijn er diverse scenario's denkbaar voor aanpassing en verbetering van de geldende juridische kaders en procedures die van toepassing zijn. Deze scenario's sluiten elkaar niet uit, maar kunnen elkaar juist versterken nu zij gericht zijn op het wegnemen of afzwakken van de struikelblokken en knelpunten op verschillende fronten. Vijf oplossingsrichtingen zijn veelbelovend:

1. **Het verder normeren en juridisch vastleggen van de Notice and Takedown-procedure, op nationaal of EU-niveau.**
   Een aantal Europese landen heeft deze stap al gezet in hun nationale wetgeving en momenteel wordt dit ook op EU-niveau voorbereid in de *Digital Services Act* waar, naar verwachting, de regulering van internetdiensten uitgebreid wordt. Bij de normering van Notice and Takedown-procedures moet aandacht uitgaan naar het voorkomen van de verwijdering van rechtmatige content en het bieden van procedurele waarborgen. Het huidige gebruik van Notice and Takedown-procedures door politie en justitie dient daarnaast ook kritisch bekeken te worden.

2. **Het experimenteren met civiele procedures door het gebruik van de Tijdelijke Experimentenwet rechtspleging.**
   Deze wet maakt het mogelijk tijdelijke civiele procedures aan te passen om te zien hoe deze functioneren in de praktijk. Meer specifiek: experimenteren met het kantonrechterskortgeding, de verzoekschriftprocedure die nu al beschikbaar is voor de uitoefening van AVG-rechten en/of de ex parte-procedure. Het kantonrechterskortgeding heeft als voordeel dat het bij uitstek geschikt is voor spoedeisende zaken, er geen verplichte procesvertegenwoordiging geldt en een grotere reikwijdte heeft dan de verzoekschriftprocedure, al is die laatste mogelijk toegankelijker voor benadeelden. Een ex parte-procedure kan uitkomst bieden in zeer spoedeisende zaken die relatief gemakkelijk af te doen zijn, maar daar verdient de uitzondering op hoor en wederhoor een bijzondere rechtvaardiging en duidelijke afbakening;

3. **Het verbeteren van de klachtenprocedure bij de AP en het uitbreiden van het werkgebied van de AP.**
   De AP zou een bredere coördinerende rol kunnen vervullen bij de aanpak van onrechtmatige online content die mensen in de persoon raakt. Dit ligt immers in het verlengde van de taken die zij nu ook al vervult en die raken aan kwesties op het gebied van privacy en de eer en goede naam. Een uitbreiding van de taken van de AP moet wel bezien worden in de bredere discussie over het gebrek aan capaciteit van de AP;

4. **Het geven van meer civielrechtelijke of bestuursrechtelijke betekenis aan de aangifte is juridisch wenselijk noch realistisch.**
   Wel ligt er een mogelijkheid om (nadere) aanwijzingen voor de opsporing en vervolging van strafbare feiten in verband met illegale online content te ontwikkelen. Dergelijke aanwijzingen zouden betrokken partijen meer houvast kunnen bieden. Voor benadeelden voor de vraag of het zin heeft om aangifte te doen en voor de politie voor de aanpak en prioritering van het type zaken dat in deze studie aan de orde is;

5. **Het verbeteren van informatievoorziening aan benadeelden, in het bijzonder op het punt van de route die zij kunnen volgen voor het (laten) verwijderen van onrechtmatige online content.**
   Dit kan ten eerste gebeuren door een verplichting voor relevante internetdiensten tot uniforme informatievoorziening over beschikbare procedures tot verwijdering. Ook kan worden voortgebouwd op bestaande initiatieven – private en van overheidswege – om voorlichting aan benadeelden te geven over hun rechten op het internet en manieren waarop zij die rechten kunnen uitoefenen.

Het rapport concludeert dat veel winst te behalen is met het inrichten van een centraal kenniscentrum of meldpunt waar belanghebbenden terecht kunnen voor een integrale routekaart. Een gelaagd aanbod van informatie – aan rechtszoekenden zelf én aan juristen die hen hulp en bijstand verlenen – is hierbij cruciaal. De onafhankelijkheid van een dergelijk meldpunt of kenniscentrum en de betrokkenheid van reeds bestaande onafhankelijke toezichthouders met taken op het gebied van onrechtmatige online content zijn belangrijke aandachtspunten.

In de eerste lijn is de aanpak van onrechtmatige inhoud het meest effectief wanneer de klacht en verwijderprocedures (Notice and Takedown-procedures) van de betrokken internetdiensten goed verlopen. Vervolgens is voor de overheid een duidelijke rol weggelegd in het verzekeren van grondrechtelijke en rechtsstatelijke waarborgen en het bieden van een stok achter de deur: het handhaven of afdwingen van individuele rechten via rechterlijk ingrijpen. Vanuit de verantwoordelijkheid voor de bescherming van grondrechten, zowel de bescherming van het recht op privéleven als de vrijheid van meningsuiting, is een actieve rol van de overheid vereist in de aanpak van onrechtmatige online content. Het belang van de bescherming van deze grondrechtelijke belangen vormt tevens het belangrijkste argument om voor de aanpak van onrechtmatige content speciale voorzieningen te overwegen. Dit onderzoek concludeert echter dat hiervoor, door de heterogeniteit van de problematiek, geen uniforme oplossing bestaat. Het biedt de bovenstaande oplossingsrichtingen om bestaande knelpunten weg te nemen en om de verschillende problemen zo goed mogelijk aan te sluiten bij de bestaande maatschappelijke behoefte.

1. Introductie

A. Algemene inleiding

Dit onderzoek heeft als doel inzicht te bieden in de juridische en praktische haalbaarheid, evenals de mogelijke vormgeving, van een voorziening die personen in staat stelt deze content op zo kort mogelijke termijn te (laten) verwijderen. Bij 'voorziening' moet zowel worden gedacht aan een aanpassing of uitbreiding van reeds bestaande (juridische) procedures, als een mogelijke nieuwe procedure en/of een specifiek meldpunt waar burgers met hun verzoek tot verwijdering terecht kunnen. Naast de juridische aspecten van een dergelijke voorziening wordt rekening gehouden met de technische en organisatorische aspecten die een rol kunnen spelen bij de inrichting daarvan. Bij de verwijdering van onrechtmatige inhoud komt in eerste instantie een belangrijk rol toe aan de internetdiensten waar sprake is van een eventuele onrechtmatige uiting of activiteit. Deze diensten zullen vaak een beroep kunnen doen op een voorwaardelijke beperking van aansprakelijkheid. Zij zullen in de regel wel een mogelijkheid bieden om de desbetreffende onrechtmatigheid te rapporteren met het oog op verwijdering.

Het onderzoek kan gezien worden tegen de achtergrond van het voorstel van de minister voor Rechtsbescherming om de positie van slachtoffers van onrechtmatige uitingen op internet te verbeteren. Daarbij zet de Nederlandse regering in op twee trajecten. Eén traject is gericht op het aanbrengen van verbeteringen in het snel verwijderd krijgen van onrechtmatige uitingen. Een tweede traject is erop gericht slachtoffers in staat te stellen de persoon die de onrechtmatige uitingen heeft geplaatst, via een civiele procedure aan te spreken tot schadevergoeding. Dit onderzoek spitst zich toe op het eerste traject. De plannen van de regering sluiten aan bij het burgerinitiatief 'Internetpesters aangepakt', dat mede aanleiding tot dit onderzoek heeft gegeven.[2]

B. Onderzoeksvragen

Het onderzoek richt zich op de volgende probleemstelling:

> In hoeverre is een voorziening voor verzoeken tot snelle verwijdering van online content in juridische en praktische zin haalbaar, hoe zou die voorziening eruit kunnen zien en waar zouden de daarvoor vereiste werkzaamheden belegd kunnen worden?

De aanpak van illegale, onrechtmatige, en schadelijke inhoud op internet is al meer dan twee decennia het onderwerp van onderzoek en beleid.[3] Toch blijft de internetomgeving, mede door nieuwe ontwikkelingen in het aanbod en gebruik van internetdiensten, een belangrijke bron van schade aan de rechten en vrijheden van veel Nederlandse burgers. Een verscheidenheid van onrechtmatige uitingen, waaronder inbreuken op de persoonlijke levenssfeer en de eer en goede naam, vindt zijn weg naar het internet. Alhoewel er voor slachtoffers verschillende middelen openstaan om vermeend onrechtmatige uitingen verwijderd te krijgen, blijft de vraag naar een laagdrempelig en effectief instrument om onrechtmatige uitingen te adresseren urgent. In het bijzonder is dat het geval ten aanzien van het verder verminderen van de drempels die slachtoffers ervaren om onrechtmatige uitingen zo snel mogelijk verwijderd te krijgen.

2 *Kamerstukken II* 2018/19, 34602, 2.

3 Voor een bespreking van het onderscheid tussen illegale (strafbare) en anderszins onrechtmatige inhoud, zie paragraaf 2.a. Niet alle schadelijke inhoud is daadwerkelijk juridisch onrechtmatig. Dit onderzoek richt zich in de kern op (de verwijdering van) onrechtmatige inhoud.

Bij de vormgeving van een dergelijke voorziening moet rekening gehouden worden met de rechten van betrokkenen, van dienstverleners en de vrijheid van meningsuiting. Er is naast het belang dat juridische procedures de juiste waarborgen bieden voor de bescherming van de vrijheid van meningsuiting, het gevaar dat sociale media en andere platforms bij het toepassen van hun gebruiksvoorwaarden en huisregels te restrictief handelen en daarmee de mogelijkheid van mensen zich vrij te uiten te veel beperken. Het belang van de vrijheid van meningsuiting maakt dat bij de vormgeving van (nieuwe) voorzieningen goed rekening gehouden moet worden met het bestaande afwegingskader, waarin betekenis wordt toegekend aan factoren als de aard van het recht waarop inbreuk wordt gemaakt en de ernst van de inbreuk. Niet altijd zal op voorhand kunnen worden vastgesteld dat een uiting onrechtmatig is. In zo een geval is een onafhankelijk oordeel over de vraag of schadelijke inhoud daadwerkelijk onrechtmatig is, van essentieel belang. Dit onderzoek is vormgegeven vanuit de gedachte dat er in de praktijk een behoefte bestaat aan een gelaagde voorziening, met effectieve middelen voor de aanpak van content waarvan de onrechtmatigheid makkelijk vast te stellen is en een meer afgewogen toets voor gevallen waarin dit niet zo is.

Op basis van bovengenoemde probleemstelling en aan de hand van de door het Wetenschappelijk Onderzoek- en Documentatiecentrum (“**WODC**”) ontwikkelde vraagstelling, zijn voor dit onderzoek de onderstaande onderzoeksvragen geformuleerd. De vragen zien op het bestaande juridisch kader (civiel- en bestuursrechtelijk); de beperkingen en mogelijkheden hiervan; alsmede de vormgeving van, de maatschappelijke behoefte aan, en de implementatie van een nieuwe voorziening voor de verwijdering van onrechtmatige online content. In lijn met de probleemstelling zien deze vragen steeds zowel op de juridische als de praktische (inclusief technische en organisatorische) aspecten van het huidige kader en de nieuwe voorziening. Bij de formulering van de onderzoeksvragen is de centrale rol van de aanbieders van internetdiensten, in het bijzonder sociale media, bij het adresseren van onrechtmatige content meegenomen. De mogelijkheden om online content verwijderd te krijgen door het rapporteren hiervan aan internetdiensten middels zogenaamde notificaties en rapportage instrumenten (e.g. *flagging* d.w.z. een ‘dit-is-niet-oké-button’), is immers, de meest laagdrempelige mogelijkheid die voor slachtoffers voorhanden is om content verwijderd te krijgen. In de onderzoeksvragen wordt ook duidelijk verwezen naar de relevante Europeesrechtelijke normen die in dit domein van toepassing zijn (waaronder de Richtlijn Elektronische Handel (“**e-Commerce richtlijn**”) en het grondrechtelijk kader). De e-Commerce richtlijn is van belang voor de aansprakelijkheid van de internetdiensten waar de onrechtmatige content op internet te vinden is.

Onderzoeksvragen:

1. Wat zijn bestaande mogelijkheden voor het indienen van een verzoek tot verwijdering van onrechtmatige online content in het burgerlijk recht (bodemprocedure, kort geding, ex parte maatregelen, etc.) en het bestuursrecht (zoals via de Autoriteit Persoonsgegevens) en welke beperkingen en mogelijkheden brengen deze met zich?

2. Welke mogelijkheden bieden aanbieders van verschillende soorten relevante internetdiensten voor het verwijderd krijgen van vermeend onrechtmatige inhoud en hoe verhouden deze buiten-juridische mogelijkheden zich tot het Nederlands en Europeesrechtelijk juridisch kader?

3. Wat is de maatschappelijke behoefte in Nederland aan een nieuwe voorziening voor de verwijdering van verschillende vormen van onrechtmatige inhoud, in termen van type en aantal onrechtmatige uitingen, type dienst, snelheid, grondslag en rechtsgang, toegankelijkheid, en effect op de vrijheid van meningsuiting?

4. Wat zijn de mogelijkheden voor de vormgeving van een nieuwe of aangepaste voorziening, in termen van materieel- en procesrechtelijke verankering, bevoegde instantie, snelheid, kosten, en toegankelijkheid, mede in het licht van het bestaande dienstenaanbod, het Europeesrechtelijk kader (i.h.b. de richtlijn elektronische handel), en de fundamentele rechten, in het bijzonder de vereiste balans tussen de bescherming van het recht op privéleven (artikel 8 Europees Verdrag Rechten van de Mens ('EVRM')) en de vrijheid van meningsuiting (artikel 10 EVRM), en welke van deze mogelijkheden komt optimaal tegemoet aan de juridische en maatschappelijke behoefte?

In de loop van het onderzoek is op verzoek van het WODC de volgende onderzoeksvraag aan het onderzoek toegevoegd:

5. Zou het doen van aangifte van een strafbaar feit bij de politie voldoende moeten zijn voor het toewijzen van een verwijderverzoek?

In bredere zin ziet deze additionele vraag op de eventuele meerwaarde van het strafrecht ten opzichte van civiel- en bestuursrechtelijke routes en de mogelijkheid om bij een nieuwe voorziening voor de verwijdering van onrechtmatige inhoud voort te bouwen op een aangifte van onrechtmatige inhoud bij de politie.

C. Opzet en methodologie

Het onderzoek is uitgezet door het WODC. Op verschillende punten gedurende het onderzoek heeft de begeleidingscommissie, ingesteld door het WODC, input geleverd.[4] Het onderzoek is in vier fasen uitgevoerd en is afgesloten op 31 augustus 2020.

In de eerste fase is de problematiek van onrechtmatige online content aan de hand van bestaande rapporten en wetenschappelijke literatuur bestudeerd en verder afgebakend. In het bijzonder is het huidige wetgevings- en beleidskader (inclusief relevant beleid en zelfregulering door relevante internetdiensten) beschreven en geanalyseerd op knelpunten. Het onderzoek in deze fase heeft geresulteerd in een overzicht van knelpunten en mogelijke richtingen voor een aangepaste ofwel nieuwe juridische voorziening, met specificatie van de juridische en praktische beperkingen en mogelijkheden hiervan in de praktijk. Bij het bestuderen van de oplossingsrichtingen voor een nieuwe juridische voorziening is ook gekeken naar de mogelijkheden om bij relevante internetdiensten onrechtmatige inhoud verwijderd te krijgen via daarvoor ingerichte procedures (Notice and Takedown).[5]

In de tweede fase van het onderzoek is door middel van verdere documentanalyse, een enquête onder de Nederlandse bevolking en een reeks expertinterviews een beeld verkregen van de maatschappelijke behoefte aan een nieuwe voorziening. De enquête bestond uit een survey afgenomen bij een representatieve steekproef van de Nederlandse bevolking (N=2000). Concreet werd het onderzoek uitgevoerd met behulp van het LISS-panel, beheerd door CentERdata. De gemiddelde leeftijd bedroeg 53.7 jaar, en ongeveer 54% van de respondenten waren vrouwen. Op het vlak van opleiding heeft ongeveer 8% een niveau van basisonderwijs, 20% vmbo, 11% havo/vwo, 25% mbo, 24% hbo, en 12% wo. Deze gemiddelde leeftijd, man/vrouw verdeling en verdeling in opleidingsniveau is niet ongebruikelijk bij een representatieve steekproef van de Nederlandse bevolking.

4 Zie annex i voor de samenstelling van de begeleidingscommissie voor het onderzoek.
5 De host moet na kennis van een schadelijk bericht overgaan tot verwijdering. Zie meer over de procedure in 4.a.

De responsgraad van de survey bedroeg 78.8% (N=1576). De survey bestond uit 15 vragen onderverdeeld in drie delen. Deel 1 omvatte vragen over ervaringen met online schadelijke content, vervolgens richtte deel 2 van de survey zich op ervaringen met rapportagemogelijkheden voor schadelijke content, en tenslotte ging deel 3 over ervaringen met juridische stappen. Gemiddeld bedroeg de responstijd ongeveer 5 minuten. De survey bestond uit gesloten vragen (meerkeuzevragen en ranking vragen aan de hand van een 7-punt Likertschaal). De volledige vragenlijst kan geraadpleegd worden in annex v en de resultaten van de survey worden besproken in de relevante passages van deze studie. Een overzicht van alle resultaten is te vinden in annex vi.[6]

De onderzochte maatschappelijke behoefte en de in de eerste fase gesignaleerde knelpunten en mogelijkheden ten aanzien van het verwijderen van onrechtmatige inhoud vormden de basis voor een reeks interviews met experts vanuit verschillende achtergronden. Er zijn in totaal 21 expertinterviews afgenomen. Deze interviews waren semigestructureerd, bedroegen tussen de 30 en 60 minuten en zijn door twee onderzoekers afgenomen. Van ieder interview is een kort verslag gemaakt. De expertinterviews zijn gebruikt voor het verdere verdiepen van de knelpuntanalyse en voor het verkrijgen van hoogwaardige feedback op onderzochte bestaande en mogelijke nieuwe voorzieningen. Bij het selecteren van experts is een representatieve selectie gemaakt van experts met de volgende achtergronden:

- Relevante internationale dienstverleners;
- Vertegenwoordigers van kleinschaligere websites en internetfora in Nederland;
- Beleidsadviseurs en wetgevers van het ministerie van Justitie en Veiligheid (“**JenV**”).
- Medewerkers bij de politie en openbaar ministerie;
- Rechters in eerste aanleg en hoger beroep;
- Toezichthouders;
- Advocaten en juridisch experts op het gebied van het procesrecht, het mediarecht en de Algemene verordening gegevensbescherming (“**AVG**”) ;
- Maatschappelijke organisaties die zich inzetten voor de rechten en vrijheden van Nederlandse burgers.[7]

In de derde fase zijn de onderzoeksresultaten geanalyseerd en getoetst door middel van twee expertworkshops. In de twee workshops zijn experts gevraagd feedback en commentaar te leveren op de onderzoeksresultaten. Hiermee zijn de voorlopige bevindingen uit de documentanalyses en de expertinterviews gevalideerd en aanvullende onderzoeksgegevens vergaard. De workshops vonden plaats op dinsdag 23 en donderdag 25 juni 2020 en duurden beide anderhalf uur. Bij beide workshops waren zeven experts met diverse achtergronden, net zoals bij de expertinterviews, aanwezig.[8] In de vierde fase is het concepttrapport en eindrapport opgesteld.

6 In aanvulling op de gestelde vragen is gekeken of met bijkomende variabelen over het LISS-panel aanvullende data toe te voegen waren aan de verkregen dataset. Specifiek waren we geïnteresseerd in het (sociaal) mediagebruik van de respondenten, alsook hun privacy percepties. Deze analyse leverde geen aanvullende resultaten op en daarom zijn deze bijkomende variabelen niet meegenomen in verdere analyses en de resultaten.

7 Zie annex iv-i.

8 Zie annex iv-ii.

2. De problematiek van onrechtmatige online content

De problematiek van onrechtmatige online content is geen eenduidig fenomeen. Om de problematiek inzichtelijk te maken zal, in de eerste plaats, afgebakend worden welke typen onrechtmatige content binnen de reikwijdte van dit onderzoek vallen. Dit onderzoek beperkt zich, met het oog op de doelstelling om de getroffene een betere voorziening voor de verwijdering van onrechtmatige online content te bieden, tot uitingen die mensen in hun persoon als zodanig treffen, zoals (onder andere) belediging, privacy-inbreuken of smaad. Deze afbakening sluit zaken als internetoplichting of inbreuken op een intellectueel eigendomsrecht (**"IE-recht"**) uit. Ten tweede wordt stilgestaan bij de wijze waarop onrechtmatige content zich online verspreidt: via internetdiensten. Bekeken wordt wat de rol is die deze diensten spelen en hoe het dienstenlandschap er uitziet. Ten derde wordt de omvang van onrechtmatige online content als maatschappelijk probleem in kaart gebracht, in samenhang met de bredere problematiek van toegang tot recht. Tot slot wordt een inschatting gemaakt van de maatschappelijke behoefte aan een procedure voor de verwijdering van onrechtmatige online content.

A. Soorten onrechtmatigheid

De problematiek van onrechtmatige uitingen op internet is een breed en reeds volwassen juridisch fenomeen. Vanuit juridisch en maatschappelijk oogpunt is sprake van een grote variëteit aan onrechtmatige content, waaronder bijvoorbeeld auteursrechtschending, schendingen van de privacy en reputatie van personen of bedrijven, misleidende commerciële informatie en materiaal van seksueel misbruik van minderjarigen. Niet alleen vanuit Nederland, maar ook op Europees en internationaal niveau doet men pogingen om deze problematiek aan te pakken. Naast het eerdergenoemde burgerinitiatief 'Internetpesters aangepakt' zijn er vele andere initiatieven om onrechtmatige content aan te pakken.[9] Zo heeft de Europese Commissie in 2018 een aanbeveling gedaan om illegale en anderszins onrechtmatige content op het internet te bestrijden.[10] Strafbare content zoals verheerlijking van terrorisme, de bestrijding van haatzaaiende content en kinderpornografie krijgen hierin aandacht, maar ook consumentenbescherming en de handhaving van intellectuele eigendom komen aan de orde. De aanbeveling van de Europese Commissie voorziet in verschillende manieren om illegale en anderszins onrechtmatige content sneller op te sporen en te verwijderen. Denk hierbij aan duidelijke Notice en Takedown-procedures, waarbij een internetdienst na kennisgeving hiervan onrechtmatige content dient te verwijderen, of aan betere waarborgen van de fundamentele rechten en nauwe samenwerking met de autoriteiten.[11]

Dit onderzoek beperkt zich, met het oog op de doelstelling om de getroffene een betere voorziening te bieden, tot onrechtmatige uitingen die mensen in hun persoon als zodanig treffen. Het gaat daarmee in het bijzonder om aantastingen van het privéleven, de eer en goede naam, en de onrechtmatige verwerkingen van persoonsgegevens. Het onderzoek richt zich niet op schendingen op het gebied van het consumentenrecht, oneerlijke handelspraktijken, en intellectuele eigendom (auteursrecht, merkenrecht, octrooien). Gezien het bestaan van een bijzonder strafrechtelijk kader voor materiaal van seksueel misbruik van minderjarigen, is er daarnaast voor gekozen ook dit onderwerp niet centraal mee te nemen in dit onderzoek.

9 *Kamerstukken II* 2018/19, 34602, 2.
10 Aanbeveling 1177 van de Europese Commissie (1 maart 2018), *Commission Recommendation on measures to effectively tackle illegal content online*.
11 Hier zal verder op ingegaan worden 3.a en 4.a.

Het onderzoek richt zich daarmee in essentie op onrechtmatige content die kan worden gekarakteriseerd als een aantasting van het recht op privéleven, zoals dit beschermd is in artikel 8 van het EVRM, alsmede artikel 7 van het Handvest van de Europese Unie (**"het Handvest"**). Tevens kan sprake zijn van een aantasting van het in artikel 8 van het Handvest opgenomen recht op de bescherming van persoonsgegevens.

Deze focus van het onderzoek op onrechtmatige online content betekent niet dat illegale of strafbare online content volledig buiten beschouwing gelaten kan worden. Hoewel illegale content en onrechtmatige content onder verschillende rechtsgebieden vallen, het strafrecht respectievelijk het civiele recht, is er wel overlap. Het civielrechtelijke begrip onrechtmatige daad is een breed begrip dat vele categorieën omvat, waaronder ook strafbare feiten. Een strafbaar feit zoals diefstal of smaad is vaak ook te kwalificeren als een onrechtmatige daad jegens het slachtoffer. Het begrip onrechtmatige daad is ruimer, er gelden andere eisen voor (bijvoorbeeld handelen in strijd met de maatschappelijke betamelijkheid of zorgvuldigheid) en de vaststelling is vaak laagdrempeliger. Deze samenhang maakt dat dit onderzoek ook de aanpak van strafbare of illegale online content beslaat. Wel wordt illegale online content primair besproken in de context van een civiele procedure en niet de strafrechtelijke opsporing en vervolging.

Het vaststellen of bij bepaalde content daadwerkelijk sprake is van onrechtmatigheid is, in het kader van de vormgeving van juridische mogelijkheden tot het verwijderen daarvan, een centraal element. De afweging is complex en nationale juridische kaders verschillen, hetgeen een spanningsveld oplevert tussen nationale juridische normen en de standaarden die door internationale dienstverleners worden gehanteerd. Voor content betreffende zogenaamde 'wraakporno', het publiceren van naaktfoto's zonder toestemming en duidelijk discriminerende of haatzaaiende berichten zal de vaststelling van onrechtmatigheid vaak makkelijker zijn dan wanneer het beledigingen of berichten van smaad en laster betreft. Het vaststellen van de mogelijke onrechtmatigheid bij de laatste categorie hangt sterk af van de inhoud en moet daarnaast afgewogen worden tegen het fundamentele recht van de vrijheid van meningsuiting (artikel 10 EVRM). De jurisprudentie van het Europese hof van de Rechten van de Mens biedt belangrijke randvoorwaarden voor deze beoordeling in het Nederlandse en Europese recht.

Ook binnen de focus van dit onderzoek – onrechtmatige uitingen die mensen in hun persoon als zodanig treffen – is er nog steeds sprake van een grote diversiteit aan denkbare onrechtmatige content. Het gaat om de volgende, niet uitputtende, mogelijkheden:

- Een eerste categorie betreft schadelijke inhoud die juridisch kan worden gekwalificeerd onder de klassieke onrechtmatige uitingen, waaronder in het bijzonder **bedreiging, belediging**, en/of valse beschuldigingen of verdachtmakingen (**smaad en laster**). Zoals hierboven vermeld is de daadwerkelijke onrechtmatigheid van dergelijke content in veel gevallen moeilijk vast te stellen zonder aanvullende gegevens. Er dient op basis van de bescherming van fundamentele rechten een afweging plaats te vinden tussen de rechten van de getroffenen en de rechten van de 'aanstichter' en relevante dienstverleners. Dit betreft vaak een afweging tussen de vrijheid van meningsuiting (artikel 10 EVRM) aan de kant van de aanstichter en het recht op privacy (artikel 8 EVRM) aan de kant van de getroffene.

- Het kan ook gaan om grove en onrechtmatige vormen van **pesten** of **stalking**, waarbij stalking in het Nederlandse recht is gedefinieerd als "het stelselmatig en opzettelijk inbreuk maken op de persoonlijke levenssfeer van een ander".[12] In de Nederlandse jurisprudentie is vastgesteld dat het gaat om de vraag of "het lastigvallen van een ander een zekere mate van indringendheid, duur en frequentie heeft".[13]

12 Art. 285 onderdeel b WvS.
13 HR 7 januari 2006, ECLI:NL:HR:2006:AU5787, r.o.. 3.6.

- Verder kan sprake zijn van aantastingen van het **recht op privacy**, zoals in het geval van de ongewilde publicatie van privé-informatie. Dergelijke schendingen kunnen onrechtmatig zijn op basis van het burgerlijk recht alsmede op basis van het gegevensbeschermingsrecht (AVG). De AVG stelt dat bij verwerking van persoonsgegevens de algemene zorgvuldigheidsnormen in artikel 5 AVG in acht genomen moeten worden. Zo is voor het verwerken van persoonsgegevens is altijd een grondslag nodig.[14] Bijvoorbeeld toestemming van de betrokkene of een gerechtvaardigd belang. In geval van ongewilde publicatie van privé-informatie zal deze toestemming vrijwel altijd ontbreken (of zijn ingetrokken). Getroffene hebben op grond van de AVG daarnaast rechten die er toe dienen controle uit te oefenen over de verwerking van hun persoonsgegevens. Zo kunnen zij hun persoonsgegevens inzien (12 jo 15 AVG), rectificatie aanvragen (16 AVG) en ook verwijdering van de gegevens aanvragen (17 AVG).

- **Onrechtmatig beeldmateriaal** (foto's en video's) kan bijzonder schadelijk zijn voor getroffenen en inbreuk maken op de privacy en eer en goede naam van betrokkenen. Een extreme variant is de verspreiding van wraakporno, bijvoorbeeld door een ex-partner, een variant die in de discussie over onrechtmatige inhoud op internet een belangrijke rol speelt. Uit een Nederlands onderzoek van EenVandaag betreffende 'sexting' blijkt dat van de 1429 ondervraagde jongeren 814 aangaven directe of indirecte ervaring te hebben gehad met de omloop van seksueel beeldmateriaal, 6% daarvan had wel eens een naaktfoto van iemand anders gemaakt en 28% van zichzelf. Van de laatste groep heeft 87% wel eens de naaktfoto of -video naar iemand anders gestuurd. 71% vertrouwde erop dat de naaktfoto of -video niet zou worden doorgestuurd naar 'iemand waarvoor deze niet bedoeld is'.[15] Hoewel uit dit onderzoek blijkt dat toch meer dan de helft vertrouwen heeft in de ontvanger van het seksueel beeldmateriaal, landen er nog altijd veel foto's en video's op het internet, die zo bekend worden gemaakt aan internetgebruikers voor wie dat niet de bedoeling was.
  Door een snelle technologische ontwikkeling blijft het niet alleen bij het lekken van 'normale' naakfoto's en -video's zonder toestemming. Zo heeft het fenomeen 'faceswap porn' zijn weg naar het internet gevonden. De nieuwe technologie in 'faceswap porn' maakt het mogelijk dat enkel een foto van iemands gezicht voldoende kan zijn om het te laten lijken alsof iemand meespeelt in een pornofilm. Dit soort video's staan bekend als 'deepfakes'. Door middel van geavanceerde data-analyse wordt het gezicht van een persoon, in veel gevallen betreft dit beroemdheden, op het gezicht van een pornoster geplakt.[16] Het verschil is vaak bijna niet op te merken. In Nederland is om deze problematiek in het algemeen aan te pakken op 1 januari 2020 de nieuwe wet over wraakporno in werking getreden. Deze nieuwe wetgeving stelt het maken, bezitten, verspreiden of openbaar maken van seksueel beeldmateriaal, zonder toestemming en met de kennis dat dit nadelig kan zijn voor de andere persoon, strafbaar.[17]
  Een ander recht dat de rechten van personen met betrekking tot beeldmateriaal beschermt, is het portretrecht, opgenomen in de Auteurswet ("**Aw**"), met name artikel 19, 20 en 21. Er moet een onderscheid gemaakt worden tussen een portret gemaakt in opdracht (artikel 19 en 20 Aw) en portretten niet in opdracht vervaardigd (21 Aw). Een portret in opdracht mag niet zonder toestemming openbaar worden gemaakt, maar wel worden verveelvoudigd door de geportretteerde. Als het portret niet in opdracht is gemaakt moet via een belangenafweging worden overwogen of de foto gepubliceerd mag worden. De publicatie van een portret is ongeoorloofd wanneer de geportretteerde een redelijk belang heeft om zich tegen de openbaarmaking te verzetten. Net zoals in artikel 8 en 10 EVRM wordt er dus een afweging gemaakt tussen

14 Art. 6 AVG.
15 JijVandaag 2017.
16 Elis 2018.
17 Rijksoverheid publicatie, 'Wraakporno', https://www.rijksoverheid.nl/onderwerpen/seksuele-misdrijven/wraakporno.

de schending van de eer en goede naam en de vrijheid van meningsuiting. Een redelijk belang kan zien op privacy belangen, maar ook op commerciële belangen.[18]

- Gerelateerd, maar te onderscheiden van de publicatie van persoonsgegevens (waarvan de feitelijke juistheid op zich niet wordt betwist), kan er sprake zijn van de **publicatie van onjuiste of verouderde gegevens**. Dergelijke publicaties kwalificeren onder voorwaarden ook als onrechtmatige uiting onder het strafrecht (bv. belediging). Zoals eerder opgemerkt hebben de betrokkenen op grond van de AVG een aantal rechten om hun persoonsgegevens (of onjuiste/verouderde gegevens) te beheren.[19] Met betrekking tot het veranderen van verouderde of onjuiste gegevens bestaat het recht op rectificatie. Dit recht geldt alleen voor de eigen gegevens en dan doorgaans alleen voor gegevens die objectief kunnen worden vastgesteld. Meningen van anderen komen voor alsnog niet in aanmerking voor het correctierecht. Wel kan eventueel op grond van artikel 18 AVG een verwerkingsrestrictie kunnen worden verzocht.

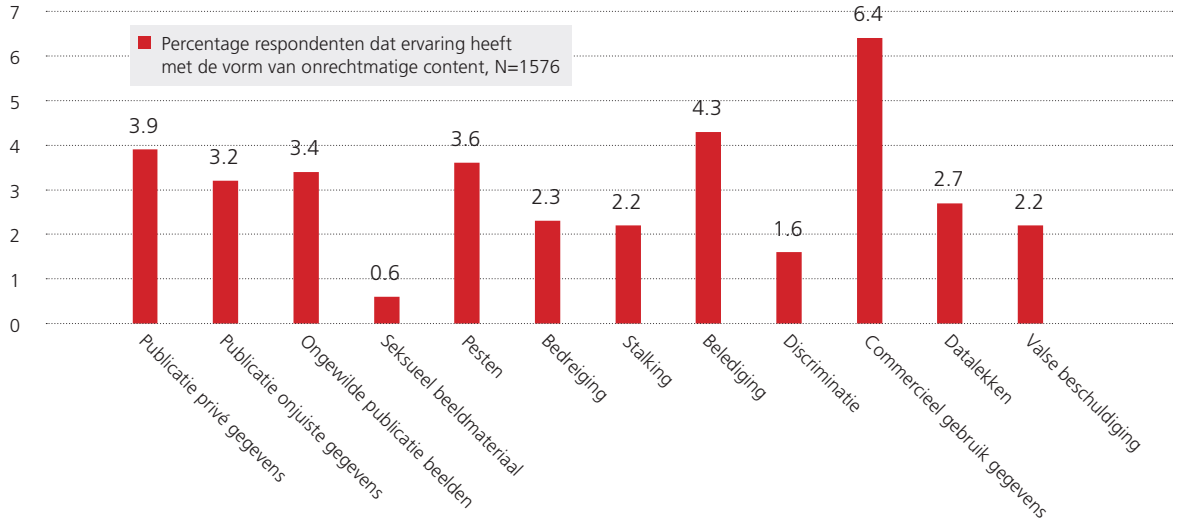
- Een nieuw fenomeen dat samenhangt met de risico's van het op grote schaal verzamelen en gebruiken van persoonsgegevens door organisaties is de mogelijkheid van **datalekken**. Dergelijke datalekken kunnen aanzienlijke schadelijke gevolgen met zich meebrengen voor de betrokkenen. Ter bescherming van de persoonsgegevens moet de natuurlijke persoon, rechtspersoon of overheidsinstantie die het doel van en de middelen voor de verwerking vaststelt, de zogenaamde verwerkingsverantwoordelijke, passende technische en organisatorische maatregelen nemen.[20] Maatregelen zoals het pseudonimiseren van persoonsgegevens kunnen de risicovolle gevolgen die verbonden zijn aan een datalek verkleinen. Daarnaast is voor de aanpak van een datalek een speciale meldplicht opgenomen in de AVG waardoor de verwerkingsverantwoordelijke de inbreuk zonder onredelijke vertraging aan de toezichthouder moet melden.[21] Wanneer de inbreuk een hoog risico oplevert voor de rechten en vrijheden van de betrokkenen moet de verwerkingsverantwoordelijke het datalek ook melden aan degenen wiens gegevens het betreft.[22] De meldplicht geldt in Nederland sinds 2016. Elk half jaar doet de AP onderzoek naar het aantal gemelde datalekken. In de eerste helft van 2019 waren dit 11.906 meldingen. De AP verwacht een stijging op jaarbasis van 14% in meldingen (het betreft het jaar 2019 tegenover 2018).[23] In 2016 verwachtte de wetgever bij het opzetten van de wetgeving omtrent de meldplicht 66.000 meldingen per jaar binnen te krijgen[24]. Op het moment wordt dit getal nog niet gehaald.

- Een laatste vorm van onrechtmatige content die mensen in hun persoon als zodanig kan treffen is inhoud of communicatie die kwalificeert als onrechtmatige **discriminatie** en het **aanzetten tot haat**.[25] In extreme gevallen van aanzetten tot haat, oftewel 'hate speech', is de betreffende

  content niet beschermd door de uitingsvrijheid. Volgens artikel 17 EVRM mag geen enkel fundamenteel recht gebruikt worden om andere fundamentele rechten teniet te doen.

18 HR 14 juni 2013, ECLI:NL:HR:2013:CA2788.
19 Hfst 3 AVG.
20 Art. 32 AVG.
21 Art. 33 AVG.
22 Art. 34 AVG.
23 Autoriteit Persoonsgegevens rapport 2019.
24 *Kamerstukken II* 2013/14, 33662, 6, p. 30-31
25 Stokkom 2007.

Uit de uitgevoerde survey blijkt dat van de 1576 ondervraagde personen, 240 (15%) personen direct of indirect (iemand in de omgeving heeft een ervaring met schadelijke inhoud gehad) ervaring hebben gehad met de bovenstaande vormen van schadelijke content. Bij de vraagstelling van deze survey is nadrukkelijk gekozen om de vraag of de content daadwerkelijk onrechtmatig was, buiten beschouwing te laten, aangezien deze vraag niet zonder de juiste juridische expertise beantwoord kan worden.



Figuur 1: **Ervaring met vormen onrechtmatige content**

Uit de bovenstaande figuur 1 blijkt dat de categorie waarmee de meeste mensen aangeven ervaring te hebben, het commercieel gebruik van informatie zonder toestemming (6,4%) is. De (schadelijke) verspreiding van seksueel beeldmateriaal wordt percentueel het minst vaak ervaren (0,6%). De resultaten laten duidelijk zien dat er over de hele linie van onderzochte problematiek ervaring bestaat onder de Nederlandse bevolking.

B. Type internetdienst

Het type internetdienst kan bepalend zijn voor de wijze waarop, en de vraag of, onrechtmatige content verwijderd kan worden. Dit komt zowel door de verschillende juridische regimes waar een specifieke dienst onder kan vallen als de wisselende technische mogelijkheden die een dienst heeft om bepaalde content daadwerkelijk te verwijderen. Ten slotte is voor een goed begrip van de wijze waarop internetdiensten met onrechtmatige informatie omgaan, ook hun bedrijfsmodel van belang.[26]

Er zijn zeer veel verschillende typen internetdiensten waar onrechtmatige online content een rol kan spelen. Gedacht moet worden aan de grote sociale media platforms zoals Facebook en Twitter, zoekmachines zoals Google, Startpage en Bing, zelfstandige websites en videoplatforms en apps zoals YouTube, Instagram en TikTok. Het omvat ook de internetdiensten waarbij het gaat om informatie of communicatie met een privékarakter zoals WhatsApp of *cloud storage* diensten waar bestanden opgeslagen kunnen worden. Kenmerkend voor het type internetdiensten dat in dit onderzoek relevant zijn, is deze diensten verschillende internetgebruikers in staat stellen met elkaar te communiceren of informatie uit te wisselen.[27]

26 Voor een discussie, zie Hoboken e.a. 2018.
27 Lodder, Schimmel & van der Winkel 2016.

Vanuit juridisch perspectief zijn twee verschillende regimes bepalend voor de vraag naar de verantwoordelijkheid die een internetdienst heeft ten aanzien van de door zijn gebruikers geplaatste content. Gezien de wettelijke beperkingen van aansprakelijkheid waarop zij een beroep kunnen doen zijn de volgende twee typen internetdiensten voor dit onderzoek van bijzonder belang:

1. *Mere conduit* diensten (doorgeefluik);
2. *Hosting providers* (host-diensten).

Mere conduit diensten bestaan uit het doorgeven van informatie tussen verschillende internetgebruikers zonder zelf controle over deze informatie uit te oefenen.[28] Het klassieke voorbeeld van dit type dienst zijn internet access providers die de aansluiting tot het internet verzorgen maar zelf in beginsel niets te maken hebben met wat hun klanten op het internet doen. Op deze manier functioneren deze diensten als 'doorgeefluik'. Naast de internet access providers zijn de zogenoemde *Over The Top* (**"OTT"**) communicatiediensten die directe communicatie tussen mensen via het internet faciliteren ook mere conduit diensten.[29] Hierbij kan gedacht worden aan diensten zoals WhatsApp, Signal of Gmail. Belangrijk is verder dat een deel van de mere conduit diensten veelal diensten zijn die privécommunicatie faciliteren, zoals de genoemde OTT-diensten. In dit rapport gebruiken we de term 'gesloten internet' om te verwijzen naar de eigenschap van deze diensten dat de informatie die uitgewisseld wordt over deze diensten niet openbaar toegankelijk is. Alleen de deelnemers aan een WhatsApp gesprek kunnen bijvoorbeeld zien wat er gezegd wordt.

Hiertegenover staan hosting providers. Hosting is juridisch gedefinieerd als het opslaan van de door een afnemer van de dienst verstrekte informatie.[30] Deze diensten stellen internetgebruikers hierdoor in staat informatie op het internet te plaatsen en omvat een breed scala aan verschillende internetdiensten. [31] Concreet moet gedacht worden aan diensten die iemand in staat stellen een eigen website te hebben, maar ook aan websites die mensen de mogelijkheid bieden zelf filmpjes, foto's of tekst te plaatsen. De grote sociale media platforms zoals Twitter, Facebook en TikTok zijn dus te kwalificeren als hosting providers, net als de internetfora of kleinere zelfstandige websites. Hosting diensten faciliteren de toegankelijkheid van voor iedereen beschikbare informatie, in dit rapport aangeduid als het 'open internet'.

Deze twee typen internetdiensten verschillen niet alleen van elkaar in karakter maar ook wat betreft het juridische regime waar ze onder vallen. Bij de mere conduit diensten zijn het passieve karakter van de internetdienst en het privékarakter van de communicatie tussen verschillende internetgebruikers het uitgangspunt van het juridisch kader. Artikel 12 van de e-Commerce richtlijn[32] sluit onder voorwaarden voor de internetdienst iedere aansprakelijkheid voor de doorgezonden informatie uit. De voorwaarden zijn dat de internetgebruiker het initiatief tot de doorgifte neemt en de ontvanger bepaalt en de internetdienst de doorgegeven informatie niet selecteert of wijzigt. Artikel 12 van de e-Commerce richtlijn is geïmplementeerd in artikel 196c lid 1 en 2 van boek 6 Burgerlijk Wetboek.

Daarnaast kunnen diensten die directe informatie-uitwisseling over het internet faciliteren, ook gekwalificeerd worden als elektronische communicatiediensten.[33] Het juridisch kader voor deze diensten is te vinden in het nog te implementeren Europees wetboek voor elektronische communicatie en de e-Privacyrichtlijn die in de Telecommunicatiewet geïmplementeerd is.[34] Bij elektronische communicatiediensten is de vertrouwelijkheid van de communicatie wettelijk vastgelegd wat ook consequenties heeft voor de

28 Art. 12 richtlijn 2000/31/EG.
29 Europese Commissie Publicatie 2009.
30 Art. 14 richtlijn 2000/31/EG.
31 Voor een overzicht van diensten zie Hoboken et al 2018.
32 Richtlijn 2000/31/EG.
33 Art. 2 richtlijn (EU) 2018/1972.
34 Richtlijn (EU) 2018/1972 en Richtlijn 2002/58/EG.

mogelijkheden van een dienst om onrechtmatige informatie te verwijderen.[35] De diensten hebben in de regel zelf geen toegang tot de communicatie en kunnen dus ook moeilijker onrechtmatige informatie verwijderen.

Het juridisch kader van toepassing op hosting providers creëert andere verantwoordelijkheden. Het doel achter dit juridische regime is om enerzijds elektronische handel en online activiteit te stimuleren door rechtszekerheid te geven aan hosting providers en hun aansprakelijkheid voor het handelen van

gebruikers. Anderzijds streeft dit regime ernaar onrechtmatige online content zo veel mogelijk tegen te houden door bepaalde verantwoordelijkheden bij hosting providers te leggen.[36] De belangrijkste normering voor dit type diensten is te vinden in de e-Commerce richtlijn. Relevant voor de verwijdering van onrechtmatige online content is de beperkte aansprakelijkheid voor onrechtmatige content in deze richtlijn.[37] Deze beperkte aansprakelijkheid geldt, kort gezegd, alleen wanneer de dienst geen kennis heeft van de onrechtmatige content. Het gevolg hiervan is dat het in het eigen belang van deze internetdiensten is om onrechtmatige informatie te verwijderen wanneer zij hiervan op de hoogte worden gebracht.[38] Relevant is dus dat hosting providers door het juridische regime waar zij onder vallen in de e-Commerce richtlijn gemotiveerd zijn, wanneer zij daarop gewezen worden, onrechtmatige content te verwijderen. De door hosting providers gevolgde Notice and Takedown-procedures zijn hier een voortvloeisel van.[39]

De juridische kaders van toepassing op mere conduit diensten en de hosting providers hebben duidelijk verschillende doelen op het oog, wat zich ook vertaalt in verschillen in verantwoordelijkheden ten aanzien van onrechtmatige online content. Zo staan bij mere conduit diensten de passiviteit van de dienst en het privékarakter en de vertrouwelijkheid van de communicatie centraal. Dit staat in contrast tot de hosting providers, waar het doel veelal juist is om informatie openbaar te maken. Dit verschil in karakter van de communicatie is gespiegeld in de verantwoordelijkheid van de internetdienst. Waar op het 'open internet' de hosting providers onder omstandigheden aansprakelijk zijn voor onrechtmatige content en ook actief ingrijpen om deze te verwijderen via onder andere Notice and Takedown-procedures, zijn op het 'gesloten internet' de communicatiediensten juist verplicht de vertrouwelijkheid van de informatie te waarborgen en kunnen zij niet zomaar ingrijpen. Zo hebben hosting providers in de regel een Notice and Takedown-procedure die gebruikt kan worden door individuen om onrechtmatige content verwijderd te krijgen terwijl mere conduit of elektronische communicatiediensten deze in de regel niet hebben.[40]

Een speciaal juridisch regime geldt tenslotte voor internetdiensten die kwalificeren als audiovisuele mediadiensten. Het betreft hier diensten die gereguleerd worden door de Richtlijn audiovisuele mediadiensten,[41] geïmplementeerd in de Mediawet. Hierbij moet gedacht worden aan de videostreaming services die programma's aanbieden zoals Netflix maar ook de diensten die gebruikers in staat stellen zelf video's te uploaden zoals YouTube. Relevant voor dit onderzoek is dat dit type videoplatforms grotere verantwoordelijkheid hebben ten aanzien van schadelijke inhoud. Ze zijn in het bijzonder verplicht maatregelen te nemen om kinderen beter te beschermen tegen schadelijke content en om het algemene publiek te beschermen tegen tot haat aanzettende, terroristische of racistische content of beelden van seksueel misbruik van kinderen.[42]

35 Richtlijn 2002/58/EC.
36 Considerans 40 richtlijn 2000/31/EG.
37 Art. 12-15 richtlijn 2000/31/EG.
38 Zie par. 4.a.
39 Voor Notice and Takedown-procedure zie verder par. 4.a.
40 Wel staan mogelijk andere procedures open zoals een Kort Geding. Zie hoofdstuk 4.b.
41 Richtlijn 2010/13/EU zoals aangepast door Richtlijn (EU) 2018/1808.
42 Respectievelijk art. 28b lid 1 Richtlijn 2010/13/EU zoals aangepast door Richtlijn (EU) 2018/1808.

Naast het juridisch kader waar een internetdienst onder valt, zijn ook de technische mogelijkheden tot verwijdering van belang. Hierbij moeten twee zaken onderscheiden worden. Aan de ene kant is er het algemene probleem dat informatie die eenmaal openbaar gemaakt is, op internet vaak moeilijk volledig te verwijderen is vanwege het gemak waarmee kopieën kunnen worden gemaakt, alsmede het open en decentrale karakter van de publicatie van gegevens op internet. Aan de andere kant is er het specifiekere probleem dat in sommige gevallen door de technische inrichting verwijdering van informatie door een dienst niet mogelijk is. Dit kan zijn door specifieke encryptie methodes die als beveiligingsmaatregel door de dienst geïmplementeerd zijn. Hierbij moet gedacht worden aan de *end-to-end*-encryptie die veel OTT-diensten zoals WhatsApp of Signal bieden. Dit houdt in dat de communicatie tussen

individuen in een WhatsApp gesprek dusdanig versleuteld is dat het voor een derde partij, waaronder ook WhatsApp zelf, onmogelijk is de informatie te ontsleutelen.[43] Dit betekent dat het voor een dienst die dit soort encryptietechnieken hanteert technisch onmogelijk is toezicht op onrechtmatige content te houden of specifieke content te verwijderen.

De technische onmogelijkheid om bepaalde content te verwijderen kan ook direct gekoppeld zijn aan de structuur van de dienst zelf zoals het geval is bij blockchain[44] of andere decentraal georganiseerde diensten.[45] Blockchain technologie is kort gezegd een decentrale vorm van databank beheer, het gebruik waarvan extra uitdagingen op kan leveren voor gegevenswissing.[46]

Voor de wijze waarop internetdiensten omgaan met onrechtmatige content, moet ook de bedrijfsstructuur en het bedrijfsmodel van de dienst meegenomen worden. In de eerste plaats kan gedacht worden aan de omvang van een internetdienst en de capaciteiten die hem ter beschikking staan om adequaat om te gaan met onrechtmatige content. Er is veel kritiek op grote sociale media platforms zoals Facebook en YouTube voor het onvoldoende investeren in het zorgvuldig modereren van hun diensten. Tegelijkertijd zijn het juist deze bedrijven die de middelen hebben om deze problemen aan te pakken. De grote sociale media platforms beschikken over geavanceerde systemen om op enorme schaal geautomatiseerd content te kunnen detecteren en filteren die in strijd is met hun gebruiksvoorwaarden.[47] In aanvulling daarop hebben deze bedrijven duizenden mensen als *content moderator* in dienst om handmatig specifieke content te beoordelen.[48] Deze specifieke diensten zijn in staat dit soort maatregelen te nemen vanwege de sterke marktpositie die zij innemen. Deze diensten kunnen dergelijke geautomatiseerde systemen creëren op basis van de enorme hoeveelheid data die zij hebben van hun gebruikers. Kleinere internetdiensten missen de data om zelf dit soort systemen te bouwen en de middelen om zo een grote hoeveelheid content moderators in te huren.[49]

Vervolgens is ook het karakter van de dienst als onderdeel van zijn bedrijfsmodel van belang. Sommige internetdiensten profileren zich als vrijplaatsen waar anoniem informatie uitgewisseld kan worden terwijl anderen zich meer positioneren als een veilige internetomgeving met relatief strenge gebruiksvoorwaarden die ook bepaalde rechtmatige content verbieden. Het kan zo respectievelijk zowel tegen als juist in het eigen belang van een dienst te zijn om strengere grenzen te stellen en zich actief te bemoeien met de door hun gebruikers gecreëerde content.[50] Ook kunnen culturele verschillen een rol spelen bij de verwijdering van schadelijke of onrechtmatige content wanneer de dienst in het buitenland gevestigd is. Zo bleek uit de expertinterviews dat Amerikaanse partijen, indien zij tot de conclusie komen dat

43 Whatsapp FAQ, 'End-to-end versleuteling', https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/..
44 Zheng e.a. 2017.
45 Zie bijvoorbeeld: Heaven 2020.
46 R. Jurdak e.a. 2018.
47 De Streel e.a. 2020. Hieronder vallen ook de meeste categorieën van onrechtmatige content.
48 Balakrishnan 2017 en Levin 2017.
49 Gorwa, Binns en Katzenbach 2020.
50 Gillespie 2018.

bepaalde content is toegestaan op basis van hun gebruiksvoorwaarden, doorgaans slechts content na de afgifte van een gerechtelijk bevel willen verwijderen. Nederlandse partijen zijn in voorkomende gevallen ook in overleg met advocaten bereid content te verwijderen. Tenslotte kan de vestigingsplaats van een internetdienst ook bepalend zijn als dit betekent dat zij buiten de jurisdictie vallen en er nagenoeg geen juridische handhavingsmogelijkheden zijn.

In de voor dit onderzoek afgenomen survey is specifiek gevraagd op welke internetdiensten mensen de onrechtmatige content tegen zijn gekomen, om een beeld te krijgen waar deze problematiek zich in Nederland het meest voordoet. De respondenten konden meerdere antwoorden aanvinken. Uit de onderstaande tabel blijkt dat Nederlanders onrechtmatige online content het meest tegenkomen op sociale media platforms zoals Facebook, Twitter en Instagram (11%).

Type internetdienst		% N=1576
1.	Sociaal medium (Fb, Twitter, Instagram)	11%
2.	Snapchat, TikTok	1%
3.	Videodienst (YouTube, Twitch)	1,5%
4.	Direct messaging (Whatsapp, Fb Messenger)	4%
5.	Datingsite / app	1%
6.	Internetforum	2%
7.	Zoekmachine	4%
8.	Blog	1%
9.	Marktplaats, e-commerce	1,5%
10.	Anders	6%

Figuur 2

De verschillende typen internetdiensten die aan de respondenten voorgelegd zijn, kunnen ruwweg onderverdeeld worden in de hierboven besproken open internetdiensten en gesloten internetdiensten. Sociale media, apps zoals Snapchat en Tiktok, videodiensten, internetfora, zoekmachines, blogs en marktplaatsen horen bij het open internet. Direct messaging, datingapp en e-mail behoren daarentegen bij het gesloten internet. In een verdere analyse van de bovenstaande cijfers zijn de verschillende diensten onderverdeeld in deze twee categorieën open of gesloten internet. Uit deze analyse blijkt dat de meeste Nederlanders onrechtmatige content op het 'open internet' tegenkomen. In totaal 13,6% (n=215) van de Nederlandse bevolking is blijkens de survey onrechtmatige online content tegengekomen op open internetdiensten. Uit de survey bleek ook dat in totaal 15% (n=240) van de steekproef (in)direct ervaring heeft met onrechtmatige online content. Dit betekent dat het overgrote merendeel van de mensen die onrechtmatige content tegen zijn gekomen, deze op openbaar toegankelijke 'open internet' diensten troffen. Daartegenover staat dat 6,7% (n=105) van de Nederlanders onrechtmatige online content tegenkwam op gesloten internetdiensten. Hieruit volgt dat een deel van de mensen die (in)direct ervaring hebben met onrechtmatige online content deze is tegengekomen op verschillende diensten die zowel onder de noemer open als gesloten internet kunnen vallen.

Het type internetdienst waar specifieke onrechtmatige content voorkomt, is, zo volgt uit het voorgaande, zeer bepalend voor de mogelijkheden tot verwijdering. Zo maakt het juridische regime waar de dienst onder valt, uit voor diens aansprakelijkheid. Daarnaast is het voor de vraag of er een Notice and Take-down-procedure wordt aangeboden bepalend of het technisch mogelijk is content te verwijderen. Ten slotte hangt de houding en handhavingsmodelijkheden van een dienst af van het bedrijfsmodel.

C. Omvang maatschappelijk probleem

Uit de expertinterviews en -workshops volgt duidelijk dat onrechtmatige online content die mensen in de persoon raakt, breed gezien wordt als een maatschappelijk probleem. Dit komt voornamelijk door het type onrechtmatige uitingen – het persoonlijke en daardoor ingrijpende karakter ervan – en doordat schadelijke content zeer snel en op grote schaal verspreid kan worden op het internet. Ook het burger-

initiatief 'Internetpesters aangepakt' laat zien dat dit type onrechtmatige online content als maatschappelijk probleem wordt ervaren.[51]

Mede om een beter beeld te krijgen van de omvang van het maatschappelijk probleem is de survey afgenomen. Hieruit blijkt dat 15% van de Nederlandse bevolking (in)direct ervaring heeft met schadelijke online content. Deze groep bestaat uit 14% die directe ervaring heeft met schadelijke informatie op het internet en een grotendeels overlappende 10% die indirect, via een lid van zijn of haar huishouden, ervaring heeft met schadelijke informatie op het internet. Ten opzichte van de gehele responsgroep bevat deze groep die aangeeft ervaring te hebben (15%) relatief meer mannen (61% versus 46 %) en meer hoger opgeleiden (19% versus 12,3 %).

Op de vraag welk type schadelijke online content Nederlanders als het grootste maatschappelijk probleem zien, worden de volgende typen het meest op nummer één gezet: ongewilde publicatie van privégegevens (25% op #1), seksueel beeldmateriaal (22% op #1) en video's die inbreuk maken op de privacy (10,2% op #1). Ook bedreiging wordt als een probleem ervaren (10,1% op #1).[52]

De survey biedt een duidelijke indicatie van de omvang en ervaring van het maatschappelijk probleem. Wel blijft het moeilijk een volledig beeld te krijgen van hoe vaak mensen in Nederland te maken krijgen met bepaalde typen onrechtmatige content. Hier ontbreekt overkoepelend onderzoek naar. Wat wel beschikbaar is, zijn cijfers van verschillende maatschappelijke organisaties die zich inzetten voor een specifieke vorm van onrechtmatige online content, zoals bijvoorbeeld discriminatie, aanzetten tot haat of wraakporno. Zo heeft het Meldpunt internetdiscriminatie ("**MiND**") in 2019 692 officiële meldingen ontvangen van online discriminatie.[53] In 2017 hebben Rutgers en Soa Aids Nederland tezamen met de GDD en het RIVM een grootschalig onderzoek uitgevoerd naar de seksuele gezondheid van jongeren onder de 25 jaar. Daaruit bleek dat één op de acht jongeren wel eens naaktfoto's verzonden heeft.[54] Parallel hieraan blijkt, uit het jaarverslag van 2019, dat de stichting Help Wanted! 2400 adviesvragen heeft ontvangen van jongeren onder de 26 jaar over online seksueel geweld. Bijna 40% van deze vragen ging over bedreiging of chantage met seksueel expliciet beeldmateriaal.[55] Hoewel geen exacte cijfers bekend zijn over de hoe vaak privacy schendingen voorkomen en schendingen van het gegevensbeschermingsrecht online, ontving de AP in 2019 in totaal 27.854 klachten over vermeende onrechtmatige verwerking van persoonsgegevens.[56] Ten slotte blijkt uit een onderzoek van het Centraal Bureau voor de Statistiek ("**CBS**") dat ruim 5% van de jongeren van 12 tot 25 jaar ervaring heeft met online pesten.[57]

De problematiek rond onrechtmatige online content die mensen in hun persoon raken, komt ook veelvuldig in de media. Vanuit de media komen er signalen dat slachtoffers van bijvoorbeeld naaktchantage uit schaamte geen aangifte durven te doen.[58] En is een filmpje eenmaal is gemaakt en verspreid, dan nog

51 Zie *Kamerstukken II* 2018/19, 34602, 2.
52 Zie annex vi.
53 MIND nieuwsbericht, 'Landelijk rapport discriminatiecijfers 2019 gepubliceerd', https://www.mindnederland.nl/actueel.
54 De Graaf e.a, Rutgers & Soa Aids Nederland 2019.
55 Zie EOKM jaarverslagen https://www.eokm.nl/kennisbank/eokm-jaarverslagen/.
56 Autoriteit Persoonsgegevens jaarverslag 2019.
57 Centraal Bureau voor de Statistiek 2019.
58 Runhaar 2019.

lukt het politie en justitie lang niet altijd om de dader op te sporen, laat staan om die te vervolgen.[59] Ook zijn er voorbeelden van mensen die naaktfoto's naar buiten brengen met de intentie iemand te schande te zetten.[60]

Ook internationaal wordt onderzoek gedaan naar de omvang van dit probleem. Zo is er sociaalwetenschappelijk onderzoek naar hoe vaak het delen van niet-consensuele beelden van seksuele aard voorkomt, zoals in Spanje, waar Gámez-Guadix et al. de prevalentie van sexting en strafbaar online seksueel gedrag onder Spaanse volwassenen hebben onderzocht.[61] In de VS hebben Garcia et al. onderzocht hoe vaak het verzenden, ontvangen en delen van seksuele beelden voorkomt.[62] Verder is er ook sociaalwetenschappelijk onderzoek naar de schade die gepaard gaat met de verspreiding van bepaalde niet-consensuele beelden.[63] In Ierland heeft Women's Aid onderzoek gedaan naar online misbruik en stalking, waarbij 41% van de misbruikte vrouwen te maken krijgt met tracking of intimidatie via elektronische middelen.[64] Women's Aid heeft een studie gepubliceerd over online pesterijen en schadelijke communicatie, waarin gegevens en statistieken over cyberstalking, pesterijen en niet-consensuele onthulling van privé, seksueel expliciete beelden zijn opgenomen.[65]

Vervolgens is het ook van belang kort in te gaan op waar de schade bij onrechtmatige online content die mensen in de persoon raken, daadwerkelijk uit bestaat. De omvang van het maatschappelijk probleem is niet alleen afhankelijk van hoe veelvoorkomend dit soort onrechtmatige content is, maar ook van hoe groot de impact op het individu is. Het valt buiten de scope van het onderzoek dit volledig in kaart te brengen. Het is echter wel van belang een beeld te verkrijgen van de impact die deze onrechtmatige online content kan hebben op een persoon. In juridische zin valt de impact te typeren als een inbreuk op iemands recht op privéleven (artikel 8 EVRM) en duidelijk is dat de schaal en snelheid van verspreiding die mogelijk is door het internet, deze persoonlijke schade vergroot. Los van deze algemene typering is de daadwerkelijke schade enorm divers en afhankelijk van het type onrechtmatige content en de persoonlijke omstandigheden van de persoon in kwestie. Om een indicatie te geven kan gedacht worden aan geestelijke of emotionele schade door schaamte, schade aan de reputatie, of angst, maar ook aan economische schade zoals verlies van inkomsten. In het voorgaande is al stilgestaan bij de verschillende vormen van onrechtmatige content,[66] hier wordt kort ingegaan op een aantal persoonlijke omstandigheden die van invloed zijn op de schadelijkheid van de onrechtmatige content.

Een eerste belangrijke factor is gender. Zo blijkt bijvoorbeeld uit het eerder aangehaalde rapport van het CBS dat bij onrechtmatige content van seksuele aard overwegend vrouwen slachtoffer zijn.[67] Ook blijkt uit hetzelfde onderzoek dat meisjes in de leeftijd van 12-18 jaar bijna twee keer zo veel last hebben van online roddelen, pesten, stalken of bedreiging dan jongens in dezelfde leeftijd.[68] Het Bureau van de Europese Unie voor de grondrechten heeft ook een onderzoek naar cyberstalken uitgevoerd: 5 procent van de vrouwen heeft sinds de leeftijd van 15 jaar met cyberstalken te maken gehad, en 2 procent in de twaalf maanden voorafgaand aan het onderzoek, waarbij vooral jonge vrouwen kwetsbaar waren.[69]

59 Van der Ven 2019.
60 Jensma 2017.
61 Gámez-Guadix e.a. 2015, p. 145-154.
62 Garcia e.a. 2016, p. 428-435.
63 Henry & Powell 2015, p. 758-799.
64 Woman's Aid, 'Digital Abuse of Woman; https://www.womensaid.ie/assets/files/pdf/digital_abuse_of_women_information_guide.pdf.
65 Women's Aid 2019.
66 Zie 2.a.
67 Centraal Bureau voor de Statistiek 2019, p. 22.
68 Centraal Bureau voor de Statistiek 2019.
69 Women's Aid 2019, p. 3.

Een tweede relevante factor speelt in het bijzonder bij onrechtmatige content van seksuele aard. Schaamte of angst voor de reactie van de familie op de content kan enorme impact hebben op een individu. In het eerder aangehaalde rapport van Gámez-Guadix et al. staan de ernstige gevolgen van seksueel misbruik op basis van beeldmateriaal beschreven, waaronder slachtoffers die een diep isolement ervaren ten opzichte van vrienden, families en de samenleving als geheel. Een aanzienlijk aantal slachtoffers ondervindt een diepe 'sociale breuk' waarbij hun leven uiteenvalt tussen voor en na het misbruik. Wat de interactie met de politie betreft, hebben slachtoffers die met de politie en het strafrechtelijk systeem in zee gaan nog steeds te maken met passiviteit, desinteresse en inadequate reacties.[70] Een andere factor van belang is of de persoon in kwestie minderjarig is. Jongeren bevinden zich vaker in een kwetsbare positie en staan nog in een afhankelijkheidsrelatie tot hun ouders. Uit het CBS-rapport blijkt dat jongeren van 12 tot 25 jaar het vaakst slachtoffer zijn van digitale criminaliteit in de brede zin.[71]

Voor de impact van onrechtmatige online content kan ook de maatschappelijke positie van de getroffene van belang zijn. Zo kan online intimidatie van journalisten of politici niet alleen gevolgen hebben voor het persoonlijk leven van de betrokkene, maar ook een negatieve impact hebben op het maatschappelijk debat. Journalisten en politici kunnen zich minder geneigd voelen deel te nemen aan het maatschappelijk debat als gevolg van doorlopende onrechtmatige online content die hen in de persoon raakt.[72] Deze problematiek is ook veelvuldig onderwerp geweest van debat in Nederland, waar ook duidelijk naar voren kwam dat overwegend vrouwelijke journalisten en politici stelselmatig geconfronteerd worden met dit type intimiderende onrechtmatige online content.[73]

Ten slotte kan ook het behoren tot een minderheidsgroep bijdragen aan de schade die een persoon ondervindt. Uit het eerder genoemde jaarverslag van MiND blijkt dat 40% van de (gemelde) online discriminatie ziet op herkomst.[74] Eerder onderzoek naar de psychologische en fysieke schade van racisme en discriminatie is bevestigd in een recent onderzoek van Umar Ikram die concludeert dat etnische minderheden door discriminatie meer kans hebben op psychiatrische klachten en hart- en vaatziekten.[75] Er zijn maar beperkt cijfers beschikbaar over de omvang en impact van online discriminatie en racisme in Nederland.[76]

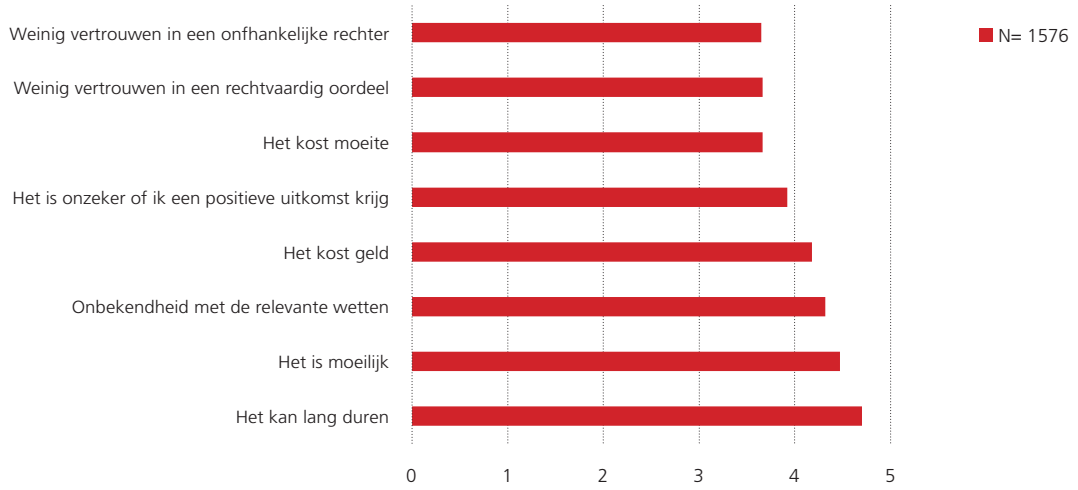
D. Toegang tot recht

De vraag naar een effectieve procedure om snel onrechtmatige online content te verwijderen, moet worden bezien tegen de achtergrond van de bredere problematiek van toegang tot recht. Toegang tot recht omvat zowel toegang tot rechtshulp als toegang tot de rechter. In deze paragraaf worden studies en rapporten besproken waaruit blijkt welke barrières er kunnen zijn voor mensen om hun recht te halen. Dat dergelijke barrières ook relevant zijn voor het onderhavige onderzoek volgt direct uit de surveyresultaten. Onderzocht is hoe verschillende mogelijke drempels mensen tegenhouden een juridische procedure te starten.

Blijkens de survey heeft slechts 1,4% van de Nederlandse bevolking, inclusief de groep die blijkens de survey (in)direct ervaring heeft met schadelijke content, overwogen om naar aanleiding daarvan juridische stappen te zetten. Aan de gehele steekproef is gevraagd in hoeverre een achttal omstandigheden

70 McGlynn 2019, p. 10.
71 Centraal Bureau voor de Statistiek 2019.
72 FRA 2016.
73 Oderkerken 2019; Buitenweg 2020; Barbier 2015; Zie 3.a.ii voor een verdere bespreking van online misbruik van vrouwelijke journalisten.
74 MIND nieuwsbericht, 'Landelijk rapport discriminatiecijfers 2019 gepubliceerd', https://www.mindnederland.nl/actueel.
75 Ikram 2016; Bouchallikht (OneWorld) 2020.
76 De meeste cijfers bouwen voort op wat geïnventariseerd wordt door MiND, zo ook de Discriminatiecijfers in 2019' waar alle officieel gerapporteerde cijfers over discriminatie in Nederland worden samengevoegd en geanalyseerd https://www.rijksoverheid.nl/documenten/rapporten/2020/04/28/discriminatiecijfers-in-2019.

een drempel zouden kunnen vormen voor het ondernemen van juridische stappen. Zoals blijkt uit de onderstaande figuur, vormen alle acht omstandigheden in bepaalde mate een belemmering.[77] Onbekendheid met de regelgeving, de moeilijkheid van het starten van een juridische procedure en de financiële kosten die daarmee gemoeid zijn, scoren tussen de 4,2 en 4,5 op een 7-punts Likertschaal, van helemaal niet tegenhouden tot erg tegenhouden. De lange doorlooptijd van een procedure wordt ervaren als de grootste drempel, met een score van 4,7. Andere overwegingen krijgen een score van 3,5-4: de moeite die een procedure kost, vertrouwen in de onpartijdigheid van de rechter, de onzekerheid van de uitkomst en de rechtvaardigheid van het uiteindelijke oordeel. De resultaten zijn in de onderstaande figuur weergegeven.



Figuur 3: **Belemmeringen voor ondernemen juridische stappen**

Wanneer alleen gekeken wordt naar de groep die daadwerkelijk ervaring heeft met onrechtmatige online content (15%), is dezelfde verdeling waar te nemen maar worden de drempels relatief als problematischer ervaren. De lengte van een juridische procedure springt er hier ook uit als belangrijke drempel, met een score van 5,1 op een schaal van 1-7.

Zoals ook uit de survey blijkt, beïnvloedt het type probleem waar mensen mee te maken krijgen of zij een gang naar de rechter overwegen. Er kan een verschil in type schadelijke content worden waargenomen, wanneer binnen de groep mensen die hiermee in aanraking zijn gekomen (15% van de Nederlandse bevolking) gekeken wordt naar de mensen die géén en de mensen die wél juridische stappen overwogen hebben. Dit is weergegeven in de onderstaande tabel. Bij deze tweede groep, dat wil zeggen de mensen die wél stappen hebben overwogen, is in de tweede en derde kolom te zien dat het type schadelijke content waar zij ervaring mee hebben, verschilt. De mensen die juridische stappen overwogen hebben, hebben vaker ervaring met ernstigere soorten uitingen: discriminatie, valse beschuldiging en bedreiging schieten omhoog. Wel moet benadrukt worden dat de groep mensen die juridische stappen hebben overwogen zeer klein is (n=13) , waardoor binnen deze groep geen echt betrouwbare analyses kunnen worden gemaakt.

77 De genoemde omstandigheden waren: het kost geld, het kost moeite, ik ben niet bekend met de relevante wetten en regels, het is moeilijk om een juridische procedure te beginnen, een juridisch proces kan lang duren, ik heb weinig vertrouwen dat er een onafhankelijke en onpartijdige rechter naar mijn zaak zal kijken, het is onzeker of ik een positieve uitkomst krijg en ik heb weinig vertrouwen dat er een rechtvaardig oordeel komt.

Er is steeds meer aandacht voor het belang van empirisch onderzoek naar behoeften van burgers en hun motieven om naar de rechter te gaan.[78] Die behoeften en motieven kunnen verschillen al naar gelang het type rechtszoekenden en het soort juridische problemen waarmee zij te maken krijgen. Maatregelen om de toegang tot recht te vergroten kunnen dus voor verschillende doelgroepen verschillende gevolgen hebben.[79]

Type schadelijke content	Gehele steekproef	Ervaring, geen stappen overwogen	Ervaring, wel stappen overwogen
	100%, N=1576	**13,6% n=219**	**1,4% n=13**
Commercieel gebruik informatie	6,4 %	29%	31%
Belediging	4,3%	15%	30%
Ongewilde publicatie informatie	3,9%	14%	15%
Pesten	3,6%	11%	23%
Foto's of video's (privacy inbreuk)	3,4%	14%	15%
Publicatie onjuiste gegevens	3,2%	13%	15%
Datalekken	2,7%	11%	23%
Bedreiging	2,3%	9%	46%
Valse beschuldigingen	2,2%	9%	38%
Stalking	2,2%	7%	15%
Discriminatie	1,6%	5%	31%
Seksueel beeldmateriaal	0,6%	2,7%	7,7%

Figuur 4

Een belangrijke bron van algemene informatie over verloop en afloop van juridische problemen van burgers is de Geschilbeslechtingsdelta 2014 van het WODC.[80] Deze biedt inzicht in de routes die Nederlandse burgers nemen om hun problemen op te lossen en drempels die zij ervaren om rechtshulp in te schakelen of een gerechtelijke procedure te starten. Het laat zien dat mensen tot op zekere hoogte een kosten-batenafweging maken: de ernst van het probleem, het daarmee gemoeide (financiële) belang en de verwachte opbrengst zijn van invloed op de stappen die zij al dan niet ondernemen. De beschikbaarheid van economische en sociaalpsychologische hulpbronnen speelt ook een rol.[81] Als belangrijkste redenen om af te zien van een gerechtelijke procedure noemden respondenten de verwachting dat het nergens toe zou leiden, dat het te veel tijd of moeite zou kosten en dat men er weinig of niets van af wist.[82] Dit sluit aan bij de surveyresultaten.

Uit onderzoek van het Europees Parlement blijkt dat EU-burgers in het algemeen kosten, (gebrek aan) toegang tot rechtshulpverlening, de lengte van procedures en de tenuitvoerlegging van rechterlijke uitspraken als belangrijke obstakels beschouwen.[83] Verder kan de complexiteit van wetgeving een barrière vormen.[84] Dat geldt temeer in grensoverschrijdende zaken, waar burgers te maken kunnen krijgen met het toepasselijke recht van een ander land. Op Europees niveau wordt daarom sterk ingezet op het wegnemen van dergelijke obstakels voor burgers om hun (Unie)rechten uit te oefenen enerzijds, en het

78 Er wordt veel internationaal onderzoek gedaan naar de toegang tot de rechter, rechtsbijstand en het effect van bepaalde online content, zoals het recente werk van Flynn en Hodgson 2017, waarin wordt onderzocht hoe de toegang tot de rechter wordt beïnvloed door de beperkingen op rechtsbijstand in het Verenigd Koninkrijk en Australië: Flynn en Hodgson 2017.
79 Zie bijvoorbeeld ook het rapport van Bauw 2019, p. 18 en Mein & De Meere 2018.
80 Het onderzoek wordt periodiek uitgevoerd (tot nu toe in 2003, 2009 en 2014). Een Geschilbeslechtingsdelta 2020 staat op het programma, maar is nog niet gepubliceerd.
81 Ter Voert & Klein Haarhuis 2014, p. 12.
82 Ibid, p. 98.
83 Europees Parlement 2017, p. 10-11.
84 FRA 2011, p. 38.

bevorderen van alternatieve en online geschillenbeslechting anderzijds. In hoofdstuk 3 zal de Europese context van de onderhavige problematiek nader worden besproken.

In de Geschilbeslechtingsdelta 2014 wordt verder gewezen op de invloed van digitalisering op het ontstaan en de aanpak van juridische problemen. Toegenomen participatie van de internettende burger kan aan de ene kant het risico op problemen vergroten, maar kan aan de andere kant ook bijdragen aan de oplossing daarvan.[85] Het rapport verwijst naar een quickscan van online voorzieningen waar burgers terecht kunnen voor zelfhulpmogelijkheden.[86] Verschillen in de mate van zelfredzaamheid van burgers kunnen

echter leiden tot ongelijke toegang tot het recht en een ongelijke positie.[87] Zo beschikken volgens onder zoek van het College voor de Rechten van de Mens vooral lager opgeleide ouderen (65+) over onvoldoende digitale vaardigheden om juridische informatie online te kunnen vinden,[88] ook al behoort Nederland volgens de Digital Economy and Society Index 2019 bij de top van de EU als het gaat om internetvaardigheden van mensen.[89] In een studie uit 2004 merkte de Raad voor Maatschappelijke Ontwikkeling al op dat het probleem niet zozeer ligt in het aanbod van informatie, maar in de lasten en een gebrek aan kennis/skills om van dat aanbod in een vroeg stadium effectief gebruik te kunnen maken. De ontoegankelijkheid die mensen ervaren wordt daarmee een reëel obstakel.[90] De bovengenoemde surveyresultaten bevestigen dat: onbekendheid met de regelgeving houdt mensen tegen om juridische stappen te ondernemen. Dit vraagt om een omvattende en proactieve benadering ten aanzien van toegang tot informatie, hulp en advies, waarbij mensen in een vroeg stadium geholpen worden.[91] Dat is een speerpunt van onder meer de Nationale Ombudsman, het Juridisch Loket en de Raad voor Rechtsbijstand. Hierin past bijvoorbeeld het initiatief 'Huizen van het Recht', waarin hulpverlenende instanties samenwerken om juridische en sociale problemen van burgers op te lossen.

Uit de survey en interviews volgt bovendien dat de tijd en kosten die met een juridische procedure gemoeid zijn in de praktijk een belangrijk obstakel zijn. Daarnaast kunnen hogere griffierechten rechtszoekenden – en dan vooral financieel minder draagkrachtige burgers – weghouden bij de rechter.[92] Uit de Geschilbeslechtingsdelta 2014 blijkt dat financiële kosten met name een drempel vormen voor het inschakelen van een advocaat.[93] Advocaten worden het meest geraadpleegd als juridisch deskundigen (in 2014 in 12% van de gevallen), aldus het WODC.[94] In 2011 is de competentiegrens voor de kantonrechter verhoogd, wat meebracht dat mensen in zaken met een belang tot EUR 25.000 in persoon (dus zonder advocaat) kunnen procederen. Dat heeft geleid tot ongeveer 20-25% meer rechtszaken over de periode 2011-2017.[95] Na de verhoging schakelde 24% van de rechtszoekenden nog steeds een advocaat in; slechts 1% startte een procedure zonder enige vorm van rechtsbijstand.[96] Wel verliezen doe-het-zelvers vaker dan partijen met een gemachtigde.[97] Er blijft dus behoefte bestaan aan professionele rechtshulp.

85 Ter Voert & Klein Haarhuis 2014, p. 41.
86 Zie ook Grootelaar 2014 en Van Veenen, 'Legal Tech Map' 2018.
87 Zie ook het rapport van Bauw 2019, p. 57 en Wetenschappelijke Raad voor het Regeringsbeleid 2017.
88 College voor de Rechten van de Mens 2018, p. 47. In dit licht oordeelde het Hof van Justitie in een uitspraak van 18 maart 2010, ECLI:EU:C:2010:146 (*Alassini/Telecom Italia*) dat als toegang alleen mogelijk is via elektronische middelen, de rechtsbescherming van bepaalde individuen in gevaar kan komen (r.o. 58).
89 Zie https://ec.europa.eu/digital-single-market/en/desi (area report Human capital/Digital skills).
90 Raad voor Maatschappelijke Ontwikkeling 2004, p. 31-32 met verwijzing naar Barendrecht & Kamminga 2004. Vgl. OECD 2016, p. 5.
91 Zie o.a. Macdonald 2012.
92 Rapport visitatie gerechten 2018, p. 15; zie ook College voor de Rechten van de Mens 2018, p. 52 en Ter Voert & Klein Haarhuis 2014, p. 53.
93 Ter Voert & Klein Haarhuis 2014, p. 190.
94 Ter Voert 2018, p. 2.
95 Eshuis & Geurts 2016, p. 47.
96 Ibid, p. 92.
97 Ibid, p. 95.

Tegelijkertijd wordt nagedacht over herziening van het stelsel van gesubsidieerde rechtsbijstand (procederen op toevoeging waarbij de overheid een deel van de kosten betaalt).[98] Daartegen zijn vanuit de advocatuur en de rechtspraak bezwaren geuit met het argument dat toegang tot recht geen luxeproduct mag worden en dat het niet aan de overheid is om te bepalen wie wanneer naar de rechter mag. De Raad voor de Rechtspraak heeft opgemerkt dat voor een groeiende groep rechtszoekenden de toegankelijkheid van de rechter onder druk staat.[99] Er zit bovendien een gat tussen de groep mensen die in aanmerking komt voor sociale rechtsbijstand omdat zij een beperkt inkomen hebben, en de groep mensen die geld heeft voor een advocaat. Een grote groep Nederlanders heeft geen rechtsbijstandsverzekering en ervaart daardoor een extra kostendrempel.[100]

De doorlooptijd van gerechtelijke procedures wordt besproken in hoofdstuk 3. De snelheid waarmee zaken worden afgerond, lijkt op zichzelf niet doorslaggevend te zijn; de ontevredenheid van rechtszoekenden daarover wordt eerder gevoed door gebrek aan transparantie over wat er gebeurt en de perceptie dat het proces niet effectief verloopt.[101] Ervaren procedurele rechtvaardigheid – de indruk die rechtszoekenden zich vormen van hoe eerlijk en rechtvaardig zij zich behandeld voelen tijdens de procedure – beïnvloedt het vertrouwen in (het gezag van) rechters en daarmee de bereidheid om naar de rechter te gaan.[102]

Expertinterviews die in het kader van dit onderzoek zijn afgenomen, bevestigen het beeld dat een gebrek aan toegankelijkheid van informatie en advies één van de belangrijkste obstakels voor toegang tot het recht is. En als men al juridische stappen overweegt of de gang naar de rechter weet te vinden, komen daar veel tijd en kosten bij kijken, wat een ontmoedigend of afschrikwekkend effect heeft. Dit speelt niet alleen bij de verwijdering van onrechtmatige online content, maar bij allerlei juridische problemen waarmee mensen zich geconfronteerd zien. Bij online content weegt de factor tijd echter extra zwaar: hoe langer iets online blijft staan, hoe groter de (potentiële) persoonlijke en/of maatschappelijke impact omdat het zich zeer snel kan verspreiden. Bovendien gaat het om specialistische problematiek, waardoor kosten en doorlooptijd vaak alleen maar toenemen.

E. Maatschappelijke behoefte

Om de maatschappelijke behoefte aan een nieuwe procedure voor de verwijdering van onrechtmatige online content goed in te kunnen schatten, moet ook een beeld verkregen worden van de praktische problemen waar mensen tegenaan lopen wanneer ze hiermee geconfronteerd worden. Hieronder zullen deze problemen uiteengezet worden. Hierbij wordt uitgegaan van het perspectief van de persoon die te maken krijgt met onrechtmatige online content die hem of haar persoonlijk raakt. Uiteindelijk zullen de verschillende relevante struikelblokken samengebracht worden in een aantal modelgevallen aan de hand waarvan geanalyseerd kan worden hoe de verschillende beschikbare procedures en mogelijke aanpassingen deze obstakels daadwerkelijk wegnemen.

Bij de verschillende te bespreken struikelblokken moet de potentiële schade die de onrechtmatige content aan een individu kan toebrengen, niet uit het oog verloren worden. Iemand wil specifieke content zo snel mogelijk verwijderd krijgen vanwege deze potentieel enorme omvang van de persoonlijke schade en de schaal en snelheid waarmee deze over het internet verspreid kan worden. Op basis van de expertinterviews en -workshops en de voorgaande analyse zijn de verschillende struikelblokken geïnventariseerd die

98 Rijksoverheid nieuwsbericht 2018, https://www.rijksoverheid.nl/actueel/nieuws/2018/11/09/rechtsbijstand-minder-procedures-meer-oplossingen
99 Bakker 2016.
100 Zie verder Van Gammeren-Zoeteweij e.a. 2017, tabel B.15.1.
101 Konings en Wolff Schoemaker 2019.
102 Zie ook Eshuis en Geurts 2016, p. 105 e.v.

iemand kan tegenkomen wanneer hij of zij geconfronteerd wordt met onrechtmatige content en wil dat deze verwijderd wordt. Hoewel deze struikelblokken niet in ieder opzicht strikt van elkaar gescheiden kunnen worden, zijn ze op te delen in zeven met elkaar samenhangende categorieën:

- Degene die de onrechtmatige uiting heeft gedaan kan **onbekend of onbereikbaar** zijn waardoor deze persoon moeilijk of niet (juridisch) aangesproken kan worden. Met onbekend wordt gedoeld op de situatie waarin de uitingen anoniem gedaan zijn en het of onmogelijk is, of een zeer langdurig en complex proces vergt om de identiteit te achterhalen. Onbereikbaar gaat over de situatie waarin iemand zich buiten de EU bevindt in een jurisdictie waar geen of slechts zeer moeizame juridische samenwerking mee is. Ook de internetdienst waar de uiting gedaan is, de website, het forum, of het platform, kan onbekend of onbereikbaar zijn. Dan valt bijvoorbeeld niet of slechts moeizaam te achterhalen welke entiteit achter een bepaalde website zit, of dan is de dienst gevestigd in een jurisdictie waardoor hij afgeschermd is van de Nederlandse rechtsmacht. Wanneer zowel degene die de uiting gedaan heeft als de relevante internetdienst niet aan te spreken zijn, is de enige mogelijkheid om via de rechter Nederlandse *internet access providers* te gelasten de gehele website te blokkeren voor hun gebruikers. Naast dit ingrijpende middel, dat in bijna alle gevallen niet proportioneel zal zijn, staan echter geen andere mogelijkheden open;

- Afhankelijk van het **type onrechtmatige uiting** dat iemand in de persoon raakt, kan het vaststellen van de onrechtmatigheid een uitgebreide en gespecialiseerde afweging vergen. Bij sommige typen schadelijke content is het redelijk eenvoudig, en onafhankelijk van de context, mogelijk om vast te stellen dat ze onrechtmatig zijn. Dit is bijvoorbeeld het geval bij beelden van seksueel misbruik van kinderen die in alle situaties strafbaar zijn, en in mindere mate bij wraakporno waar relatief makkelijk vast te stellen is dat de content zonder toestemming geplaatst is. Als de onrechtmatigheid eenvoudig vast te stellen is, zijn internetdiensten die de publicatie van de content faciliteren sneller geneigd mee te werken en zonder rechterlijk bevel de content te verwijderen. Aan het andere eind van het spectrum bevinden zich onrechtmatige uitingen zoals smaad of belediging waar de daadwerkelijke onrechtmatigheid moeilijk vast te stellen is, sterk afhangt van de context, en een diepgaandere analyse vereist om tot een oordeel te komen. Ook speelt de vrijheid van meningsuiting een belangrijkere rol bij dit type uitingen, nu de vaststelling van de onrechtmatigheid een afweging van grondrechten met zich meebrengt. Dit type uitingen vereist daarom in de regel een juridische procedure met een rechterlijke toets of uitspraak. Het tweede struikelblok ziet dus specifiek op hoeveel moeite het kost om de onrechtmatigheid juridisch vast te stellen;

- Het **type internetdienst** waar de onrechtmatige informatie op voorkomt kan ook bepalend zijn voor de mogelijkheden tot verwijdering.[103] Allereerst is van belang of er sprake is van publiek toegankelijke of privé communicatie nu de internetdienst daar respectievelijk vrij veel of slechts beperkt controle kan uitoefenen op specifieke content. Het type dienst alsmede de vraag of deze een zogenaamde Notice en Takedown procedure voert is dus bepalend voor de vraag of een internetdienst gemakkelijk specifieke content kan verwijderen.[104] Ten tweede is van belang of het voor de internetdienst, of een andere derde partij, technisch mogelijk is de content te verwijderen. Bij de toepassing van *end-to-end*-encryptie in communicatiediensten is dit bijvoorbeeld onmogelijk. Ook zijn, ten derde, het bedrijfsmodel van een dienst en culturele normen van

103 Zie par. 2.b.
104 De problematiek van (de vormgeving en juridische normering van) Notice en Takedown-procedures wordt in par. 4.a en 5.b uitgebreid besproken.

belang voor de vraag in hoeverre de dienst bereid is mee te werken en hoe gevoelig de dienst is voor maatschappelijke druk of bijvoorbeeld alleen op rechterlijk bevel content verwijdert;

- Ook wanneer specifieke onrechtmatige online content verwijderd wordt, kan het voorkomen dat een individu nog steeds schade ondervindt. Dit kan het geval zijn omdat de content na verwijdering steeds op andere plekken **terugkomt** of omdat de stappen die iemand onderneemt om de content te verwijderen tot meer bekendheid en dus meer schade leidt. Dit laatst staat bekend als het **'Streisand-effect'** en kan optreden bij het type persoonlijke en vaak gevoelige informatie zoals centraal staat in dit onderzoek en daarmee een extra drempel vormen voor de verwijdering;

- Het verwijderd krijgen van onrechtmatige online content zal in veel gevallen **specialistische juridische en feitelijke kennis** vergen. Dit geldt zowel voor de inschatting of een specifieke uiting onrechtmatig is en of er stappen tegen ondernomen kunnen worden, als ook voor de vraag welke entiteit of organisatie iemand het beste kan aanspreken om de content daadwerkelijk verwijderd te krijgen. Het is vaak onduidelijk tot wie iemand zich moet wenden (de internetdienst of degene die de uiting doet?) en wat de mogelijke routes tot verwijdering zijn. Waar het tweede struikelblok betrekking heeft op het vaststellen van de onrechtmatigheid, gaat dit struikelblok over het vinden van de juiste route tot verwijdering en het identificeren van de stappen die genomen moeten worden;

- Afhankelijk van de aard van de onrechtmatige content en de persoonlijke situatie van degene die met deze content geconfronteerd wordt, kan er sprake zijn van **schaamte** of **terughoudendheid** om stappen te ondernemen.[105] Dit kan bijvoorbeeld het geval zijn wanneer seksueel beeldmateriaal verspreid wordt en iemand vreest voor de reactie van de sociale omgeving. Ook bij jongeren en kinderen kan schaamte of angst voor de reactie van de omgeving een bepalende rol spelen bij het ondernemen van stappen, nu zij afhankelijk zijn van de ouders of andere volwassenen om sommige verdergaande stappen, zoals het starten van een procedure, te zetten;

- Ten slotte zijn de algemene obstakels die onder de noemer **toegang tot de rechter** gebracht kunnen worden mogelijk aanwezig.[106] De kosten verbonden aan een juridische procedure of advies, de complexiteit van de procedures, vertrouwen in de rechtspraak en de lange doorlooptijd kunnen mensen ervan weerhouden juridische stappen te zetten. Dit kan ook gekoppeld worden aan het specialistische karakter van de problematiek van onrechtmatige online content en de problemen die mensen in het algemeen ervaren om gemakkelijk betrouwbare juridische informatie te vinden.

De laatste vier struikelblokken (vereiste van specialistische kennis, terugkomende content, persoonlijke omstandigheden en toegang tot recht) spelen ongeacht de specifieke casus. Een centrale bevinding van dit onderzoek is dat deze problemen over de gehele breedte een rol spelen en ook breder dan alleen de problematiek van onrechtmatige online content. Dit betekent dat zij een eigen oplossing vereisen, zoals verbeterde informatievoorziening, voorlichting of de mogelijkheid anoniem melding te kunnen doen. Daarentegen verschuiven de procedurele mogelijkheden aanzienlijk al naar gelang de eerste drie struikelblokken: onbekendheid van degene die de uiting doet of de internetdienst, type internetdienst en type onrechtmatige content. De configuratie van deze punten in een specifieke casus is bepalend voor een goede kwalificatie van de juridische routes die iemand ter beschikking staan.

105 Zie par. 2.c.
106 Zie par. 2.d.

Om de verschillende combinaties van type onrechtmatigheid, type dienst en bekendheid van de dienst of degene die de uiting doet, beter te kunnen analyseren is het nuttig om voor dit onderzoek te werken met een viertal 'modelgevallen'. In deze modelgevallen wordt een specifieke casus uitgewerkt waar deze drie belangrijke struikelblokken in verschillende configuraties voorkomen. De casussen zijn mede ontwikkeld op basis van de bevindingen in de expertinterviews en -workshops. Aan de hand van de modelgevallen kan bij de latere analyse in hoofdstuk 5 de heterogeniteit van de problematiek geïllustreerd worden en zichtbaar worden gemaakt in hoeverre de verschillende bestaande en mogelijke nieuwe routes daadwerkelijk een oplossing bieden voor mensen die geconfronteerd worden met onrechtmatige content op internet.

- **Modelgeval 1: Belediging op Twitter**
  Iemand wordt geconfronteerd met een bericht op Twitter waarbij hij beledigd wordt. Onder omstandigheden is belediging een onrechtmatige uiting die iemand in de persoon raakt. Of er daadwerkelijk sprake is van onrechtmatige belediging is echter moeilijk vast te stellen en vergt een uitgebreide afweging van alle contextuele factoren. In deze situatie is de onrechtmatigheid dus moeilijk vast te stellen. Twitter is één van de grotere sociale media platforms en is hier de internetdienst waarop de uiting gedaan is.

  In dit modelgeval is de onrechtmatigheid moeilijk vast te stellen maar is de internetdienst bekend en bereikbaar. Of degene die de uiting gedaan heeft bekend en bereikbaar is, is niet van invloed op de beschikbare juridische procedures. Wanneer Twitter niet bereid is de onrechtmatige uiting te verwijderen moet de getroffen persoon een formele juridische procedure starten om via een rechtelijk bevel Twitter te dwingen de uiting te verwijderen.

- **Modelgeval 2: Bedreiging op YouTube**
  Er wordt een serieuze bedreiging met een strafbaar feit zoals moord of zware mishandeling op YouTube geplaatst. Van dit type illegale content is de onrechtmatigheid relatief gemakkelijk vast te stellen. YouTube is één van de grootste sociale media platforms met vestigingen in de Europese Unie. In deze casus is dus de onrechtmatigheid relatief gemakkelijk vast te stellen en is de internetdienst bekend en bereikbaar. In veel gevallen waar de onrechtmatigheid gemakkelijk is vast te stellen, zal de internetdienst de content verwijderen indien de daarvoor ingerichte klachtenprocedures worden gevolgd. Wanneer dit niet gebeurt kan een juridische procedure gestart worden.

- **Modelgeval 3: Persoonsgegevens op zelfstandige website**
  Op een zelfstandige website (geen platform) worden persoonsgegevens gedeeld die herleidbaar zijn tot een bepaald persoon, bijvoorbeeld een journalist of publiek figuur. Wie er achter deze website zit is echter niet of zeer lastig te achterhalen en het bedrijf dat de website host geeft niet thuis of is buiten de EU gevestigd. De (mate van) onbekendheid of onbereikbaarheid van de dader en/of de internetdienst is een belangrijk obstakel in het verwijderd krijgen van de gegevens in kwestie, zowel in het voortraject (Notice and Takedown-procedure) als bij het opstarten van een civiele procedure. Ook kan iemand in deze casus aanlopen tegen de capaciteitsproblemen bij de politie en de AP. Afhankelijk van de ernst van de situatie valt het namelijk binnen de discretionaire bevoegdheid van de politie of de AP om te besluiten wel of niet de verschillende verregaande bevoegdheden in te zetten. Wanneer het bijvoorbeeld gaat om ernstig onrechtmatig materiaal met betrekking tot een publiek figuur, of zeer schadelijke content zoals seksueel beeldmateriaal van kinderen, zal de politie of de AP zijn gewicht achter de zaak zetten wat de kans op verwijdering aanzienlijk vergroot. De uitkomst van Modelgeval 3 verschilt dus aanzienlijk al naargelang de mate waarin de dienst aan te spreken is (buiten de EU gevestigd of volledig onbekend?) en de mate van prioriteit die instanties met bevoegdheden aan de zaak geven (aanzienlijke schade of een publiek figuur?).

- **Modelgeval 4: Naaktfoto's verspreid via WhatsApp**

  In deze situatie worden ongewenst naaktfoto's verspreid via WhatsApp. Net zoals in modelgeval 2 is het bewust schade toebrengen door het ongewenst verspreiden van naaktfoto's strafbaar en is de onrechtmatigheid relatief gemakkelijk vast te stellen. Echter, in deze situatie is WhatsApp de internetdienst en is het voor derden en de aanbieder van WhatsApp, Facebook, door de *end-to-end*-encryptie onmogelijk om de content te verwijderen. De internetdienst is bekend en bereikbaar, maar door de technische inrichting kan de content niet van buitenaf verwijderd worden. De enige mogelijkheid is om degenen die de onrechtmatige content verspreiden, juridisch aan te spreken in een civiele of strafrechtelijke procedure.

De hierboven beschreven struikelblokken en modelgevallen kunnen helpen om de effectiviteit van de verschillende mogelijke juridische routes tot verwijdering van onrechtmatige online content vanuit het perspectief van de betrokken persoon te beoordelen. Deze komen terug in de knelpuntenanalyse en beschrijving van mogelijke oplossingsrichtingen in hoofdstuk 5.

F. Conclusie

In dit hoofdstuk is onrechtmatige inhoud op internet als maatschappelijk probleem in kaart gebracht. Het gaat in dit onderzoek om onrechtmatige uitingen die mensen in hun persoon treffen. Dat is een brede categorie, met een grote variëteit aan soorten uitingen en schade die zij kunnen veroorzaken. Ook zijn er veel verschillende typen internetdiensten waarbij zulke uitingen een rol kunnen spelen. In het kader van het onderzoek is een survey uitgevoerd waaruit blijkt dat 15% van de Nederlandse bevolking (in)direct ervaring heeft met schadelijke online content. De ongewilde publicatie van privégegevens staat op de eerste plaats, gevolgd door seksueel beeldmateriaal, video's die inbreuk maken op de privacy en bedreiging. Mede door de schaal en snelheid van verspreiding op internet kan de persoonlijke impact groot zijn.

Een belangrijk facet van het probleem is toegang tot recht, dat zowel toegang tot de rechter als toegang tot juridische informatie, hulp en advies omvat. De survey laat zien dat mensen drempels ervaren om juridische stappen te zetten, in het bijzonder onbekendheid met de regelgeving, de moeilijkheid van het starten van een procedure, financiële kosten en doorlooptijd. Bij online content weegt de factor tijd extra zwaar. Op basis van de expertinterviews en -workshops zijn vervolgens de belangrijkste struikelblokken geïdentificeerd. Deze zullen worden meegenomen in de knelpuntenanalyse.

3. Grondrechtelijk kader en internationale context

De verschillende procedurele routes om onrechtmatige online content te verwijderen staan niet op zichzelf, maar moeten worden bezien in een bredere grondrechtelijke en internationale context. Het toepasselijke grondrechtelijk kader bestaat uit minimumnormen waar alle verschillende procedurele routes, zo ook eventuele nieuwe procedures, aan moeten voldoen. De internationale context is vanuit verschillende perspectieven relevant. Zo kampen anderen landen ook met deze problematiek en heeft een aantal verschillende Europese lidstaten hun eigen oplossingen voor deze problematiek ontwikkeld. Daarnaast wordt er momenteel op EU-niveau gewerkt aan nieuwe wetgeving die direct raakt aan dit onderzoek.

A. Grondrechtelijke kader

Tijdens het overwegen van een mogelijke nieuwe regeling voor het aanvragen van een snelle verwijdering van onrechtmatige content moet, in het bijzonder, ook rekening worden gehouden met het kader van de grondrechten. Een aantal rechten, gewaarborgd door het EVRM, moet in het bijzonder in overweging worden genomen. In het bijzonder het recht op privéleven overeenkomstig artikel 8 EVRM, het recht op de vrijheid van meningsuiting overeenkomstig artikel 10 EVRM en het recht op een eerlijk proces overeenkomstig artikel 6 EVRM. Om de toepassing van deze grondrechten te begrijpen moeten we ons wenden tot de jurisprudentie van het Europees Hof voor de Rechten van de Mens ("**EHRM**").

i. Artikel 8 EVRM (Recht op privéleven)

Artikel 8 EVRM garandeert het recht op eerbiediging van het privéleven. Belangrijk voor dit onderzoek is dat het EHRM heeft bevestigd dat het recht op de bescherming van reputatie een afzonderlijk recht is dat, als onderdeel van het recht op de eerbiediging van het privéleven, wordt beschermd op grond van artikel 8 EVRM.[107] Om in aanmerking te komen voor de bescherming van artikel 8 moet de aantasting van de persoonlijke levenssfeer echter een relatief ernstig karakter hebben. Ook moet de aantasting plaatsvinden op een manier die schade toebrengt aan de persoonlijke genot van het recht op eerbiediging van het privéleven.[108] Zo werd het plaatsen van een foto op Instagram waarbij iemand werd beschreven als een "rapist bastard", door het EHRM als ernstig beschouwd en "capable of damaging the applicant's reputation" op grond van artikel 8 EVRM.[109] Verder heeft het EHRM met betrekking tot intieme beelden en video's ook bevestigd dat de publicatie van beelden en video's van een individu "participating in sexual acts" ongetwijfeld in strijd is met de rechten van een individu op grond van artikel 8, en een significante impact heeft op het privéleven van de getroffene.[110] Daarnaast heeft het EHRM ook de vernedering en de geleden schade als gevolg van de verspreiding van dergelijk materiaal erkend.[111]

Met betrekking tot de verplichting van de staat om de persoonlijke levenssfeer te beschermen, heeft het EHRM geoordeeld dat artikel 8 EVRM niet alleen vereist dat de staat zich onthoudt van inmenging in de persoonlijke levenssfeer, maar ook dat het positieve verplichtingen voor de staat met zich meebrengt om het effectieve genot van dit recht te waarborgen.[112] Deze positieve verplichtingen kunnen inhouden

107 EHRM 7 februari 2012 *Springer/Germany*, ECLI:NL:XX:2012:BW0603, r.o. 83.
108 EHRM 7 februari 2017 *Pihl/Sweden*, ECLI:CE:ECHR:2017:0207DEC007474214, r.o. 24.
109 EHRM 7 november 2017 *Egeill Einarsson/IJsland*, ECLI:CE:ECHR:2017:1107JUD002470315, r.o. 52.
110 EHRM 10 mei 2011 *Mosley/Verenigd Koninkrijk*, ECLI:CE:ECHR:2011:0510JUD004800908, r.o. 71.
111 Ibid., r.o. 71.
112 Ibid., r.o. 106.

dat de staat maatregelen dient te nemen "even in the sphere of the relations of individuals between themselves".[113] In dit verband heeft het EHRM een aantal belangrijke uitspraken gedaan over het soort maatregelen dat de staat moet nemen om het privéleven te beschermen. Het ziet op maatregelen zoals dwangbevelen om lasterlijke online inhoud te verwijderen, maatregelen om de identiteit van de persoon die een lasterlijke reclame online heeft geplaatst bekend te maken, maatregelen om een persoon te beschermen tegen de publicatie van intieme beelden en video's en de verplichtingen van de autoriteiten om maatregelen te nemen wanneer seksvideo's online worden geüpload.

Een toonaangevende uitspraak over deze positieve verplichtingen van de staat om het privéleven te beschermen is *K.U. tegen Finland*.[114] De zaak betrof een nepadvertentie die was geüpload naar een datingsite, met daarbij de foto, leeftijd en contactgegevens van een minderjarige. De vader van het kind vroeg de politie om de persoon die de advertentie had geplaatst, te identificeren en de politie verzocht een gerechtelijk bevel tegen een internetprovider om het IP-adres van degene die de content plaatst bekend te maken. De Finse rechter oordeelde echter dat de politie op grond van de Finse telecommunicatiewetgeving destijds geen recht had op het verkrijgen van telecommunicatiegegevens ter identificatie van het betrokken delict - "kwaadwillige misleiding". De minderjarige diende vervolgens een verzoek in bij het EHRM met het argument dat er sprake was van een schending van artikel 8 EVRM, aangezien er een inbreuk op de persoonlijke levenssfeer had plaatsgevonden en er geen effectief rechtsmiddel was om de identiteit van de persoon die een lasterlijke advertentie op het internet had geplaatst, bekend te maken. Van cruciaal belang is dat in deze zaak het EHRM unaniem een schending van artikel 8 EVRM heeft vastgesteld, door te stellen dat Finland heeft nagelaten de praktische en effectieve bescherming van het privéleven te bieden, zoals "effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement".[115]

Het EHRM heeft ook een belangrijk arrest gewezen over de onlineverspreiding van expliciete video's van een publieke figuur en over de vraag of de beschikbare nationale rechtsmiddelen op grond van artikel 8 van het EVRM toereikend waren. Het betreft de uitspraak *Mosley tegen het Verenigd Koninkrijk*, waarbij een publieke figuur met succes heeft geprocedeerd tegen dit soort online video's. Hoewel de klager voor de nationale rechter een schadevergoeding kreeg toegewezen, diende hij alsnog een verzoek in bij het EHRM. Hij beargumenteerde dat de rechtsmiddelen met betrekking tot artikel 8 ontoereikend waren en dat er een positieve verplichting bestond voor de staat om een verplichting tot voorafgaande kennisgeving in de wetgeving op te nemen, zodat particulieren voorafgaand aan de inbreukmakende publicatie van content een verzoek tot een bevel kunnen indienen.[116] Na dit onderzocht te hebben concludeerde het EHRM uiteindelijk dat artikel 8 geen juridisch bindende verplichting tot voorafgaande kennisgeving inhoudt en vond unaniem dat er geen sprake was van een schending van artikel 8 EVRM.

Het EHRM merkte op dat een persoon, die op de hoogte is van een hangende publicatie met betrekking tot zijn privéleven, het recht heeft deze publicatie te verhinderen door het aanvragen van een tussentijds bevel. Nu dit niet gebeurd was, wees het Hof erop dat er geen maatregelen waren genomen om artikel 8 te beschermen. Het Hof heeft ook gewezen op de beschikbaarheid van civiele procedures en voorlopige bevelen. Verdere bescherming werd geboden door het recht om verzamelde of onjuiste gegevens te laten vernietigen in de UK Data Protection Act.[117] Cruciaal is dat het Hof oordeelde dat er bij het opleggen van een verplichting tot voorafgaande kennisgeving nog een andere doorslaggevende factor speelt. Een dergelijke verplichting is slechts zo streng als de sancties die worden opgelegd voor het niet naleven van deze regel. Hoewel strafmaatregelen of strafrechtelijke sancties doeltreffend zouden kunnen zijn om de

113 EHRM 14 januari 2020 *Beizaras en Levickas/Litouwen*, ECLI:CE:ECHR:2020:0114JUD004128815, r.o. 110.
114 EHRM 2 december 2008 *K.U./Finland*, ECLI:CE:ECHR:2008:1202JUD000287202.
115 Ibid., r.o. 49.
116 Ibid., r.o. 79.
117 Ibid., r.o. 119.

naleving van de verplichting tot voorafgaande kennisgeving aan te moedigen, is het Hof van oordeel dat deze onverenigbaar dreigen te zijn met de vereisten van artikel 10 van het EVRM. Het Hof concludeerde dat bijzondere zorg moet worden betracht in het beoordelen van beperkingen die een vorm van censuur zouden kunnen opleveren. Het Hof is ervan overtuigd dat de dreiging met strafrechtelijke sancties of boetes een *chilling effect* zou hebben op de politieke berichtgeving en de onderzoeksjournalistiek, die beide een hoog niveau van bescherming in het kader van de Conventie genieten.[118]

Tot slot betreft het oordeel in *Khadija Ismayilova tegen Azerbeidzjan* een recente uitspraak over de publicatie van intieme video's online.[119] Verzoekster in de zaak kreeg intieme foto's en video's van zichzelf toegestuurd. Daarnaast werd zij gechanteerd dat als zij niet zou stoppen met haar baan als onderzoeksjournalist, deze foto's en video's via het internet verspreid zouden worden. Ismayilova diende een verzoek in bij het Europees Hof voor de Rechten van de Mens wegens schending van artikel 8 EVRM, waarbij zij de binnenlandse autoriteiten verweet geen effectief onderzoek in te stellen. Het EHRM oordeelde dat artikel 8 EVRM van toepassing was, aangezien het ging om een "serious, flagrant and extraordinarily intense invasion of her private life in the form of unauthorised filming of the most intimate aspects of her private life, which had taken place in the sanctity of her home, and subsequent public dissemination of those video images".[120]

Maar vervolgens verklaarde het Hof dat de "choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States' margin of appreciation".[121] Desalniettemin oordeelde het Hof na uitgebreid onderzoek dat er sprake was van een schending van artikel 8 EVRM. Het Hof verklaarde dat de autoriteiten niet hadden voldaan aan hun positieve verplichting om de adequate bescherming van het privéleven van verzoekster te waarborgen door een doeltreffend strafrechtelijk onderzoek in te stellen naar de zeer ernstige inbreuken op haar privéleven.[122] De bescherming is doeltreffend wanneer in het strafrechtelijk onderzoek effectieve maatregelen worden genomen zodat de daders van deze feiten te identificeren zijn en vervolgd kunnen worden.[123]

ii. Artikel 10 EVRM (Vrijheid van meningsuiting)

Uit het bovenstaande blijkt dat het soort onrechtmatige online content waar dit onderzoek zich op richt in de regel zal raken aan de bescherming van artikel 8 van het EVRM. Echter, bij elke nieuwe wettelijke regeling inzake snelle verwijdering van dergelijke inhoud moet ook rekening worden gehouden met het recht op de vrijheid van meningsuiting in artikel 10 EVRM. Het Hof heeft immers verklaard dat wanneer wordt beweerd dat bepaalde nieuwe maatregelen nodig zijn op grond van positieve verplichtingen uit hoofde van artikel 8, "regard must be had to the fair balance that has to be struck between the competing rights and interests arising under Article 8 and Article 10, rights which merit, in principle, equal respect".[124]

Het Hof heeft benadrukt dat bijzondere zorg moet worden besteed aan "restraints which might operate as a form of censorship prior to publication".[125] Zo oordeelde het Hof in de zaak *Mosley tegen het Verenigd Koninkrijk* dat de dreiging met strafrechtelijke sancties of boetes een *chilling effect* zou hebben

118 EHRM 10 mei 2011 *Mosley/Verenigd Koninkrijk*, ECLI:CE:ECHR:2011:0510JUD004800908, r.o. 129.
119 EHRM 10 oktober 2019 *Khadija Ismayilova/Azerbeidzjan*, ECLI:CE:ECHR:2019:0110JUD006528613.
120 Ibid., r.o. 115.
121 Ibid.
122 Ibid.
123 Ibid., r.o. 118.
124 EHRM 10 mei 2011 *Mosley/Verenigd Koninkrijk*, ECLI:CE:ECHR:2011:0510JUD004800908, r.o. 111.
125 Ibid., r.o. 129.

dat invloed heeft op de politieke verslaggeving en de onderzoeksjournalistiek, die beide een hoog niveau van bescherming uit hoofde van het Verdrag genieten.[126]

Het recht op de vrijheid van meningsuiting krachtens artikel 10 EVRM betekent echter niet dat er geen aanvullende maatregelen ter bescherming van het privéleven kunnen worden ingevoerd. Het Hof heeft benadrukt dat artikel 10 het opleggen van *prior restraints* aan de bekendmaking niet verbiedt, maar dat de gevaren die inherent zijn aan voorafgaande beperkingen van dien aard zijn dat zij de meest zorgvuldige beoordeling vereisen.[127] Van cruciaal belang is dat het Hof heeft geoordeeld dat voorafgaande beperkingen gemakkelijker te rechtvaardigen zijn in gevallen waarin geen dringende noodzaak tot onmiddellijke publicatie wordt aangetoond en waarin geen duidelijke bijdrage aan een debat van algemeen publiek belang wordt geleverd.[128]

Daarnaast omvat de vrijheid van meningsuiting in de kern niet alleen bescherming voor ideeën die wenselijk zijn, maar ook voor meningen die "offend, shock and disturb the State or any sector of the population".[129] Het in het geheel niet toelaten van beledigende en schokkende meningen zou de democratie van het land tenietdoen. Daarnaast zal het er bij de laatste categorie ook vanaf hangen wie de getroffen persoon in kwestie is. Het Europese Hof heeft namelijk in een smaad-zaak geconcludeerd dat publieke personen in hun hoedanigheid een zwaardere mate van beledigende meningen moeten accepteren.[130] Verder moet er een verschil gemaakt worden tussen feiten en waardeoordelen; feiten kunnen worden aangetoond, maar de 'waarheid' van een waardeoordeel is niet aan bewijs onderhevig. Echter, het Hof oordeelt dat waardeoordelen, hoewel de waarheid niet kan worden bewezen, binnen de sfeer van artikel 10 EVRM vallen.[131]

Als zodanig zou elke nieuwe bepaling die een snelle verwijdering van de inhoud mogelijk maakt, ervoor moeten zorgen dat er geen *chilling effect* optreedt dat van invloed is op de politieke expressie of op de journalistieke verslaggeving van zaken van algemeen belang en rekening houdt met de brede bescherming die artikel 10 EVRM biedt.

Ten aanzien van artikel 10 EVRM en het begrip *hate speech* komt men niet altijd toe aan een belangenafweging. Zodra het uitingen betreffen die duidelijk onrechtmatig zijn, doet een aanspraak op de vrijheid van meningsuiting afbreuk aan de rechten en vrijheden in het EVRM. Dit kan worden toegelicht door een aantal arresten. Ten eerste oordeelde het Hof in de zaak *Geraudy tegen Frankrijk*[132] (waarin de verzoeker in zijn boek de holocaust ontkende) dat het ontkennen van de holocaust een dermate evidente onjuistheid betreft en dit binnen de reikwijdte van artikel 17 EVRM valt. Artikel 17 EVRM houdt een verbod in van misbruik van recht. Daarmee vallen dergelijke uitingen buiten de reikwijdte van artikel 10 EVRM en is zijn beroep op de vrijheid van meningsuiting in zulke gevallen niet ontvankelijk. Ook in het arrest *M'Bala M'Bala tegen Frankrijk*[133] oordeelde het Hof dat artikel 10 EVRM geen bescherming biedt tegen antisemitisme of ontkenning van de holocaust. Ten tweede, concludeerde het Hof in de zaak van *Norwood tegen het Verenigd Koninkrijk*[134] (betrof een poster van klager met de brandende Twin Towers waarop stond: 'Islam out of Britain – Protect the British People') dat het linken van de hele groepering aan een ernstige daad van terrorisme een situatie was zoals in artikel 17 EVRM. De daad was namelijk gericht op het teniet doen of verder beperken van de rechten en vrijheden onder het EVRM. Ten slotte,

126 Ibid.
127 Ibid., r.o. 117.
128 Ibid.
129 EHRM 7 december 1976 *Handyside/Verenigd Koninkrijk*, ECLI:CE:ECHR:1976:1207JUD000549372, r.o. 49.
130 Zie voor politieke figuren EHRM 8 juli 1986, ECLI:CE:ECHR:1986:0708JUD000981582 en zie voor publieke personen EHRM 24 juni 2004 ECLI:CE:ECHR:2004:0624JUD005932000.
131 EHRM 8 juli 1986 *Lingens/Oostenrijk*, ECLI:CE:ECHR:1986:0708JUD000981582, r.o. 46.
132 EHRM 24 juni 2003 *Garaudy/Frankrijk*, ECLI:CE:ECHR:2003:0624DEC006583101.
133 EHRM 20 oktober 2015 *M'Bala M'Bala/Frankrijk*, ECLI:CE:ECHR:2015:1020DEC002523913.
134 EHRM 16 november 2004 *Norwood/Verenigd Koninkrijk*, ECLI:CE:ECHR:2004:1116DEC002313103.

oordeelde het Hof in de zaak van *Glimmerveen & Hagenbeek tegen Nederland*[135] (betrof het verspreiden van folders die aanzetten tot racisme) dat de verzoekers door middel van het verspreiden van racistische ideeën artikel 10 EVRM gebruikte om de rechten en vrijheden in het EVRM teniet te doen. Uit de voorgaande arresten blijkt dat een zuivere toepassing van artikel 17 EVRM leidt tot een niet-ontvankelijkheidsverklaring van een beroep op artikel 10 EVRM. Het uiten van racistische, homofobe of andere controversiële opmerkingen leidt niet altijd tot een niet-ontvankelijkheidsverklaring. Wanneer de onrechtmatigheid van de content onduidelijk is, moet alsnog een afweging gemaakt worden tussen de in het geding zijnde grondrechten.

Ten slotte is relevant dat het EHRM recentelijk een belangrijk arrest heeft gewezen, dat specifiek betrekking heeft op wetgeving die korte termijnen bevat voor het verwijderen van bepaalde informatie. Net als de hieronder te bespreken Avia-wet heeft het EHRM schendingen van het recht op de vrijheid van meningsuiting vastgesteld. *Kablis tegen Rusland* uit 2019 is het eerste arrest waar het Hof de Russische wet inzake informatie, informatietechnologieën en de bescherming van informatie in overweging heeft genomen. Deze wet schrijft voor dat online platforms bepaalde onrechtmatige inhoud binnen 24 uur moeten blokkeren op bevel van een openbare aanklager.[136] Het Hof oordeelde unaniem dat het blokkeren van een sociaal netwerkaccount en inzendingen op een blog het recht op de vrijheid van meningsuiting in Artikel 10 EVRM schendt. Het EHRM bestempelde de maatregel als "*prior restraint*", wat de inherente gevaren verbonden aan preventieve beperkingen van de vrijheid van meningsuiting met zich brengt.[137] Als zodanig heeft het Hof de meest strikte toets op grond van Artikel 10 toegepast en vastgesteld dat de blokkeringsprocedure in strijd was met dit artikel. Dit zou zelfs het geval zijn wanneer er sprake was van rechterlijke toetsing, waarbij het Hof oordeelde dat een dergelijke rechterlijke toetsing niet voldoende effectief was om de gevaren van zo'n maatregel van voorafgaande terughoudendheid ten aanzien van de vrijheid van meningsuiting te overkomen.[138] Het oordeel in *Brzezinski tegen Polen* in 2019 is vergelijkbaar met het bovengenoemde arrest over Rusland. Het Hof bekeek in deze zaak een bepaling in de Poolse verkiezingswetgeving op grond waarvan kandidaten een regionaal gerecht kunnen verzoeken om een bevel tot beperking van de publicatie van informatie die onjuiste informatie of gegevens bevat. Het gerecht is dan verplicht om de aanvraag binnen 24 uur te onderzoeken.[139] Het Hof concludeerde unaniem een schending van Artikel 10 EVRM aangezien de nationale rechtbanken de verklaringen van een politicus tijdens een verkiezing " *immediately classified as lies*" hebben aangemerkt en "[b]y following such an approach the domestic courts effectively deprived [the politician] of the protection afforded by Article 10".[140] In een eerder arrest – *Kwieicién tegen Polen* – waarin een soortgelijke beschikking werd overwogen, had het Hof ernstige tekortkomingen vastgesteld. Het Hof oordeelde in het kader van een procedure wegens onjuiste informatie dat "fairness of the proceedings may be called into question".[141] Het lijkt er daarom op dat het Hof een strikte controle uitoefent op wetgeving die voorziet in korte termijnen voor het verwijderen van bepaalde informatie. Om een onevenredige aantasting van de vrijheid van meningsuiting te voorkomen moet bij het opstellen van dergelijke wetgeving rekening worden gehouden met de beginselen van artikel 10 EVRM.

Online intimidatie van (vrouwelijke) journalisten

Een relevant aspect dat ook internationaal bijzondere aandacht heeft betreft de online intimidatie van (vrouwelijke) journalisten. Het Comité van ministers en de Raad van Europa hebben een belangrijke aanbeveling over de bescherming van de journalistiek en de veiligheid van journalisten en andere media-actoren aangenomen, waarin de aandacht in het bijzonder wordt gevestigd op de onveilige omgeving die

135 EHRM 11 oktober 1979 *Glimmerveen en Hagenbeek/Nederland* (appl. nos. 8348/78 & 8406/78).
136 EHRM 30 april 2019 Kablis/Rusland (appl. nos. 48310/16 en 59663/17); Fathaigh en Voorhoof 2019.
137 EHRM 30 april 2019 Kablis/Rusland, r.o. 91.
138 Ibid., r.o. 97.
139 EHRM 25 juli 2019 *Brzeziński/Polen* (appl. no. 47542/07); Fathaigh 2019.
140 EHRM 25 juli 2019 *Brzeziński/Polen*, r.o. 58.
141 EHRM 9 januari 2007 Kwiecién/Polen, ECLI:CE:ECHR:2007:0109JUD005174499, r.o. 55.

vrouwelijke journalisten online ervaren.[142] De aanbeveling beschrijft dat vrouwelijke journalisten steeds vaker te maken krijgen met seksistische en misogynistische vernederingen, bedreigingen, intimidatie, pesterijen en seksuele agressie. Er is daarom dringend behoefte aan een systematische aanpak van dit probleem.[143] In het bijzonder kan dit soort misbruik online leiden tot een *chilling effect* op de vrijheid van meningsuiting van de vrouwelijke journalisten. Benadrukt moet worden de "insufficient efforts by relevant State authorities to bring the perpetrators to justice", wat kan leiden tot een cultuur van straffeloosheid.[144] Het Comité van Ministers raadt de lidstaten aan een wetgevingskader in te voeren om vrouwelijke journalisten tijdens hun werk doeltreffend te beschermen tegen gender gerelateerde gevaren. Daarnaast hebben de vertegenwoordigers van de Organisatie voor Veiligheid en Samenwerking in Europa ('OVSE') in 2019 een belangrijk persbericht over de veiligheid van vrouwelijke journalisten gepubliceerd.[145] Hierin is een aantal specifieke aanbevelingen opgenomen, welke onder meer omvatten dat (a) de huidige wettelijke kaders periodiek moeten worden herzien en ook gecontroleerd moeten worden om ervoor te zorgen dat de bestaande wetten effectief worden uitgevoerd, evenzeer online; en (b) de wethandhavingsinstanties moeten ervoor zorgen dat personeel wordt opgeleid om de online bedreigingen voor de veiligheid te identificeren binnen het kader van de bestaande wetgeving en in overeenstemming met de internationale normen inzake mensenrechten.

iii. Artikel 6 EVRM (eerlijk proces)

Een ander fundamenteel recht dat in aanmerking moet worden genomen, is het recht op een eerlijk proces dat is neergelegd in artikel 6 EVRM. Op grond van deze bepaling, die van toepassing is op alle civiel- en strafrechtelijke procedures, rust er een positieve verplichting op de Staat om een systeem voor rechtspraak in te richten dat is omkleed met procedurele waarborgen én om ervoor te zorgen dat die waarborgen in concrete gevallen worden nageleefd. Partijen moeten hun standpunt naar voren kunnen brengen en op elkaar kunnen reageren in een gerechtelijke procedure op tegenspraak, met inachtneming van het beginsel van *equality of arm*s. Dat dient ertoe om zowel de belangen van partijen te verzekeren als het belang van een goede rechtspleging en de rechtszekerheid in het algemeen.[146]

Artikel 6 EVRM omvat onder meer het recht op toegang tot een onafhankelijke en onpartijdige rechter, het recht op een openbare en mondelinge behandeling en het recht op berechting van de zaak binnen een redelijke termijn. Het recht op toegang is niet absoluut, maar het moet wel praktisch en effectief zijn en de rechtszoekende moet een "clear, practical opportunity to challenge an act that is an interference with his rights" hebben.[147] Er moeten dus zo min mogelijk feitelijke (met name financiële) en wettelijke belemmeringen bestaan om de procedure daadwerkelijk te beginnen en te doorlopen.[148] Dat houdt bijvoorbeeld in dat de kosten verbonden aan een procedure – zoals griffierecht niet prohibitief hoog mogen zijn in het licht van de financiële draagkracht van de rechtszoekende in kwestie.[149] Wat de kosten van rechtsbijstand betreft heeft het EHRM geoordeeld dat de Staat onder omstandigheden verplicht kan zijn om gefinancierde rechtshulp beschikbaar te stellen.[150] Dat hangt af van een aantal factoren, waaronder het belang van de zaak, de complexiteit van het toepasselijke recht en de toepasselijke procedure, het vermogen van de rechtszoekende om zichzelf daadwerkelijk in rechte te vertegenwoordigen en diens kans van slagen in de procedure.[151]

142 Aanbeveling CM/Rec (2016)4[1].
143 Ibid., par. 2.
144 Ibid., par. 3.
145 Organization for security and Co-operation in Europe (OSCE) and the representative on freedom of the media (Harlem Désir), 2019.
146 Zie o.a. EHRM 18 februari 1997 *Nideröst-Huber/Zwitserland* (appl. no. 18990/91), r.o. 30.
147 EHRM 4 december 1995 *Bellet/Frankrijk*, ECLI:CE:ECHR:1995:1204JUD002380594, r.o. 36-38.
148 EHRM 21 februari 1975 *Golder/Verenigd Koninkrijk*, ECLI:NL:XX:1975:AB5466. Zie ook Stein/Rueb 2018, p. 23.
149 EHRM 19 juni 2001 *Kreuz*/Polen (appl. no. 28249/95), r.o. 60-67.
150 EHRM 9 oktober 1979, *Airey/Ierland* (appl. no. 6289/73), r.o. 26 en EHRM 7 mei 2002 *McVicar v Verenigd Koninkrijk* (appl. no. 46311/99), r.o. 48 en 51.
151 EHRM 15 februari 2005 *Steel and Morris v Verenigd Koninkrijk* (appl. No 68416/01), ECLI:CE:ECHR:2004:0406DEC006841601, r.o. 61-62. Zie ook HvJEU 22 december 2010 *DEB v Bondsrepubliek Duitsland* ECLI:EU:C:2010:811.

De procedurele waarborgen van artikel 6 EVRM gelden voor alle geschillen waar het gaat om de vaststelling van burgerlijke rechten en verplichtingen, maar in het bijzonder als er andere (botsende) grondrechten in het spel zijn, zoals artikel 8 en 10 EVRM. Als er een beperking van de vrijheid van meningsuiting in het geding is, kan het ontbreken van effectieve en adequate waarborgen niet alleen een schending van artikel 6 opleveren maar ook van artikel 10.[152]

In civiele procedures moet er een *fair balance* worden gevonden tussen de procedurele rechten van beide partijen: het recht op toegang van de eiser en het recht op een eerlijk proces van de gedaagde. In het kader van dit onderzoek betekent dit dat het recht op een eerlijk proces van het individu dat de beweerdelijk onrechtmatige content heeft geüpload in aanmerking moet worden genomen. Artikel 6 EVRM waarborgt ook het fundamentele recht op hoor en wederhoor. Zo heeft het EHRM heeft met betrekking tot versnelde procedures die een snelle verwijdering van lasterlijk materiaal in verkiezingstijd mogelijk maken, geoordeeld dat "as desirable as the expeditious examination of election-related disputes may be, it should not result in the undue curtailment of the procedural guarantees afforded to the parties to such proceedings, in particular the defendants."[153] Beperkingen van procedurele waarborgen zijn toegestaan, maar niet in zodanige mate dat de essentie van het recht op een eerlijk proces in het gedrang komt. In bijzondere gevallen kan het voorkomen dat niet aan alle vereisten van artikel 6 EVRM wordt voldaan, zoals in spoedeisende zaken waarin "the effectiveness of the measure sought depends upon a rapid decision-making process" en "one or more specific procedural safeguards could not be applied without unduly prejudicing the attainment of the objectives sought by the interim measure in question".[154] Ook in die gevallen moet degene tegen wie rechtsmaatregelen worden getroffen echter de mogelijkheid hebben om daartegen in rechte op te komen.

B. Europese context

Eerder in het rapport is al verwezen naar de aanbeveling van de Europese Commissie over het effectief aanpakken van illegale online content. Naast deze aanbeveling zijn er vele andere regelingen, aanbevelingen, en andere initiatieven, op nationaal, Europees en internationaal niveau, die zien op de aanpak van onrechtmatige (en illegale) content. Het wettelijk kader voor diensten van de informatiemaatschappij en de aansprakelijkheid van tussenpersonen is in de basis onveranderd gebleven sinds de inwerkingtreding van de Richtlijn Elektronische Handel in 2000. Hier komt verandering in met de plannen voor nieuwe wetgeving voor digitale diensten (de Digital Services Act, kortweg 'DSA'), welke onderdeel is van de plannen van de Europese Commissie om de digitale interne markt te versterken.[155] Naast de ontwikkelingen op Europees niveau wordt hieronder ook een aantal relevante kaders en ontwikkelingen in omringende Europese landen besproken die voor de aanpak van onrechtmatige content in Nederland in het bijzonder interessant zijn.

i. Digital Services Act

De Europese Commissie heeft in juni 2020 een aantal voorlopige wetgevingsopties uiteengezet die kunnen worden opgenomen in de plannen voor de DSA, die zeer relevant zijn voor deze studie.[156] In het bijzonder wordt er momenteel gediscussieerd over het codificeren van regels met betrekking tot de verantwoordelijkheden van digitale diensten voor de omgang met en procedures voor onrechtmatige en illegale inhoud, waarbij deze problematiek in de volle breedte wordt bezien. De Europese Groep van regelgevende instanties voor audiovisuele mediadiensten ("**ERGA**)", het orgaan dat bestaat uit de hoofden

152 EHRM 6 december 2018 Słomka/Polen (appl. no. 68924/12), r.o. 69-70.
153 EHRM 9 januari 2007 *Kwiecién/Polen*, ECLI:CE:ECHR:2007:0109JUD005174499, r.o. 55.
154 EHRM 15 oktober 2009 M. v Malta (appl. no. 17056/06), r.o. 68.
155 Europese Commissie publicatie 2020.
156 Zie: Europese Commissie publicatie, 'Digital Service Act – deepening the internal market and clarifying responsibilities for digital services', https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services.

van de nationale regelgevende instanties van de EU voor audiovisuele mediadiensten (met inbegrip van het Commissariaat voor de Media), heeft aanbevolen om in het kader van de DSA nieuwe regels in te voeren voor ernstige "persoonlijke" schadelijke online content, zoals cyberpesten of berichten die zelfmoord of voedselonthouding aanmoedigen.[157]

Hoewel het nog niet duidelijk is welke onrechtmatige of schadelijke content onder het DSA-pakket zal vallen, overweegt de Commissie momenteel drie beleidsopties. De eerste optie betreft een beperkt rechtsinstrument dat de procedurele verplichtingen van het online platform zou regelen. Deze optie zou een aantal verplichtingen opleggen voor het effectief melden en actie ondernemen bij het rapporteren van onrechtmatige content, maar zal de aansprakelijkheidsregels in de huidige e-Commerce richtlijn niet veranderen. Daarnaast zal deze optie een aantal verhaalverplichtingen omvatten zoals het in verzet gaan wanneer content die door iemand geplaatst is, onderwerp wordt van een Notice and Takedown-procedure.[158]

De tweede optie die wordt overwogen is uitgebreider en actualiseert de aansprakelijkheidsregels voor internetdiensten, maar behoudt wel de belangrijkste beginselen van de e-Commerce richtlijn. In het bijzonder harmoniseert deze optie een reeks specifieke en bindende verplichtingen, waaronder (a) geharmoniseerde verplichtingen om meldingsregelingen – met betrekking tot alle soorten illegale producten, diensten en inhoudelijke berichten – te behouden en (b) effectievere verhaalsmogelijkheden en betere bescherming tegen ongerechtvaardigde verwijdering van legitieme content. Deze laatste verplichting zou ook regels bevatten voor effectieve samenwerking van onlineplatforms met de relevante autoriteiten en belangenorganisaties (voor een snelle verwijdering van illegale content).

De derde beleidsoptie zou de meest substantiële zijn, die bedoeld is om een systeem van regelgevend toezicht, handhaving en samenwerking tussen de lidstaten van de EU tot stand te brengen (en het een en ander op EU-niveau te ondersteunen).[159] De regels zijn vooralsnog gebaseerd op het "land van herkomst beginsel". De regels bevatten ook snelle en effectieve samenwerkingsprocedures wanneer het aankomt op grensoverschrijdende gevallen met betrekking tot de regulering en het overzicht van online platformen. Ook wordt gekeken naar opties voor effectieve gerechtelijke verhaalsmogelijkheden.

Er zullen nog veel discussies en onderhandelingen over het DSA-pakket plaatsvinden, maar het ligt in de verwachting dat dominante sociale media en andere platformen in ieder geval onderworpen zullen worden aan aangescherpte procedurele verplichtingen die betrekking hebben op meldingsmechanismen voor illegale content, maar ook beroepsmogelijkheden, zoals regelgevende procedures. Voor nieuwe nationale regelingen op het gebied van onrechtmatige content is het van groot belang te bezien hoe zij zich verhouden tot deze plannen.

Conflictoplossing en verhaalsmogelijkheden

Een belangrijk kenmerk van de EU-voorstellen in het kader van het DSA-pakket heeft betrekking op mechanismen voor het melden van illegale inhoud op onlineplatforms. Dit mechanisme werpt een bijzondere kwestie op die ook in de Nederlandse situatie speelt bij het zoeken naar de juiste procedures voor de snelle verwijdering van onrechtmatige content. Het gevaar is dat relevante procedures leiden tot de ongerechtvaardigde verwijdering van rechtmatige content. De plannen voor de DSA omvatten regels met betrekking tot conflictoplossing, effectieve verhaalsmogelijkheden en bescherming tegen ongerechtvaardigde verwijdering van legitieme content.[160] In de context van de DSA-discussie hebben wetenschappers

157 ERGA 2020, p. 10.
158 Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services - Inception Impact Assessment, Ref. Ares(2020)2877686, 4 June 2020, p. 5.
159 Ibid., p. 6.
160 Ibid.

ook nieuwe mechanismen voor conflictoplossing met betrekking tot inhoudsmodificatie voorgesteld, zoals het gebruik van sociale-mediaraden, online arbitrage-instanties en e-rechtbanken[161]. Verder heeft een aantal belangenorganisaties voor de bescherming van digitale grondrechten voorstellen gedaan voor het creëren van organen voor geschillenbeslechting.[162] Deze voorstellen zijn gebaseerd op het idee dat gebruikers een gemakkelijkere, snellere, goedkopere en minder procedureel ingewikkelde manier van verhaal moeten hebben dan zij in het traditionele rechtsstelsel ervaren.

ii. Andere landen [163]

Spanje

Een eerste voorbeeld is dat van Spanje, waar de Spaanse gegevensbeschermingsautoriteit een speciaal meldingskanaal voor de verwijdering van "gevoelige inhoud" heeft, dat zich onderscheidt van de indiening van gewone vorderingen.[164] Het mechanisme is beschikbaar als de claim betrekking heeft op seksuele inhoud of afbeeldingen van daden van agressie, waarbij de verspreiding een "hoog risico" vormt en het individu er niet in geslaagd is om de inhoud te laten verwijderen via het rapportagemechanisme van een platform. De claim moet een gedetailleerde beschrijving geven van de omstandigheden waarin de niet-consensuele verspreiding van de beelden heeft plaatsgevonden, waarbij met name moet worden aangegeven of de getroffen persoon slachtoffer is van geweld tegen vrouwen, seksueel misbruik of aanranding of intimidatie, en tot een andere bijzonder kwetsbare groep behoort (bv. minderjarige, persoon met een handicap of ernstige ziekte of met een risico op sociale uitsluiting). De vordering moet ook (a) het webadres of het account/profiel met de inhoud bevatten, (b) of er aangifte is gedaan bij de politie, en (c) de actie die is ondernomen om aangifte te doen bij een serviceprovider.[165]

Na analyse van de claim zal de gegevensbeschermingsautoriteit bepalen of er "dringende maatregelen" kunnen worden genomen die de voortzetting van de verwerking van persoonsgegevens beperken. In voorkomend geval zal de gegevensbeschermingsautoriteit opdracht geven de inhoud te verwijderen van de dienstverlener of het platform waar deze wordt verspreid. Bovendien zullen zij, als er aanwijzingen zijn voor een misdrijf, de politie op de hoogte brengen. In dergelijke omstandigheden verklaart de toezichthouder dat het individuen van deze stappen op de hoogte zal brengen. In voorkomend geval zal het onderzoek een sanctieprocedure tegen de voor de verspreiding verantwoordelijke personen voortzetten.

Verenigd Koninkrijk

Een tweede voorbeeld is dat van het Verenigd Koninkrijk: er is een aantal civiele rechtsmiddelen beschikbaar voor de snelle verwijdering van bepaalde inhoud die beschikbaar is op grond van de onrechtmatige daad en de privacy, en op grond van de 'Protection from Harassment Act 1977' en de 'Data Protection Act 2018', met inbegrip van voorlopige en eeuwigdurende dwangbevelen. Een belangrijke zaak is het arrest van 2017 in *Al-Ko Kober v. Balvinder Sambhi*, waar de High Court een tussentijds bevel uitvaardigde voor laster, en een eeuwigdurend bevel onder de Data Protection Act, met betrekking tot YouTube-video's, en beval dat de uploader content moest verwijderen, en niet "enige audio-opname, video-opname, foto of andere informatie verder moest verwerken of laten verwerken, onder meer door deze aan het publiek bekend te maken".[166] Verder kan op grond van de Protection from Harassment Act 1977 aan elke persoon die verantwoordelijk is voor een gedraging die als intimidatie kan worden beschouwd, met inbegrip van het online plaatsen van expliciete seksuele foto's en video's van een voormalige partner, door een rechter

161 Zie bijvoorbeeld Tworek 2020.
162 European Digital Rights (EDRi) position paper 2020.
163 Het rechtssysteem van de Verenigde Staten is in het onderstaande overzicht niet meegenomen, aangezien het geldende grondrechtelijk kader en de aansprakelijkheid van internetdiensten een andere regeling kent. In het bijzonder is in de V.S. de zogenaamde Communications Decency Act (Artikel 230) van toepassing, welke een absolute vrijwaring van aansprakelijkheid inhoudt voor het soort onrechtmatige online content waarop deze studie betrekking heeft. Om die reden is de verwijdering van dit type onrechtmatige content in de meeste gevallen afhankelijk van zelfregulering door betreffende diensten.
164 Zie de Website van de Agencia Espanola Proteccion Datos, https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/inicio.jsf.
165 Ibid.
166 Zie HC (QB) 6 oktober 2017, HQ17M03348.

een bevel worden opgelegd om de verdere publicatie te verhinderen en om ervoor te zorgen dat dergelijk materiaal wordt verwijderd. Verder is het Verenigd Koninkrijk momenteel bezig met de ontwikkeling van wetgeving die de Notice and Takedown-procedure van internetdiensten moet codificeren. Deze *Online Harms Bill* zal ook handhavingsmogelijkheden bieden voor een onafhankelijke toezichthouder en beoogt de verantwoordelijkheid van internetdiensten voor onrechtmatige online content juridisch in te kaderen en aan te scherpen.[167]

Ten slotte bestaat er een opmerkelijk en controversieel mechanisme in de Engelse wet genaamd een 'super-injunction'. Dit is een voorlopig bevel dat de publicatie van informatie over de naam of gegevens van de verzoeker verbiedt, maar daarnaast kan ook het bestaan en de procedure van het bevel geheim worden gehouden.[168] Super-injuncties zijn zeer controversieel; zij verhinderen niet alleen dat de media verslag uitbrengen over diegene die een bevel aanvraagt, maar ook over het bestaan van het bevel zelf. Super-injuncties zijn door NGO's bekritiseerd als "*a serious threat to both freedom of speech and democracy*" en een "*extreme form of censorship*".[169] Bovendien zijn de super-injuncties eigenlijk alleen beschikbaar voor rijke procespartijen. In 2010 brak een mediastorm uit over het vermeende gebruik door een aantal beroemdheden om publicatie van mediaverhalen over buitenechtelijke relaties te voorkomen. Er werd een regeringscommissie opgericht om deze problematiek van de super-injuncties te onderzoeken.[170] Het rapport erkende dat er een "clear danger that the use of super-injunctions, unless kept within strict bounds, could be thought to create, or to have created, a form of permanent secret justice".[171] De commissie deed een aantal aanbevelingen en merkte vervolgens uit de recente jurisprudentie dat super-injuncties "rarely applied for and rarely granted", en dat waar ze werden aangevraagd, ze in hoger beroep werden vernietigd.[172]

Duitsland

In Duitsland is in het bijzonder relevant de wet op de netwerkhandhaving (ook wel 'NetzDG' genoemd), die een aantal jaar geleden van kracht is geworden en waar bepaalde onlineplatforms een mechanisme moeten bieden voor het indienen van klachten over illegale inhoud.[173] Het gaat bij deze wetgeving om de verwijdering van onder het Duitse recht strafbare (illegale) content. Voor de definitie van illegale inhoud wordt aangesloten bij 22 specifieke delicten volgens het Duitse wetboek van strafrecht, waaronder belediging, smaad en laster. De wet werkt samengevat als volgt. Ten eerste legt artikel 3 lid 1 NetzDG, de platforms de verplichting op om een "doeltreffende en transparante procedure voor de behandeling van klachten over illegale inhoud" te hanteren en moet "de gebruikers een gemakkelijk herkenbare, rechtstreeks toegankelijke en permanent beschikbare procedure voor het indienen van klachten over illegale inhoud ter beschikking worden gesteld". In artikel 3 lid 2 NetzDG wordt vervolgens uiteengezet hoe de procedure moet werken. Eerst moeten de platforms "onmiddellijk kennisnemen" van elke klacht en nagaan "of de inhoud die in de klacht wordt gemeld onwettig is en moet worden verwijderd of dat de toegang tot de inhoud moet worden geblokkeerd". Ten tweede, en dit is van cruciaal belang, moeten platforms de toegang tot inhoud die duidelijk onwettig is binnen 24 uur na ontvangst van de klacht verwijderen of blokkeren. De wet geeft geen definitie van kennelijk onrechtmatig. Met name platforms moeten "alle onwettige inhoud onmiddellijk verwijderen of de toegang daartoe blokkeren, in de regel binnen 7 dagen na ontvangst van de klacht". De termijn van 7 dagen kan worden overschreden wanneer de beslissing over de onrechtmatigheid van de inhoud afhankelijk is van de onjuistheid van een feitelijke

167 Zie Department for Digital, Culture, Media & Sport, 'Online Harms White Paper – Initial consultation response, 12 februari 2020, https://www.gov.uk/government/consultations/online-harms-white-paper en BBC nieuwsbericht 2020.
168 Zie bijvoorbeeld Smartt 2017, p. 413-420; Matthiesson, 2010, p. 153-167; Report of the Committee on Super-Injunctions 2011.
169 Zie bijvoorbeeld Article 19 persbericht 2011.
170 Jones 2010.
171 Report of the Committee on Super-Injunctions 2011, p. 24.
172 Report of the Committee on Super-Injunctions 2011.
173 Wet ter verbetering van de handhaving van de wet op de sociale netwerken (wet op de netwerkhandhaving) 2017, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf?__ blob=publicationFile=2.

bewering of duidelijk afhankelijk is van andere feitelijke omstandigheden (het sociale netwerk kan de gebruiker dan de gelegenheid geven om op de klacht te reageren voordat de beslissing wordt genomen).

Frankrijk

In 2018 heeft Frankrijk de wet op de manipulatie van informatie uitgevaardigd, die bepaalt dat een rechtbank gedurende de drie maanden voorafgaand aan een verkiezing een online platform kan gelasten om onjuiste of misleidende beschuldigingen of aantijgingen te verwijderen, die de eerlijkheid van een aankomende verkiezing kunnen aantasten en die met opzet, kunstmatig of geautomatiseerd zijn verspreid.[174] Op verzoek van een dergelijk bevel moet de rechtbank binnen 48 uur na de indiening van een verzoek tot verwijdering, een beslissing nemen.

De wet legt de platformen ook de verplichting op om rapporteringsmechanismen in te voeren zodat gebruikers bepaalde onjuiste informatie kunnen melden. Voorts heeft het Franse nationale Assemblee in 2020 de wet op het tegengaan van online haat aangenomen (de zogenaamde Avia-wet).[175] De wet voorziet in meerdere verplichtingen voor de platformen, waaronder een 'samenwerkingsplicht' van grote online platformen met betrekking tot hate speech en andere schadelijke content. Ook heeft de wet een systeem van melding en actie geïmplementeerd. Daarnaast vereist de wet van platforms om duidelijke onwettige haatzaaiende berichten en andere content binnen 24 uur na melding te verwijderen. Als het om bepaalde terroristische content of kinderpornografie gaat, hebben de platforms een uur na de kennisgeving om de content te verwijderen.

Belangrijk is echter dat de Franse Constitutionele Raad (*Conseil Constitutionnel*) in juni 2020 de wet grotendeels ongrondwettig heeft verklaard, omdat deze het recht op vrijheid van meningsuiting schond.[176] Het Franse Hof was van oordeel dat de verplichting om duidelijk onrechtmatige haatzaaiende uitlatingen en andere inhoud binnen 24 uur te verwijderen, in strijd was met het recht op vrijheid van meningsuiting, evenals de verplichting om terroristische en kinderpornografie binnen een uur te verwijderen. De Raad was van mening dat de bepalingen slechts de online diensten aansporen om de content die wordt gerapporteerd te verwijderen, los van de vraag of deze content onmiskenbaar onrechtmatig is.[177] In andere woorden, de wet creëerde een *chilling effect* waardoor platforms niet voldoende nauwkeurig waren en content verwijderden die niet noodzakelijkerwijs onrechtmatig was.

De Europese Commissie had tijdens het opstellen van de Avia-wet zijn zorgen over deze wet geuit. De Commissie stelde dat de wet "*may overlap with the EU Digital Services Act initiative recently announced*" en zij heeft er bij de lidstaten op aangedrongen "*exercise restraint and postpone the adoption of national initiatives on this same matter, such as the notified draft*".[178] Het voorstel voor de DSA zal rekening moeten houden met de bezorgdheid van de Constitutionele Raad over de vrijheid van meningsuiting, nu er voor de DSA regelingen overwogen worden die vergelijkbaar zijn met het mechanisme van de Franse wet.

Italië

Er zijn ook specifieke procedures aangaande de snelle verwijdering van onrechtmatige content in Italië, waarbij ook de politie betrokken is. Ten eerste, met betrekking tot reputatierechten, heeft Italië zijn zogenaamde "Rode Knop Operationele Protocol voor de Bestrijding van de Verspreiding van Nep Nieuws

174 LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1), https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte; Blocman 2019.

175 Zie Proposition de loi n° 388, adoptée par l'Assemblée nationale, en nouvelle lecture, visant à lutter contre les contenus haineux sur internet, http://www.assemblee-nationale.fr/dyn/15/textes/l15t0388_texte-adopte-seance#B2298414350.

176 Zie Décision n° 2020-801 DC du 18 juin 2020, https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm; Berthélémy 2020; Article 19 2020; Breeden 2020.

177 Décision n° 2020-801 DC du 18 juin 2020, r.o. 19.

178 Zie Europese Commissie notificatie 2019 COM(2019) 8585 final.

over het Web" ten uitvoer gelegd.[179] Het protocol is ontworpen om desinformatie, hetgeen slechts ten dele geldt als onrechtmatige content, maar ook laster te bestrijden. Een tak van de Italiaanse politie die onderzoek doet naar cyber-crime – Polizia Postale – kreeg de taak om rapporten te beoordelen en dienovereenkomstig te handelen.

De Polizia Postale zal vervolgens de ingediende berichten beoordelen met als doel aanwijzingen te geven voor de te nemen maatregel voor content die onmiskenbaar ongegrond en bevooroordeeld is of openlijk lasterlijk. Als wordt vastgesteld dat content onrechtmatig is, kunnen de autoriteiten gerechtelijk stappen ondernemen. Indien de content als vals of misleidend wordt beschouwd, maar niet onrechtmatig is, dan kunnen de autoriteiten openbaar afstand doen van de content. Met name de speciale VN-rapporteur voor de vrijheid van meningsuiting publiceerde zijn bezorgdheid over het Protocol van de 'Rode Knop'. De Italiaanse regering antwoorde daarop dat dit protocol pas tijdens de verkiezingsperiode van kracht was geweest.[180]

Australië

Een laatste voorbeeld is van buiten de EU, in Australië, waar er een speciaal agentschap is genaamd de *eSafety Commissioner*, waar individuen een klacht kunnen indienen over online pesten, op beeld gebaseerd misbruik en illegale en schadelijke inhoud. Het Cyber Report team onderzoekt klachten en helpt bij het laten verwijderen van de inhoud. Met name de *Enhancing Online Safety Act 2015* heeft een civielrechtelijke sanctieregeling ingesteld om het niet-consensuele deel van intieme beelden aan te pakken, die in september 2018 is ingevoerd. Het gaf de *eSafety Commissioner* de bevoegdheid om zo snel mogelijk beeldmisbruikmateriaal te laten verwijderen.[181]

C. Conclusie

Dit hoofdstuk biedt verdere context voor de onderzochte problematiek middels de bespreking van het grondrechtelijk kader en internationaal perspectief. Wat fundamentele rechten betreft gaat het in het bijzonder om het recht op privéleven, het recht op de vrijheid van meningsuiting en het recht op een eerlijk proces (respectievelijk artikel 8, 10 en 6 EVRM). De staat heeft positieve verplichtingen om de persoonlijke levenssfeer te beschermen, ook in de online context – waaronder het nemen van maatregelen om inbreuken te voorkomen of te beëindigen. Wel moet er een belangenafweging ('*fair balance*') worden getroffen met het recht op de vrijheid van meningsuiting. Tot slot geldt het recht op toegang tot de rechter en het recht op een eerlijk proces zowel voor degene die content verwijderd wil krijgen als voor degene die de content heeft geüpload.

Het onderzoek moet ook worden bezien tegen de achtergrond van de plannen van de Europese Commissie voor de Digital Services Act. Het pakket heeft onder meer betrekking op mechanismen voor het melden van illegale inhoud op onlineplatforms, welke in de volgende hoofdstukken nader zullen worden besproken. Het hoofdstuk geeft tenslotte voorbeelden van juridische mechanismen voor verwijdering in andere Europese landen, zoals Spanje (een speciaal meldingskanaal van de gegevensbeschermingsautoriteit), Duitsland en Frankrijk (waar in dit verband vooral verplichtingen aan platforms worden opgelegd) en Italië (een zogenaamd "Red Button" protocol).

179 Zie Commissariato di P.S. 2018.
180 Zie UN Special Rapporteur 2018.
181 Zie voor het rapporteren naar commissaris voor eSafety in Australia: https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-esafety-commissioner.

4. Bestaande juridisch kader voor verwijdering en knelpunten

Er is een aantal verschillende (juridische) routes beschikbaar voor het verwijderd krijgen van onrechtmatige online content: de Notice and Takedown-procedure, civielrechtelijke procedures, bestuursrechtelijke procedures en via het strafrecht. Notice and Takedown en de civielrechtelijke procedures staan in beginsel open voor elk type onrechtmatige informatie terwijl de bestuursrechtelijke route is gebaseerd op de AVG en de strafrechtelijke route alleen open staat voor specifieke strafbare informatie. In dit hoofdstuk worden de verschillende routes besproken en geanalyseerd op knelpunten, om in hoofdstuk 5 verder geanalyseerd te worden op oplossingsrichtingen in het licht van de problematiek zoals uiteengezet in hoofdstuk 2. Naast het bespreken van de verschillende routes zal hier ook het bredere juridische kader besproken worden, bestaande uit de grondrechtelijke bepalingen en Europees recht en beleid op het gebied van onrechtmatige online-informatie.

A. Notice and Takedown-procedure

Vaak zal er sprake zijn van de betrokkenheid van een zogenaamde internettussenpersoon en zal de effectieve verwijdering van de onrechtmatige inhoud afhankelijk zijn van het handelen van deze dienstverlener. Aanbieders van diensten die bestaan uit de 'doorgifte' (mere conduit diensten) of de 'opslag' (hosting providers) van communicatie of inhoud van derden kunnen een beroep doen op een beperking van aansprakelijkheid (voor schade) onder de voorwaarden van de e-Commerce richtlijn. [182]

Deze e-Commerce richtlijn bevat voorwaardelijke aansprakelijkheidsvrijstellingen (*safe harbours*) voor drie soorten diensten verleend door internettussenpersonen: mere conduit (artikel 12), *caching* (artikel 13) en hosting (artikel 14). Artikel 14 e-Commerce richtlijn, geïmplementeerd in Artikel 6:196c lid 4 en lid 5 BW, is de meest relevante bepaling voor deze studie. Op basis van deze bepaling is een hosting provider een "dienst van de informatiemaatschappij" die bestaat uit de opslag van door een afnemer van de dienst verstrekte informatie. Het artikel bepaalt verder dat deze dienstverlener niet aansprakelijk is voor de informatie die op verzoek van een afnemer van de dienst is opgeslagen. Belangrijk is dat deze vrijstelling alleen van toepassing is als de dienstverlener niet daadwerkelijk op de hoogte is van illegale of onrechtmatige activiteiten of informatie, of wanneer hij/zij snel handelt om de informatie te verwijderen of de toegang tot de informatie te blokkeren als de dergelijke kennis of bewustwording is verkregen. Deze voorwaarden voor de beperking van aansprakelijkheid van hosting providers, impliceert dus een route om als individu of organisatie onrechtmatige informatie verwijderd te krijgen. Doordat de vrijwaring van de aansprakelijke partij voorwaardelijk is, is het in het belang van de dienst adequaat te reageren op een melding dat specifieke content onrechtmatig is. Zo zijn uit deze voorwaardelijke aansprakelijkheid de Notice and Takedown-procedures ontstaan. Omgekeerd staat deze route in de regel niet open bij mere conduit diensten nu deze diensten een passievere rol innemen in het communicatieproces, niet onder de beperkte aansprakelijkheid van artikel 14 e-Commerce richtlijn vallen.

Op grond van artikel 12 lid 3 en 14 lid 3 e-Commerce richtlijn en artikel 6:196c lid 5 BW, staat de beperking van aansprakelijkheid niet in de weg van het verkrijgen van een rechterlijk verbod of bevel. Dergelijke verboden of bevelen van de rechter met betrekking tot internet tussenpersonen kunnen dus op basis van

182 Zie 2.b.

het nationale recht worden opgelegd. Er is geen specifieke juridische procedure voorgeschreven voor het verkrijgen van een dergelijk verbod of bevel jegens een internetdienst die een beroep kan doen op artikel 6:196c BW. In beginsel kan op basis van het Nederlandse recht een bevel worden verkregen indien door de rechter vastgesteld wordt dat er sprake is van onrechtmatige inhoud. Wel bepaalt artikel 15 van de richtlijn dat lidstaten geen algemene toezichtverplichting op kunnen leggen aan de dienstverleners die onder de artikelen 12 tot en met 14 e-Commerce richtlijn vallen, met betrekking tot de informatie die zij doorgeven of opslaan, of een algemene verplichting om actief te zoeken naar feiten of omstandigheden die wijzen op illegale activiteiten. Het verdient opmerking dat de beperking van aansprakelijkheid in het BW en de e-Commerce richtlijn, in elk geval in grote lijn, voorvloeien uit algemene beginselen van het aansprakelijkheidsrecht. Het primaire doel van Artikel 12-15 e-Commerce richtlijn bestond, naast het beperken van rechtsonzekerheid voor aanbieders van relevante diensten en het stimuleren van e-commerce, uit het harmoniseren van beperkingen van aansprakelijkheid op Europees niveau.[183]

Momenteel wordt op Europees niveau gewerkt aan de Digital Services Act die de e-Commerce richtlijn uiteindelijk zou moeten gaan vervangen. Voor alsnog lijkt de beperkte aansprakelijk in de e-Commerce richtlijn in grote lijnen te worden gehandhaafd. Wel is onder andere te verwachten dat hosting providers substantieel meer verantwoordelijkheid krijgen voor het tegenaan van onrechtmatige online content en dat de bestaande zelfregulering ter invulling van de Notice and Takedown-procedure wettelijk vastgelegd wordt.[184]

i. Zelfregulering

In de loop der jaren is binnen de grenzen van deze beperking van aansprakelijkheid aanvullende zelfregulering en *soft law* ontwikkeld ten aanzien van de verantwoordelijkheid van hosting providers voor onrechtmatige inhoud.[185] Specifiek zien deze regels op Notice and Takedown-procedures als onderdeel van het beleid van de tussenpersonen zelf. In deze procedures wordt uiteengezet hoe individuen of organisaties een melding kunnen maken van (vermeende) onrechtmatige content, hoe de tussenpersoon deze melding beoordeelt en hoe daar vervolgens op gehandeld wordt. Door de ontwikkeling van uitgebreide zelfregulering en *soft law* zijn Notice and Takedown-procedures uitgegroeid tot een volwaardige route om onrechtmatige informatie online verwijderd te krijgen. Belangrijk om te vermelden is wel dat de grote sociale media platforms bij de meeste content die verwijderd wordt dit niet doen op basis van het geldende recht en nationale bepalingen met betrekking tot de vermeende onrechtmatigheid, maar op basis van hun eigen gebruiksvoorwaarden.[186] Deze gebruiksvoorwaarden sluiten uiteraard ook onrechtmatige content uit maar gaan vaak ook verder door bijvoorbeeld naakt of grof taalgebruik te verbieden. In de nieuwe Digital Services Act wordt gewerkt aan de gedeeltelijke codificering van de bestaande Notice and Takedown-procedures. [187]

Wat betreft de zelfregulering is in Nederland de 'Gedragscode Notice-and-Take-Down' (**"NTD-gedragscode"**) van belang.[188] Op basis van deze code verplichten deelnemers zich tot het voeren van een openbare en toegankelijke Notice and Takedown-procedure. In de meest simpele variant van deze procedure leidt een melding van onrechtmatige inhoud tot een beoordeling en eventuele verwijdering door de betreffende dienstverlener. De code bepaalt ook dat melder van onrechtmatige inhoud de tussenpersoon

183 Considerans 40 richtlijn 2000/31/EG.
184 Zie verder 3.a voor een bespreking van de Digital Services Act.
185 Europese commissise communicatie, *Takling Illegal Content Online – Towards an enhanced responsibility of online platforms,* 28 september 2017; Ministers' deputies recommendations 2018; Website betreffende de Manilla principesp zie https://www.manilaprinciples.org/.
186 Zie bijvoorbeeld Facebook Transparency, *Community Standards Enforcement Report*, Facebook mei 2020, https://transparency.facebook.com/community-standards-enforcement en Twitter Transparency report*, Twitter Rules Enforcement*, Twitter januari tot juni 2019, https://transparency.twitter.com/en/twitter-rules-enforcement.html.
187 Voor meer over de DSA zie 3.b.i en Europese Commissie publicatie 2020, https://ec.europa.eu/digital-single-market/en/digital-services-act-package.
188 Notice and Takedown 2018.

kan verzoeken "de melding met spoed af te handelen" (artikel 4 lid c NTD-gedragscode). De code bepaalt in artikel 5 en 6 dat indien de tussenpersoon vaststelt dat er sprake is van onmiskenbaar onrechtmatige of strafbare inhoud, de melder hiervan op de hoogte wordt gesteld en de betreffende inhoud onverwijld verwijdert.

Een belangrijke toevoeging aan de NTD-gedragscode is de aanwijzing van het Expertisebureau Online KinderMisbruik (**"EOKM"**) als zogenoemde *trusted flagger*. Op EU-niveau wordt een *trusted flagger* gedefinieerd als een organisatie of persoon die over specifieke expertise beschikt waardoor de notificaties van deze persoon of organisatie met extra prioriteit, of zelfs zonder extra check, worden overgenomen.[189] Bij het EOKM houdt dit dus in dat een melding van hen door de internetdienst niet verder inhoudelijk beoordeeld wordt, maar dat er onverwijld naar gehandeld wordt door de desbetreffende content te verwijderen.[190] Het achterliggende idee is dat het EOKM dusdanig onafhankelijk en kundig is dat de beoordeling aan hen overgelaten kan worden. Door de Notice and Takedown-procedure zo in te richten wordt dit type onrechtmatige informatie veel sneller verwijderd. *Trusted flagger*s worden ook buiten de NTD-gedragscode om steeds meer gebruikt voor verschillende soorten onrechtmatige en illegale content. De Europese Commissie heeft in 2017, middels een mededeling, en nogmaals in een aanbeveling uit 2018, expliciet de inzet van *trusted flagger*s voor het melden van onrechtmatige of illegale content aanbevolen.[191] Ook in de Europese 'Code of Conduct on countering illegal hate speech' wordt de inzet van maatschappelijke organisaties als *trusted flagger*s aangemoedigd.[192] Uit de expertinterviews blijkt dat *trusted flagger*s ook veel worden ingezet op het gebied van het IE-recht. De rechthebbenden worden geacht beter in staat te zijn een inbreuk te herkennen, wat de internetdienst veel tijd en moeite bespaart. Er zijn, echter, ook zorgen over de mate waarin rechthebbenden en andere belangenorganisaties als *trusted flagger*s rekening houden met de vrijheid van meningsuiting. Het gevaar kan zijn dat zij te veel rechtmatige content verwijderen.[193]

Een groot deel van de relevante partijen in het Nederlandse internetlandschap is aangesloten bij de Nederlandse code. Dat geldt ook voor vanuit Nederland internationaal opererende internetdiensten zoals WeTransfer[194] en Leaseweb.[195] De Nederlandse politie en Openbaar Ministerie zijn bij de code aangesloten in verband met de opsporing en vervolging van strafbare online content. Daarentegen zijn de grote internationale internetdiensten, waaronder Facebook, Microsoft, Google, Amazon en Twitter niet aangesloten bij de Nederlandse code en voeren zij hun eigen beleid. Zo heeft Facebook recentelijk een eigen orgaan opgericht dat bindende uitspraken kan doen over de vraag of specifieke informatie verwijderd moet worden of niet.[196]

ii. Beleid van internetdiensten en automatisering

Hoewel de zelfregulering van de Notice and Takedown-procedures van belang is, blijft het beleid van de internetdienst zelf bepalend voor welke content online staat. In de praktijk speelt de Notice and Takedown-procedure een redelijk beperkte rol in het geheel van maatregelen en systemen om online content op een platform te beheren, ook wel *content moderation* genoemd. In deze content moderation wordt de hoofdrol gespeeld door het beleid van de internetdiensten zelf en de geautomatiseerde uitvoering

189 Aanbeveling 1177 van de Europese Commissie (1 maart 2018), *Commission Recommendation on measures to effectively tackle illegal content online*.
190 Notice and Takedown 2018, Addendum nummer 1: kinderpornografische contenten EOKM als melder.
191 EC mededeling 2017; EC aanbeveling 2018.
192 Zie voor de gedragscode: Europese Commissie publicatie 2019.
193 Schwemer 2019; Keller en Leerssen 2019.
194 Zie We Transfer, 'Notice and Take Down policy', 11 juni 2013, https://wetransfer.com/legal/takedown.
195 Leaseweb geeft aan dat alleen in Leaseweb Netherlands de betreffende gedragscode geldt: Leaseweb, Legal Framework, https://www.leaseweb.com/abuse-prevention/legal-framework.
196 Clegg (Facebook) 2020.

daarvan.[197] In tegenstelling tot de Notice and Takedown-procedure moet het beleid van de internetdienst zelf niet gezien worden als een (buitenrechtelijke) procedure om onrechtmatige content verwijderd te krijgen door een individu. Toch is het belangrijk kort stil te staan bij dit beleid en de geautomatiseerde uitvoering daarvan om een compleet beeld te krijgen van hoe internetdiensten omgaan met ongewenste content.

De gebruiksvoorwaarden vormen de juridische basis voor internetdiensten om zelf de regels voor het platform te stellen en te handhaven. Een privaat bedrijf mag immers zijn eigen voorwaarden stellen voor de levering van zijn dienst, en wanneer een gebruiker akkoord gaat met deze voorwaarden staat de internetdienst vrij weinig in de weg om content te verwijderen wanneer hij de content in strijd acht met de gebruiksvoorwaarden.[198] De gebruiksvoorwaarden bevatten dus de regels voor welk typen content wel en welk type niet toegestaan zijn op het platform. Deze zijn veelal strikter dan de juridische grenzen voor online content. Zo is het op veel sociale media verboden naaktbeelden of gewelddadige beelden te plaatsen, terwijl deze juridisch vaak [199]

Op de grote sociale media platforms wordt de meeste content dus verwijderd op basis van de gebruiksvoorwaarden en niet op basis van vermeende onrechtmatigheid of illegaliteit. Een mogelijke aanvullende verklaring hiervoor is dat bij het toepassen van de eigen gebruiksvoorwaarden een internetdienst geen complexe juridische afweging hoeft te maken over de onrechtmatigheid van specifieke content. Vooralsnog is er weinig verschil, juridisch gezien, in de status van de verwijdering als de dienst het doet op basis van zijn eigen gebruiksvoorwaarden of op basis van illegaliteit of rechtmatigheid via de Notice and Takedown-procedure.[200] Het enige verschil is dat bij de Notice and Takedown-procedure de dienst de stimulans heeft om gerapporteerde content te verwijderen uit angst voor aansprakelijkheid en die stimulans niet zozeer aanwezig is bij het zelf verwijderen op basis van de Notice and Takedown-procedure.

Vervolgens is ook de wijze waarop content opgespoord wordt die in strijd is met de gebruiksvoorwaarden belangrijk. Dit gebeurt bij de grote sociale media platforms zoals Facebook, YouTube en Twitter namelijk steeds meer geautomatiseerd door middel van algoritmische of kunstmatige intelligentie systemen.[201] Deze systemen worden onder andere ingezet om de door gebruikers gemaakte content te analyseren en de content die in strijd is met de gebruiksvoorwaarden weg te filteren. Automatisering van content moderation wordt als noodzakelijk gezien omdat er dagelijks zo veel content gecreëerd wordt dat het onmogelijk is alles door mensen te laten controleren. Wel roept het gebruik van deze geautomatiseerde systemen nieuwe vragen op over, onder andere, de betrouwbaarheid, eerlijkheid en de transparantie van deze systemen, waarover hieronder meer. In aanvulling op de geautomatiseerde systemen zijn er ook menselijke 'moderators' die specifieke content die gesignaleerd is door het systeem, of in een Notice and Takedown-procedure naar boven komt, controleren.[202]

De inzet van geautomatiseerde systemen en vormen van kunstmatige intelligentie voor content moderation zal naar verwachten alleen maar toenemen. Tijdens de eerste golf van de COVID-19 pandemie is de inzet en afhankelijkheid van geautomatiseerde systemen voor content moderation in een stroomversnelling geraakt. Door de verschillende maatregelen om de verspreiding van het virus tegen te gaan, zaten

197 Zie bijvoorbeeld Facebook transparency report, *Bullying and harassment*, Facebook mei 2020, https://transparency.facebook.com/community-standards-enforcement#bullying-and-harassment. Google Transparantierapport, *Handhaving van de Communityrichtlijnen van Youtube*, https://transparencyreport.google.com/youtube-policy/removals.

198 Klonick 2018; van Hoboken en Keller 2019.

199 Er is bijvoorbeeld veel verzet tegen het beleid van Facebook geen beelden van vrouwen met ontbloot bovenlijf te accepteren. Zie Paul 2019 en Gillespie 2018.

200 Douek 2020; Gillespie 2018; Tworek e.a. 2020; Leerssen en Harambam 2020.

201 Voor een overzicht en typologie van verschillende geautomatiseerde content moderation systemen zie: Gorwa, Binns en Katzenbach 2020.

202 Er is veel controverse over de werkomstandigheden van de content moderators van de grote sociale media bedrijven. Zie bijvoorbeeld: Newton (The Verge) 2019; Holmes 2019; Feiner (CNBC) 2019.

veel moderators verplicht thuis en konden zij hun werk niet uitvoeren. Veel internetdiensten werden daardoor gedwongen nagenoeg volledig over te schakelen op geautomatiseerde content moderation.[203]

Hoewel dus in de praktijk de meeste ongewenste content geautomatiseerd verwijderd wordt door de grote sociale mediaplatforms, vaak zelfs nog voor het online komt, is de Notice and Takedown-procedure de meest belangrijke route voor een individu om content te verwijderen wanneer het eenmaal online staat. Wel is het belangrijk om te realiseren dat het bulk van de content moderation geautomatiseerd plaatsvindt aan de voorkant op basis van de spelregels van de internetdiensten zelf en, voor alsnog, geheel buiten het juridische domein valt.

iii. Gebruik en knelpunten

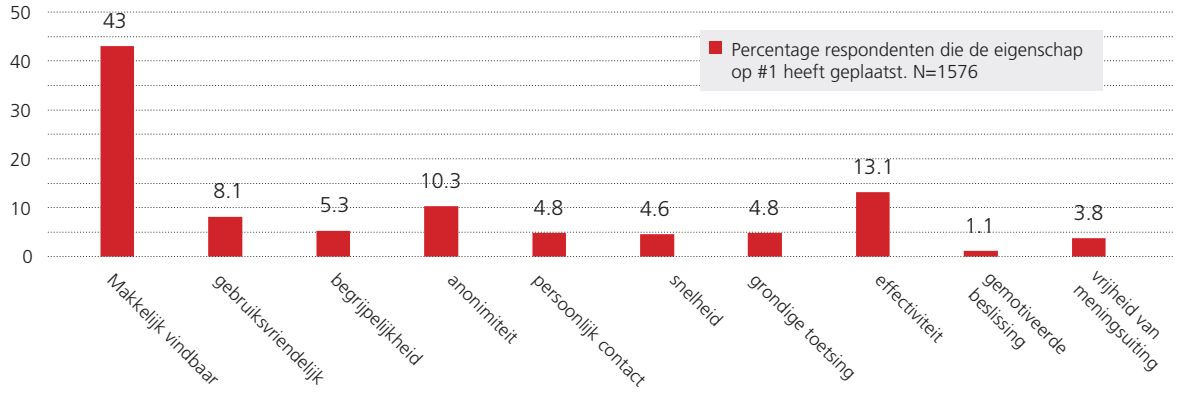
Nu de Notice and Takedown-procedure de meest laagdrempelige procedure is om content te verwijderen, is het belangrijk stil te staan bij het gebruik van deze procedure. Hiervoor zijn in de eerste plaats relevant de cijfers die de grote internetdiensten zoals Facebook, Twitter en YouTube publiceren over het gebruik van hun notificatieprocedures. Uit deze zogenaamde *transparency reports* rijst een wisselend beeld, mede omdat er geen gedeelde standaard is voor welke data op welke manier openbaar gemaakt wordt. Zo blijkt bij YouTube dat het om een enorme hoeveelheid verwijderende content gaat dat oploopt in de tientallen miljoenen per jaar.[204] Zoals hierboven aangegeven wordt bij YouTube het overgrote merendeel verwijderd na detectie door de dienst zelf en op basis van de gebruiksvoorwaarden. Na de eigen detectie van de YouTube komen verwijderingen op basis van notificaties van gebruikers via de Notice and Takedown-procedure op de tweede plaats. Ten slotte wordt slechts een klein percentage van de content verwijderd naar aanleiding van vonnissen.[205] Bij Facebook wordt in het transparency report de verwijderde content gecategoriseerd naar type content. Zo heeft Facebook in de eerste helft van 2020 wereldwijd bij bijna 5 miljoen *posts* actie ondernomen omdat deze vielen onder de categorie 'Bullying and Harassment'. Daarvan is meer dan 75% door gebruikers zelf gerapporteerd.[206] Ondanks de verscheidenheid aan type data kan op basis van deze transparency reports geconcludeerd worden dat het gaat om een grote hoeveelheid onrechtmatige content en dat bij de verwijdering hiervan de notificatie door gebruikers een belangrijke rol speelt.

Naast de algemene cijfers die door de internetdiensten zelf aangeleverd worden, is het ook nodig een beeld te verkrijgen van hoe bekend mensen in Nederland zijn met deze Notice and Takedown-procedure. Uit de voor dit onderzoek uitgevoerde survey blijkt een groot deel van de Nederlandse weinig tot geen gebruik van de procedure te maken. Concreet bleek grofweg 16% van de Nederlandse bevolking wel eens gebruik gemaakt te hebben van de mogelijkheid schadelijke informatie bij een internetdienst te rapporteren. Dit beeld verschuift enigszins als alleen gekeken wordt naar de mensen die ervaring hebben met schadelijke informatie op het internet. Van deze groep heeft 1/3 de rapportagemogelijkheid wel eens gebruikt.[207]

Wat betreft de de algemene bekendheid met de rapportagemogelijkheid blijkt uit onze survey onder een representatieve steekproef van de bevolking dat 28% hiermee bekend is. Aan het andere uiterste is 33% volledig onbekend met deze mogelijkheid. Dit beeld verschuift weer als alleen de groep bekeken wordt die wel ervaring heeft met schadelijke content, maar geen stappen heeft ondernomen; in deze groep is bijna 40% bekend met de rapportagemogelijkheden. Het percentage mensen binnen deze groep dat volledig onbekend is met de rapportagemogelijkheid, ligt op 20%.

203 Rodriquez (CNBC) 2020; Newton (The Verge) 2020; Nu.nl 2020.
204 Zie Google Transparantierapport, *Handhaving van de Communityrichtlijnen van Youtube*, https://transparencyreport.google.com/youtube-policy/removals.
205 Ibid.
206 Zie Facebook transparency report, *Bullying and harassment*, Facebook mei 2020, https://transparency.facebook.com/community-standards-enforcement#bullying-and-harassment.
207 Zie annex vi.

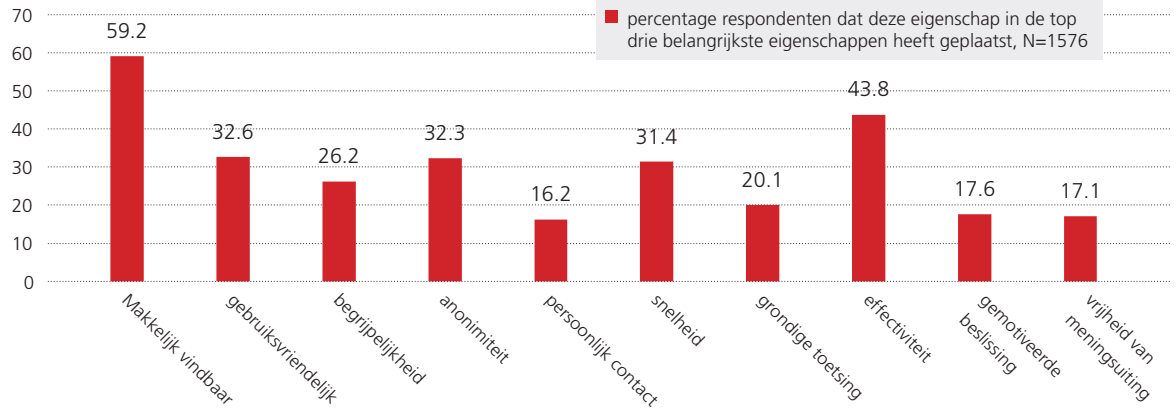
In deze survey is de representatieve steekproef ook gevraagd welke drie eigenschappen, uit een keuze uit 10 eigenschappen, zij het meest belangrijk vinden bij een rapportagemogelijkheid. Zoals weergegeven in de onderstaande figuur (5a) wordt de meeste waarde gehecht aan de vindbaarheid van de rapportagemogelijkheid, 43% van de respondenten geeft aan deze eigenschap het belangrijkst te vinden. Vervolgens geeft 13% aan het meeste waarde te hechten aan de effectiviteit van de rapportage: de schadelijke content moet ook daadwerkelijk verwijderd worden. De laatste eigenschap waarvan een substantieel aandeel, 10%, aangeeft het belangrijkst te vinden is de mogelijkheid om anoniem te rapporteren. De gebruiksvriendelijkheid en begrijpelijkheid wordt door tussen de 5% en 10% van de representatieve steekproef als belangrijkst gezien waar de mogelijkheid tot persoonlijke contact, de snelheid, de grondige toetsing van de rapportage en de aandacht voor de vrijheid van meningsuiting door niet meer dan 5% als belangrijkste eigenschap wordt gezien. De minste animo ontving de eigenschap dat de beslissing gemotiveerd is: slechts 1.1% hecht hier het meeste waarde aan.



Figuur 5a: **Belangrijkste eigenschappen rapportagemogelijkheid**

In de onderstaande figuur (5b) is weergegeven welk percentage respondenten de specifieke eigenschap opgenomen hebben in hun top drie. Deze figuur biedt een algemeen beeld van aan welke eigenschappen het grootste belang toegekend wordt. Weer springt de vindbaarheid van de procedure eruit als belangrijkste eigenschap nu bijna 60% deze in de top drie belangrijkste eigenschappen geplaatst heeft. Ook volgt de effectiviteit van de procedure weer op de tweede plaats met 44% en delen en de gebruiksvriendelijkheid en anonimiteit vlak daarna met 32.6 en 32.3%.

De grootste verschillen met de voorgaande figuur, waar alleen de eerste keuzes weergegeven zijn, zijn bij de eigenschap snelheid en gemotiveerde beslissing. Een substantieel aandeel van de respondenten heeft deze twee mogelijkheden opgenomen in de top drie waardoor deze eigenschappen relatief in belang toenemen. In de onderstaande figuur heeft nu niet de eigenschap gemotiveerde beslissing het laagste percentage, maar de eigenschap persoonlijk contact.



Figuur 5b: **Percentage respondenten dat deze eigenschap in de top drie belangrijkste eigenschappen heeft geplaatst, N=1576**

Samenhangend met de relatieve (on)bekendheid met relevante Notice and Takedown-procedures is het feit dat er geen helderheid bestaat over de daadwerkelijke procedure. Iedere dienst kan in beginsel zijn eigen procedures hanteren en daar op verschillende manieren de aandacht op vestigen. Uit de bovenstaande figuren kan voorzichtig afgeleid worden hoe een goede procedure er uit zou kunnen zien, maar de bestaande procedures voldoen lang niet aan al deze criteria. Deze onbekendheid en onduidelijkheid zal in de praktijk vaak betekenen dat voor internetgebruikers niet duidelijk is wat precies hun rechten en mogelijkheden zijn om onrechtmatige of schadelijke inhoud door een internetdienst verwijderd te krijgen.

Los van het daadwerkelijke gebruik van de Notice and Takedown-procedure bestaat er een levendig debat over de staatsrechtelijke aspecten van deze procedure en de invloed op de vrijheid van meningsuiting.[208] Wanneer de internetdiensten onrechtmatige content uit zichzelf of op verzoek van derden verwijderen, wordt er geen onafhankelijke, rechterlijke toets uitgevoerd. Zoals hierboven aangegeven zullen internetdiensten over het algemeen bij het beoordelen van meldingen van onrechtmatige of schadelijke inhoud, deze meldingen beoordelen aan de hand van hun gestelde gebruiksvoorwaarden ten aanzien van inhoud op de dienst. Deze gebruiksvoorwaarden zullen in de regel de verschillende vormen van onrechtmatige en strafbare inhoud omvatten, alsmede door de dienst gestelde aanvullende beperkingen. Daarnaast zijn de internetdiensten als private partijen niet zonder meer verplicht de vrijheid van meningsuiting van hun gebruikers te beschermen, en stimuleert de safe harbour uit de e-Commerce richtlijn deze diensten om, uit angst voor aansprakelijkheid, mogelijk onrechtmatige content snel te verwijderen. Dit alles bijeengenomen maakt dat mogelijk veel rechtmatige en toegestane uitingen verwijderd worden.

Vervolgens wordt degene die de vermeend onrechtmatige content geplaatst heeft, niet altijd de mogelijkheid geboden zich te verdedigen of zich na verwijdering te verzetten. Ook bleek uit de bovenstaande uiteenzetting over de transparency reports dat het nog zeer moeilijk is zicht te krijgen op het daadwerkelijk functioneren van de Notice and Takedown-procedures van de verschillende grote internetdiensten. Hier moet nog aan toegevoegd worden dat het gebruik van geautomatiseerde systemen om onrechtmatige of ongewilde content op te sporen en te verwijderen problematische aspecten heeft. Deze geautomatiseerde content moderation bij de grote sociale mediabedrijven kampt met meerdere fundamentele gebreken zoals het gebrek aan transparantie over het functioneren van deze systemen en aan mogelijkheden voor betrokkenen om in verzet te gaan.[209] Al deze haken en ogen maken het feit de Notice and Takedown-procedures een centrale rol spelen bij de verwijdering van onrechtmatige online content problematisch vanuit het perspectief van de vrijheid van meningsuiting.

Een laatste aandachtspunt met betrekking tot de buitengerechtelijke Notice and Takedown-procedures is of relevante publieke instanties, waaronder toezichthouders en de politie, gebruik kunnen maken van de door internetdiensten opengestelde mogelijkheden strafbare, onrechtmatige en/of schadelijke inhoud te melden.

Hoewel de Notice and Takedown-procedures een relatief laagdrempelige manier vormen om onrechtmatige content te verwijderen zit er ook een aantal duidelijke haken en ogen aan. Zo is slechts beperkt helder hoe deze procedures in de praktijk functioneren nu de internetdiensten wisselende en incomplete data openbaar maken. Daarnaast bleek uit de survey dat de bekendheid en het gebruik van deze procedure vrij laag ligt. Los van deze praktische punten is er ook een aantal meer fundamentele vragen verbonden aan de inzet van deze procedure. Zo wordt er geen onafhankelijk oordeel gegeven over de onrechtmatigheid, missen (momenteel) verdere juridische waarborgen zoals de mogelijkheid van hoor en wederhoor en is het gebruik van de procedure door overheidsinstanties bekritiseerd. Dit maakt dat

208 Suzor 2018; Kuczerawy 2018; Angelopoulos 2015.; Gillespie, 2018; Kaye 2018; Gorwa 2018; Suzor 2019.
209 Gorwa e.a. 2020; Annany en Crawford 2018; Keller en Leerssen 2019.

de procedure niet zonder meer onproblematisch is, voornamelijk vanuit het perspectief van de vrijheid van meningsuiting. Dit alles leidt ertoe dat een individu zich in een afhankelijke positie bevindt ten opzichte van de internetdienst. Wanneer de Notice and Takedown-procedure niet tot verwijdering leidt, moet iemand zich wenden tot de hieronder te bespreken formele juridische procedures binnen het civiel, bestuurs- of strafrecht. Deze verschillende juridische procedures zijn dan beschikbaar als escalatiemogelijkheid.

B. Civielrechtelijke routes

i. Modaliteiten

Welke civiele rechtsingang openstaat voor het instellen van een vordering of het indienen van een verzoek, hangt af van de vraag wat wordt gevorderd of verzocht en jegens welke partij(en). Er zijn verschillende modaliteiten, waarvan hieronder belicht wordt of en zo ja, in welke mate zij zich lenen voor een verzoek of vordering tot verwijdering van onrechtmatige online content als in dit onderzoek aan de orde:

- In het algemeen kan een rechterlijk bevel – gebod of verbod (art. 3:296 Rv) dan wel rectificatie (art. 6:167 BW) – op straffe van een dwangsom worden gevorderd in een **bodemprocedure of kort geding**, bijvoorbeeld tegen degene die de onrechtmatige content heeft geplaatst of tegen de internetdienst in kwestie (art. 6:196c jo. 3:15d lid 3 BW) om de content te verwijderen of om gegevens te verstrekken van de gebruiker.[210] Om een civiele procedure aanhangig te kunnen maken en de verkregen rechterlijke uitspraak ten uitvoer te kunnen leggen, moet de benadeelde weten tegen wie hij procedeert – dus aan wie en op welk adres de dagvaarding moet worden betekend en bij wie eventuele dwangsommen geïncasseerd kunnen worden.
- In geval van een beslissing op een verzoek op grond van de artikelen 15 tot en met 22 AVG[211] – strekkende tot bijvoorbeeld inzage, rectificatie of verwijdering van persoonsgegevens – dat is gericht tot een niet-bestuursorgaan, kan de belanghebbende de rechtbank binnen zes weken vragen om het betreffende verzoek alsnog toe of af te wijzen (art. 35 Uitvoeringswet AVG).[212] Aan de rechterlijke beschikking kan een dwangsom worden verbonden (art. 611a Rv).
- Daarnaast wordt de **ex parte-procedure op grond van art. 1019e Rv** bij een (dreigende) inbreuk op IE-rechten in kaart gebracht, die als zodanig niet van toepassing is maar wel gezien wordt als aanknopingspunt voor de inrichting van een eventuele nieuwe voorziening voor de verwijdering van onrechtmatige online content.

Voor bovenstaande modaliteiten is kenmerkend dat deze niet specifiek zijn toegesneden op de aanpak van onrechtmatige online content. Verder is er al discussie over knelpunten in de civiele rechtspleging – zoals (over)belasting van de rechterlijke macht – en de noodzaak van innovatie in het algemeen.[213] Daarbij wordt onder andere gedacht aan het beter organiseren van eerstelijns rechtshulp – waarin bijvoorbeeld het Juridisch Loket voorziet[214] – en het versterken van de regiefunctie van de (civiele) rechter over het procesverloop. Aan het slot van dit hoofdstuk zal worden ingegaan op de Tijdelijke Experimentenwet rechtspleging. Ook bestaat er in de praktijk behoefte aan meer inhoudelijke rechterlijke specialisatie, omdat er in de civiele procedure geen 'one size fits all' oplossingen zijn. Zo bestaat er voor IE-zaken binnen een aantal rechtbanken een aparte sectie.

210 Zie bijvoorbeeld Rb. Amsterdam 25 juni 2015, ECLI:NL:RBAMS:2015:3984.
211 Zie hierna paragraaf 4.c.ii over individuele rechten AVG.
212 Overigens kan verwerking van persoonsgegevens in strijd met de AVG worden beschouwd als onrechtmatig handelen tegenover de betrokkene, zodat deze zich ook na het verstrijken van de termijn van zes weken nog tot de civiele rechter kan wenden met een vordering tot staking of ongedaan making: Rb. Rotterdam 27 augustus 2018, ECLI:NL:RBROTRBOT:2018:7070, met verwijzing naar Hof Den Haag 15 december 2015, ECLI:NL:GHDHA:2015:3815.
213 Zie bijvoorbeeld Groenewald 2019.
214 Van Gammeren-Zoeteweij 2017.

In het hiernavolgende zal ervan uit worden gegaan dat de Nederlandse rechter bevoegd is om kennis te nemen van het geschil. In grensoverschrijdende zaken, bijvoorbeeld als de verweerder in een andere EU-lidstaat woont of is gevestigd, kan de Nederlandse rechter ook bevoegd zijn (art. 7 lid 2 Brussel Ibis Verordening). Volgens het Hof van Justitie van de EU geldt bij een schending van persoonlijkheidsrechten via het internet dat de gevolgen daarvan het beste beoordeeld kunnen worden door de rechter van de plaats waar het slachtoffer het centrum van zijn belangen heeft.[215] Voor voorlopige maatregelen is de bevoegdheid van de rechter territoriaal beperkt: er moet een reële band bestaan met het voorwerp van de gevraagde maatregel. Een rechterlijk verbod (in kort geding) strekt zich dus niet automatisch uit over andere landen.[216]

Alternatieve geschillenbeslechting wordt hieronder niet verder uitgewerkt, omdat dit in beginsel afhankelijk is van medewerking van beide partijen en ook als het resulteert in een bindend advies of arbitrale uitspraak, verlof voor tenuitvoerlegging van de overheidsrechter vereist is. In de context van dit onderzoek lijkt deze route weinig toe te voegen ten opzichte van de (buitenrechtelijke) Notice and Take-down-procedure; hierover meer in hoofdstuk 5.

ii. Bodemprocedure vs. kort geding

Een bodemprocedure lijkt zich alleen al vanwege de duur ervan niet goed te lenen voor een vordering tot verwijdering van onrechtmatige online content. De doorlooptijd van een bodemprocedure is minimaal 3 maanden, maar in de praktijk eerder 6-9 maanden (inclusief mondelinge behandeling); 62% van de zaken wordt afgedaan binnen 1 jaar. In 2016 werd 71% van de zaken bij verstek afgedaan, wat betekent dat de gedaagde niet is verschenen en geen verweer heeft gevoerd.[217] In dat geval toetst de rechter of het gestelde onrechtmatige karakter van de uitingen voldoende aannemelijk is en de vordering (tot rectificatie) hem niet onrechtmatig of ongegrond voorkomt.

De dagvaarding wordt gewoonlijk opgesteld door een advocaat en uitgebracht door een gerechtsdeurwaarder, tegen een vast tarief.[218] Bij de kantonrechter geldt geen verplichte procesvertegenwoordiging (art. 79 lid 1 Rv). De kantonrechter is bevoegd om kennis te nemen van geldvorderingen met een beloop van ten hoogste EUR 25.000 en van zogenoemde aardvorderingen, die betrekking hebben op o.a. een arbeidsovereenkomst, een consumentenkredietovereenkomst of een huurovereenkomst. Vorderingen van onbepaalde waarde, zoals een verzoek tot verwijdering van onrechtmatige online content, worden in beginsel niet door de kantonrechter behandeld en beslist, tenzij er een onderliggende schadeclaim is waarvan er duidelijke aanwijzingen bestaan dat die het bedrag van EUR 25.000 niet te boven gaat.

Het griffierecht in kort geding is even hoog als in een bodemprocedure. De doorlooptijd van een kort geding is echter aanzienlijk korter: die kan variëren van 2 dagen tot 6 maanden, afhankelijk van de spoedeisendheid (93% van de zaken wordt afgedaan binnen 3 maanden). Eén van de redenen hiervoor is dat de formele regels van bewijsrecht niet van toepassing zijn. Het Procesreglement kort gedingen voorziet in speciale regels voor bijzonder spoedeisende gevallen die nog dezelfde week of zelfs nog dezelfde dag/avond/nacht moeten worden behandeld. Een spoed-kort geding wordt echter beschouwd als uiterst redmiddel.

Het zwaartepunt bij de inrichting van het kort geding ligt meer bij de bescherming tegen (de risico's van) het te lang uitblijven van rechtsmaatregelen dan bij de inperking van het risico dat de rechtsverhouding

215 HvJEU 25 oktober 2011, ECLI:EU:C:2011:685 (*eDate/Martinez*).
216 HvJEU 17 november 1998, ECLI:EU:C:1998:543 (*Van Uden/Deco-Line*). Zie verder Kramer 2012; Vgl. echter Hof Den Haag 29 januari 2013, ECLI:NL:GHDHA:2013:BZ0458 en Rb. Amsterdam 15 juni 2012, ECLI:NL:RBAMS:2012:BW9838.
217 Eshuis en Diephuis 2018.
218 Besluit van 4 juli 2001, houdende nadere regels inzake de tarieven ambtshandelingen van gerechtsdeurwaarders en de tarieven (Besluit tarieven ambtshandelingen gerechtsdeurwaarders).

anders is of later anders blijkt te zijn.[219] Daarbij gaat het om een belangenafweging. Het voor een kort geding vereiste spoedeisend belang (art. 254 Rv) wordt in de praktijk vrij snel aangenomen, tenzij het gaat om een geldvordering – dan gelden strengere eisen.

De rechterlijke beslissing in kort geding heeft een voorlopig karakter. In plaats van hoger beroep kan ook (alsnog) een bodemprocedure worden ingesteld, waarin het kortgedingvonnis kan worden 'overruled'. Partijen dragen het risico van aansprakelijkheid voor schade als gevolg van tenuitvoerlegging van het kortgedingvonnis doordat in een bodemprocedure een andersluidend oordeel wordt gegeven. In de overgrote meerderheid van de gevallen – volgens deskundige schatting 95% – nemen partijen met het kortgedingvonnis genoegen en zien ervan af een bodemgeschil aanhangig te maken.[220]

Het aantal kort gedingen ten opzichte van bodemprocedure in eerste aanleg bedroeg in 2016:[221]

- Kanton: 7.332 kort gedingen en 427.058 bodemprocedures
- Civiel: 11.648 kort gedingen en 13.701 bodemprocedures

In "slechts" 6.249 zaken werd hoger beroep ingesteld.

De Rechtbank Amsterdam voert op dit moment een experiment uit met een versnelde bodemprocedure die qua behandeling lijkt op een kort geding. Dit experiment ondervangt het nadeel dat in kort geding geen constitutieve en declaratoire uitspraken kunnen worden gedaan. Spoedeisendheid is anders dan bij een kort geding niet vereist.[222]

iii. Verzoekschriftprocedure en collectieve actie

Hierna zal kort worden ingegaan op enkele relevante verschillen tussen de verzoekschriftprocedure en de dagvaardingsprocedure (bodemprocedure). Daarnaast zal worden stilgestaan bij de collectieve actie. Beide typen procedures hebben kenmerken die obstakels voor rechtszoekenden zouden kunnen verlichten of zelfs wegnemen, in het bijzonder omdat de verantwoordelijkheid voor bepaalde procedurele handelingen (gedeeltelijk) wordt verlegd naar de griffier van de rechtbank resp. een belangenorganisatie.

De wet schrijft voor welke zaken met een verzoekschrift moeten worden ingeleid. Voorbeelden hiervan zijn art. 6 Handelsnaamwet (veroordeling tot wijziging van verboden handelsnaam), art. 35 Uitvoeringswet AVG (verzoek gericht aan niet-bestuursorgaan) en de ex parte-procedure ex art. 1019e Rv die hieronder nader wordt beschreven. De verzoekschriftprocedure onder de AVG is beperkt tot een bevel om alsnog te voldoen aan een verzoek als bedoeld in art. 15 t/m 22 AVG. Het gaat om een bijzondere rechtsgang met een beperkte reikwijdte; zo kan er geen verklaring voor recht worden gevorderd of een verbod om in de toekomst persoonsgegevens te verwerken.

In de verzoekschriftprocedure is er minder ruimte voor partijautonomie: de rechter vervult een centrale rol, onder meer bij de oproeping van partijen. Naar aanleiding van een ingediend verzoekschrift worden de verzoeker, de verweerder en eventuele andere belanghebbenden opgeroepen door de griffier (art. 279 lid 1 Rv). Als een betrokken partij niet geïdentificeerd kan worden, dan is deze nog niet meteen uitgesloten van de procedure. Iedere belanghebbende kan, ook als hij/zij niet is opgeroepen, tot de aanvang van de behandeling een verweerschrift indienen. De zaak wordt mondeling behandeld. Alle opgeroepen partijen kunnen in persoon verschijnen.

219 Boonekamp 2020.
220 Stein/Rueb 2018 p. 375; Asser 2006, p. 115.
221 Ter Voert 2018.
222 Hendrikse 2020, p. 69.

De verzoekschriftprocedure kent een compacter partijdebat. De doorlooptijd is ongeveer 3 maanden vanaf de indiening van het verzoekschrift bij de rechtbank tot de datum van de beschikking. Een ander verschil met de dagvaardingsprocedure is dat procesvertegenwoordiging door een advocaat niet verplicht is in een verzoekschriftprocedure op grond van de AVG (art. 35 lid 4 Uitvoeringswet AVG). De rechter heeft de vrijheid om al dan niet (ambtshalve) een proceskostenveroordeling uit te spreken.[223] Zo kan er aanleiding zijn om de verzoeker niet in de proceskosten te veroordelen, ook als hij in het ongelijk wordt gesteld, in het licht van het recht op toegang tot de rechter (art. 47 EU-Grondrechtenhandvest).[224]

Al met al wordt de verzoekschriftprocedure sneller, doeltreffender en minder kostbaar geacht dan de dagvaardingsprocedure.[225] De verzoekschriftprocedure is ook de aangewezen procedure voor stichtingen of verenigingen die opkomen voor de bescherming van consumenten tegen oneerlijke handelspraktijken (art. 3:305d jo. art. 6:193a BW). Op verzoek van zo'n stichting of vereniging kan de rechter bevelen dat degene die een overtreding pleegt van de wettelijke bepalingen op dit terrein, die overtreding staakt en misleidende informatie zo nodig rectificeert. Op deze manier is het mogelijk om gelijksoortige belangen van personen, in dit geval consumenten, te behartigen. Hetzelfde mechanisme is zichtbaar bij een collectieve actie op grond van art. 3:305a BW. Deze personen behoeven dan zelf geen actie te ondernemen, maar kunnen zich wel beroepen op de uitspraak waarin de collectieve procedure resulteert. In de AVG (art. 80) is uitdrukkelijk het recht opgenomen om een belangenorganisatie opdracht te geven een klacht in te dienen en namens een betrokkene AVG-rechten uit te oefenen. Maar de mogelijkheid van een collectieve actie strekt zich uit tot andere rechtsvorderingen en is niet beperkt tot oneerlijke handelspraktijken of schendingen van de AVG.

Een voorbeeld van een collectieve actie in deze context is een rechtszaak gestart door de Stichting Stop Online Shaming (SOS) tegen een website die zonder toestemming naaktbeelden exploiteert.[226] SOS komt op voor slachtoffers van online privacy-inbreuken en daarmee samenhangende onrechtmatige uitingen, ook als hun identiteit onbekend is. Het gaat dan niet om een enkele post, maar om stelselmatige inbreuken door dezelfde partij (in dit geval Vagina.nl). Daarvoor leent een collectieve actie zich bij uitstek. Een belangenorganisatie als SOS beschikt dikwijls over meer kennis en middelen dan individuele benadeelden, en kan hun anonimiteit waarborgen.

iv. Ex parte-procedure op grond van art. 1019e Rv

Artikel 1019e Rv voorziet in de mogelijkheid om de rechter te verzoeken, in geval van een dreigende inbreuk op een IE-recht, een verbod op straffe van een dwangsom uit te spreken. Dit zonder de wederpartij op te roepen of te horen (ex parte). Dit is een belangrijk verschil met de hierboven besproken procedures. Ratio achter deze ex parte-procedure is ten eerste dat de wederpartij mogelijk bewijs kan verduisteren of anderszins de positie van de rechthebbende kan benadelen als hij wel vooraf gehoord wordt. Ten tweede is deze procedure veel sneller dan een normaal kort geding en kan onherstelbare schade zo beter voorkomen worden.[227] De procedure is ingesteld in het kader van de implementatie van art. 9 eerste en vierde lid Handhavingsrichtlijn.[228] De richtlijn voorziet in minimumharmonisatie ten aanzien van handhavingsmiddelen die gunstig zijn voor de IE-rechthebbende.[229]

223 Zie in het kader van de Wbp bijvoorbeeld Hof 's-Hertogenbosch 1 februari 2018, ECLI:NL:GHSHE:2018:363, besproken in van Duin 2018, p. 177-183; Vgl. echter Rb. Den Haag 28 juni 2019, ECLI:NL:RBDHA:2019:6302.
224 Eshuis en Diephuis 2018.
225 Zie o.a. Molenaars en De Jong 2019, p. 222-229.
226 De website van SOS (Stop Online Shaming), https://stoponlineshaming.org/.
227 *Kamerstukken II* 2005/06, 30392, 3, p. 23.
228 Ibid., p. 7.
229 Art. 2 Richtlijn 2004/48/EG.

Materiële toets

De ex parte-procedure op grond van art. 1019e Rv is alleen van toepassing op IE-rechten.[230] De maatregel kan grensoverschrijdend opgelegd worden.[231] Vereist is dat het een spoedeisende zaak betreft, met name indien uitstel onherstelbare schade zou veroorzaken. In principe moet het dus gaan om dreigende onherstelbare schade, maar in de rechtspraak is erkend dat voortdurende inbreuken ook voldoen.[232] Deze toets van spoedeisendheid zal hoger liggen dan de eis van spoedeisendheid in een kort geding (art. 254 Rv e.v.).[233]

In de procedure kan alleen een verbod opgelegd worden, op straffe van een dwangsom en uitvoerbaar bij voorraad.[234] Alle andere gebruikelijke IE-nevenvorderingen zoals een recall of opgave kunnen niet opgelegd worden.[235] Er kan ook geen proceskostenveroordeling ex artikel 1019h Rv opgelegd worden.[236] De verzoeker kan verplicht worden zekerheid te stellen (art. 1019e lid 3 Rv) en draagt de risicoaansprakelijkheid bij schade veroorzaakt door een ten onrechte opgelegd verbod (art. 1019g Rv, zie ook art. 7(4) jo. 9(7) Handhavingsrichtlijn).

Procesverloop

De vordering kan ingesteld worden jegens zowel de inbreukmaker als een tussenpersoon. Dit volgt direct uit art. 9(1) a jo. 9(4) Handhavingsrichtlijn, waar een tussenpersoon degene is 'wiens diensten door een derde worden gebruikt om op een recht van intellectueel eigendom inbreuk te maken'. De voorziening kan niet worden ingesteld jegens andere derden die geen 'tussenpersoon' zijn.[237]

De procedure zelf is zeer summier en binnen maximaal een paar dagen afgerond. De advocaat van de verzoeker dient het verzoekschrift in, waarna vaak nog telefonisch contact is tussen de voorzieningenrechter en de advocaat. De beschikking volgt direct daarna.[238] In principe is voorafgaande sommatie niet vereist, maar in sommige gevallen kan dit dusdanig voor de hand liggen dat dit wel eerst dient te gebeuren.[239] De voorzieningenrechter stelt de redelijke termijn in waarop een eis in hoofdzaak moet worden ingesteld (artikel 1019i(1) Rv). Indien dit niet gebeurt, verliest het ex parte-verbod zijn kracht. Dit heeft geen terugwerkende kracht.

Bij een aantal rechtbanken is het mogelijk een ex parte-verzoek grijs te maken.[240] Dit houdt in dat van tevoren bezwaren kenbaar gemaakt kunnen worden bij de rechtbank tegen een mogelijk ex parte-verzoek. Bij een ex parte-procedure ex art. 1019e Rv zal de voorzieningenrechter deze bezwaren dan bij zijn oordeel betrekken. Dit heeft geen wettelijke basis maar is vastgelegd in reglementen.[241] Een grijsmaking is beperkt geldig maar kan telkens opnieuw ingediend worden.[242]

Tegen een toegewezen verzoek kan worden opgekomen via een vordering in kort geding tot herziening (art. 1019e derde lid Rv). Zo kan schending van de plicht om de relevante feiten volledig en naar waarheid aan te voeren (art. 21 Rv) tot herziening leiden wanneer de niet gemelde informatie van aanzienlijk

230 Pinckaers 2011, p. 114-123; Vzr. Rb. Den Haag 5 maart 2010, IER 2010, nr. 54, p. 375, m.nt F. Eijsvogels (Yell/YPM).
231 Bijv, Rb. Den Haag 19 december 2008, B9 7519 (Go Fast Sports/Lucky Time c.s.). ook niet meteen vindbaar. Deze vind ik in artikelen of stukken, maar niet op rechtspraak.nl. Hierdoor weet ik niet wat het ECLI nr is wat ik voor elke rechtszaak gebruik.
232 Vzr. Rb. Den Haag 26 maart 2010, B9 8722 (Vlisco/V&D). ook niet meteen vindbaar.
233 HR 29 juni 2001, ECLI:NL:HR:2001:AB2391; van der Berg en Visser 2009; Pinckaers 2016, p. 166.
234 Pinckaers 2016, p. 163.
235 Ibid.
236 Pinckaers 2011; *Kamerstukken II* 2005/06, 30392, 3, p. 23.
237 Pinckaers 2016, p. 165.
238 Van den Berg en Visser 2009.
239 Pinckaers 2016, p. 167; Rb Haarlem 31 augustus 2007, ECLI:NL:RBHAA:2007:BB3561.
240 Rechtbank Den Haag, Amsterdam, Haarlem en Leeuwarden.
241 Reglement grijsmaken maatregelen volgens 1019b-d en 1019e Rv, https://www.rechtspraak.nl/SiteCollectionDocuments/Reglement-grijsmaken-maatregelen-volgens-1019b-d-en-1019e-Rv.pdf.
242 Pinckaers 2011.

belang is.[243] In dat geval kan ook een veroordeling in de (volledige) proceskosten van de oorspronkelijke verzoeker worden gevorderd (art. 1019h Rv). In 2011 werd één op de zes beschikkingen herzien.[244] De ex parte-beschikking gaat niet in kracht van gewijsde; herziening is altijd mogelijk. Het is onduidelijk of de herziening van de beschikking terugwerkende kracht heeft.[245]

v. Evaluatie en knelpunten

Wanneer de kenmerken van de bodemprocedure en het kort geding worden afgezet tegen de bekende gegevens over (obstakels voor) toegang tot recht – zie hoofdstuk 2 – lijkt een kort geding aantrekkelijk door de relatieve snelheid en eenvoud van de procedure. Het Procesreglement biedt ruimte om bepaalde zaken met meer spoed te behandelen. Toch rijst de vraag of een gemiddelde doorlooptijd van enkele weken tot maanden niet (nog steeds) te lang is om onrechtmatige online content snel verwijderd te krijgen.

Verder valt de verplichte procesvertegenwoordiging op. Ook als benadeelde partijen hun weg weten te vinden naar professionele rechtshulp, moeten zij een advocaat inschakelen om te procederen. Dat kan een (kosten)drempel vormen met een ontmoedigend of afschrikwekkend effect. Verplichte procesvertegenwoordiging wordt doorgaans gerechtvaardigd met een verwijzing naar de complexiteit van zowel het materiële als het formele recht, het belang van een geordend verloop van de procedure en de 'zeeffunctie' of 'poortwachtersfunctie' van advocaten om procedures te voorkomen door deskundige en onafhankelijke voorlichting.[246] Verplichte proces-vertegenwoordiging geldt in beginsel ook in de verzoekschriftprocedure, maar niet in AVG-zaken. Deze procedure is laagdrempeliger dan een dagvaardingsprocedure: zo draagt de griffier zorg voor de oproeping van partijen en andere belanghebbenden kunnen zich melden. Een verzoekschriftprocedure kan zowel partijen als de rechter meer flexibiliteit bieden. Verder kan een stichting of vereniging die gelijksoortige belangen behartigt in rechte optreden voor, namens of in de plaats van benadeelde partijen waar die de stap naar de rechter zelf niet willen of kunnen zetten. Een collectieve actie leent zich echter niet goed voor individuele gevallen waarin het gaat om het verwijderen van specifieke content. Om die reden zal deze route in dit rapport verder buiten beschouwing gelaten worden.

De ex parte-procedure heeft vergeleken met andere civiele procedures een zeer korte doorlooptijd, mede omdat de wederpartij niet gehoord wordt. De maatregel heeft een voorlopig karakter: deze kan in eerste instantie doeltreffend zijn, maar verliest zijn kracht als geen eis in de hoofdzaak wordt ingesteld. Er is empirisch onderzoek gedaan naar het gebruik van de ex parte-procedure van art. 1019e Rv tussen 2007 en 2012, waaruit blijkt dat de procedure snel verloopt en dat 10% van de verzoeken wordt afgewezen. Ook bleek dat in 89% van de gevallen geen rechtsmiddel wordt ingesteld, maar wanneer dat wel gebeurde, was dat in 90% toewijzend. Een verzoek tot herziening, dat in 11% van de gevallen werd ingesteld, leidde in 80% van de gevallen tot herziening.[247] Tegenover de snelheid van de ex parte-procedure staat het ontbreken van een (inhoudelijk) partijdebat. Dat vraagt om een bijzondere rechtvaardiging – dreigende onherstelbare schade of voortdurende inbreuken – en duidelijke afbakening: op dit moment staat de procedure alleen open voor inbreuken op IE-rechten.

243 Zie bijvoorbeeld Rb. Den Haag 31 augustus 2018, ECLI:NL:RBDHA:2018:10449, r.o. 4.4.
244 Pinckaers 2011.
245 Vzr. Rb. Den Haag 18 december 2009, B9 8486 (Ten Berg/Bodum); Vzr. Rb. Den Haag 14 december 2009, B9 8453 (Kruidvat/Adventure Bags) deze zaken zijn niet meteen vindbaar (alleen in artikelen); Vzr. Rb. Den Haag 4 mei 2011, ECLI:RBSGR:2011:BQ3525; Art 1019i lid 1 Rv: redelijke termijn voor indienen eis in hoofdzaak, indien dit net gebeurd verliest het ex parte verbod zijn kracht. Dan geen terugwerkende kracht, 1019g Rv risicoaansprakelijkheid indiener.
246 Stein/Rueb 2018, p. 52.
247 De Jong 2014, p. 104-114.

C. Bestuursrechtelijke route

De bestuursrechtelijke klachtprocedure bij de AP kan ingezet worden om online content die een inbreuk op de AVG vormt, te verwijderen. Naast deze klachtprocedure biedt de AVG een scala aan rechten voor individuele betrokkenen die ook ingezet kunnen worden om onrechtmatige online inhoud te verwijderen. Hoewel de uitoefening van individuele rechten onder de AVG in eerste instantie geen administratiefrechtelijke procedure vormt, worden zij gezien de inhoudelijke samenhang met de klachtenprocedure bij de AP hier besproken.[248]

i. Klachtenprocedure Autoriteit Persoonsgegevens

De voor dit onderzoek relevante bestuursrechtelijke procedure om onrechtmatige informatie offline te halen verloopt via de AP. Op hoofdlijnen ziet de procedure er als volgt uit. Op basis van de AVG heeft iedereen de mogelijkheid om bij de gegevensbeschermingsautoriteit, in Nederland de AP, een klacht in te dienen als zijn of haar persoonsgegevens onrechtmatig verwerkt worden.[249] Dit recht komt toe aan zowel ieder natuurlijk persoon dat betrokkene is,[250] als een daartoe bestemde stichting die de individuele betrokkene vertegenwoordigt.[251] Wanneer iemand de onrechtmatige verwerking van persoonsgegevens meldt die niet op hem of haarzelf betrekking heeft, classificeert de AP dit als een 'tip'.

Een klacht op basis van de AVG moet binnen het Nederlands bestuursrecht gezien worden als een verzoek tot handhaving.[252] De betrokkene verzoekt de toezichthouder immers in essentie om handhavend op te treden tegen een overtreding van de AVG zijnde de onrechtmatige verwerking van persoonsgegevens. Het doel van de klacht is dat de AP zijn bevoegdheden uit de AVG en de Uitvoeringswet AVG inzet om die specifieke onrechtmatige content te verwijderen. De AP heeft onderzoeksbevoegdheden,[253] kan corrigerende maatregelen opleggen[254] en heeft de mogelijkheid om informeel interventies te plegen.[255]

De AP is verplicht om op de klacht te reageren, maar in hoeverre de klacht daadwerkelijk inhoudelijk behandeld wordt, bepaalt de AP zelf. De AVG laat de toezichthoudende autoriteit veel ruimte om zelf, binnen de nationaalrechtelijke kaders, vast te stellen hoe omgegaan wordt met klachten van individuele betrokkenen. Wel verplicht de AVG de nationale toezichthoudende instantie om de betrokkene te informeren over de voortgang van de behandeling en de mogelijkheid een voorziening in rechte aan te vragen.[256] Dit moet in ieder geval binnen drie maanden gebeuren.[257] De betrokkene kan bezwaar en vervolgens beroep bij de bestuursrechter instellen als hij of zij het niet eens is met een besluit van de AP om de klacht niet te behandelen, als de klacht niet tijdig wordt behandeld of als hij of zij niet tijdig wordt geïnformeerd. Deze bestuursrechtelijke rechtsgang staat echter alleen open voor een belanghebbenden in de zin van de Awb.[258] Hoewel dit in de meeste gevallen geen probleem zal vormen, kan een betrokkene uit de AVG niet gelijkgesteld worden aan een belanghebbende in de zin van de Awb.[259]

Wat de inhoudelijke behandeling betreft geldt dat de AP de capaciteit mist om elke klacht (grondig) te behandelen. Daarom wordt een prioriteringssysteem gehanteerd, gepubliceerd in beleidsregels.[260] Op basis daarvan wordt bepaald welk type klacht op welke wijze wordt behandeld. De AP kijkt hierbij naar de mate waarin de betrokkene wordt geraakt door de overtreding van de AVG, de bredere maatschap-

248 Zie par. 4.b.iii voor een bespreking van de verzoekschriftprocedure.
249 Art. 77 jo. art. 80 jo. ov. 141-142 AVG.
250 Art. 4 lid 1 jo. 77 AVG.
251 Art. 80 jo. ov. 142 AVG.
252 *Kamerstukken II* 2017/18, 34851, 3., p. 27; de Jong 2018.
253 Art. 58 lid 1 AVG jo. Hfst 5 Awb.
254 Art. 58 lid 2 AVG jo. art. 5:32 Awb.
255 Besluit Autoriteit Persoonsgegevens 2018, par. 2.5.
256 Art. 77 lid 2 AVG.
257 Art. 78 lid 2 jo. art. 57 lid 1 sub f jo. 77 lid 2 AVG.
258 Art. 1:2 jo. 7:1 jo. 8:1 Awb..
259 RvS 21 februari 2018, ECLI:NL:RVS:2018:590.
260 Besluit Autoriteit Persoonsgegevens 2018.

pelijke relevantie van optreden bij dit soort overtredingen en de mate waarin de AP doeltreffend kan optreden in de specifieke context.[261] Vervolgens is nog relevant dat de AP vereist dat de betrokkene, voor het indienen van een officiële klacht, eerst de klacht meldt bij de verantwoordelijke zelf. Ook vereist de AP dat de betrokkene ermee akkoord gaat dat zijn of haar gegevens worden gebruikt richting de organisatie waar de klacht op gericht is.[262]

Het voorgaande houdt in dat veel van de klachten niet inhoudelijk behandeld worden. Als de klacht wel opgepakt wordt, is vaak (tijdrovende) internationale afstemming nodig wanneer de internetdienst niet in Nederland gevestigd is.[263] De AVG voorziet in een uitgebreide procedure voor coördinatie en afstemming tussen de toezichthouders van de verschillende lidstaten ingeval grensoverschrijdende verwerking.[264] Deze procedure is noodzakelijk om de coherentie in de handhaving van de AVG te bewaren nu veel van de verwerking een internationaal karakter zal hebben en iedere betrokkene een klacht kan indienen bij zijn eigen nationale toezichthouder.[265]

ii. Individuele rechten uit de AVG

Zoals aangegeven vormen de individuele rechten uit de AVG geen procedurele route, maar materiële grondslagen voor handhaving. Deze rechten stellen betrokkenen instaat zelf snel actie te ondernemen om schade te minimaliseren, terwijl een formele procedure wordt afgewacht. De handhaving van de individuele rechten uit de AVG kan via drie routes: (i) een klacht bij de AP en de hierboven beschreven bestuursrechtelijke route,[266] (ii) de civielrechtelijke route door middel van een verzoekschrift waarbij de verwerkingsverantwoordelijke direct wordt aangesproken,[267] en (iii) buitengerechtelijk door bijvoorbeeld bemiddeling van de AP of andere vormen van buitengerechtelijke geschilbeslechting.[268]

Recht op beperking van de verwerking

Voor het onderhavige onderzoek lijkt het recht op beperking van de verwerking uit artikel 18 AVG het meest relevant te zijn. Door het inroepen van dit recht jegens de verwerkingsverantwoordelijke kan de betrokkene ervoor zorgen dat de (vermeend) onrechtmatige verwerking tijdelijk wordt stopgezet zodat verdere schade zo veel mogelijk beperkt wordt. Bij onrechtmatige content online zou dit bijvoorbeeld betekenen dat een betrokkene een internetplatform kan vragen content tijdelijk offline te halen totdat vastgesteld kan worden of het daadwerkelijk onrechtmatig is.

Het recht kan worden ingeroepen wanneer (i) de juistheid van de gegevens wordt betwist door de betrokkene. De verwerking wordt dan beperkt gedurende het onderzoek door de verantwoordelijke. Ook kan het recht worden ingeroepen wanneer (ii) de verwerking onrechtmatig is, maar de betrokkene verzet zich tegen wissen, of (iii) de verantwoordelijke de gegevens niet meer nodig heeft, maar de betrokkene wel in het kader van een rechtsvordering en ten slotte (iv) als de betrokkene bezwaar heeft gemaakt tegen de verwerking en de verantwoordelijke de verwerking beperkt gedurende zijn onderzoek. Vooral optie (i) en (iv) zijn hier relevant, aangezien de beperking tijdelijk is en dient om de mogelijke schade van verwerking te minimaliseren voor het geval de klachten van de betrokkene gegrond blijken te zijn. Dan is van belang hoe 'de beperking van de verwerking' uitgelegd wordt. Uit de AVG kan opgemaakt worden dat dit betekent dat er slechts verwerkt wordt met de toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering/algemeen belang. De gegevens kunnen

261 Art. 2 lid 2 Besluit Autoriteit Persoonsgegevens 2018.
262 Autoriteit Persoonsgegevens 'Klacht melden', https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap.
263 Zie hoofdstuk VII AVG.
264 Art. 60 ev. AVG.
265 Art.77 jo. 57 lid 2 jo. Ov. 116 AVG.
266 Art. 77-78 AVG.
267 Art. 15-21 AVG jo. 35 UAVG en art. 79 AVG, zie ook 4.b.iii.
268 Art. 36 UAVG.

bijvoorbeeld worden overgebracht naar een apart systeem, worden niet meer beschikbaar gesteld of offline gehaald.[269]

Hoewel dit recht tot beperking van de verwerking zeer effectief lijkt te kunnen zijn in het indammen van eventuele schade door onrechtmatige content, blijft de relevantie ervan in de praktijk beperkt. Dit is voornamelijk het geval omdat een individu volledig afhankelijk is van de medewerking van de betreffende verantwoordelijke c.q. internetdienst voor de uitoefening van het recht. Wanneer bijvoorbeeld een internetplatform de onrechtmatige content niet offline haalt bij een beroep op artikel 18 AVG, zou de desbetreffende betrokkene of naar de civiele rechter of de AP moeten om het platform te dwingen dat wel te doen. Dit zou vervolgens evenveel tijd kosten wanneer de betrokkene direct naar de rechter was gestapt om de content te verwijderen.

Overige individuele rechten

Dan zijn er nog verschillende andere individuele rechten uit de AVG die op bepaalde wijze kunnen bijdragen aan het beperken van de schade door onrechtmatige content online. Voor al deze rechten geldt echter dezelfde tekortkoming als hierboven beschreven bij artikel 18: doordat de medewerking van de verwerkingsverantwoordelijke noodzakelijk is, is er geen garantie dat het recht daadwerkelijk *snel* en dus effectief uitgeoefend kan worden.

Het recht op rectificatie uit artikel 16 AVG kan bijvoorbeeld ingezet worden om onrechtmatige content verwijderd te krijgen. De betrokkene heeft dan het recht op 'onverwijlde' rectificatie van onjuiste persoonsgegevens.[270] Ook artikel 17 AVG, het recht op het wissen van gegevens, zou op die manier gebruikt kunnen worden. Wel voorziet het derde lid van artikel 17 in een aantal uitzonderingen waar in de meeste gevallen een afweging nodig is met andere rechten en verplichtingen.

Ten slotte kan het recht van bezwaar uit artikel 21 AVG mogelijk gebruikt worden om onrechtmatige content verwijderd te krijgen. Een betrokkene heeft namelijk het recht om bezwaar te maken tegen een verwerking wanneer deze gebaseerd is op de grondslag 'gerechtvaardigd belang van de verwerkingsverantwoordelijke' of 'de vervulling van een taak van algemeen belang'.[271] Wanneer er bezwaar gemaakt is kan de verantwoordelijke alleen doorgaan met de verwerking wanneer er 'dwingende gerechtvaardigde gronden' zijn die zwaarder wegen dan het belang van de betrokkene of ingeval van een rechtsvordering.

iii. Evaluatie en knelpunten

Het duidelijke voordeel aan de bestuursrechtelijke route via de klachtenprocedure is het zeer uitgebreide arsenaal aan bevoegdheden dat de AP ter beschikking staat. Wanneer de AP voldoende grond heeft bepaalde content te zien als inbreuk makend op de AVG én de AP de wil heeft om in dat concrete geval te handhaven, zijn er voldoende mogelijkheden om een internetdienst er snel toe te bewegen de content te verwijderen.

Vanuit het belang van een snelle verwijdering van onrechtmatige inhoud wegen de nadelen die verbonden zijn aan deze procedure echter zwaarder dan het genoemde voordeel. Al met al zal deze klachtprocedure vaak niet een snelle of effectieve route zijn om online content verwijderd te krijgen. Ten eerste heeft de procedure een lange doorlooptijd. Het leidt (in potentie) tot een bestuursrechtelijke procedure in drie instanties om een toezichthouder te bewegen de daadwerkelijke overtreder aan te pakken. Ten tweede bestaat er geen verplichting voor de AP om de klacht te behandelen. Ten derde is de klachtenprocedure op basis van de AVG alleen van toepassing als er sprake is van de verwerking van persoonsgegevens.

269 Art 18 lid 2 jo. ov. 67 AVG.
270 Zie ook ov. 65 AVG.
271 Zie art. 6 lid 1 sub e-f AVG.

Hoewel daar al snel sprake van zal zijn, hoeft deze verwerking niet de kern van de onrechtmatigheid te betreffen.

Ten slotte zijn er vragen over de effectieve doorwerking van de vrijheid van meningsuiting in de AVG. Zo zijn de bevoegdheden van de AP en de mogelijkheid voor betrokkenen om hun rechten uit te oefenen beperkt ingeval verwerking "voor uitsluitend journalistieke doeleinden en ten behoeve van academische, artistieke of literaire uitdrukkingsvormen".[272] Deze journalistieke exceptie moet ruim uitgelegd worden en geldt voor alle in de journalistiek werkzame personen en bedrijven.[273] Bepalend is of de activiteit bekendmaking aan het publiek van informatie, meningen of ideeën tot doel heeft.[274]

D. Raakpunten Strafrecht

Onder de brede scope van onrechtmatige content die mensen in hun persoon raken, valt een grote hoeveelheid mogelijke strafbare uitingen, zoals smaad, laster, bedreiging, belediging, discriminatie of wraakporno. Deze inhoudelijke overlap maakt het van belang om de procedurele raakvlakken en samenloop van het strafrecht met de andere procedurele routes voor het verwijderen van de informatie te bespreken. Daarnaast is in het kader van dit onderzoek de vraag gerezen of het mogelijk en wenselijk zou zijn om bij een nieuwe voorziening voor de verwijdering van onrechtmatige content voort te bouwen op een aangifte bij de politie.

i. Verwijderen informatie via strafprocesrecht

Het strafrecht is primair gericht op preventie en repressie – het heeft tot doel te bepalen of er sprake is van een strafbaar feit en een daarbij horende verdachte – en niet op het verwijderen of ontoegankelijk maken van onrechtmatige of strafbare content als zodanig. Er zijn twee formele wegen waarlangs het strafrecht betrokken kan worden bij een zaak over onrechtmatige content op het internet: door middel van een aangifte door een burger of rechtspersoon dan wel via eigen opsporingsonderzoek.

Aangifte

Burgers kunnen aangifte doen van strafbare feiten bij de politie. Een dergelijke aangifte is uiteraard alleen zinnig indien onrechtmatige inhoud ook strafrechtelijk kwalificeert als illegale inhoud. Vooropgesteld moet worden dat aangifte niet meer of minder is dan een melding aan de politie dat een vermeend strafbaar feit heeft plaatsgevonden. Dat geeft nog geen zekerheid dat opsporing en vervolging zal of kan plaatsvinden: aangifte verplicht daar niet toe en doorkruist dan ook niet het opsporings- en vervolgingsbeleid.[275] Verdergaande rechten kunnen er niet aan worden ontleend. Een strafrechtelijk onderzoek is ook niet (primair) gericht op het bieden van hulp aan slachtoffers bij het verwijderen van de illegale inhoud. Bovendien zal degene tegen wie aangifte wordt gedaan niet altijd de partij zijn aan wie het verwijderverzoek is gericht. De strafrechtelijke vervolging van internetdiensten zelf voor het niet verwijderen van illegale inhoud is een bijzonder geval. Het opleggen van een verplichting aan internetdiensten om content te verwijderen naar aanleiding van (enkel) de aangifte zou voorts een verandering van wetgeving vergen. Het is de vraag of dat noodzakelijk, wenselijk en grondrechtelijk aanvaardbaar is.

Elk jaar komen er meer dan een miljoen aangiftes binnen bij de politie. Dat betekent dat de politie in nauw overleg met het Openbaar Ministerie en het lokale bestuur prioriteiten stelt. De aangifte vormt het begin van de gehele strafrechtketen. Slachtoffers hebben de keuze om hun aangifte te doen op een politiebureau, telefonisch of via internet. Het is dus vaak de baliemedewerker van de politie die in eerste

272 Art. 43 UAVG ter implementatie van art. 85 AVG.
273 HvJEU 16 december 2008, ECLI:EU:C:2008:727 (*Satamedia*), r.o. 56 en 58.
274 Ibid., r.o. 61.
275 Van Bemmelen e.a. 2016, p. 286.

instantie beoordeelt of er sprake is van een strafbaar feit. Als de baliemedewerker van oordeel is dat er geen sprake is van een strafbaar feit, wordt de aangifte niet opgenomen.

Alle aangiftes, ook die online zijn gedaan, worden ter beoordeling voorgelegd aan een 'casescreener'. Deze casescreener beoordeelt of er sprake is van voldoende aanknopingspunten voor een vervolgonderzoek. De casescreener volgt daarbij de Aanwijzing voor de Opsporing (Stcrt. 2013, 35757) van het Openbaar Ministerie. Die houdt in dat steeds afgewogen moet worden of in een zaak tot opsporing wordt overgegaan, en zo ja, met welke inzet (in tijd en in capaciteit). Bij high impact crimes zoals inbraken en overvallen, en bij ondermijningszaken zoals drugs- en mensenhandel vindt altijd vervolgonderzoek plaats. Bij veel voorkomende criminaliteit (VVC) zoals vernieling in de regel niet.[276] Voor de aanpak van 'strafbare uitingen op het internet' zijn in de Aanwijzing voor de Opsporing geen aanwijzingen te vinden.

Als er voldoende aanknopingspunten zijn en er voldoende 'prioriteit vanuit het lokale gezag' is, wordt een vervolgonderzoek gestart. Daarbij geldt dat de zaken met de hoogste prioriteit en met de meeste aanknopingspunten als eerste worden behandeld. Bij dat vervolgonderzoek kunnen alle opsporingsbevoegdheden (waaronder de hieronder besproken bevoegdheid van art. 125p Sv) worden ingezet indien aan de daarvoor geldende voorwaarden (zoals de ernst van het strafbare feit) wordt voldaan. Indien dat vervolgonderzoek leidt tot een concrete verdachte, zal het Openbaar Ministerie in de regel tot vervolging overgaan. Of en welke bevoegdheden er in het vervolgonderzoek worden ingezet, wordt bepaald door de politie (in samenspraak met de verantwoordelijke Officier van Justitie). De burger heeft daarop geen invloed.

Empirische gegevens ontbreken over wanneer en hoe vaak aangifte wordt gedaan met betrekking tot onrechtmatige online content, welke aanpak/strategie politie en justitie hierin volgen en in hoeverre die effectief is.

Bevoegdheid van art. 125p Sv

Wanneer een burger aangifte doet van onrechtmatige of strafbare informatie op het internet, staat de bevoegdheid van art. 125p Sv open, namelijk het door de officier van justitie richten van een bevel aan de aanbieder van een communicatiedienst[277] om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken. Daar wordt een belangrijke beperking bij gegeven 'voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten'. Bovendien mag deze bevoegdheid slechts worden gebruikt bij een verdenking van een misdrijf als omschreven in art. 67 lid 1 Sv. Hieronder vallen bijvoorbeeld wel het aanzetten tot haat of geweld en alle zedenmisdrijven, waaronder het recent ingevoerde verbod op wraakporno,[278] maar niet (groeps)belediging, laster, of smaad. Het bevel is schriftelijk[279] en bevat een opgave van de gegevens die ontoegankelijk moeten worden gemaakt. Het bevel bevat tevens een aanduiding van het strafbare feit en de feiten en omstandigheden

276 Behalve als er sprake is van een heterdaadzaak en daarmee vergelijkbare zaken waarbij de identiteit van de verdachte bij de aangever bekend is dan wel zeer gemakkelijk is te achterhalen (de zgn. kant-en-klaar zaken); dan volgt er altijd een vervolging (onderzoek) (Aanwijzing voor de Opsporing (*Stcrt*. 2013, 35757, onder 3)).

277 Dat zijn de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.

278 Art. 139h Sr. In dit artikel is het verbod neergelegd om van een persoon een afbeelding van seksuele aard openbaar te maken, terwijl men weet dat die openbaarmaking nadelig is voor die persoon.

279 De NVvR had zich bij de introductie van deze bepaling afgevraagd of de voorgestelde mogelijkheid in dit artikel voldoende slagvaardig is. Doordat digitale informatie snel kan worden verspreid, kan het afwachten van een schriftelijke machtiging van de rechter-commissaris teveel tijd kosten. Het geven van een mondeling en een mondeling machtiging zou voldoende moeten zijn. Dit advies van de NVvR is niet overgenomen omdat het bevel tot het ontoegankelijk maken van gegevens een verstrekkende bevoegdheid betreft, aldus de memorie van toelichting, waarbij de vrijheid van meningsuiting in het geding kan zijn (Wetsvoorstel Computercriminaliteit III, *Kamerstukken II* Tweede Kamer 2015/16, nr. 34 372, nr. 3, p. 96).

waaruit zou blijken dat het ontoegankelijk maken van de gegevens noodzakelijk is om een strafbaar feit te beëindigen of nieuwe strafbare feiten te voorkomen (art. 125p lid 2 Sv).

Het bevel mag bovendien slechts worden gegeven na voorafgaande schriftelijke machtiging door de rechter-commissaris. De rechter-commissaris zal zich - net als de officier van justitie - een oordeel moeten vormen over alle wettelijke eisen die samenhangen met deze bevoegdheid voordat hij de benodigde machtiging verstrekt (art. 125p lid 4 Sv). De rechter-commissaris zal daarbij een afweging moeten maken tussen de in het geding zijnde belangen. Het betreft de belangen die zijn gediend bij strafrechtelijke handhaving van de rechtsorde, de belangen van degene die de gegevens op het internet heeft gepubliceerd, het belang van de vrijheid van meningsuiting alsmede de belangen van de aanbieder indien het bevel tot hem is gericht.[280] De rechter-commissaris moet voordat hij de machtiging verstrekt, de aanbieder tot wie het bevel is gericht in de gelegenheid stellen te worden gehoord (art. 125p lid 4 Sv). Tegen een afwijzende beslissing van de rechter-commissaris staat voor de officier van justitie hoger beroep open (art. 446 Sv). Vanwege de mogelijke verstrekkende consequenties van een bevel, staat voor de belanghebbende – degene tegen wie het bevel zich richt maar ook degene die de gegevens beschikbaar heeft gesteld voor de verspreiding via het internet – de beklagprocedure van art. 552a Sv open.[281] Op een klaagschrift moet zo spoedig mogelijk worden beslist en tegen de door de raadkamer gegeven beschikking staat zowel voor klager als de officier van justitie beroep in cassatie open.

Onder ontoegankelijk maken wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van het geautomatiseerde werk[282] of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens uit het geautomatiseerde werk, met behoud van die gegevens ten behoeve van de strafvordering (art. 125o lid 2 Sv). Het ontoegankelijk maken moet terstond. Daarmee wordt tot uitdrukking gebracht dat van de aanbieder van een communicatiedienst wordt verwacht dat deze zo snel mogelijk alle maatregelen neemt die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken, ter beëindiging van een strafbaar feit of ter voorkoming van strafbare feiten. Aangezien het in bepaalde gevallen technisch niet goed mogelijk kan zijn om de gegevens effectief ontoegankelijk te maken, is de verplichting tot het ontoegankelijk maken geclausuleerd tot wat redelijkerwijs van hem gevergd mag worden. Het ontoegankelijk maken van de gegevens kan plaatsvinden door de desbetreffende gegevens te verwijderen, dan wel de toegang daartoe te blokkeren. Blokkering kan aan de orde zijn als de gegevens niet kunnen worden verwijderd, zodat de gegevens voor de gebruikers niet raadpleegbaar zijn.

Om aan het bevel tot het ontoegankelijk maken te voldoen, dient de blokkering voort te duren zolang de gegevens worden aangeboden.[283] Het bevel moet worden gericht tot degene die daarvoor het meest in aanmerking komt. Als de gewraakte gegevens in Nederland worden gehost, zal dit in de eerste plaats de hosting provider zijn. Als de gegevens in het buitenland worden gehost en het ontoegankelijk maken noodzakelijk is, kan het bevel in beginsel ook tot de access providers worden gericht. De kosten en inspanningen aan de kant van de aanbieder, die voortvloeien uit het ontoegankelijk maken, vormen een factor die bij het bevel mede betrokken moet worden. De aanbieder kan op grond van het eerste lid immers uitsluitend worden bevolen dat hij alle redelijkerwijs van hem te vergen maatregelen treft om gegevens ontoegankelijk te maken. [284]

280 Wetsvoorstel Computercriminaliteit III, *Kamerstukken II* 2015/16, nr. 34 372, nr. 3, p. 97.
281 Consequentie van de beklagprocedure is overigens wel dat de gewraakte gegevens zolang als de procedure loopt ontoegankelijk zijn gemaakt.
282 Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken (art. 80sexies Sr).
283 Wetsvoorstel Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 96-97.
284 Ibid, p. 95.

Het bevel zal ook duidelijkheid moeten verschaffen over de feiten en omstandigheden waaruit blijkt dat het ontoegankelijk maken van de gegevens nodig is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen (lid 2, onderdeel b). Om – in geval van uitingsdelicten – te voorkomen dat de vrijheid van meningsuiting verder dan noodzakelijk wordt ingeperkt, zal de officier van justitie nauwkeurig bepalen welke gegevens een strafbaar feit behelzen en – dus – ontoegankelijk moeten worden gemaakt door degene tot wie het bevel is gericht (lid 2, onderdeel c). De officier van justitie zal hierbij rekening houden met de technische mogelijkheden om onderdelen van pagina's of websites te kunnen verwijderen. Hiermee kan voorkomen worden dat tot de aanbieder een bevel wordt gericht dat technisch niet kan worden uitgevoerd.[285]

Het niet voldoen aan het bevel levert een zelfstandig strafbaar feit op (art. 184 Sr) en kent een maximale strafbedreiging van drie maanden gevangenisstraf en een geldboete van de tweede categorie.[286] Deze bepaling is in de wet gekomen door de Wet Computercriminaliteit III,[287] en in werking getreden op 1 maart 2019. Voor zover de onderzoekers bekend, is art. 125p Sv in de praktijk nog niet ingezet. Uit de expertinterviews kwam naar voren dat in de praktijk de voorkeur wordt gegeven aan de hieronder beschreven route van Notice and Takedown, omdat deze sneller en vaak effectief is.

NTD-gedragscode[288]

Deze formele strafrechtelijke mogelijkheden staan in de praktijk los van de mogelijkheid dat de internetproviders vrijwillig voldoen aan de vraag van de politie of het Openbaar Ministerie om bepaalde gegevens van het internet te verwijderen of ontoegankelijk te maken. Het Openbaar Ministerie is medeondertekenaar van de NTD-gedragscode. Echter de politie en justitie kunnen ook bij partijen die niet aangesloten zijn bij de code, een informeel verzoek doen. Uit de expertinterviews blijkt als gezegd dat van deze mogelijkheid (veel) vaker gebruik gemaakt wordt dan van art. 125p Sv, hoewel er geen exacte cijfers beschikbaar zijn op dit punt. Ook kwam nadrukkelijk naar voren dat de internetdiensten nagenoeg altijd gevolg geven aan de meldingen en de desbetreffende informatie verwijderen. Bij het doen van een dergelijke melding is geen tussenkomst van een rechter-commissaris vereist, wat de procedure aanzienlijk versimpelt. Naast het gemak en het informele karakter van het doen van een Notice and Takedown-melding speelt ook een rol dat op deze manier van de informatie verwijderen voor de verdachte vaak nog verborgen gehouden kan worden dat er een strafrechtelijk onderzoek speelt.

Uit de parlementaire geschiedenis bij de Wet Computercriminaliteit III blijkt dat art. 125p Sv door de wetgever is bedoeld voor de gevallen waarin de zelfregulering binnen de bedrijfstak tekortschiet.[289] In de gevallen waarin de NTD-gedragscode niet afdoende is voor de verwijdering van de gegevens, kan de officier van justitie gebruik maken van de bevoegdheid van artikel 125p Sv. De bevoegdheid is dus vooral van belang in die gevallen waarin de aanbieder van een communicatiedienst niet bereid is op basis van de NTD-gedragscode de gegevens ontoegankelijk te maken. Dat zal mogelijk het geval kunnen zijn in (uitzonderlijke) gevallen waarin de officier van justitie en de provider van mening zouden (blijven) verschillen over de vraag of bij het ontoegankelijk maken de vrijheid van meningsuiting in het geding is. In de expertinterviews werd als voorbeeld gegeven dat 125p Sv gebruikt wordt wanneer het gaat om georganiseerde misdaad waarbij de hosting provider zelf ook betrokken is en een Notice and Takedown-procedure sowieso geen zin zou hebben. Belangrijker is echter dat het bevel ook kan worden gericht tot aanbieders van een communicatiedienst die de NTD-gedragscode niet hebben ondertekend. Daaronder zouden kunnen vallen hosting providers en beheerders van een website.

285 Wetsvoorstel Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 96
286 Een geldboete van maximaal € 3350.
287 Wet van 27 juni 2018, *Stb*. 2018, 322
288 Zie ook par. 4.a.i en 4.a.iii voor een bespreking van de NTD-gedragscode.
289 Wetsvoorstel Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 57.

ii. Samenloop met civiel recht

Uit het bovenstaande volgt dat het stellen van de eis dat slachtoffers eerst aangifte moeten doen vooral een drempel opwerpt. Aan de aangifte zijn verder geen civiel- of bestuursrechtelijke consequenties verbonden en het slachtoffer heeft geen formele positie in het strafproces, op de mogelijkheid om zich te voegen als benadeelde partij na. De eventuele toegevoegde waarde van een strafrechtelijke route in het kader van de problematiek als in dit onderzoek aan de orde, is lastig te bepalen. Als een aangifte resulteert in opsporing en vervolging en uiteindelijk in een strafrechtelijke veroordeling voor een bepaald feit, dan levert dit dwingend bewijs op ten aanzien van de *feiten* in civiele procedures (art. 161 Rv) – maar er kan nog steeds tegenbewijs worden geleverd. De civielrechtelijke rechtsgevolgen staan voorts ter beoordeling van de civiele rechter. Reeds hierom ligt het niet voor de hand om een koppeling te maken tussen het doen van aangifte door het slachtoffer en het toewijzen van een verwijderverzoek door de rechter.

Door de inzet van opsporingsbevoegdheden zouden politie en justitie wel een rol kunnen spelen bij het identificeren van de dader en het vergaren van bewijs. De vraag is echter of dit de (primaire) functie van het strafrechtapparaat zou moeten zijn en zo ja, of het voor de hand ligt dat politie en justitie optreden als eerste aanspreekpunt voor slachtoffers die in eerste instantie met name behoefte hebben aan informatie, advies en een laagdrempelige procedure.

iii. Evaluatie en knelpunten

Het strafrecht biedt geen geschikte route voor burgers om onrechtmatige of strafbare informatie offline te krijgen. Een strafrechtelijk onderzoek is daar niet (primair) op gericht, voor zover een aangifte daar al aanleiding toe geeft. Een aangifte als zodanig is niet meer dan bewijs van een melding aan de politie van een vermeend strafbaar feit. Een aangifte verplicht politie en justitie ook niet om de zaak op te pakken. Dat hangt mede af van de prioriteit die eraan wordt gegeven en welke aanknopingspunten er zijn voor eventueel vervolgonderzoek. Burgers hebben bovendien geen invloed op de inzet van opsporingsbevoegdheden. En zelfs als een en ander resulteert in een strafrechtelijke veroordeling, staan de civielrechtelijke rechtsgevolgen daarvan ter beoordeling van de civiele rechter.

De bevoegdheid van de officier van justitie op grond van art. 125p Sv om, met een machtiging van de rechter-commissaris, de aanbieder van een communicatiedienst te bevelen informatie ontoegankelijk te maken, kan alleen worden ingezet bij verdenking van een misdrijf als bedoeld in art. 67 lid 1 Sv. Deze bevoegdheid wordt in de praktijk nog niet of nauwelijks gebruikt. In plaats daarvan kiezen politie en justitie vaak voor de informele route van Notice and Takedown, omdat dit simpeler en sneller is. Anders dan bij art. 125p Sv vindt er geen toetsing door een onafhankelijke en onpartijdige instantie plaats. Dat kan problematisch zijn vanuit het oogpunt van rechtsstatelijkheid en de waarborgen die voortvloeien uit het EVRM.

E. Conclusie

In dit hoofdstuk zijn de verschillende beschikbare (juridische) routes beschreven voor het verwijderd krijgen van onrechtmatige online content: Notice and Takedown, civielrechtelijke procedures, bestuursrechtelijke procedures en via het strafrecht. Voor deze routes zijn diverse knelpunten geconstateerd en geëvalueerd, in het bijzonder qua doorlooptijd, complexiteit, doeltreffendheid en (een gebrek aan) waarborgen van procedurele en fundamentele rechten.

Ten aanzien van het strafrecht geldt specifiek dat de eventuele toegevoegde waarde in het kader van de onderzochte problematiek lastig te bepalen is; daarover meer in het volgende hoofdstuk. Voor de overige routes zal de knelpuntenanalyse zichtbaar worden gemaakt aan de hand van een matrix. In dat hoofdstuk zal ook de koppeling worden gemaakt met de maatschappelijke behoefte zoals die uit hoofdstuk 2 naar voren komt.

5. Knelpuntenanalyse en oplossingsrichtingen

Voortbouwend op de probleemanalyse in hoofdstuk 2, de grondrechtelijke en internationale context in hoofdstuk 3 en de uiteenzetting van de verschillende procedurele routes in hoofdstuk 4 zal nu geanalyseerd worden in hoeverre de bestaande juridische voorzieningen adequaat zijn. Allereerst worden de verschillende procedures geëvalueerd aan de hand van criteria ontleend aan de voorgaande analyses. Vervolgens zullen mogelijke oplossingen bij de Notice and Takedown-procedure, het civielrecht, het strafrecht, het bestuursrecht, de informatievoorziening en het toezicht voor de geïdentificeerde problemen besproken worden.

A. Knelpuntenanalyse

In het voorgaande zijn de bestaande buitengerechtelijke, civiel- en bestuursrechtelijke procedures om onrechtmatige inhoud te verwijderen besproken. Concreet zijn dat de bodemprocedure (civiel en kanton), het kort geding, de verzoekschriftprocedure, de klachtprocedure bij de AP, de inzet van individuele rechten uit de AVG en de klachtenprocedure bij een internetdienst. Daarnaast is aandacht besteed aan de ex parte-procedure op grond van art. 1019e Rv en de relatie tot het strafrecht. Deze procedures bieden verschillende voor- en nadelen, zoals de evaluatie aan het slot van elke paragraaf laat zien.

i. Analyse procedurele routes

Voortbouwend op de besproken problematiek rond toegang tot het recht, het normatieve kader van artikel 6, 8 en 10 EVRM en de ervaringen van mensen met onrechtmatige online inhoud worden de procedures op de volgende criteria beoordeeld: doorlooptijd, drempels om te procederen uitgesplitst in kosten en complexiteit, procedurele waarborgen, waarborgen voor de vrijheid van meningsuiting, doeltreffendheid en capaciteit/schaalbaarheid.

De criteria doorlooptijd en doeltreffendheid, alsmede de kosten van een procedure en complexiteit als drempels om te procederen, zijn ontleend aan studies over de toegang tot recht in het algemeen.[290] Ook komen deze criteria tot uitdrukking in de onderzoeksvragen die ten grondslag liggen aan dit onderzoek. De criteria die zien op de procedurele waarborgen en de waarborgen voor de vrijheid van meningsuiting zijn direct ontleend aan respectievelijk het fundamentele recht op een eerlijk proces en het de vrijheid van meningsuiting.[291] Deze grondrechtelijke inbedding wordt ook direct genoemd in de onderzoeksvragen. Ten slotte is het laatste criterium, dat ziet op de capaciteit die een procedure heeft en de mogelijkheden tot opschaling, ontleend aan de expertinterviews. Hieruit kwam duidelijk naar voren dat de enorme hoeveelheid potentieel onrechtmatige online content een belangrijke, en specifieke, eigenschap is van deze problematiek. Een mogelijk procedure zou hierop berekend moeten zijn.[292]

De doorlooptijd refereert aan het tijdsverloop tussen de start van de procedure en de uiteindelijke verwijdering van de onrechtmatige inhoud. Dit criterium is van bijzonder belang gezien de onderzoeksvraag en gezien het feit dat in veel situaties de schade voor de benadeelde groter wordt naar mate de inhoud langer online staat. Een factor hierbij is de handhaving/tenuitvoerlegging van een bestuurlijk besluit (met

290 Zie 2.d. toegang tot recht voor een uiteenzetting van deze literatuur, specifiek FRA 2011, p. 38. Europees Parlement 2017, p. 10-11. Ter Voert & Klein Haarhuis 2014, p. 12 en p. 98.
291 Zie 3.a. voor een uiteenzetting van het grondwettelijk kader en de vereisten die daaruit voortvloeien.
292 Zie annex iii en iv voor een lijst van de geïnterviewden en een indicatie van de interviewvragen.

oplegging van een sanctie, zoals een last onder dwangsom) of een rechterlijke uitspraak (executie door een deurwaarder). Er kan enige tijd overheen gaan voordat, al dan niet vrijwillig, gehoor wordt gegeven aan een bevel om bepaalde content te verwijderen.

Bij de drempel kosten gaat het om de kosten die verbonden zijn aan de procedure, zoals griffierecht en het aanzoeken van professionele rechtshulp (bijvoorbeeld het inschakelen van een advocaat bij verplichte procesvertegenwoordiging).

Bij de drempel complexiteit gaat het specifiek om de toegankelijkheid van informatie en de materiële en procedurele regels die in de procedure van toepassing zijn. Dit hangt samen met de vraag of het mogelijk is om de procedure zelfstandig te voeren, dus zonder professionele rechtshulp.

Het criterium van procedurele waarborgen is ingestoken vanuit het perspectief van de benadeelde. Concreet gaat het er om of er waarborgen zijn die verzekeren dat de klacht daadwerkelijk inhoudelijk behandeld wordt, of de criteria en de procedure transparant en openbaar zijn, of de beslissing voldoende gemotiveerd wordt en of de benadeelde gehoord wordt.

Bij "waarborgen vrijheid van meningsuiting" gaat het om waarborgen vanuit het perspectief van de verdachte/verweerder en, meer in zijn algemeen, het belang van mensen toegang te hebben tot rechtmatige informatie op internet. Bezien wordt of er in de betreffende procedure voldoende aandacht wordt besteed aan zijn belangen en of het recht op vrijheid van meningsuiting voldoende wordt afgewogen bij de uiteindelijke beslissing. Een civiele procedure zal mogelijk (alleen) aangespannen worden tegen de internetprovider, waarbij degene die de content heeft geplaatst geen partij is.

Het doeltreffendheidscriterium ziet op in hoeverre de maatregelen die bij een procedure ingezet kunnen worden, daadwerkelijk het gewenste resultaat bereiken, of dat de onrechtmatige inhoud na inzet van deze mogelijke middelen niet definitief verwijderd is. De vraag is dus in hoeverre bij de keuze voor deze route er een goede garantie is dat de route tot verwijdering zal leiden.

Ten slotte verwijst capaciteit/schaalbaarheid naar de mogelijkheid die een specifieke route biedt om de procedures op (grote) schaal uit te voeren. Eén van de kenmerkende aspecten van de problematiek van onrechtmatige online content is dat het zich op grote schaal voordoet, zowel in de zin dat de content zich zeer wijd kan verspreiden maar ook in de zin dat de hoeveelheid onrechtmatige online content zeer groot is.

Deze criteria konden toegepast worden op de verschillende procedures op basis van de uiteenzetting en analyse van de verschillende procedurele mogelijkheden tot verwijdering van onrechtmatige content.[293] De toepassing van deze criteria op de verschillende procedures levert het beeld op in figuur 6 (pagina 82).

Bij de bodemprocedure, de verzoekschriftprocedure en de klachtenprocedure bij de AP zijn de doorlooptijden te lang om bij deze procedures in zijn algemeenheid te kunnen spreken van een adequate route voor de snelle verwijdering van onrechtmatige online inhoud. Hoewel een kort geding in twee weken afgerond kan zijn, is dit mogelijk te lang als het gaat om gevoelig online materiaal dat in de tussentijd verder verspreid kan worden. Een spoed kort geding of versnelde behandeling in de verzoekschriftprocedure zou hier mogelijk een uitkomst kunnen bieden, hoewel de grote hoeveelheid potentiële zaken dan wellicht een te groot beslag zou leggen op de rechterlijke macht.

293 Zie hoofdstuk 4.

Bij de vier civielrechtelijke procedures (de bodemprocedure, verzoekschrift, kort geding en de ex parte-procedure) ligt vervolgens de drempel voor gebruik van deze procedures erg hoog wat betreft de kosten. Er moet namelijk griffiegeld betaald worden en in de meeste gevallen is procesvertegenwoordiging ook verplicht wat financieel een zware last kan zijn.

Ook de drempel wat betreft de complexiteit van de procedure ligt vrij hoog bij de vier civielrechtelijke procedures. Voornamelijk in de bodemprocedure zijn de bewijs- en procesvoorschriften zeer technisch en is het vaak niet mogelijk zonder vertegenwoordiging te procederen. De bewijsregels bij het kort geding en de ex parte-procedure zijn aanzienlijk eenvoudiger, hoewel dit voor een niet-jurist ook nog een uitdaging kan zijn.

Daarnaast zijn er bij klachten bij de AP, de individuele AVG-rechten en klachten bij de internetdienst onvoldoende procedurele waarborgen voor de benadeelde. In deze procedures zijn de AP en de desbetreffende internetdienst/verantwoordelijke niet verplicht om de klacht daadwerkelijk in behandeling te nemen of om de klager te horen. Wel bestaan in het latere traject bij de AP voldoende waarborgen in de vorm van de mogelijkheid in bezwaar te gaan en uiteindelijk de bestuursrechter. Het probleem zit echter in de eerste fase, van het indienen van de klacht tot het besluit. De AP is hier niet verplicht de klacht op te pakken, kan hier veel tijd overheen laten gaan en uit het prioriteringsbeleid blijkt dat de kans zeer groot is dat een klacht niet inhoudelijk behandeld zal worden. In deze fase ontbreken daarom de procedurele waarborgen. Daarnaast hoeft de internetdienst, als die besluit te reageren, zich bij de inrichting van de procedure en de inhoudelijke behandeling van de klacht in beginsel aan geen enkel procedureel voorschrift te houden. De buitenrechtelijke Notice and Takedown-procedure bij een internetdienst is in elk geval de meest laagdrempelige voorziening, maar benadeelden zijn bij deze mogelijkheid tot op heden erg overgeleverd aan het specifieke beleid en handelen van de betreffende dienst. Dit beleid en handelen is in Nederland voor het soort onrechtmatige inhoud waar deze studie zich op richt, minimaal wettelijk gereguleerd.

Vervolgens zijn er duidelijke nadelen en gebreken voor de bescherming van de vrijheid van meningsuiting van de verweerder/verdachte bij de ex parte-procedure, de individuele rechten uit de AVG, de klachtenprocedure bij de AP en de klachtenprocedure bij de internetdiensten. De individuele AVG-rechten en de klachten bij de internetdienst hebben het nadeel dat de afweging en uiteindelijke beslissing over het wel of niet verwijderen van vermeende onrechtmatige inhoud bij de internetdienst liggen. Deze private partijen hebben niet steeds de benodigde expertise en kennis om een juist oordeel te vellen en zijn bij deze beslissingen ook niet (duidelijk) verplicht de vrijheid van meningsuiting goed af te wegen. Met betrekking tot de ex parte-procedure geldt dat hier het perspectief van de wederpartij onvoldoende mee wordt genomen omdat hij niet gehoord wordt, hoewel de rechter wel geacht wordt zijn belangen mee te wegen in de beslissing.

Wat betreft de doeltreffendheid zijn de individuele AVG-rechten, de ex parte-procedure, de AP-klachtenprocedure en de Notice and Takedown-procedures niet altijd doeltreffend. Er is bij alle vier de procedures namelijk geen afdoende garantie dat onrechtmatige inhoud ook daadwerkelijk verwijderd wordt. Bij de AVG-rechten en de ex parte procedure is dit het geval omdat het tijdelijke of niet-definitieve maatregelen zijn.
Hoewel een kort geding vonnis niet in gezag van gewijsde gaat, volgt veelal geen bodemprocedure en blijft de voorlopige voorziening in stand. De Notice and Takedown en klachtprocedure bij de AP zijn in veel gevallen onvoldoende doeltreffend nu de klachten vaak niet opgepakt worden en in het geheel geen of niet afdoende actie volgt. Daarbij biedt de Notice and Takedown-procedure zelf geen escalatiemogelijkheid. Er is bijvoorbeeld veelal geen interne mogelijkheid tot beroep. Daarvoor moet iemand zich tot een formele juridische procedure wenden.

Ten slotte blijkt dat de Notice and Takedown-procedure schaalbaar is. Omdat de procedure wordt uitge-

voerd door de internetdienst zelf, veelal geautomatiseerd wordt uitgevoerd en de internetdienst niet verplicht is zich te houden aan fundamenteelrechtelijke waarborgen kan de procedure relatief gemakkelijk op grote schaal uitgevoerd worden. Ook de uitoefening van de AVG-rechten is schaalbaar nu het ook direct bij de dienst, de verantwoordelijke, zelf is belegd. De klachtenprocedure bij de AP en de ex parte procedure zouden schaalbaar kunnen zijn wanneer daar de middelen voor worden vrijgemaakt.[294] De andere civiele procedures, de bodemprocedure, verzoekschriftprocedure en het kort geding zijn daarentegen niet schaalbaar nu het een uitgebreide weging van de rechter vergt en de noodzakelijke procedurele waarborgen tijd en energie kosten.

Wanneer de figuur in zijn geheel wordt bekeken, wordt zichtbaar waar bepaalde afwegingen moeten worden gemaakt. Er lijken enerzijds procedurele routes te zijn die snel, laagdrempelig en schaalbaar zijn, en anderzijds procedures die voldoende rechtstatelijke waarborgen bieden. Een combinatie van al deze kwaliteiten in één procedure lijkt uitgesloten.

	Schaalbaarheid	Doorlooptijd	Drempelkosten	Drempel complexiteit	Proceswaarborg	VvMU waarborg	Doeltreffendheid
Civielrecht							
Bodemprocedure							
Verzoekschrift							
Kort geding							
Ex parte							
Bestuursrecht							
Klacht AP							
AVG rechten							
Buiten juridisch							
Notice & Takedown							

Rood: de procedure scoort niet goed op het criterium.
Oranje: de procedure scoort niet goed maar ook niet slecht op het criterium.
Groen: de procedure scoort goed op het criterium.

Figuur 6

ii. Koppeling maatschappelijke behoefte

In het voorgaande zijn zeven verschillende procedures om onrechtmatige online content te verwijderen geanalyseerd aan de hand van zeven criteria. Dit biedt inzicht in het algemeen functioneren van de procedures en de verhouding tussen de verschillende eigenschappen. Dit op zichzelf is, echter, onvoldoende om te kunnen beoordelen in hoeverre deze procedures, vanuit het perspectief van degene die met de onrechtmatige content geconfronteerd wordt, effectief en adequaat zijn met het oog op verwijdering van de content. Daarvoor is noodzakelijk om de bovenstaande knelpuntenanalyse te koppelen aan de geïdentificeerde struikelblokken. Op deze wijze kan zichtbaar gemaakt worden welke struikelblokken al toereikend geadresseerd worden door de huidige procedures en waar nog mogelijke ruimte voor verbetering bestaat. Naast elkaar geplaatst zijn de procedurele knelpunten en de struikelblokken.

294 Zie respectievelijk 4.d en 4.c.

Procedurele Knelpunten
Doorlooptijd
Kosten
Complexiteit
Waarborgen VvMU
Waarborgen slachtoffer
Doeltreffendheid
Schaalbaarheid

Figuur 7

Individuele struikelblokken
Bekendheid & bereikbaarheid dienst
Type onrechtmatige content
Type internetdienst
Mate van vereiste specialistische kennis
Terugkomende content
Persoonlijke omstandigheden
Toegang tot de rechter

Figuur 8

Uit de eerdere analyse van de maatschappelijke behoefte in hoofdstuk 2 bleek dat een viertal van de hierboven uiteengezette individuele struikelblokken bredere problematiek vormen die een eigen oplossingsbenadering behoeven. De geanalyseerde procedures op zichzelf bieden geen soelaas voor deze struikelblokken. Dit wordt voor deze vier struikelblokken kort toegelicht.

Ten eerste is de problematiek verbonden met het struikelblok **toegang tot de rechter** met geen van deze procedures op zichzelf (volledig) weggenomen. De toegang tot de rechter, geplaatst binnen de bredere problematiek van toegang tot het recht, vergt een brede verscheidenheid aan samenhangende maatregelen, van gesubsidieerde rechtsbijstand tot het verkorten van de doorlooptijd van rechterlijke procedures. Het vinden van een integrale oplossing voor dit probleem gaat de scope van dit onderzoek te buiten. Wel wordt dit struikelblok expliciet meegenomen in de verschillende oplossingsrichtingen die in het vervolg van dit hoofdstuk besproken zullen worden.

Ook voor de verschillende **persoonlijke omstandigheden** van een persoon die geconfronteerd wordt met onrechtmatige online content, geldt dat de zeven besproken procedurele routes geen sluitende oplossing bieden. Wel biedt de Notice and Takedown-procedure een zeer laagdrempelige mogelijkheid om, zonder het in de openbaarheid treden of bijvoorbeeld het betrekken van ouders, wel online content te verwijderen. Echter, in de situaties waar de internetdienst niet bereid is de content te verwijderen bieden de andere procedures geen (relatieve) anonimiteit. De wijze waarop persoonlijke omstandigheden zoals schaamte, angst voor de reactie van de sociale omgeving of afhankelijkheid van ouders een rol kunnen spelen in iemands bereidheid en mogelijkheden stappen te ondernemen, speelt breder dan slechts de problematiek van onrechtmatige online content. Een algehele oplossing kan hier dan ook niet geboden worden. Wel wordt bij de oplossingsrichting stilgestaan bij manieren waarop deze problematiek daar terugkomt en het op procedureel vlak voor een individu makkelijker gemaakt kan worden wel stappen te ondernemen ondanks dit soort persoonlijke omstandigheden.

Het probleem van steeds **terugkomende content** en het zogeheten Streisandeffect is nauw verbonden met de decentrale structuur van het internet. Een verwijdering als uitkomst van een Notice and Takedown-procedure heeft betrekking op geïndividualiseerde content die op een specifieke plek staat. Wanneer na verwijdering de content, al dan niet in enigszins aangepaste vorm, op een andere plek of opnieuw op dezelfde plek terugkomt, moet de Notice and Takedown-procedure opnieuw doorlopen worden. Hetzelfde geldt voor de verschillende juridische procedures. Een civiele uitspraak heeft immers slechts bindende kracht tussen de partijen. Wanneer de content op een andere website terugkomt, zou in theorie een nieuwe procedure gestart moeten worden.

Ook het struikelblok dat het verwijderd krijgen van onrechtmatige online content veelal **specialistische kennis** vereist en dat in veel gevallen mensen moeite hebben met het vinden van de juiste procedurele route, wordt niet weggenomen door de zeven besproken procedures. Dit probleem zit in belangrijke mate niet zozeer in de procedures zelf en meer in de informatievoorziening over en de bijstand bij deze

procedures. Bij de oplossingsrichtingen 'informatievoorziening' en 'toezichthouder' wordt nader stilgestaan bij hoe dit struikelblok daar mogelijk verminderd kan worden.

De relevante configuraties van de overige drie struikelblokken – type dienst, type onrechtmatigheid en onbekendheid/onbereikbaarheid van de dienst of degene die de uiting doet – zijn in de vier modelgevallen gevat. Per modelgeval zal hierna worden bekeken in hoeverre de verschillende procedures een oplossing bieden.

- **Modelgeval 1: Belediging op Twitter**
  In dit scenario was de onrechtmatigheid niet gemakkelijk vast te stellen maar is de internetdienst wel bekend en bereikbaar.

  Het is waarschijnlijk dat de internetdienst niet bereid is de content te verwijderen in een Notice and Takedown-procedure, omdat de onrechtmatigheid zeer moeilijk vast te stellen is. De bestuursrechtelijke routes vallen af nu er geen sprake is van onrechtmatige verwerking van persoonsgegevens. Hetzelfde geldt voor de verzoekschriftprocedure op grond van de AVG. Wat resteert, zijn de bodemprocedure en het kort geding. Gezien de doorlooptijden ligt een kort geding hier het meest voor de hand. Hierbij moet wel opgemerkt worden dat dit aanzienlijke kosten meebrengt, het een zeer complexe procedure kan zijn en de doorlooptijd nog steeds in de weken kan lopen.

- **Modelgeval 2: Bedreiging op YouTube**
  Hier is de onrechtmatigheid relatief gemakkelijk vast te stellen en is de internetdienst bekend en bereikbaar.

  De grotere sociale media platformen zoals YouTube en andere internetdiensten met voldoende capaciteit zullen dit type onrechtmatige content of uit zichzelf of in een Notice and Takedown-procedure verwijderen. Wanneer dit gebeurt, is de onrechtmatige online content snel en vaak ook effectief verwijderd. In de gevallen wanneer een internetdienst niet bereid is de content te verwijderen, is iemand aangewezen op de formele juridische procedures. Het bestuursrecht biedt geen mogelijkheden nu het geen AVG-zaak is. Het civiele recht biedt een stok achter de deur, maar ook hier zijn er procedurele drempels.

- **Modelgeval 3: Persoonsgegevens op zelfstandige website**
  In deze situatie wordt onrechtmatige content geplaatst op een internetdienst die in meer of mindere mate onbereikbaar is.

  De bereikbaarheid van de internetdienst is bepalend voor de mogelijkheden die iemand die met deze onrechtmatige content geconfronteerd wordt, ter beschikking heeft. Wanneer de dienst onbereikbaar is, omdat deze bijvoorbeeld buiten de EU gevestigd is of onbekend is, en de politie en AP geen bijzondere prioriteit geven aan deze zaak, staan het individu nagenoeg geen juridische mogelijkheden ter beschikking. De Notice and Takedown-procedure en individuele AVG-rechten zullen geen resultaat opleveren wanneer de dienst onbereikbaar is en civielrechtelijke procedures kunnen niet gestart worden wanneer de tegenpartij onbekend of onbereikbaar is. Hoewel, afhankelijk van de ernst van de onrechtmatige content en of er een publiek figuur betrokken is, zijn er escalatiemogelijkheden denkbaar. Wanneer de AP of de politie prioriteit

geven aan de zaak, kunnen zij verregaande opsporingsbevoegdheden inzetten, rechtshulpverzoeken instellen, overgaan tot internationale coördinatie of druk uitoefenen wat meer resultaat op zal leveren dan het individu in de regel zelfstandig zal kunnen bereiken.

- **Modelgeval 4: Naaktfoto's verspreid via WhatsApp**
  Hoewel de onrechtmatigheid hier relatief gemakkelijk vast te stellen is, is het technisch onmogelijk voor derden of de internetdienst zelf om de content te verwijderen. De mogelijkheden hangen dan af van de vraag of degene die de uiting doe, bekend en bereikbaar is.

  Omdat het technisch onmogelijk is voor de internetdienst om de content te verwijderen, valt de Notice and Takedown-procedure, samen met alle andere juridische procedures gericht tegen de internetdienst, af als optie. Wanneer degene die de content verspreidt wel bekend en bereikbaar is, vormt deze het enige mogelijke aanspreekpunt. De verschillende civielrechtelijke procedures kunnen ingezet worden om deze persoon te gelasten de content te verwijderen. Ook zou de klachtenprocedure ingezet kunnen worden, hoewel dit gezien de vaak lange doorlooptijd niet effectief kan zijn. Wanneer degene die de onrechtmatige content plaatste niet aangesproken kan worden omdat deze onbekend of onbereikbaar is, kan de content niet verwijderd worden. De internetdienst kan slechts de gebruiker blokkeren.

Uit het voorgaande blijkt dat de huidige procedures in bepaalde situaties een adequate voorziening voor het verwijderen van onrechtmatige content bieden, maar dat een aantal struikelblokken onopgelost blijft. Zo worden in modelgeval 2, wanneer de onrechtmatigheid relatief gemakkelijk vast te stellen is en de internetdienst bereikbaar, vaak afdoende oplossingen geboden door de bestaande routes, in het bijzonder Notice and Takedown. De drempels om daadwerkelijk gebruik te maken van de beschikbare juridische procedures kunnen echter nog steeds hoog zijn. Dit hangt samen met de (overstijgende) problematiek van toegang tot de rechter. In modelgeval 3 en 4 komen situaties voor waar degene die hiermee te maken krijgt, überhaupt niet in staat zal zijn de content te (doen) verwijderen. Een en ander kan als volgt worden samengevat:

1. Wanneer de internetdienst bekend is maar de onrechtmatigheid van content moeilijk vast te stellen is, of wanneer de dienst de content niet vrijwillig wil verwijderen (zonder rechterlijk bevel), moet er een juridische procedure gestart worden die lang kan duren, complex is en kostbaar kan zijn (Modelgeval 1);

2. Dit geldt ook in andere situaties waar de internetdienst niet zonder meer bereid is om de content te verwijderen (zie Modelgeval 2) – de ex parte-procedure staat op dit moment (nog) niet open voor het type onrechtmatige content waar het in dit onderzoek om gaat;

3. De internetdienst of degene die de uiting doet, is onbekend, onbereikbaar of geeft geen gehoor (Modelgeval 3), in welk geval de benadeelde partij met lege handen staat of mogelijk verder geholpen wordt door de politie (ingeval van illegale content) of de AP (ingeval AVG-schendingen) afhankelijk van de ernst van de situatie en het prioriteringsbeleid/ discretionaire bevoegdheid van deze instanties;

4. Het kan zeer moeizaam zijn content verwijderd te krijgen van een gesloten internetdienst. Degene die de onrechtmatige content verspreidt, moet dan in een formeel juridische procedure aangesproken worden, anders kan de content niet (blijvend) verwijderd worden (Modelgeval 4).

B. Notice and Takedown

De Notice and Takedown-procedures van de internetdiensten zelf vormen de meest laagdrempelige en effectieve manier om onrechtmatige content te verwijderen. Echter, uit de eerdere analyse bleken er een groot aantal haken en ogen aan de procedure te zitten. Zo is onduidelijk hoe de procedures exact functioneren omdat de internetdiensten wisselende en incomplete data publiceren.[295] Vervolgens blijkt uit de survey dat Nederlanders overwegend onbekend zijn met de procedure en deze ook niet vaak gebruiken.

Verder blijkt uit de koppeling met de maatschappelijke behoefte (de modelgevallen) dat de Notice and Takedown-procedure alleen onder specifieke omstandigheden effectief is. De Notice and Takedown-procedure is alleen een goede procedure voor het verwijderen van onrechtmatige online content in de situatie waarin zowel (i) de onrechtmatigheid relatief gemakkelijk vast te stellen is als (ii) de dienst bekend is. Deze situatie is weergegeven in modelgeval 2. De procedure werkt niet goed in de andere drie modelgevallen. Bij modelgeval 1, waar de onrechtmatigheid zeer moeilijk vast te stellen is en de internetdienst die afweging niet zelf wil of kan maken, bleek iemand aangewezen op een juridische procedure. Deze situatie kan ook niet zonder meer opgelost worden binnen een Notice and Takedown-procedure omdat de internetdienst als private partij in dit soort moeilijke gevallen ook niet de aangewezen partij is om deze complexe beslissingen te nemen over de invulling van de vrijheid van meningsuiting. Een (aangepaste vorm van) een civiele procedure is in de situatie van modelgeval 1 ook gewenst vanuit grondrechtelijk perspectief. Een andere situatie waarin de Notice and Takedown-procedure niet werkt, vervat in modelgeval 3, is wanneer de internetdienst onbereikbaar is, zelf onderdeel van het probleem vormt (bij bijvoorbeeld malafide websites) of in zijn geheel weigert mee te werken. Ook dan is iemand aangewezen op formele procedures. Ten slotte geldt de Notice and Takedown-procedure alleen voor hostingproviders. Mere conduit diensten, of directe communicatiediensten, bieden geen Notice and Takedown-procedure aan. Dit komt door zowel verschillen in het juridisch kader waar de diensten onder vallen, als ook vaak vanwege technische onmogelijkheid bij bijvoorbeeld *end-to-end* encryptie.[296] Deze situatie is gevat in modelgeval 4, waar de Notice and Takedown-procedure ook geen soelaas bood.

Uit de knelpuntenanalyse blijkt, vervolgens, dat één van de grootste problemen van de Notice and Takedown-procedure zit in de afwezigheid van rechtstatelijke en grondrechtelijke waarborgen. Dit is des te meer problematisch gezien de belangrijke rol die deze laagdrempelige en relatief effectieve procedure in de praktijk speelt, en in toenemende mate zal spelen,[297] in het verwijderen van onrechtmatige online content. De internetdienst, die de Notice and Takedown-procedure zowel vormgeeft als toepast, blijft een private partij die niet zonder meer verplicht is de vrijheid van meningsuiting van zijn gebruikers te borgen.[298] Zo ontbreken waarborgen als hoor en wederhoor en voldoende aandacht voor het niet verwijderen van rechtmatige content. Parallel hieraan is het problematische gebruik van deze informele procedure door overheidsinstanties zoals de politie of het Openbaar Ministerie waarbij alle rechtstatelijke waarborgen die verbonden zijn aan de inzet van formele bevoegdheden voor het verwijderd krijgen van illegale content omzeild worden. Ook zijn er geen beroep of escalatiemogelijkheden.[299]

Er zijn verschillende methodes denkbaar om voor dit gebrek aan waarborgen te compenseren, hoewel het fundamentele probleem dat een private partij de (on)rechtmatigheid van een specifieke uiting vaststelt, niet weggenomen kan worden. Vijf oplossingsrichtingen worden hier verkend.

295 Zie hoofdstuk 4.a.
296 Zie hfst 2.b.
297 Zie 3.b.i voor een bespreking van de Digital Services Act.
298 Zie Angelopoulos 2015 voor een uitgebreide bespreking van deze problematiek.
299 Deze gebreken hebben de laatste jaren veel aandacht gekregen en zijn er verschillende initiatieven om betere beroepsmogelijkheden te creëren. Zie voor een recente bespreking Tworek e.a. 2020. Zie ook Clegg (Facebook) 2020.

Een eerste mogelijke manier is de inzet van meer onafhankelijke *trusted flaggers* voor specifieke onrechtmatige content zoals al het geval is bij online discriminatie (MiND) en beelden van seksueel misbruik van kinderen waar het EOKM deze rol vervult. Het voordeel van een dergelijke constructie is dat de inschatting van de onrechtmatigheid verlegd wordt van de internetdienst naar een gespecialiseerde en meer onafhankelijke partij. Daarmee wordt de kans vergroot op een goede afweging waarbij de vrijheid van meningsuiting gerespecteerd wordt. Een probleem is, echter, dat een trusted flagger alleen nut heeft bij voor duidelijk afgebakende en specifieke type onrechtmatige content waarbij geen uitgebreide belangenafweging gemaakt moet worden aan de hand van de context. Voor bijvoorbeeld belediging of smaad zou dit waarschijnlijk niet goed functioneren. Ook zijn veel bestaande trusted flaggers wel onafhankelijk van de internetdienst maar niet onafhankelijk ten aanzien van de content, zoals bijvoorbeeld rechthebbenden.

Een voor de hand liggende tweede oplossingsrichting om het gebrek aan waarborgen te compenseren is het verder normeren en codificeren van de Notice and Takedown-procedures. De vormgeving van deze procedures is nu immers volledig overgelaten aan de internetdiensten zelf. De enige codificatie wordt gevormd door artikel 14 e-Commerce richtlijn waarin de diensten aansprakelijk zijn voor onrechtmatige content indien zij het niet 'onverwijld' verwijderen nadat zij op de hoogte zijn van de onrechtmatigheid.[300] Het verloop van de procedure en de afwegingen die daarin gemaakt moet worden, kunnen wettelijk vastgelegd worden. Gedacht kan worden aan het vastleggen van termijnen, het bieden van een bezwaarmogelijkheid, meer transparantie, recht op terugplaatsing van de verwijderde content, het uniform en duidelijk weergeven van de procedure en het verder invullen van de afwegingen die gemaakt moeten worden door de dienst. Op deze manier kan tegemoetgekomen worden aan belangrijke waarborgen zoals hoor en wederhoor en de bescherming van rechtmatige uitingen. Ook kan wettelijk vastgelegd worden hoe en wat voor transparantie de diensten moeten bieden over het functioneren van de procedures, zodat daar meer inzicht in verkregen kan worden en toekomstig beleid of wetgeving daarop aangepast kan worden. Het verder normeren en codificeren van de Notice and Takedown-procedure zou een goede oplossing vormen voor het gebrek aan waarborgen en het gebrek aan inzicht in het functioneren van de procedures.

Naast het normeren van de Notice and Takedown-procedure kan, op de derde plaats, ook gedacht worden aan het instellen van vormen van toezicht op de naleving van deze normen. Eén van de problematische aspecten van de huidige procedures is immers dat wanneer een internetdienst niet bereid is mee te werken, de procedure volledig ineffectief is. Binnen het huidige systeem is, in dergelijke gevallen, de enige escalatiemogelijkheid het instellen van een formele juridische procedure. Maar wanneer er door een onafhankelijke toezichthouder gehandhaafd wordt op de naleving van een gecodificeerde Notice and Takedown-procedure, zou voor een individu ook deze toezichthouder een escalatiemogelijkheid bieden.

Andere EU-lidstaten zoals Frankrijk en Duitsland hebben al voor de route gekozen om de Notice and Takedown-procedure te codificeren, in respectievelijk de Avia-wet en de NetzDG. Ook het Verenigd Koninkrijk overweegt dergelijke wetgeving.[301] Zowel de Duitse NetzDG en de Britse *Online Harms bill* omvatten ook vormen van toezicht op de naleving van gecodificeerde Notice and Takedown-procedure door de internetdiensten. Nederland zou in lijn met deze ontwikkelingen ook kunnen overwegen op nationaal niveau de Notice and Takedown-procedure te normeren. Wel spelen hier drie complicerende factoren. Ten eerste moet nauwkeurig gekeken worden naar de impact die dit type wetgeving heeft op

300 Zie hfst. 2.b, 3.b.i en 4.a.
301 Zie 3.b.

de vrijheid van meningsuiting. Zowel de NetzDG als de Avia-wet hebben op dit gebied vrij stevige kritiek ontvangen.[302] Ten tweede kan Nederland in principe slechts wetgeving maken die bindend is voor

internetdiensten die in Nederland gevestigd zijn.[303] Dit is een gevolg van het 'land van oorsprong beginsel', vastgelegd in artikel 3 e-Commerce richtlijn. Nu veel internetdiensten niet in Nederland gevestigd zijn, zal die wetgeving in principe niet van toepassing zijn op deze diensten. Ten derde spelen er op EU-niveau nu grote ontwikkelingen op dit gebied. Momenteel is een nieuw wetgevingspakket in de maak, ter vervanging van de e-Commerce richtlijn, die ook beoogt Notice and Takedown-procedures te codificeren en mogelijk om toezicht mechanismen te creëren.[304] De eerste aanzet tot deze Digital Services Act is tot september 2020 in de consultatiefase.[305] Het is raadzaam om bij de ontwikkeling van nationale wetgeving rekening te houden met dergelijke ontwikkelingen op EU-niveau.

Een vierde mogelijkheid is om alternatieve of online geschilbeslechtingsprocedures te verkennen. Hierin zijn verschillende modaliteiten denkbaar.[306] Zo kan het aan de internetdiensten zelf overlaten worden (semi)onafhankelijke organisaties op te richten die een bindend oordeel kunnen geven. Gebruikers zouden bij deze organisatie in beroep kunnen gaan tegen de beslissing die uit een Notice and Takedown-procedure komt of de internetdienst kan aan deze organisatie zelf moeilijke gevallen voorleggen. Facebook heeft gekozen voor deze mogelijkheid met de oprichting van een eigen *Facebook Oversight Board*. Dit orgaan kan een onafhankelijk en bindend oordeel geven over specifieke content moderation gevallen.[307] Hoewel de *Oversight Board* in veel opzichten een verbetering vormt, zal het niet kunnen compenseren voor het gebrek aan waarborgen in specifieke gevallen nu het alleen een klein percentage aan moeilijke gevallen zal behandelen. De organisatie zou in potentie vooral waarde kunnen hebben bij het aanscherpen van de wijze waarop de gebruikersvoorwaarden van Facebook gecreëerd worden en om een podium te bieden voor gebruikers om onrecht aan te kaarten.[308]

Een ander voorbeeld van alternatieve geschilbeslechting, ontstaan middels zelfregulering, is te vinden in de domeinnaamregulering. De *International Corporation for Assigned Names and Numbers* ("**ICANN**") is een non-profit organisatie die, onder andere, grotendeels verantwoordelijk is voor de uitgifte van domeinnamen wereldwijd.[309] Geschillen over een domeinnaam kunnen, afhankelijk van het type domeinnaam, worden beslecht in de *Uniform Domain Name Dispute Resolution Policy* gecreëerd door ICANN zelf of de procedure van de *World Intellectual Property Organisation*.[310] Deze vormen van alternatieve geschilbeslechting functioneren al jaren naar (relatieve) tevredenheid.[311] Echter, het probleem met deze vormen van alternatieve geschilbeslechting is dat deze nog steeds volledig binnen de invloedsfeer van de internetdiensten zelf vallen en het functioneren afhankelijk is van de medewerking van de internetdiensten en de betrokken personen.

Ook denkbaar is een vorm van verplichte alternatieve online geschilbeslechtingsprocedures waarbij de internetdienst en de betrokken persoon verplicht een geschil over vermeende onrechtmatige online inhoud in een geschilbeslechtingsprocedure moeten oplossen. Varianten hiervan bestaan al in het Europees consumentenrecht.[312] Vanuit het oogpunt van toegang tot de rechter zal online geschilbeslech-

302 Zie 3.b. Zie verder ook de aanbeveling van de Council of Europe 2018 waar expliciet wordt stil gestaan bij de wijze waarop staten internetdiensten kunnen reguleren.
303 Hier kan onder bepaalde voorwaarden wel van afgeweken worden, doch onder strenge voorwaarden. Zie art. 3 lid 4 Richtlijn 2000/31/EG.
304 Zie hfst 3.b.
305 Zie Europese Commissie publicatie 2020.
306 Voor een bespreking van verschillende vormen zie Tworek e.a. 2020.
307 Zie https://about.fb.com/news/2020/05/welcoming-the-oversight-board/.
308 Klonick 2020; Douek 2019.
309 Zie https://www.icann.org/get-started.
310 Zie https://www.icann.org/resources/pages/policy-2012-02-25-en en https://www.wipo.int/amc/en/domains/.
311 Sorkin 2001; Alpin 2020.
312 Loos 2015.

ting in ieder geval niet zonder meer verplicht gesteld kunnen worden voor rechtszoekenden.[313] Er doet zich nog een aantal andere moeilijkheden voor. Ten eerste zijn er juridisch-technische bezwaren. In de meeste gevallen zal voor de tenuitvoerlegging van de beslissing alsnog rechterlijk verlof nodig zijn of een gerechtelijke procedure gestart moeten worden. Daarnaast speelt jurisdictie en het land van oorsprongsbeginsel als een complicerende factor. Het zal een uitdaging vormen internetbedrijven die niet in Nederland gevestigd zijn alsnog te verplichten zich aan een dergelijke geschilbeslechtingsprocedure te onderwerpen.[314]

Verder rijst de meer fundamentele vraag in hoeverre een (verplichte) alternatieve geschilbeslechtingsprocedure daadwerkelijk voor een individu een oplossing vormt voor het snel verwijderen van onrechtmatige online content. Hiervoor is het nuttig terug te grijpen op de modelgevallen. Een geschilbeslechtingsprocedure is pas werkbaar wanneer de internetdienst bereikbaar is en ook daadwerkelijk de mogelijkheid heeft de onrechtmatige content te verwijderen. Hierdoor blijven alleen modelgeval 1 en 2 over. Bij modelgeval 2 was de onrechtmatigheid relatief gemakkelijk vast te stellen. Voor deze situaties bleek dat in de praktijk de internetdiensten zelf de onrechtmatige content snel verwijderen. In de praktijk doet zich zodoende vaak geen probleem voor en zal een alternatieve geschilbeslechtingsprocedure geen waardevolle toevoeging bieden. Daartegenover wordt in modelgeval 1 de situatie beschreven waar de onrechtmatigheid moeilijk vast te stellen is maar de dienst wel bereikbaar is. In deze gevallen is vanuit het perspectief van de vrijheid van meningsuiting een grondig, professioneel en onafhankelijk oordeel gewenst. Concreet betekent dit dat een procedure gewenst is die (nagenoeg) alle waarborgen van een rechterlijke procedure heeft. Wanneer deze eisen ook aan een alternatieve geschilbeslechtingsprocedure gesteld worden, is het maar de vraag in hoeverre het zinvol is deze aparte procedure op te tuigen. Alles bij elkaar genomen kan een vorm van (verplichte) alternatieve online geschilbeslechting een waardevolle versteviging van de Notice and Takedown-procedure zijn,[315] maar vormt het geen zinvolle oplossing voor het concrete probleem van snel onrechtmatige online content verwijderd krijgen.

Ten slotte kan ook breder worden nagedacht over de vraag of het wenselijk is het huidige systeem van de beperkte aansprakelijkheid voor de internetdiensten te handhaven. Dit systeem stimuleert namelijk dat internetdiensten reactief omgaan met onrechtmatige content terwijl dit niet in alle gevallen houdbaar is. Het gaat echter het bestek van dit onderzoek te buiten om deze mogelijkheid verder te verkennen.

Alles bij elkaar opgeteld kan de Notice and Takedown-procedure gezien worden als een laagdrempelige en vaak effectieve manier om onrechtmatige online content te verwijderen, maar met een viertal belangrijke tekortkomingen. Deze zijn dat de procedures onvoldoende transparant zijn, dat mensen onvoldoende op de hoogte zijn van de procedure, dat er een gebrek aan waarborgen is en dat de procedure slechts effectief is in bepaalde situaties. Van de verschillende oplossingsrichtingen die hierboven besproken zijn, kan van de verdere normering en codificering het meest verwacht worden. Deze ontwikkeling is al ingezet op EU-niveau en kan veel van de huidige tekortkomingen van de Notice and Takedown-procedure wegnemen. Ook kan deze codificering en verdere normering gecombineerd worden met de mogelijkheid van alternatieve geschilbeslechting en specifiek toezicht.

C. Civiele recht

i. Gefaseerde opbouw van procedurele mogelijkheden

Bovenstaande modelgevallen illustreren dat het antwoord op de vraag welke routes rechtszoekenden kunnen of moeten volgen om onrechtmatige online content verwijderd te krijgen, afhangt van diverse

313 HvJEU 18 maart 2010, ECLI:EU:C:2010:146 (*Alassini/Telecom Italia*).
314 Zie bijvoorbeeld artikel 3 Richtlijn 2000/31/EG.
315 Zie 3.b over de Digital Services Act waar voorgesteld wordt veel aspecten van de Notice and Takedown-procedure te codificeren, wat dicht bij het vormgeven van een alternatieve of online geschilbeslechtingsprocedure komt.

factoren. Een juridische procedure, zo ook een civiele procedure, geldt vrijwel altijd als laatste redmiddel of stok achter de deur, in aanmerking genomen dat er allerlei redenen kunnen zijn om af te zien van een gang naar de rechter ("ik wil anoniem blijven", "ik weet niet hoe ik het moet aanpakken", "het heeft toch geen zin", "het kost te veel tijd en moeite") – die hierboven kort zijn samengevat in vier overstijgende struikelblokken: persoonlijke omstandigheden, specialistische kennis, terugkomende content en toegang tot de rechter. Internetdiensten beschikken als professionele partijen bovendien vaak over meer kennis en middelen dan natuurlijke personen die voor het eerst met deze problematiek in aanraking komen. Nog los van de vraag of verplichte procesvertegenwoordiging noodzakelijk of wenselijk is, bestaat er een duidelijke behoefte aan informatievoorziening, advisering en rechtshulpverlening – ook in zaken die weinig complex lijken.

Uit de expertinterviews en -workshops komt duidelijk naar voren dat de oplossing voor de problematiek van onrechtmatige content niet per se gelegen is in het versnellen of vereenvoudigen van bestaande procedures. Ten eerste zijn de bestaande procedures volgens veel experts op zichzelf toereikend. Zoals de modelgevallen laten zien is onbekendheid of onbereikbaarheid van de wederpartij vooral een struikelblok, dat niet zonder meer wordt weggenomen door een snellere of simpeler procedure. Procederen voor of tegen een anonieme partij is (vooralsnog) niet mogelijk in Nederland. De drempel complexiteit hangt er bovendien mee samen dat de vaststelling van onrechtmatigheid veelal een inhoudelijke beoordeling en partijdebat vergt. Ten tweede volgt uit de knelpuntenanalyse dat snelheid en procedurele waarborgen met elkaar op gespannen voet staan. Zo ligt het, als geen sprake is van evidente onrechtmatigheid, niet direct voor de hand een ex parte-bevel te geven zonder degene die de content heeft geplaatst te horen. Ook gaat het in complexere zaken om maatwerk, wat een reden is om terughoudend te zijn met uitbreiding van de reikwijdte van de ex parte-procedure. Ten derde is capaciteit/schaalbaarheid een belangrijke factor. Meer rechtszaken leiden tot extra werklast voor de rechterlijke macht en mogelijk langere doorlooptijden. Aan de ene kant is het niet wenselijk om de behandeling en beslissing van bijvoorbeeld beledigingszaken (modelgeval 1) weg te halen bij de rechter als onafhankelijke en onpartijdige instantie in een procedure die met voldoende procedurele waarborgen is omkleed. In dergelijke gevallen bestaat het gevaar dat internetdiensten voor eigen rechter gaan spelen. Aan de andere kant kan het ook problematisch zijn als internetdiensten in twijfelgevallen een afwachtende houding aannemen en het structureel laten aankomen op een rechterlijke uitspraak.

De heterogeniteit en complexiteit van de problematiek vraagt om een gefaseerde opbouw van procedurele mogelijkheden. Als Notice and Takedown nergens toe leidt en de wederpartij bekend is, kan een benadeelde partij naar de civiele rechter stappen. Zoals volgt uit de in hoofdstuk 2 besproken surveyresultaten, zijn de doorlooptijd en complexiteit van een procedure, onbekendheid met regelgeving en financiële kosten belangrijke drempels. Bij het inrichten van een eventuele nieuwe voorziening zou allereerst moeten worden stilgestaan bij de vraag hoe deze drempels zich tot elkaar verhouden. De factor tijd kan een belangrijke reden zijn om prioriteit te geven aan snelheid, maar dat staat op gespannen voet met grondrechtelijke waarborgen (zowel procedureel als de vrijheid van meningsuiting). Tegen die achtergrond ligt het ook niet voor de hand om de oplossing te zoeken in het mogelijk maken van anoniem procederen. Het is eerder van belang om aandacht te besteden aan de vraag hoe procedures overzichtelijker en transparanter gemaakt kunnen worden, met het oog op procedurele rechtvaardigheid en de bereidheid van rechtszoekenden om naar de rechter te gaan. Daarnaast rijst de vraag of het loslaten van de eis van verplichte procesvertegenwoordiging wenselijk is: de betrokkenheid van rechtsbijstandsverleners en in het bijzonder advocaten kan juist bijdragen aan het zakelijke, professionele en effectieve verloop van procedures.

Kantonrechterskortgeding

Volgens geïnterviewden is het kort geding als zodanig toereikend: in spoedeisende gevallen kan op korte termijn een uitspraak van de rechter worden verkregen.[316] Wel zou er als gezegd kunnen worden nagedacht over het loslaten van de eis van verplichte procesvertegenwoordiging, al rijst de vraag hoe zich dat verhoudt tot het struikelblok specialistische kennis (drempel complexiteit) en of dit de werklast voor rechters niet nog verder vergroot (met het oog op doorlooptijd, capaciteit en de kwaliteit van de procesvoering).

De eis van verplichte procesvertegenwoordiging geldt niet ten overstaan van de kantonrechter. De introductie van een kantonrechterskortgeding voor deze problematiek zou een uitbreiding met zich meebrengen van de competentie van de kantonrechter. Uiteraard neemt dit de behoefte aan, en noodzaak van (toegang tot) rechtsbijstand niet weg, maar met de nodige hulp worden mensen zo in staat gesteld om in persoon te procederen.[317]

Verzoekschriftprocedure

Een alternatief is het openstellen van de verzoekschriftprocedure voor dit soort zaken, zoals nu al mogelijk is voor de uitoefening van AVG-rechten (zonder verplichte procesvertegenwoordiging) – eventueel in een versneld traject. Het zou dan gaan om een verzoek tot een rechterlijk bevel tot het verwijderen van specifieke onrechtmatige content. Zoals besproken in hoofdstuk 4, zou dit bovendien het obstakel kunnen wegnemen dat de benadeelde verantwoordelijk is voor de oproeping van de wederpartij(en).[318] Zeker als een wederpartij in het buitenland is gevestigd, kunnen problemen ontstaan met betekening van de dagvaarding. De adresgegevens van de partij in kwestie kunnen moeilijk vindbaar zijn en er gelden langere termijnen.

Het verzoek zou primair kunnen worden gericht tegen de betrokken internetdienst of website. De partij die de content heeft geplaatst, kan zich dan als belanghebbende melden. Een vervolgstap zou zijn om het mogelijk te maken dat verzoeken worden ingediend door een daarvoor aangewezen instantie of organisatie die opkomt voor de belangen van benadeelde partijen. De grote variëteit aan typen content en betrokken actoren maakt het echter lastig om op voorhand de gevallen af te bakenen die zich hiervoor lenen. Ook de verzoekschriftprocedure onder de AVG heeft een beperkte reikwijdte.[319] Voor een breder scala van zaken ligt de hierboven besproken mogelijkheid van een kantonrechterskortgeding daarom meer voor de hand, mede met het oog op snelheid.

Ex parte-procedure

Een eventuele uitbreiding van de ex parte-procedure vraagt om een duidelijke rechtvaardiging en tegelijkertijd begrenzing, omdat er geen indringende rechterlijke toets plaatsvindt en het fundamentele recht op hoor en wederhoor wordt uitgesloten. Daardoor bestaat het gevaar dat rechtmatige content te snel offline wordt gehaald, wat mede in het licht van de vrijheid van meningsuiting problematisch is. Over het algemeen is er op voorhand geen reden om de betrokken internetdienst of degene die de content heeft geplaatst, niet te horen, anders dan het belang dat is gemoeid met snelheid.

Voor het maken van een uitzondering buiten het afgebakende kader van IE-zaken zou in ieder geval voldaan moeten worden aan strenge voorwaarden. Ten eerste moet sprake zijn van een zeer spoedeisende zaak en van dreigende onherstelbare schade, zoals ook in de bestaande ex parte-procedure het

316 Een voorbeeld van een zaak waarin het ging om onrechtmatige uitingen in een besloten WhatsApp-groep en waarin binnen 2,5 uitspraak werd gedaan is te vinden in Rb. Noord-Nederland 16 september 2016, ECLI:NL:RBNO:2016:7720. Deze zaak illustreert in het bijzonder de problematiek van besloten kanalen.

317 Zie hierna ook de passage over de Tijdelijke Experimentenwet rechtspleging.

318 Zie 4.c.

319 Zie ook Molenaars en De Jong 2019, p. 222-229, aangehaald in hfst. 3, die om deze reden een kantonrechterprocedure suggereren als de standaardroute.

geval is. Ten tweede moet de aangesproken partij bekend zijn. Wanneer dat de betrokken internetdienst of website is, is van belang dat ook degene die de content heeft geplaatst, op de hoogte wordt gebracht van het bevel, zodat hij in staat is om bezwaar te maken tegen verwijdering van de content. Ten derde moet de onrechtmatigheid op voorhand evident zijn of eenvoudig zijn vast te stellen, zoals in modelgeval 2 waar het gaat om illegale (strafbare) content. Voor dergelijke gevallen is ook een strafrechtelijke aanpak mogelijk, maar het gaat er juist om, onafhankelijk daarvan, de benadeelde een instrument in handen te geven om bepaalde content snel offline te krijgen. Voor de maatstaf kan aansluiting worden gezocht bij het criterium "onmiskenbaar onrechtmatig" in de Notice and Takedown-procedure. De ex parte-procedure heeft dan vooral meerwaarde als de internetdienst of degene die de content geplaatst heeft wel bekend is, maar geen gehoor wordt gegeven aan een Notice and Takedown-verzoek. De vraag is echter hoe vaak het zich in de praktijk voordoet dat benadeelden te maken krijgen met een weigerachtige internetdienst in gevallen waar het evident gaat om onrechtmatige of strafrechtelijke inhoud.

ii. Tijdelijke Experimentenwet rechtspleging

Of bovengenoemde nieuwe routes – het kantonrechterskortgeding of een uitbreiding van de verzoekschriftprocedure dan wel ex parte-procedure – daadwerkelijk zullen leiden tot een verbetering in het licht van de geïdentificeerde knelpunten, kan alleen in de praktijk worden getest door middel van een pilot. De recent aangenomen Tijdelijke Experimentenwet rechtspleging kan hiervoor een wettelijke basis bieden.[320] Een dergelijke pilot kan ook beter zicht geven op de te verwachten toename in het aantal zaken als bovengenoemde drempels (deels) zouden worden weggenomen.

Er wordt al geëxperimenteerd in de rechtspraak op grond van art. 96 Rv, bijvoorbeeld met pilots voor de 'regelrechter' in Rotterdam en de 'wijkrechter' in Den Haag in het kader van het programma Maatschappelijk effectieve rechtspraak van de Raad voor de rechtspraak. Voorwaarde is dat partijen het geschil samen aan de kantonrechter voorleggen (art. 96 Rv). Zij kunnen hun zaak zelf aandragen met een digitaal aanmeldformulier. De kantonrechter bepaalt de wijze waarop het geding wordt gevoerd, in overleg met partijen. Kenmerkend voor deze experimenten zijn laagdrempeligheid, snelheid en oplossingsgerichtheid. Uit de evaluatie van pilots blijkt dat deze voorzien in een maatschappelijke behoefte.[321] Wel is de selectie van zaken een belangrijke randvoorwaarde, niet alleen om rechtszoekenden duidelijk te maken welke zaken geschikt zijn maar ook om de rechter een helder afwegingskader te bieden. Daarnaast is een goed functionerend bureau (met administratief en juridisch medewerkers) ter ondersteuning van de rechter essentieel, onder meer om met partijen te communiceren. De daarmee samenhangende investerings- en uitvoeringskosten hangen mede af van de gehanteerde selectiecriteria, de mate waarin rechtszoekenden hulp "aan de voorkant" wordt geboden en de procedurele inbedding, zoals de vraag of en op welke termijn een zitting moet worden gehouden en in hoeverre partijen processtukken mogen uitwisselen.

Op 23 juni 2020 is de Tijdelijke Experimentenwet rechtspleging aangenomen door de Eerste Kamer.[322] De wet, die inmiddels is gepubliceerd in het Staatsblad,[323] treedt in werking op een bij koninklijk besluit te bepalen tijdstip. De wet heeft als doel experimenten met innovatieve gerechtelijke procedures mogelijk te maken door hiervoor een wettelijke grondslag te bieden. De wet beoogt door middel van experimenten de meest effectieve procedures te onderzoeken. Bij algemene maatregel van bestuur kunnen bepalingen uit o.a. het Wetboek van Burgerlijke Rechtsvordering, de Wet op de rechterlijke organisatie en de Wet griffierechten burgerlijke zaken terzijde worden geschoven. De voorgestelde regeling wordt beoordeeld door een toetsingscommissie – die onder meer toetst of deze regeling grondrechten en fundamentele beginselen van procesrecht waarborgt – en wordt vervolgens voorgelegd aan de Eerste en Tweede Kamer

320 Zie meer uitgebreid Hoogervorst en Jahan 2020.
321 Grootelaar, Schelfhout en Duijneveldt 2020.
322 *Kamerstukken II* 2019/20, 35263, 21.
323 *Stb*. 2020, 223.

en de Raad van State. Een experiment duurt maximaal drie jaar. Het kan facultatief, vrijwillig of dwingend zijn: in dat laatste geval kunnen partijen zich niet aan de experimentele procedure onttrekken.

De Experimentenwet kan een mogelijkheid bieden om binnen het civiele recht op beperktere schaal te experimenteren met een pilot voor nieuwe procedures voor het oplossen van de problematiek van onrechtmatige online content. Daarbij zijn verschillende modaliteiten denkbaar, zoals hierboven uiteengezet, in het bijzonder een kantonrechterskortgeding of een verzoekschriftprocedure gemodelleerd naar de AVG.[324] Bij de vormgeving van het experiment zal uitdrukkelijk moeten worden stilgestaan bij de juridische, organisatorische en financiële implicaties. Met het oog op de houdbaarheid van inrichtingskeuzes kan gekeken worden naar de evaluatie van bovengenoemde pilots met de regel- en wijkrechter. Procedurele waarborgen en capaciteit verdienen in dit verband bijzondere aandacht.

Gelet op haalbaarheid en schaalbaarheid valt of staat een eventuele pilot met de afbakening tot een bepaald type zaken. Daarvoor zou bijvoorbeeld kunnen worden aangesloten bij de meest voorkomende problemen zoals die uit de survey naar voren komen: de ongewilde publicatie van privégegevens (wat deels overlapt met de AVG), seksueel beeldmateriaal en bedreiging – de laatste categorie speelt met name ook een rol in het licht van toegang tot de rechter.[325] Een ander uitgangspunt voor afbakening zou art. 67 Sv kunnen zijn: content waarvoor de bevoegdheid van art. 125p Sv kan worden ingezet, maar waar slachtoffers nu nog geen afzonderlijk instrument in handen hebben om de content offline te krijgen en waar Notice and Takedown niet altijd uitkomst biedt. Modelgeval 2 en 4 zijn hiervoor illustratief.

D. Bestuursrecht

De twee besproken bestuursrechtelijke routes, de klachtprocedure bij de AP en de uitoefening van de individuele AVG-rechten, spitsen zich beide toe op de handhaving van het gegevensbeschermingsrecht. De problematiek van onrechtmatige online content die iemand in de persoon raakt heeft daarentegen een bredere scope. Hierdoor kan slechts een deel van de mensen die geconfronteerd wordt met onrechtmatige online content gebruik maken van deze twee routes. Dit kan problemen opleveren, nu het voor mensen niet altijd even makkelijk is in te schatten waar deze grens ligt. Uit de expertinterviews bleek bijvoorbeeld dat de AP zichzelf onbevoegd acht bij smaad en dit ziet als een zaak voor het strafrecht. Dit kan het voor mensen moeilijker maken om te weten welke routes tot hun beschikking staan.

Naast dit type beperkingen in de taak van de AP spelen ook capaciteitsproblemen een rol. Door de beperkte capaciteit kan slechts een deel van de klachten die bij de AP binnenkomen daadwerkelijk behandeld worden. Om dit in goede banen te leiden heeft de AP een prioriteringsbeleid opgesteld.[326] Enerzijds laat dit veel ruimte voor de AP om de beoordeling af te stemmen op de specifieke situatie, maar anderzijds creëert dit veel onzekerheid bij het individu over in hoeverre zijn of haar klacht daadwerkelijk opgepakt wordt. Door de onduidelijkheid over de afbakening van de bevoegdheid van de AP en de onzekerheid omtrent de klachtbehandeling speelt de klachtprocedure bij de AP een beperkte rol bij de verwijdering van onrechtmatige online content die mensen in de persoon raken. Dit staat haaks op de aanzienlijke en effectieve bevoegdheden die de AP heeft om inbreuken te beëindigen en op het feit dat de AP in Nederland relatief grote bekendheid geniet. Bijna 75% van de Nederlanders is bekend met de

324 Hierin zal een keuze moeten worden gemaakt: als de verzoekschriftprocedure wordt opengesteld voor een bepaald type zaken ligt het niet voor de hand om daarnaast een kort geding toe te staan, behoudens gevallen waarin de verzoekschriftprocedure niet kan worden afgewacht. Daarbij moet bedacht worden dat in de verzoekschriftprocedure in spoedeisende gevallen om een voorlopige voorziening kan worden verzocht: vgl. Hof Amsterdam 5 november 2019, ECLI:NL:GHAMS:2019:3966.

325 Zie hfst. 2.

326 *Stct.* 2018, 54287.

AP,[327] en in 2019 werden er 27.854 klachten ingediend,[328] wat suggereert dat Nederlanders de procedure weten te vinden.

Mogelijke oplossingsrichtingen moeten gevonden worden, enerzijds, in het verbeteren van de klachtenprocedure van de AP en, anderzijds, in het verbreden van het werkgebied. Zo zou de klachtprocedure uitgebreid kunnen worden zodat deze kan uitgroeien tot één van de geëigende routes om onrechtmatige content te verwijderen. Het voordeel hiervan is dat het voor degene die geconfronteerd wordt met de onrechtmatige content, veel kan schelen in het navigeren van de verschillende stappen die tot verwijdering moeten leiden. Zo zou een toezichthouder beter kunnen inschatten welke entiteit exact aan gesproken moet worden en heeft de toezichthouder de kennis in huis om correct bewijs te vergaren en een onderzoek te starten. Bij verbeterde capaciteit heeft de AP ook meer ruimte om moeilijke zaken op te pakken waar de verantwoordelijke internetdienst ongrijpbaar is, zoals in Modelgeval 3. Verregaander is het idee dat de AP een bredere rol toebedeeld wordt wat betreft onrechtmatige online content die mensen in hun persoon raken. De problematiek ligt in het verlengde van het huidige werkgebied van de AP en persoonsgegevens spelen in nagenoeg iedere casus een centrale rol. Een dergelijke constructie zou het makkelijker maken de verschillende routes te navigeren en kan een groot aantal van de door mensen ervaren struikelblokken met betrekking tot de vereiste specialistische kennis en toegang tot de rechter verminderen.[329]

Deze twee mogelijke oplossingsrichtingen zijn, echter, niet zonder problemen. Naast het behandelen van individuele klachten, veel waarvan niet betrekking hebben op onrechtmatige content op internet, is de AP nog met tal van andere taken bedeeld die van belang zijn voor de handhaving van het gegevensbeschermingsrecht. Daarnaast heeft de AP duidelijk aangegeven onvoldoende capaciteit te hebben om het huidige klachtenbeleid naar wens uit te voeren.[330] Het uitbreiden van de klachtenprocedure lijkt met de huidige financiering en werkcapaciteit dus onrealistisch. Hetzelfde geldt uiteraard voor het uitbreiden van de rol van de AP, echter, hierbij geldt nog een additioneel probleem. De problematiek van onrechtmatige online content die mensen in de persoon raken is slecht één onderdeel van alle vormen van onrechtmatige online content. In de volle breedte omvat dit ook andere rechtsgebieden zoals het consumentenrecht, fraude of het audiovisuele mediarecht. Andere toezichthouders zoals de Autoriteit Consument & Markt (“**ACM**”) of het Commissariaat voor de Media zijn dan ook betrokken. Deze problematiek hangt allemaal met elkaar samen. Wanneer de oplossing van problemen over onrechtmatige online content die mensen in de persoon raakt, geïsoleerd en volledig bij de AP belegd wordt, zal deze samenhang uit het oog verloren worden.[331]

Daarnaast is ook stilgestaan bij de uitoefening van de individuele AVG-rechten. Deze nemen een bijzondere positie in nu zij direct tegenover de verantwoordelijke uitgeoefend worden. De knelpunten bij de handhaving van de individuele AVG-rechten komen hier ook direct uit voort. Voor de daadwerkelijke handhaving moet men zich namelijk tot de civiele rechter wenden door middel van een verzoekschriftprocedure.[332] De knelpunten van complexiteit, doorlooptijd en kosten zijn voor een deel weggenomen door dit vorm te geven als een verzoekschriftprocedure zonder verplichte procesvertegenwoordiging. Deze route is daarmee al zo vormgegeven om de uitoefening voor een individu zo laagdrempelig mogelijk te maken. Deze procedure heeft echter een beperkte reikwijdte.[333]

327 FRA 2020, p. 14.
328 Autoriteit Persoonsgegevens Jaarverslag 2019.
329 Zie verder 5.f.
330 Autoriteit Persoonsgegevens nieuwsbericht 2020; Tweede Kamer, 2018-2019, 32761, nr. 135; Tweede Kamer, 2019-2020, 020D11306.
331 Zie de sectie 5.g. ’Toezichthouder’ voor een verdere bespreking van de rol die een overkoepelende toezichthouder zou kunnen spelen.
332 Art. 15-21 AVG jo. art. 35 UAVG en art. 79 AVG.
333 Zie verder 4.c.ii.

Duidelijk is dat de AP en de klachtenprocedure een grotere rol zouden kunnen spelen in de verwijdering van onrechtmatige online content die mensen in de persoon raken. Dit zou enerzijds kunnen door het versterken van de positie van benadeelden in de klachtenprocedure en anderzijds door de AP een bredere, waaronder coördinerende rol te laten vervullen bij de aanpak van deze problematiek, in het verlengde van de taken die zij nu ook al vervult en die raken aan kwesties op het gebied van privacy en de eer en goede naam. Ongeacht de mogelijke rol die de AP kan spelen, moet een uitbreiding van de taken van de AP wel bezien worden in de bredere discussie over het gebrek aan capaciteit van de AP.

E. Strafrecht

i. Kan de strafrechtelijke procedure worden vereenvoudigd?

Via het formele strafrecht bestaat er geen mogelijkheid om strafbare informatie snel van het internet verwijderd te krijgen, terwijl dat gezien de snelheid waarmee deze informatie zich verspreidt, juist wenselijk is. De vraag is dan ook of de wettelijke voorwaarden zouden moeten worden aangepast zodat er een snelle(re) strafrechtelijke route bestaat om strafbare informatie van het internet te verwijderen of ontoegankelijk te maken. Ter beantwoording van deze vraag is een juridische analyse gemaakt (zie hoofdstuk 4) en gesproken met drie experts uit de strafrechtketen: een parketsecretaris bij het Kennis- en Expertisecentrum Cybercrime, een officier van justitie gespecialiseerd in Cybercrime en Digitaal Bewijs, en de teamleider van het Landelijk Meldpunt Internetoplichting.

Moet de machtiging van de rechter-commissaris komen te vervallen?

Voor een bevel op grond van art. 125p Sv is de machtiging van de rechter-commissaris vereist. Juist vanwege de belangen die bij een bevel tot ontoegankelijk maken in het geding zijn, en in het bijzonder de vereisten van art. 10 EVRM, is gekozen voor een voorafgaande rechterlijke machtiging. Een rechter-commissaris is bij uitstek in staat om een onpartijdige en zorgvuldige afweging tussen de verschillende belangen te maken.[334] In die gevallen waarin de NTD-gedragscode[335] geen uitweg biedt, zal het vooral gaan om gevallen waarin er een verschil van inzicht bestaat over de strafbaarheid van de gegevens. Daarbij kan de vrijheid van meningsuiting in het geding zijn. Dat vergt een zeer specialistische en casuïstische beoordeling, die in ons rechtsstelsel aan de rechter is toebedeeld. Bij de vrije meningsuiting staat bovendien het censuurverbod voorop: een uiting mag worden gedaan *totdat* deze onrechtmatig is beoordeeld, en die beoordeling is aan de rechter.[336] Juist in dat grijze gebied (wel of geen ongewenste of strafbare gegevens, wel of geen vrijheid van meningsuiting) moet eerst een rechter oordelen *voordat* content weggehaald mag worden. In het oorspronkelijke conceptwetsvoorstel Versterking Bestrijding Computercriminaliteit is door de regering getracht om het vereiste van een machtiging van de rechter-commissaris te schrappen.[337] De officier van justitie zou aldus zelfstandig het bevel hebben kunnen geven om bepaalde uitingen te verwijderen. Een dergelijke constructie zou slecht te verenigen zijn geweest met de vereisten van artikel 10 EVRM. Het voorstel stuitte echter ook op veel tegenstand in de Tweede Kamer vanwege het feit dat dit ernstig afbreuk zou doen aan de rechtswaarborgen rondom de uitingsvrijheid op het internet en onder andere deze tegenstand heeft ertoe geleid dat de voorwaarde van de machtiging van de rechter-commissaris werd behouden.[338] In de memorie van toelichting wordt de terugkeer van de rechterlijke machtiging verder gerechtvaardigd onder verwijzing naar rechtspraak van het EHRM.[339]

334 Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 58.
335 Zie par. 4.a.i.
336 Koops 2010, p. 2461-2466.
337 Oerlemans 2017.
338 Newitt 2019.
339 In het arrest van het EHRM 14 september 2010 *Sanoma/Nederland* (appl.no. 38224/03) werd – kort gezegd – geoordeeld dat bij een vordering tot uitlevering van een voorwerp waarbij het recht op bescherming van een journalistieke bron in het geding kan zijn, een wettelijke plicht moet zijn voorzien van voorafgaande toetsing door een rechter. Met de tussenkomst van de rechter-commissaris wordt hieraan voldaan (Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 58).

Het vereiste van een schriftelijk bevel en een schriftelijke machtiging

Het bevel tot ontoegankelijk maken moet voldoen aan een aantal eisen. Allereerst geldt het vereiste dat het bevel schriftelijk is, en ook de machtiging van de rechter-commissaris moet schriftelijk zijn gegeven. Omdat digitale informatie snel kan worden verspreid, kan het afwachten van een schriftelijk bevel en een schriftelijke machtiging van de rechter-commissaris te veel tijd kosten. De Nederlandse Vereniging voor Rechtspraak heeft al bij de introductie van deze bevoegdheid aangedrongen op een mondeling te geven bevel en machtiging. Daar is destijds niet voor gekozen "omdat de betekenis van een mondeling bevel en een mondelinge machtiging in de praktijk vooralsnog van onvoldoende belang wordt geacht om een dergelijke mogelijkheid in de wet op te nemen. Het bevel tot ontoegankelijk making van gegevens betreft een verstrekkende bevoegdheid waarbij de vrijheid van meningsuiting in het geding kan zijn'.[340] Bovendien zijn er nog meer procedurele waarborgen in de wet opgenomen zoals het vereiste dat degene tot wie het bevel is gericht, in de gelegenheid wordt gesteld te worden gehoord. De aanbieder tot wie het bevel is gericht, is bovendien bevoegd zich bij het horen door een raadsman te doen bijstaan. 'De mogelijkheid van een mondeling bevel lijkt niet goed te verenigen met deze procedurele eisen en aldus met een zorgvuldige procedure ter voorbereiding van het bevel'.[341] De hier beschreven argumenten die zijn gebruikt om het advies van de NVvR niet over te nemen, gelden nog onverkort.

Uitbreiding van de bevoegdheid naar alle misdrijven

Het bevel tot ontoegankelijkmaking van gegevens is beperkt tot gevallen waarin sprake is van verdenking van een misdrijf als omschreven in art. 67 lid 1 Sv en moet noodzakelijk zijn ter beëindiging of voorkomen van dit misdrijf. Onder de in de wet bedoelde misdrijven vallen bijvoorbeeld wel het zogenaamde verbod op wraakporno maar niet belediging, laster, of smaad. Om de reikwijdte van deze bevoegdheid te vergroten zou ervoor kunnen worden gekozen deze beperking op te heffen en mogelijk te maken bij een verdenking van elk misdrijf, zodat deze bevoegdheid ook kan worden ingezet bij smaad, belediging of laster.

Omdat deze bevoegdheid zal worden ingezet in gevallen waarin de vrijheid van meningsuiting vaak een rol speelt, dreigt het risico dat het Openbaar Ministerie in de rol van een censurerende internetpolitie wordt gedrongen. Dat was ook precies het argument dat de minister gebruikte nadat hij het advies van het College van procureurs-generaal met deze strekking had overgenomen.[342] Ook dit argument geldt nog onverkort.

ii. De rol van de aangifte bij een vereenvoudigde procedure

Zou de aangifte een verdergaande rol kunnen spelen dan het nu doet? De aangifte is op dit moment slechts het (mogelijke) startpunt van een strafrechtelijk onderzoek. De vraag is echter of het ook een rol kan spelen in een nieuwe privaatrechtelijke of bestuursrechtelijke voorziening voor de verwijdering van onrechtmatige of illegale inhoud. De mogelijkheid dat het doen van aangifte voldoende zou moeten zijn voor het toewijzen van een verwijderverzoek is nadrukkelijk aan de orde gesteld tijdens het parlementaire debat 'Internetpesters aangepakt' dat op 12 februari 2020 heeft plaatsgevonden in de Tweede Kamer. [343] Deze mogelijkheid miskent echter de beperkte betekenis van een aangifte in het Nederlandse

340 Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 96.

341 Ibid.

342 Computercriminaliteit III, *Kamerstukken II* 2015/16, 34 372, nr. 3, p. 56-58. In het oorspronkelijke conceptvoorstel was deze bevoegdheid mogelijk bij elk strafbaar feit.

343 Burgerinitiatief "Internetpesters aangepakt", Handelingen II, 53ste vergadering, 12 januari 2020, p. 53-4-1. In zijn antwoord geeft de minister aan dat de Hoge Raad duidelijke criteria heeft ontwikkeld voor het verstrekken van accountgegevens, zoals NAW-gegevens (HR 25 november 2005, ECLI:NL:HR:2005:AU4019). Dat zijn: 1. Platformen en providers moeten deze gegevens verstrekken als voldoende aannemelijk is dat de content onrechtmatig is jegens een slachtoffer. 2. Het slachtoffer heeft een reëel belang bij de verkrijging van de NAW-gegevens. 3. Aannemelijk is dat er in het concrete geval geen minder ingrijpende mogelijkheid bestaat om de NAW-gegevens te achterhalen. 4. De afweging van alle betrokken belangen brengt met zich mee dat dat van het slachtoffer het zwaarst weegt. De minister stelt voor deze criteria te codificeren zodat niet (altijd) gewacht hoeft te worden op een rechterlijk oordeel, dat neemt echter niet weg dat een aangifte sec voldoende zou (moeten) zijn voor het verstrekken van deze gegevens aan het slachtoffer (p. 53-4-11).

recht.[344] Het bewijs dat sprake is van een strafbaar feit zal (nog) moeten worden geleverd door het Openbaar Ministerie op basis van het onderzoek dat naar aanleiding van de aangifte is verricht door een opsporingsdienst. Het is bovendien onwenselijk om het aan de politie over te laten om te bepalen of een bepaald feit aangiftewaardig is.[345] Aan de aangifte een dergelijke betekenis verlenen maakt van de politie een censurerend orgaan, wat onwenselijk is in een democratische rechtsstaat.

Samengevat kan gesteld worden dat het strafrecht in het kader van dit onderzoek geen reële oplossingsrichting biedt. Vanuit rechtsstatelijk oogpunt is het niet wenselijk om de inzet van de bevoegdheid van art. 125p Sv te versnellen of versimpelen door de eis van een schriftelijke machtiging van de rechter-commissaris los te laten. Het geven van een grotere betekenis aan de aangifte is evenmin wenselijk, omdat het slechts een startpunt vormt van onderzoek naar vermeend illegale content en het niet aan de politie is om te bepalen welke feiten wel en niet aangiftewaardig zijn.

Verdere bevindingen of aanbevelingen over de rol van het strafrecht gaan het bestek van dit onderzoek te buiten. Wel lijkt het logisch en wenselijk om (nadere) aanwijzingen te ontwikkelen voor de opsporing en vervolging van onrechtmatige online content, voor zover het gaat om potentieel strafbare feiten. Politie en justitie zouden op basis van dergelijke aanwijzingen een beter ingekaderde rol kunnen spelen in de aanpak hiervan door het starten van een vervolgonderzoek en/of het inzetten van opsporingsbevoegdheden, uit eigen beweging of naar aanleiding van een aangifte.

F. Informatievoorziening

i. Routekaart

Uit de interviews kwam naar voren dat de grootste en meest urgente behoefte bestaat aan verbetering van de informatievoorziening en voorlichting op ten minste drie punten: welke partij(en) kunnen benadeelden aanspreken, op welke manier(en) kunnen zij dat doen en wat is daarvoor nodig met het oog op bewijsvergaring en onderbouwing van het verwijderingsverzoek? Geïnterviewden benadrukten dat het startpunt van rechtszoekenden bij het vinden van een oplossing voor een concreet probleem is, niet de juridische kwalificatie van dat probleem als bestuursrechtelijk, strafrechtelijk of civielrechtelijk. Benadeelden moeten snel en adequaat geadviseerd worden over hun rechten en over de juiste route(s) om die rechten te kunnen uitoefenen.

Benadeelden moeten niet alleen geholpen worden bij het in kaart brengen van hun opties, maar ook worden begeleid in het maken van keuzes. Afhankelijk van het precieze geval kan een **routekaart** worden gevolgd, waar bij elke stap concreet advies kan worden gegeven:

- De eerste stap is helder krijgen waar het precies om gaat, met name om welk type content en welk type internetdienst. Hoe kan de onrechtmatigheid worden vastgesteld en zijn de betrokken partijen bekend en bereikbaar?
- Vervolgens ligt voor de hand om te beginnen met Notice and Takedown en/of een sommatie tot verwijdering van de content.
- Als daar geen gehoor aan wordt gegeven of de aangesproken partij onbekend of onbereikbaar is, kan – afhankelijk van het type content – een melding bij de AP worden gedaan voor AVG-schendingen en/of aangifte bij de politie voor potentieel strafbare content.
- Een civiele procedure dient als stok achter de deur. Kosten en complexiteit zijn hier de voornaamste drempels. Benadeelden hebben onder meer hulp nodig bij het identificeren van de

344 Zie ook de opmerking van Minister Dekker; Burgerinitiatief "Internetpesters aangepakt", Handelingen II, 53ste vergadering, 12 januari 2020, p. 53-4-12.
345 *Stct.* 2018, 54287.

wederpartij(en) en het formuleren van de vordering of het verzoek.
- Oproepings- en betekeningsproblemen zouden deels kunnen worden opgelost door de verzoekschriftprocedure open te stellen voor een aantal afgebakende zaken waarbij internetdiensten zijn betrokken en andere belanghebbenden zich kunnen melden.
- Denkbaar is dat benadeelden in een dergelijke verzoekschriftprocedure verdergaand worden geholpen doordat voor of namens hen een verzoek kan worden ingediend.
- Hoe groter de potentiële impact van het online laten staan van de content (de ernst van de gevolgen voor de benadeelde), hoe spoedeisender de zaak. Kan de onrechtmatigheid relatief eenvoudig worden vastgesteld, dan zou een kort geding (eventueel ten overstaan van de kantonrechter waar geen verplichte procesvertegenwoordiging geldt) mogelijk uitkomst bieden.
- Een eventuele ex parte-procedure zou alleen aangewezen zijn onder bepaalde strikte voorwaarden.[346]

Deze routekaart zou kunnen worden opgezet aan de hand van een keuzemenu met verschillende modaliteiten en een escalatieladder. Deze routekaart zou (deels) kunnen worden geautomatiseerd, waarbij uit de formulering van problemen waar benadeelden mee komen relevante factoren worden gefilterd en vervolgvragen worden gesteld, zodat snel geïdentificeerd kan worden wat voor hen de beste route is om onrechtmatige online content verwijderd te krijgen.

ii. Juridische informatie en rechtshulp

Er staat veel praktische informatie op internet over de aanpak van onrechtmatige online content, die benadeelden op weg kan helpen – voor zover zij deze informatie weten te vinden. Allereerst geven sociale media platforms als Facebook, Twitter, Instagram en LinkedIn zelf informatie over wanneer content schadelijk kan worden bevonden en hoe het verwijderd kan worden.[347] Dergelijke informatie kan daarnaast worden gevonden op noticeandtakedowncode.nl en websites als die van de Consumentenbond.[348] Maatschappelijke organisaties als Bits of Freedom gaan een stap verder en bieden 'tips en tools' om inzicht te krijgen in online persoonsgegevens en geven antwoord op vragen over privacy, vrijheid en veiligheid online.[349] Voor eerstelijns rechtshulp en advies kunnen rechtszoekenden onder meer terecht bij het Juridisch Loket – dat op zijn website ook voorbeeldbrieven heeft staan[350] – en Slachtofferhulp Nederland. Voorbeeldbrieven zijn ook te vinden op de website van de AP.[351] Een andere mogelijke bron van informatie zijn diverse advocaten(kantoren) die blogs plaatsen over deze problematiek. Tot slot geeft de website van de politie informatie over verschillende vormen van illegale content, zoals gestolen naaktfoto's of -video's.[352]

Een routekaart zoals hierboven beschreven, met een compleet overzicht van alle mogelijkheden die benadeelden ten dienste staan, lijkt echter nog niet te bestaan. Mogelijk hangt dat samen met de al eerder aangestipte heterogeniteit van de problematiek en de veelheid aan betrokken actoren. Dit kan echter een probleem vormen met het oog op toegang tot recht, in het bijzonder de zelfredzaamheid van burgers en de beschikbaarheid van hulpbronnen – waarvan het belang is besproken in hoofdstuk 2.

346 Zie paragraaf 4.b.iv.
347 Zie bijvoorbeeld Facebook Helpcentrum, 'Iets rapporteren', https://www.facebook.com/help/263149623790594/.
348 Kulche 2019.
349 Bits of Freedom is een burgerrechtenorganisatie die opkomt voor privacy en vrijheid van communicatie op het internet. Zie Bits of Freedom, 'Tips en Tools, https://www.bitsoffreedom.nl/tips-en-tools/. Zie ook Mijn Online IDentiteit, 'Informatie van het internet verwijderen; zo doe je dat', https://www.mijnonlineidentiteit.nl/informatie-van-het-internet-verwijderen/.
350 Zie o.a. Het Juridisch Loket, 'Voorbeeldbrief verzoek om verwijderen beeldmateriaal', https://www.juridischloket.nl/voorbeeldbrieven/voorbeeldbrief-verzoek-om-verwijderen-beeldmateriaal/
351 Autoriteit Persoonsgegevens, 'Voorbeeldbrief Privacyrechten', https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorbeeldbrieven-privacyrechten.
352 Politie.nl, 'Naaktofot's gelekt', https://www.politie.nl/themas/naaktfotos-gelekt.html en Vraag het de politie, 'Pesten & Online', https://www.vraaghetdepolitie.nl/pesten-en-online.

Hiervoor zijn twee oplossingsrichtingen denkbaar. Een eerste mogelijke richting is gelegen in een verplichting tot uniforme informatievoorziening over relevante juridische procedures en Notice and Takedown-procedures door relevante diensten, in het bijzonder diensten die derde partijen (gebruikers) informatie laten publiceren op internet. Een dergelijke verplichting zou kunnen worden meegenomen in een eventuele codificering van vereisten ten aanzien van gevoerde Notice and Takedown-procedures. De tweede oplossingsrichting is gelegen in het verbeteren van de informatievoorziening door de overheid aan rechtzoekenden. De verantwoordelijkheid daarvoor zou belegd kunnen worden bij reeds betrokken instanties en toezichthouders, waaronder de AP. Ook kan worden gedacht aan een centraal meldpunt of kenniscentrum, zoals hierna besproken. Een goede coördinatie tussen betrokken instanties is bij het een en ander van bijzonder belang.

De Nederlandse Orde van Advocaten heeft al eerder gepleit voor een integrale online wegwijzer voor burgers met juridische problemen.[353] Voor specifieke rechtsgebieden bestaan er al websites met praktische informatie (o.a. checklists en voorbeeldbrieven), zoals het consumentenrecht. ConsuWijzer is bijvoorbeeld een initiatief van de ACM. Voordeel van de institutionele inbedding van een dergelijke website bij een onafhankelijke toezichthouder is dat informatie bij elkaar wordt gebracht op één centraal punt, dat er een kwaliteitscheck plaatsvindt én dat gegevens over het gebruik van de website inzicht geeft in de vraag naar juridisch advies. Dit hangt ook samen met het gesignaleerde punt over het (kunnen) navigeren van de stappen die tot verwijdering moeten leiden.

iii. Meldpunten

Benadeelden kunnen op dit moment al terecht bij verschillende meldpunten voor informatie over schadelijke content op internet en mogelijkheden tot het verwijderen daarvan. Er zijn de volgende meldpunten:

- Meldpunt privacy klacht (AP)
- Meldpunt datalek (AP)
- Meldpunt kinderporno
- Meldpunt identiteitsfraude- en -fouten
- Landelijk Meldpunt Internetoplichting
- Meldpunt internetdiscriminatie

Daarnaast geeft de website Meldknop.nl informatie op het gebied van o.a. (chantage met) naaktbeelden, internetoplichting, hacking, stalking en pesten/bedreiging.[354] Deze website heeft een portalfunctie en geleidt bezoekers door naar andere websites, zoals vraaghetdepolitie.nl, helpwanted.nl en veiliginternetten.nl.[355] De laatstgenoemde website is een initiatief van Veilig internetten en wordt ondersteund door de politie. Veilig internetten is op zijn beurt een initiatief van de Rijksoverheid en van het Electronic Commerce Platform Nederland (Platform voor de InformatieSamenleving (**"ECP"**)), een publiek-privaat platform voor kennisuitwisseling over de digitale samenleving. De pagina veiliginternetten.nl biedt "eerste hulp bij problemen" door informatie te geven over een aantal thema's op het gebied van digitale veiligheid. De vraag is echter of mensen met problemen deze website wel weten te vinden en, zo ja, in hoeverre zij daarmee zijn geholpen. Noch Meldknop.nl, noch veiliginternetten.nl geeft een compleet en uitputtend overzicht van de problematiek als in dit onderzoek aan de orde. Geen van beide websites biedt de mogelijkheid om direct een melding te doen; zij verwijzen voor voorlichting en hulpverlening door naar andere instanties met eigen expertise.

353 Droogleever Fortuyn 2018.

354 Volgens informatie die door Meldknop.nl is aangeleverd zijn dit de meest bekeken onderwerpen op de website.

355 Vraaghetdepolitie.nl is een website van de Politie die speciaal bedoeld is voor jongeren. Onderwerpen die aan bod komen zijn o.a. privacy, pesten & online en dwang & seks. Ook is er een zoekfunctie en een chatfunctie. Helpwanted.nl is onderdeel van het EOKM. Het is een website over online seksueel misbruik van kinderen en jongeren tot 26 jaar, die er terecht kunnen voor advies en informatie. Ook deze website heeft een chatfunctie. Veiliginteternetten.nl is, net als Meldknop.nl, een initiatief van de overheid, het ECP en het bedrijfsleven; dit wordt hierna verder besproken.

De website van de politie biedt die mogelijkheid wel: er is o.a. een contactformulier voor internetoplichting bij aan- en verkoopfraude. Daarnaast kunnen burgers online aangifte doen. Het Landelijk Meldpunt Internetoplichting (LMIO) vervult in dit verband een frontoffice-functie:[356] het biedt een keuzehulp als voorportaal voor burgers om te bepalen of het zin heeft om aangifte te doen. Het LMIO analyseert vervolgens alle binnengekomen meldingen/aangiftes en selecteert zaken voor verder onderzoek. Het LMIO vervult ook een coördinerende rol ten opzichte van de politie-eenheden. In voorkomende gevallen worden banken, betaaldiensten en de ACM als toezichthouder ingelicht en worden barrières opgeworpen voor malafide webshops, bijvoorbeeld door voorlichtingssites voor consumenten te alerteren, Notice and Takedown verzoeken te doen of het SIDN te vragen een houdernaamonderzoek in te stellen. In dat geval wordt een websitehouder gevraagd om binnen vijf dagen te bewijzen dat hij "bestaat", anders wordt de domeinnaam buiten gebruik gesteld.[357]

Internetoplichting valt buiten de reikwijdte van dit onderzoek. In de expertinterviews werden bestaande meldpunten, zoals het LMIO, echter wel genoemd als model voor een geïntegreerde aanpak van onrechtmatige online content. Deze oplossingsrichting betreft dan het aanwijzen of inrichten van een laagdrempelig meldpunt waar specialisten zitten die een melding op de juiste wijze kunnen beoordelen en de juiste vervolgactie kunnen initiëren. Voor zeer spoedeisende gevallen zou een apart noodloket kunnen worden ingericht. Het gaat dan eerst en vooral om de rechtsbescherming van individuele burgers, los van de vraag of een dergelijk meldpunt ook een functie zou kunnen of moeten vervullen in de strafrechtketen. De focus ligt op informatievoorziening, eventueel gekoppeld aan een kenniscentrum, en doorverwijzing aan de hand van de hierboven besproken routekaart. Integratie van deze routekaart met het al bestaande initiatief Meldknop.nl en het Meldpunt van de AP ligt voor de hand. Zo biedt Meldknop.nl een overzicht van verschillende problemen waarmee mensen te maken kunnen krijgen op internet en tips voor de aanpak daarvan. Dat kan nog worden uitgebouwd met bijvoorbeeld een keuzehulp (waar het LMIO al mee werkt), tools voor het doen van een Notice and Takedown-melding en specifieke informatie over eventuele escalatiemogelijkheden, in het bijzonder juridische procedures. Voor zeer spoedeisende gevallen zou een apart noodloket kunnen worden ingericht.

Een meldpunt zou ook een faciliterende rol kunnen vervullen in het contact of de bemiddeling met betrokken partijen. Dat vergt echter wel extra capaciteit en speciale competenties van de aan zo'n meldpunt verbonden medewerkers. Een ander aandachtspunt is het vergroten van de bekendheid van het meldpunt, zodat burgers de weg er naartoe weten te vinden. Tot slot is de onafhankelijkheid van een dergelijk meldpunt of kenniscentrum een belangrijk aandachtspunt. De veelheid aan betrokken partijen – markpartijen zoals internetdiensten en socialemediaplatforms, maar ook politie en justitie en slachtoffers zelf – en belangen onderstreept de waarde van onafhankelijkheid van een meldpunt.

G. Toezichthouder

In het bovenstaande is de mogelijkheid van een actievere rol van de overheid op het gebied van de informatievoorziening en het bieden van overzicht in de bestaande mogelijkheden voor de aanpak van onrechtmatige content besproken, alsmede de organisatie en inrichting van relevante meldpunten. Een verdergaande mogelijkheid, waarin de Nederlandse overheid een actievere rol op zich neemt om de problematiek van onrechtmatige content in juiste en rechtstatelijke banen te leiden, bestaat uit het organiseren van onafhankelijk toezicht op deze problematiek, door een nieuwe toezichthouder of een combinatie van bestaande toezichthouders.

356 Zie het rapport de Inspectie van Veiligheid en Justitie 2015.
357 Zie verder SIDN, 'Klacht over inhoud website', https://www.sidn.nl/nl-domeinnaam/klacht-over-inhoud-website.

Bij de problematiek van onrechtmatige content is reeds een aantal toezichthouders actief betrokken op basis van relevante bestaande wetgeving. Zo heeft de AP een duidelijke rol met betrekking tot onrechtmatige verwerkingen van persoonsgegevens. De ACM heeft een rol in het kader van onrechtmatige informatie bestaande uit de misleiding van consumenten. Het Commissariaat voor de Media (CvdM) heeft een taak op het gebied van audiovisuele diensten op internet. Naast deze onafhankelijke toezichthouders hebben politie en justitie en ook de AIVD een rol in het toezicht vanuit de overheid op de problematiek van onrechtmatige content op internet.

Zoals reeds in detail besproken, is de regeling voor de verwijdering van illegale en onrechtmatige content door relevante dienstverleners grotendeels overgelaten aan zelfregulering.[358] Op dit punt is de laatste jaren in Europa een duidelijke kentering te zien. In het kader van de problematiek van desinformatie is de fragmentatie van het toezicht vanuit de overheid een belangrijk aandachtspunt.[359] In Duitsland is de besproken NetzDG wetgeving aangenomen, die bepaalde wettelijke voorschriften bevat voor de behandeling van illegale content door de grootste sociale media diensten in Duitsland. De naleving van deze voorschriften is onderwerp van toezicht vanuit de overheid. Zo kunnen bijvoorbeeld boetes worden opgelegd in het geval de klachtenprocedure door de diensten niet goed wordt geïmplementeerd of in het geval dat bepaalde rapportageverplichtingen niet worden nagekomen. In de voorstellen in Frankrijk en het Verenigd Koninkrijk met betrekking tot de aanpak van onrechtmatige en illegale content op internet is toezicht een belangrijke component en hetzelfde geldt voor de recente DSA voorstellen op Europees niveau.[360] Een bijkomende reden voor het organiseren van beter toezicht vanuit de overheid is het feit dat er in de markt sprake is van duidelijke machtsconcentraties.

De Europese Commissie overweegt voor de DSA in het bijzonder de beleidsoptie om een systeem van toezicht, handhaving en samenwerking te creëren, ondersteund op EU-niveau. Deze optie zou complementair aan de optie om bestaande aanwijzingen van de Europese Commissie op het gebied van illegale en onrechtmatige content in wetgeving vast te leggen kunnen worden geïmplementeerd. Dergelijke wetgeving zou de problematiek waar dit onderzoek zich op richt omvatten, maar in verschillende opzichten, waaronder het type onrechtmatigheid, een stuk breder terrein beslaan. Een dergelijk systeem van toezicht en handhaving zou het voor de Europese interne markt van groot belang zijnde 'land van oorsprong' beginsel, welke nu reeds van toepassing is op basis van de e-Commerce richtlijn, als uitgangspunt behouden. Het verdient aanbeveling om in de oplossingen die op nationaal niveau kunnen worden overwogen en geïmplementeerd voor wat betreft het instellen van toezicht op de problematiek van onrechtmatige content, zoveel als mogelijk aansluiting te zoeken bij de aanstaande wijzigingen op Europees niveau.

H. Conclusie

Dit hoofdstuk bevat de knelpuntenanalyse van de verschillende routes die zijn beschreven in hoofdstuk 3. Deze knelpuntenanalyse is gemaakt op grond van documentonderzoek, de survey en gesprekken met experts. Vervolgens is deze knelpuntenanalyse gekoppeld aan de in hoofdstuk 2 geïdentificeerde struikelblokken bij de verwijdering van onrechtmatige online content. Vier modelgevallen illustreren dat een aantal van die struikelblokken onopgelost blijft, met name als de onrechtmatigheid moeilijk is vast te stellen en de dienst of degene die de uiting doet onbereikbaar is dan wel geen gehoor geeft. Er worden uiteenlopende oplossingsrichtingen besproken, die hierna nog eens kort zullen worden weergegeven in hoofdstuk 6.

358 Zie 4.a.iii.
359 Van Hoboken e.a. 2019.
360 Voor een verdere bespreking zie 3.b.

6. Conclusie

Sinds de opkomst van het Internet en het World Wide Web is de publicatie en verspreiding van onrechtmatige content online een groot probleem, dat de Nederlandse landgrenzen overstijgt. Hier wordt reeds een aantal decennia wetgeving en beleid voor ontwikkeld, op nationaal, Europees en internationaal niveau. Onrechtmatige content, zoals de publicatie van gevoelige privégegevens en valse beschuldigingen of aanstootgevende uitingen, kunnen slachtoffers daarvan aanzienlijke schade bezorgen en in sommige gevallen zelfs ontwrichtende gevolgen hebben voor hun leven. Tegelijkertijd dienen wetgeving en procedures voor de verwijdering van onrechtmatige content rekening te houden met rechtstatelijke waarborgen, waaronder de vrijheid van meningsuiting in het bijzonder. Dit onderstreept de complexiteit en het belang van een goed juridisch kader voor de aanpak van onrechtmatige content op internet en door internet gefaciliteerde media en diensten zoals sociale netwerken.

Hieronder worden de belangrijkste bevindingen en conclusies van het onderzoek samengebracht en daarmee de onderzoeksvragen beantwoord.

Onderzoeksvragen:

1. Wat zijn bestaande mogelijkheden voor het indienen van een verzoek tot verwijdering van onrechtmatige online content in het burgerlijk recht (bodemprocedure, kort geding, ex parte maatregelen, etc.) en het bestuursrecht (zoals via AP) en welke beperkingen en mogelijkheden brengen deze met zich?

2. Welke mogelijkheden bieden aanbieders van verschillende soorten relevante internetdiensten voor het verwijderd krijgen van vermeend onrechtmatige inhoud en hoe verhouden deze buiten-juridische mogelijkheden zich tot het Nederlands en Europeesrechtelijk juridisch kader?

3. Wat is de maatschappelijke behoefte in Nederland aan een nieuwe voorziening voor de verwijdering van verschillende vormen van onrechtmatige inhoud, in termen van type en aantal onrechtmatige uiting, type dienst, snelheid, grondslag en rechtsgang, toegankelijkheid, en effect op de vrijheid van meningsuiting?

4. Wat zijn de mogelijkheden voor de vormgeving van een nieuwe of aangepaste voorziening, in termen van materieel- en procesrechtelijke verankering, bevoegde instantie, snelheid, kosten, en toegankelijkheid, mede in het licht van het bestaande dienstenaanbod, het Europeesrechtelijk kader (i.h.b. de richtlijn elektronische handel), en de fundamentele rechten, in het bijzonder de vereiste balans tussen de bescherming van het recht op privéleven (artikel 8 EVRM) en de vrijheid van meningsuiting (artikel 10 EVRM), en welke van deze mogelijkheden komt optimaal tegemoet aan de juridische en maatschappelijke behoefte?

In de loop van het onderzoek is op verzoek van het WODC de volgende onderzoeksvraag aan het onderzoek toegevoegd:

5. Zou het doen van aangifte voldoende moeten zijn voor het toewijzen van een verwijderverzoek?

De analyse van de bestaande wettelijk kader en de mogelijke procedurele routes tot verwijdering van illegale en onrechtmatige online content vormt de beantwoording van **onderzoeksvraag 1** en **2**, die tezamen besproken worden. Dit is te vinden in hoofdstuk 3 en 4.

In het grondrechtelijk kader staan het recht op een eerlijk proces, het recht op een privéleven en de vrijheid van meningsuiting centraal. Het recht op een eerlijk proces stelt voorwaarden aan de inrichting van een mogelijke procedure tot verwijdering. Het recht op een privéleven vormt de afbakening van de type onrechtmatige content die in dit onderzoek besproken zijn en omvat ook een positieve verplichting voor de overheid om dit recht in verhoudingen tussen burgers (en bedrijven) onderling te beschermen. Ten slotte stelt ook de vrijheid van meningsuiting eisen aan een mogelijke procedure voor de verwijdering van onrechtmatige online content. Belangrijk is namelijk dat er ook waarborgen zijn om te garanderen dat rechtmatige content voldoende tegen verwijdering beschermd wordt.

Vervolgens zijn in totaal zeven procedures geanalyseerd, in de onderstaande figuur 9 (zie volgende pagina) te vinden op de y-as. De zeven criteria, te vinden op de x-as, zijn ontleend aan de analyse van de maatschappelijke behoefte en de expertinterviews. De resultaten van deze analyse zijn gevalideerd door de expertinterviews en –workshops. Het door de figuur geboden overzicht laat zien dat er bepaalde afwegingen en keuzes gemaakt moeten worden tussen verschillende eigenschappen van een procedure. Zo lijken er enerzijds procedurele routes te zijn die snel, laagdrempelig en schaalbaar zijn, en anderzijds procedures die voldoende rechtstatelijke waarborgen bieden. Een combinatie van al deze kwaliteiten in één procedure lijkt uitgesloten.

	Schaalbaarheid	Doorlooptijd	Drempelkosten	Drempel complexiteit	Proceswaarborg	VvMU waarborg	Doeltreffendheid
Civielrecht							
Bodemprocedure							
Verzoekschrift							
Kort geding							
Ex parte							
Bestuursrecht							
Klacht AP							
AVG rechten							
Buiten juridisch							
Notice & Takedown							

Rood: de procedure scoort niet goed op het criterium.
Oranje: de procedure scoort niet goed maar ook niet slecht op het criterium.
Groen: de procedure scoort goed op het criterium.

Figuur 9

De civielrechtelijke procedures dienen als stok achter de deur als geen gehoor wordt gegeven aan een Notice and Takedown verzoek of een verzoek op grond van de AVG. In dat laatste geval staat de verzoekschriftprocedure (zonder verplichte procesvertegenwoordiging) open, die over het algemeen als sneller, informeler en doeltreffender kan worden gezien. De reikwijdte van deze procedure is echter op dit moment nog beperkt. Een ex parte-procedure is ook een rekestprocedure, maar zonder dat hoor en wederhoor plaatsvindt. Dit is illustratief voor het spanningsveld tussen snelheid enerzijds en waarborgen anderzijds; het kort geding vormt een middenweg maar dat is in voorkomende gevallen niet snel genoeg.

De beantwoording van **onderzoeksvraag 3** is grotendeels te vinden in hoofdstuk 2. Uit de uitgevoerde survey is af te leiden dat 15% van de Nederlandse bevolking direct of indirecte ervaring heeft met het soort van schadelijke, en mogelijk onrechtmatige, inhoud waar deze studie zich op richt. Uit de survey en expertinterviews blijkt verder dat het moeilijk verwijderd krijgen van onrechtmatige online content breed gezien wordt als een maatschappelijk probleem. Dit komt voornamelijk voort uit de snelheid en grote schaal waarop de content verspreid kan worden. De juridische afbakening is te vinden in artikel 8 EVRM en omvat nog steeds een grote verscheidenheid aan verschillende typen content te omvatten die

hun basis vinden in zowel het civiel, bestuurs- als strafrecht. De omvang van de schade voor een individu is moeilijk in algemene zin vast te stellen nu, zo blijkt, het heterogene problematiek betreft en niet voor elk type content empirisch onderzoek beschikbaar is over de impact die deze heeft op een persoon.

Voor de mogelijkheden tot verwijdering is van belang dat de specifieke problematiek van onrechtmatige online content die mensen in de persoon raakt, zich bevindt op het snijvlak van de bredere problematiek van de toegang tot recht en internetregulering. Zo sluiten de surveyresultaten aan bij eerder onderzoek dat is gedaan naar de problematiek van toegang tot recht en toegang tot de rechter. Een gebrek aan juridische kennis en informatie is een belangrijk struikelblok. In algemene zin vormen advocaatkosten en doorlooptijden grote procedurele drempels voor rechtszoekenden. In dat verband wordt een brede, proactieve benadering voorgestaan ten aanzien van toegang tot informatie, advies en eerstelijns rechtshulp. Daarnaast is het type internetdienst, hosting providers op het open internet of directe communicatiediensten op het gesloten internet, in grote mate bepalend voor de mogelijke routes tot verwijdering die iemand ter beschikking staan. Zo vormt de Notice and Takedown-procedure, indien beschikbaar, de meest laagdrempelige route tot verwijdering.

De problemen die een individu tegen kan komen wanneer deze geconfronteerd wordt met onrechtmatige content en op zoek is naar een manier tot verwijdering, zijn samengevat in zeven struikelblokken, weergegeven in figuur 10. Vier modelgevallen zijn ontwikkeld om te analyseren hoe de verschillende struikelblokken 'bekendheid & bereikbaarheid dienst', 'type onrechtmatige content' en 'type internetdienst' in verschillende configuraties verschillende problemen veroorzaken. Om daadwerkelijk zicht te krijgen op de maatschappelijke behoefte aan een nieuwe procedure, zijn de verschillende bestaande mogelijkheden geanalyseerd. Geen van de bestaande procedures nemen de geïdentificeerde struikelblokken (volledig) weg. Zo is een civiele procedure weliswaar een stok achter de deur als de Notice and Takedown-procedure nergens toe leidt, bijvoorbeeld omdat de onrechtmatigheid zeer moeilijk vast te stellen is of de internetdienst onbereikbaar is, maar daar zijn doorlooptijd, complexiteit en kosten belangrijke drempels.

Individuele struikelblokken
Bekendheid & bereikbaarheid dienst
Type onrechtmatige content
Type internetdienst
Mate van vereiste specialistische kennis
Terugkomende content
Persoonlijke omstandigheden
Toegang tot de rechter

Figuur 10

In hoofdstuk 5 van dit rapport zijn aan de hand van de geïdentificeerde maatschappelijke behoefte en de geanalyseerde knelpunten mogelijke oplossingsrichtingen besproken. Daarbij wordt een gefaseerde benadering voorgestaan, met verschillende routes en escalatiemogelijkheden al naar gelang de specifieke problemen die zich voordoen. Dit vormt de beantwoording van **onderzoeksvraag 4** en **5.** Er is niet één alomvattende oplossing in de zin van één specifieke juridische procedure, in verband met de eerder gesignaleerde heterogeniteit van de problematiek. Wel zijn er diverse scenario's denkbaar voor aanpassing en verbetering van de geldende juridische kaders en procedures die van toepassing zijn. Deze scenario's sluiten elkaar niet uit, maar kunnen elkaar juist versterken nu zij gericht zijn op het wegnemen of afzwakken van de struikelblokken en knelpunten op verschillende fronten.

Een eerste scenario is het verder normeren en codificeren van Notice and Takedown-procedures en het daarvoor geldende afwegingskader. Andere Europese landen hebben deze stap al gezet in hun nationale wetgeving en momenteel wordt dit op EU-niveau overwogen in de vorm van de Digital Services Act. Bij de normering van Notice and Takedown-procedures moet aandacht uitgaan naar het voorkomen van de verwijdering van rechtmatige content en het bieden van procedurele waarborgen. Daarnaast dient het huidige gebruik van Notice and Takedown-procedure door politie en justitie ook kritisch bekeken te worden.

Een tweede scenario is het experimenteren met civiele procedures, meer specifiek het kantonrechterskortgeding, de verzoekschriftprocedure die nu al beschikbaar is voor de uitoefening van AVG-rechten en/of de ex parte-procedure. Een experiment biedt ruimte voor zaken die mogelijk op dit moment niet bij de rechter terechtkomen, vanwege uiteenlopende drempels die rechtszoekenden ervaren. Niet alle struikelblokken worden hiermee weggenomen. De focus ligt in dit scenario met name op advocaatkosten en doorlooptijd. Het kantonrechterskortgeding heeft als voordeel dat het bij uitstek geschikt is voor spoedeisende zaken en een grotere reikwijdte heeft dan de verzoekschriftprocedure, die op haar beurt informeler is en daarmee mogelijk doeltreffender. Een ex parte-procedure kan uitkomst bieden in zeer spoedeisende zaken die relatief gemakkelijk af te doen zijn, maar daar verdient de uitzondering op hoor en wederhoor een bijzondere rechtvaardiging. Met het oog op de afbakening van het experiment kan prioriteit wordt gegeven aan een bepaald type zaken, bijvoorbeeld ernstige vormen van bedreiging.

Een derde scenario is het verbeteren van de klachtenprocedure AP en het uitbreiden van het werkgebied van de AP. De AP zou een bredere coördinerende rol kunnen vervullen bij de aanpak van deze problematiek, in het verlengde van de taken die zij nu ook al vervult en die raken aan kwesties op het gebied van privacy en de eer en goede naam. Dit scenario raakt direct aan de bredere discussie over de rol en de huidige capaciteit van de AP, die het bestek van dit onderzoek te buiten gaat.

Een vierde scenario is het ontwikkelen van (nadere) aanwijzingen voor de opsporing en vervolging van strafbare feiten in verband met illegale online content. Het geven van meer betekenis aan de aangifte is juridisch wenselijk noch realistisch. Wel zouden dergelijke aanwijzingen de betrokken partijen meer houvast kunnen bieden: voor benadeelden voor de vraag of het zin heeft om aangifte te doen en voor de politie voor de aanpak en prioriteit van het type zaken als hier aan de orde. Dit gaat het bestek van dit onderzoek verder te buiten, maar grenst wel aan de problematiek van toegang tot recht en in het bijzonder het bieden van hulp aan benadeelden.

Een laatste en overkoepelend scenario is het verbeteren van informatievoorziening aan benadeelden, in het bijzonder op het punt van de route die zij kunnen volgen voor het (laten) verwijderen van onrechtmatige online content. Het betreft specialistische problematiek, wat het belang van goede bewegwijzering onderstreept. Dat kan ten eerste gebeuren langs de band van een verplichting voor internetdiensten tot uniforme informatievoorziening over beschikbare (buiten)gerechtelijke procedures. Ten tweede kan worden voortgebouwd op bestaande initiatieven – privaat en van overheidswege – om voorlichting aan benadeelden te geven over hun rechten op internet en manieren waarop zij die rechten kunnen uitoefenen. Dit laatste scenario lijkt het meest veelbelovend, althans een belangrijke eerste stap in de aanpak van struikelblokken waar benadeelden mee te maken krijgen in deze context.

In het licht van het uitgevoerde onderzoek valt de meeste winst te behalen in het inrichten van een centraal kenniscentrum of meldpunt waar belanghebbenden terecht kunnen voor een integrale routekaart. Hierbij moet de kanttekening worden geplaatst dat het veronderstelt dat mensen de weg naar een dergelijk meldpunt in een vroeg stadium weten te vinden, dat wil zeggen dat zij er bekend mee zijn en beschikken over de vaardigheden om voor hen relevante informatie te ontsluiten. Een gelaagd aanbod van informatie – aan rechtszoekenden zelf én aan juristen die hen hulp en bijstand verlenen – is daarom cruciaal.

Voor de overheid is een duidelijke rol weggelegd in het verzekeren van grondrechtelijke en rechtsstatelijke waarborgen en het bieden van een stok achter de deur: het handhaven of afdwingen van individuele rechten via rechterlijk ingrijpen. Vanuit de verantwoordelijkheid voor de bescherming van grondrechten, zowel de bescherming van het recht op privéleven als de vrijheid van meningsuiting, is een actieve rol van de overheid vereist in de aanpak van onrechtmatige content. Het belang van de bescherming van deze grondrechtelijke belangen vormt tevens het belangrijkste argument om voor de aanpak van onrechtmatige content speciale voorzieningen te overwegen. Dit onderzoek concludeert dat hiervoor, door de

heterogeniteit van de problematiek, geen uniforme oplossing bestaat. Het biedt de bovenstaande oplossingsrichtingen om bestaande knelpunten weg te nemen en voor de verschillende problemen zo goed mogelijk aan te sluiten bij de bestaande maatschappelijke behoefte.

Literatuurlijst

Literatuur

- Aanbeveling CM/Rec (2016)4[1] van het Comité van Ministers aan de lidstaten betreffende de bescherming van de journalistiek en de veiligheid van journalisten en andere media-actoren, 13 april 2016, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415d9#_ftn1.

- Aanbeveling 1177 van de Europese Commissie (1 maart 2018), *Commission Recommendation on measures to effectively tackle illegal content online*.

- Aplin, Tanya Frances. *Research Handbook on Intellectual Property and Digital Technologies* . Cheltenham, UK: Edward Elgar Publishing, 2020. Print.

- Ananny, Mike, and Kate Crawford. "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability." *New Media & Society*, vol. 20, no. 3, Mar. 2018, pp. 973–989, doi:10.1177/1461444816676645.

- Angelopoulos, C. e.a., *Study of fundamental rights limitations for online enforcement through self-regulation*, Institute for Information Law, University of Amsterdam 2015.

- Article 19 Persbericht, 'UK: "Super-Injunctions" illegitimate Limit to Free Speech, Londen 19 mei 2011, https://www.refworld.org/pdfid/4def36d73de.pdf.

- Article 19, "France: Constitutional Council declares French hate speech 'Avia' law unconstitutional", 18 Juni 2020, www.article19.org.

- Asser, W., e.a., *Uitgebalanceerd. Eindrapport fundamentele herbezinning Nederlands burgerlijk procesrecht* (eindrapport), Den Haag: Boom Juridische Uitgevers 2006, wodc.nl.

- Aurelien Breeden, "French Court Strikes Down Most of Online Hate Speech Law," *New York Times*, 18 June 2020.

- Autoriteit Persoonsgegevens Jaarverslag, 'Balans', 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarverslag_ap_2019.pdf.

- Autoriteit Persoonsgegevens 'Klacht melden', https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/klacht-melden-bij-de-ap.

- Autoriteit Persoonsgegevens nieuwsbericht, 'Forse stijging privacyklachten in 2020, 14 februari 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/forse-stijging-privacyklachten-2019.

- Autoriteit Persoonsgegevens, 'Voorbeeldbrief Privacyrechten', https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/voorbeeldbrieven-privacyrechten.

- Autoriteit Persoonsgegevens rapport, *Meldplicht datalekken: feiten en cijfers eerste helft 2019,* 19 september 2019, www.autoriteitpersoonsgegevens.nl.

- Bakker, F. 'Maatschappelijk effectieve rechtspraak', NJB 8 september 2016, www.njb.nl.

- Balakrishnan, A. 'Facebook Pledges to double its 10,000-person safety and security staff by end of 2018', *CNBC* 31 oktober 2017, www.cnbc.com.

- Barbier, J. 'Vrouwelijke journalisten steeds vaker slachtoffer van online intimidate', *De Volkskrant* 6 februari 2015, www.volkskrant.nl.

- Barendrecht, J., en Kamminga, Y., *Toegang tot het recht: de lasten van een uitweg, (*RMO-advies; Nr 32), Den Haag: RMO december 2004.

- Bauw, E., e.a., *Naar een nabijheidsrechter? Een onderzoek naar de inpasbaarheid van de vrederechter in België en Frankrijk in het Nederlandse Rechtsbestel,* Utrecht: Universiteit Utrecht -Montaigne Centrum voor Rechtsstaat en Rechtspleging 2019, www.wodc.nl.

- BBC nieuwsbericht, 'Online Harms bill: Warning over 'unacceptable' delay', 29 juni 2020, https://www.bbc.com/news/technology-53222665.

- Bemmelen van, J., e.a., Ons strafrecht 2 – Strafprocesrecht, Alphen aan de Rijn: Wolters Kluwer 2016, p. 286.

- Berg van der, J., en Visser D., 'Ex parte-praktijk in het auteursrecht', *AMI* 2009/3, Amsterdam: DeLex 2009.

- Berthélémy, C., French Avia law declared unconstitutional: what does this teach us at EU level? , *EDRi* 24 Juni 2020.

- Bits of Freedom, 'Tips en Tools, https://www.bitsoffreedom.nl/tips-en-tools/.

- Blocman, A., 'Law on manipulation of information, validated by the constitutional council, is published, *IRIS* 2019-2:1/11.

- Boonekamp, R., *Mr C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 6. Procesrecht. Het kort geding*, Alphen aan den Rijn: Wolters Kluwer 2020.

- Bouchallikht, Kauthar 'Racisme maakt letterlijk ziek', 2 juni 2020 One World, https://www.oneworld.nl/lezen/discriminatie/racisme/discriminatie-maakt-letterlijk-ziek/ .

- Brand Mr, Toegankelijkheid van het recht in Nederland, Den Haag 7 oktober 2019, https://www.brandmr.nl/pers/onduidelijkheid-en-te-hoge-kosten-hoofdredenen-om-rechtshulp-te-mijden/.

- Buitenweg, K. 'Essay Seksisme op sociale media: Vogelvrije vrouwen', *De groene Amsterdammer* 26 februari 2020, www.groene.nl.

- Centraal Bureau voor de Statistiek, *Digitale Veiligheid & Criminaliteit 2018*, Den Haag: Centraal Bureau voor de Statistiek 2019.

- Clegg, N. 'Welcoming the Oversight Board, Facebook nieuws 6 mei 2020, https://about.fb.com/news/2020/05/welcoming-the-oversight-board/.

- College voor de Rechten van de Mens, *Jaarlijkse rapportage mensenrechten in Nederland. Toegang tot het recht,* 2018, mensenrechten.nl.

- Commissariato di P.S., 'Protocollo operative per il contrasto alle fake news', 18 januari 2018, https://www.commissariatodips.it/notizie/articolo/attenzione-nuova-ondata-di-e-mail-con-allegato-virus-cryptolocker/index.html.

- De OSCE Representative on Freedom of the Media on Media Pluralism, Safety of Female Journalists and Safeguarding Marginalized Voices Online, 'Persbericht Nr. 1/2019', https://www.osce.org/files/2019-02-21%20SOFJO%20Communique.pdf.

- De Streel, A. et al., *Online Platforms' Moderation of Illegal Content Online*, Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.

- De website van SOS (Stop Online Shaming), https://stoponlineshaming.org/.

- De Wetenschappelijke Raad voor het Regeringsbeleid, *Weten is nog geen doen: een realistisch perspectief op zelfredzaamheid*, Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid 2017.

- Décision n° 2020-801 DC du 18 juin 2020, https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

- Department for Digital, Culture, Media & Sport, 'Online Harms White Paper – Initial consultation response, 12 februari 2020, https://www.gov.uk/government/consultations/online-harms-white-paper.

- Digital Services Act package: deepening the Internal Market and clarifying responsibilities for digital services - Inception Impact Assessment, Ref. Ares(2020)2877686, 4 June 2020, https://ec.europa.eu/info/law/better-regulation/.

- Douek, E. 'The Rise of Content Cartels' K*inght First Amendment Institute,* 2020

- Douek, E. 'Facebook's Oversight Board: Move Fast with Stable Infrastructure and Humility,' *North Carolina Journal of Law & Technology,* Vol. 21, Issue 1 (October 2019), pp. 1-78.

- Droogleever Fortuyn, S., 'Nova in actie voor toegang tot het recht', Advocatenblad 30 mei 2018, advocatenblad.nl

- Duin van, J., 'Wie betaalt de rekening? De kostenverdeling in de context van het EU-consumentenrecht', *Tijdschrift voor Consumentenrecht en Handelspraktijken* 2018 4, p. 177-183.

- Elis, E., 'People can put your face on Porn – and the law can't help you', *Wired* 26 januari 2018, www.wired.com.

- EOKM jaarverslagen op https://www.eokm.nl/kennisbank/eokm-jaarverslagen/.

- eSafetyComissioner Australia, https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-esafety-commissioner.

- Eshuis, R., en Diephuis, B., Civiele rechtspraak (Fact sheets 2018-01), Den Haag: WODC 2018, wodc.nl.

- Eshuis, R., en Geurts, T., *Lagere drempels voor rechtzoekenden. Evaluatie van de Verhoging van de Competentiegrens in 2011* (Cahiers 2016-14), Den Haag: WODC 2016, www.wodc.nl.

- European Digital Rights (EDRi), *Platform Regulation Done Right: EDRI position paper on the EU Digital Services Act*, Brussel 9 april 2020.

- European Regulators Group for Audiovisual Media Services (ERGA), *ERGA position paper on the Digital Service Act*, 5 juni 2020.

- Europees Parlement, Effective Access to Justice, 2017, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)596818.

- Europese commissie mededeling, 'Mededeling van de Commissie aan het Europees Parlement, De Raad, Het Europees Economisch en Sociaal Comité en het Comité van de regio's. De bestrijding van illegale online-inhoud Naar een grotere verantwoordelijkheid voor onlineplatforms , COM(2017) 555 final, 28 september 2017.

- Europese Commissie notificatie, 'Notification 2019/412/F Law aimed at combating hate content on the internet - Delivery of comments pursuant to Article 5(2) of Directive (EU) 2015/1535 of 9 September 2015', C(2019) 8585 final, 22 November 2019.

- Europese Commissie publicatie, 'The Digital Service Act package', 22 juni 2020, www.ec.europa.eu.

- Europese Commissie publicatie, 'Digital Service Act – deepening the internal market and clarifying responsibilities for digital services', https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services.

- Europese Commissie publicatie, 'Countering Illegal hate speech online #NoPlace4Hate', 18 maart 2019 https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300.

- Europese Commissie, Aanbeveling 1177, 1 maart 2018, *Commission Recommendation on measures to effectively tackle illegal content online*.

- Europese Commissie publicatie, *Legal analysis of a Single Market for the Information Society. New rules for a new age? 6. Liability of online intermediaries,* november 2009.

- Facebook Helpcentrum, 'Iets rapporteren', https://www.facebook.com/help/263149623790594/.

- Facebook transparency report, *Bullying and harassment*, Facebook mei 2020, https://transparency.facebook.com/community-standards-enforcement#bullying-and-harassment.

- Facebook Transparency, *Community Standards Enforcement Report*, Facebook mei 2020, https://transparency.facebook.com/community-standards-enforcement.

- Fathaigh, R., "Brzezi ski v. Poland: Fine over 'false' information during election campaign violated Article 10", *Strasbourg Observers*, 8 augustus 2019.

- Fathaigh, R., en Voorhoof, D., "Kablis v. Russia: prior restraint of online campaigning for a peaceful, but unauthorised demonstration violated Article 10 ECHR", *Strasbourg Observers* 17 mei 2019.

- Feiner, L., 'Facebook content moderators break NDAs to expose shocking working conditions involving gruesome videos and feces smeared on walls', *CNBC* 19 juni 2019, www.cnbc.com.

- Flynn, A., en Hodgson, J., *Access to Justice and Legal Aid. Comparative Perspectives on Unmet Legal Need*, Oxford: Hart Publishing 2017.

- FRA (European Union Agency For Fundamental Rights), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburg: Publications Office of the European Union 2011, fra.europa.eu.

- FRA (European Union agency for Fundamental Rights), *Violence, threats and pressures against journalists and other media actors in the EU. Contribution to the second Annual Colloquium on Fundamental Rights,* Luxemburg: Publications Office of the European Union 2016.

- FRA (European Union Agency For Fundamental Rights), Your Rights Matter: data protection and privacy: fundamental rights survey, Luxemburg: publications office of the European Union 2020.

- Gámez-Guadix, M., e.a., Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults', *Sexuality Research and Social Policy: Journal of NSRC* 2015 12(1), p. 145-154.

- Gammeren-Zoeteweij van, M., e.a., *Monitor Gesubsidieerde Rechtsbijstand 2016* (factsheet), Oisterwijk: Wolf Legal Publishers (WLP), 2017, https://www.rvr.org/binaries/content/assets/rvrorg/informatie-over-de-raad/monitor/rechtsbijstand-factsheet-nuldelijns-grb-2016.pdf.

- Gammeren-Zoeteweij, M. van e.a., *Monitor Gesubsidieerde Rechtsbijstand 2017*, Utrecht: Raad voor Rechtsbijstand 2017; https://www.rvr.org/binaries/content/assets/rvrorg/informatie-over-de-raad/monitor/mgr-2017-def-versie-mgr.pdf

- Garcia, J., e.a., 'Sexting among singles in the USA: Prevalence of sending, receiving, and sharing sexual messages and images', *Sexual Health* 2016 13(5), p. 428-435.

- Gillespie, T. *Custodians of the Internet: Platforms,* Content moderation*, and the Hidden Decisions That Shape Social Media*m Yale University Press, 2018.

- Google Transparantierapport, *Handhaving van de Communityrichtlijnen van Youtube*, https://transparencyreport.google.com/youtube-policy/removals.

- Gorwa, R. Binns, R. Katzenbach, C. 'Algorithmic content moderation: Technical and political challanges in the automation of platform governance', *Big Data & Society (BD&S) journal* 28 februari 2020, https://doi.org/10.1177/2053951719897945.

- Graaf de, H. e.a., Rutgers/Soa Aids Nederland, *Seks onder je 25e. Voortgezet Special Onderwijs Seksuele gezondheid van jongeren in cluster 3 en 4*, Utrecht, maart 2019.

- Groenewald, E., e.a., *Naar vernieuwing van de (civiele) rechtspleging),* Den Haag: Boom juridisch 2019.

- Grootelaar H., e.a., *Toegang tot het recht: een actueel portret. Een verkennend onderzoek naar relevante Nederlandse overheidsmaatregelen sinds 2008 en de gevolgen daarvan voor rechtszoekenden,* Utrecht: Universiteit Utrecht -Montaigne Centrum voor rechtspleging en conflictoplossing 2014.

- Grootelaar, H., Schelfhout, D., Duijneveldt van, I., Evaluatie Rotterdamse Regelrechter en Haagse Wijkrechter: onderzoeksrapportage, Research Memoranda nummer 1/2020 jaargang 15, Den Haag: Sdu Uitgevers bv.

- Heaven, W., 'A plan to redesign the internet could make apps that no one controls', *MIT technology review* 1 juli 2020, www.technologyreview.com.

- Hendrikse, R., e.a., 'Kroniek Burgerlijk Procesrecht 2019', Advocatenblad 2020 2, Den Haag: Boom Juridische Uitgevers 2020.

- Henry, N., en Powell, A., 'Embodied Harms: Gender, Shame, and Technology-Facilitated Sexual Violence', *Violence against woman* 2015 21(6), p. 758-799.

- Hoboken van, J., *Het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties: Eindrapport*, Instituut voor Informatierecht (IViR) Universiteit van Amsterdam 2019.

- Hoboken van, J. & D. Keller, Design Principles for Intermediary Liability Laws, Working Paper, Transatlantic working group on content moderation, October 8, 2019.

- Hoboken van, J., et al., *Hosting Intermediary Services and Illegal Content Online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape,* Instituut voor Informatierecht (IViR) Universiteit van Amsterdam 2018, DOI 10.2759/284542.2018, https://www.ivir.nl/publicaties/download/hosting_intermediary_services.pdf.

- Holmes, A., 'The company behind Facebook's nightmarish moderation center in Florida has canceled its contract with the social network', *Business Insider* 31 oktober 2019, www.businessinsider.nl.

- Hoogervorst, E. en Jahan, P., 'De Tijdelijke Experimentenwet rechtspleging nader beschouwd', Tijdschrift voor Civiele Rechtspleging 2020/3, p. 122-131

- Ikram, M. U. Z., 'Social determinants of ethnic minority health in Europe.' 2016

- Inspectie van Veiligheid en Justitie, *Aanpak van internetoplichting door de politie: Inspectieonderzoek naar een vorm van cybercrime*, 2015.

- Jensma, F., 'Slechte recensie online? Naar de rechter gaan loont', *NRC Handelsblad* 2017, www.nrc.nl.

- JijVandaag, *Onderzoek: Sexting*, 24 april 2017, www.eenvandaag.avrotros.nl.

- Jones, S., 'John Terry case sparks government concern over super-injunctions', *The Guardian*, 31 januari 2010.

- Jong de, R., e.a., 'Het ex parte-bevel', *BIE* mei 2014, p. 104-144.

- Jong de, J., 'AVG, UAVG en Awb', *Nederlands Tijdschrift voor Bestuursrecht* 2018/53.

- Jurdak, R., e.a., 'Protecting the 'right to be forgotten' in the age of blockchain', *The Conversation* 30 oktober 2018, www.theconversation.com.

- Kaye D., *Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* OL ITA 1/2018, 20 maart 2018, www.ohchr.org.

- Keller, D. en Leerssen, P., 'Facts and Where to Find Them: empirical research on internet platforms and content moderation', 16 december 2019, https://papers.ssrn.com/sol3/papers.cfm ?abstract_id=3504930.

- Klonick K 'The new governors: The people, rules, and processes governing online speech', 2018, Harvard Law Review 131: 1598–1670.

- Konings, F. en Wolff Schoemaker, F., *Kijk op doorlooptijden bij (potentieel) rechtszoekende Nederlanders,* 2019.

- Koops, E., 'Tijd voor Computercriminaliteit III, *Nederlands Juristenblad* 85(38), 2010, p. 2461-2466.

- Kramer, X., 'Civiele sancties in het internationale geval in Europees perspectief', in: Hoek van, A., e.a. (red), *Offerhauskring vijftig jaar,* Den Haag: Boom juridisch 2012, p. 73-81.

- Kuczerawy, A. Intermediary Liability and Freedom of Expression in the EU from concepts to safeguards, *KU Leuven Centre for IT & IP law Series* december 2018.

- Kulche, P., 'Persoonlijke Informatie van internet verwijderen', Consumentenbond 28 oktober 2019, https://www.consumentenbond.nl/internet-privacy/persoonlijke-informatie-van -internet-verwijderen.

- Lodder, A. R., Schimmel, M., & van den Winkel, Y., *Hoofdstuk 6 Aansprakelijkheid internet providers*. Amsterdam: Eigen Beheer, 2016.

- Loos, Marco, 'Consumer ADR after Implementation of the ADR Directive: Enforcing European Consumer Rights at the Detriment of European Consumer Law'(October 28, 2015). E*uropean Review of Private Law* 2016/1, p. 61-80, Amsterdam Law School Research Paper No. 2015-42.

- Macdonald, R., 'Access to Civil Justice', in: *The Oxford Handbook of Emperical Research*, Oxford: Oxford University Press 2012.

- Matthiesson, S., 'Who's Afraid of the Limelight? The Trafigura and Terry Super-Injunctions, and the subsequent Fallout', *Journal of Media Law* Volume 2(2), 2010, p. 153-167.

- McGlynn, C.,e.a., *Shattering Lives and Myths: A report on Image-based Sexual Abuse*, Durham: University of Durham 2019, research.monash.edu.

- Mein, A. & Meere, F. de, *Motieven van burgers om (niet) naar de rechter de gaan. Onderzoeksrapportage*, Raad voor de Rechtspraak Research Memoranda 2018/3; https://www.rechtspraak .nl/SiteCollectionDocuments/RM-2018-3.pdf

- Mijn Online IDentiteit, 'Informatie van het internet verwijderen; zo doe je dat', https://www.mijnonlineidentiteit.nl/informatie-van-het-internet-verwijderen/.

- MIND nieuwsbericht, 'Landelijk rapport discriminatiecijfers 2019 gepubliceerd', https://www.mindnederland.nl/actueel.

- Molenaars, L. en Jong de, H., 'De verzoekschriftprocedure ex art. 35 UAVG in het internet-tijdperk. Een noodzakelijke rechtsingang voor de betrokkene?', *Tijdschrift voor Internetrecht* 2019-6, p. 222-229

- Newitt, B., 'Wet Computercriminaliteit III', *Tijdschrift voor Sanctierecht & Onderneming* 2019 nr. 1.

- Newton, C. 'The coronavirus is forcing tech giants to make a risky bet on AI', 18 maart 2020, *The Verge,* https://www.theverge.com/interface/2020/3/18/21183549/coronavirus-content-moderators-facebook-google-twitter /

- Newton, C., 'The Trauma Floor', *TheVerge* 25 februari 2019, www.theverge.com.

- Nieuwsbericht van de Rechtspraak, 'Heerlen krijgt een 'Huis van het Recht", Rechtspraak.nl 2020, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Limburg/Nieuws/Paginas/Heerlen-krijgt-een-Huis-van-het-Recht.aspx.

- Nu.nl (redactie), 'Facebook markeerde nieuwsartikelen over corona perongeluk als spam' 18 maart 2020, https://www.nu.nl/tech/6038360/facebook-markeerde-nieuwsartikelen-over-corona-per-ongeluk-als-spam.html

- Leaseweb, Legal Framework, https://www.leaseweb.com/abuse-prevention/legal-framework.

- Leerssen, P. & J. Harambam. Artificial Intelligence, Content Moderation, and Freedom of Expression, February 26, 2020, Transatlantic Working Group on Content Moderation Online and Freedom of Expression

- Levin, S. 'Google to hire thousands of moderators after outcry over YouTube abuse videos', The Guardian 5 december 2017, www.theguardian.com.

- OECD, *Understanding effective access to justice,* OECD Conference Centre, Paris 4 november 2016, OECD.org.

- Oerlemans, J., 'De Wet computercriminaliteit III: meer handhaving op het internet', *Strafblad 2017/49.*

- Organization for security and Co-operation in Europe (OSCE) and the representative on freedom of the media (Harlem Désir), Communiqué by Representative on Freedom of the Media on Media Pluralism, Safety of Female Journalists and Safeguarding Marginalized Voices Online', Persbericht nr 1/2019, https://www.osce.org/files/2019-02-21%20SOFJO%20Communique.pdf.

- Paul, Kari 'Naked protesters condemn nipple censorship at Facebook headquarters', 3 juni 2019, The Guardian https://www.theguardian.com/technology/2019/jun/03/facebook-nude-nipple-protest-wethenipple

- Pinckaers, J. in: F. Grosheide (red.), *Handhaving van Intellectuele eigendom*, Amsterdam: DeLex 2016.

- Pinckaers, J., 'Ontwikkelingen op het gebied van ex parte verbod, bewijsbeslag en proceskostenveroordeling', *AMI* 2011/4, p. 114-123, Amsterdam: Delex 2011.

- Politie.nl, 'Naaktofot's gelekt', https://www.politie.nl/themas/naaktfotos-gelekt.html.

- Proposition de loi nº 388, adoptée par l'Assemblée nationale, en nouvelle lecture, visant à lutter contre les contenus haineux sur internet, http://www.assemblee-nationale.fr/dyn/15/textes/l15t0388_texte-adopte-seance#B2298414350.

- Raad van Europa, Ministers' Deputies Recommendations, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies*, 7 maart 2018, https://rm.coe.int/1680790e14.

- Raad voor Maatschappelijke Ontwikkeling, *Toegang tot recht* (Advies 32), Den Haag 2014; https://www.rvr.org/binaries/content/assets/rvrorg/informatie-over-de-raad/onderzoeken-en-rapportages/toegang-tot-het-recht/toegang-tot-recht.pdf

- Rapport visitatie gerechten 2018 *Goede rechtspraak sterke rechtsstaat*; https://www.rechtspraak.nl/SiteCollectionDocuments/Rapport%20Visitatie%202018.PDF

- Reglement grijsmaken maatregelen volgens 1019b-d en 1019e Rv, https://www.rechtspraak.nl/SiteCollectionDocuments/Reglement-grijsmaken-maatregelen-volgens-1019b-d-en-1019e-Rv.pdf.

- Report of the Committee on Super-Injunctions*, Super-Injunctions, Anonymised Injunctions and Open Justice*, 20 mei 2011, https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Reports/super-injunction-report-20052011.pdf.

- Rijksoverheid nieuwsbericht, 'Rechtsbijstand: minder procedures, meer oplossingen', 9 november 2018, rijksoverheid.nl.

- Rijksoverheid publicatie, 'Wraakporno', https://www.rijksoverheid.nl/onderwerpen/seksuele-misdrijven/wraakporno.

- Stein/Rueb, *Compendium Burgerlijk procesrecht*, Alphen aan de Rijn: Wolters Kluwer 2018.

- Rodriquez, Salvador 'Covid-19 slowed Facebook's moderation for suicide, self-injury and child exploitation content' 11 augustus 2020, *CNBC* https://www.cnbc.com/2020/08/11/facebooks-content-moderation-was-impacted-by-covid-19.html;

- Runhaar, H., 'Naaktchantage is booming, veel slachtoffers durven niet naar de politie te stappen', *Noordhollands Dagblad* 2019, www. Noordhollandsdagblad.nl.

- Schwemer, S. 'Trusted notifiers and the privatization of online *enforcement*', *Computer Law & Security Review*, Volume 35, Issue 6, 2019, https://doi.org/10.1016/j.clsr.2019.105339.

- SIDN, 'Klacht over inhoud website', https://www.sidn.nl/nl-domeinnaam/klacht-over-inhoud-website.

- Smartt, U., 'Are privacy injunctions futile in the digital age?: Why Scottish papers choose to name the super injunction A-listers -and why they cannot do so online', *European Intellectual property review* Volume 39(7), 2017, p. 413-420.

- Sorkin, David E. 'Judicial Review of ICANN Domain Name Dispute Decisions' *Santa Clara Computer & High Tech*. L.J. 35 (2001-2002).

- Spaink, K., 'Straatverbod', *column op Sargasso* 2017, sargasso.nl.

- *Staatsblad van het Koninkrijk der Nederlanden* 2018, 322.

- *Staatsblad van het Koninkrijk der Nederlanden* 2020, 223.

- *Staatscourant van het Koninkrijk der Nederlanden* 2013, 35757.

- *Staatscourant van het Koninkrijk der Nederlanden* 2018, 54287.

- Stokkom, B., e.a., *Godslastering, discriminerende uitingen wegens godsdienst en haatuitingen. Een inventariserende studie*, (Onderzoek en beleid deel 248), Den Haag: Boom Juridische uitgevers 2007, www.wodc.nl.

- Streel de, A. et al., *Online Platforms' Moderation of Illegal Content Online*, Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.

- Suzor, Nicolas P. *Lawless: The Secret Rules That Govern Our Digital Lives*. Cambridge University Press, 2019.

- Twitter Transparency report*, Twitter Rules Enforcement*, Twitter januari tot juni 2019, https://transparency.twitter.com/en/twitter-rules-enforcement.html.

- Tworek, H R. Ó Fathaigh, L. Bruggeman & C. Tenove, *Dispute resulotion and* content moderation*: Fair, Accountable, Independent, Transparant, and Effective*, Translantic Working Group on Content Moderation Online and Freedom of expression, 2020, https://www.ivir.nl/publicaties/download/Dispute_Resolution_Content_Moderation_Final.pdf.

- UN Special Rapporteur, 'UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', *OL ITA* 1/2018.

- Veenen van, J., 'Legal Tech Map', 17 april 2018, dutchlegaltech.nl.

- Ven van der, H., 'Leerlinge Commanderij College Gemert slachtoffer trucagefilmpje: 'lastig om dader te achterhalen", *Eindhovens Dagblad* 2019, ed.nl.

- Voert ter, M., en Klein Haarhuis, C., *Geschilbeslechtingsdelta 2014. Over verloop en afloop van (potentieel) juridische problemen van burgers* (onderzoek en beleid 315), Den Haag: Boom Lemma 2015, wodc.nl.

- Voert, M. ter, *Factsheet 2018-6: Rechtshulp civiel- en bestuursrechtelijke problemen*, Den Haag: WODC 2018; https://www.wodc.nl/binaries/FS%202018-6_tcm28-331870.pdf

- Vraag het de politie, 'Pesten & Online', https://www.vraaghetdepolitie.nl/pesten-en-online.

- Website betreffende de Manilla Principes: https://www.manilaprinciples.org/.

- Website van de Agencia Espanola Proteccion Datos, https://sedeagpd.gob.es /sede-electronica-web/vistas/infoSede/inicio.jsf.

- Wetenschappelijke Raad voor het Regeringsbeleid, *Weten is nog geen doen. Een realistisch perspectief op redzaamheid*, Den Haag 2017; https://www.wrr.nl/publicaties/rapporten /2017/04/24/weten-is-nog-geen-doen

- We Transfer, 'Notice and Take Down policy', 11 juni 2013, https://wetransfer.com/legal /takedown.

- Whatsapp FAQ, 'End-to-end versleuteling', https://faq.whatsapp.com/general/security-and -privacy/end-to-end-encryption/.

- Woman's Aid, 'Digital Abuse of Woman; https://www.womensaid.ie/assets/files/pdf/digital _abuse_of_women_information_guide.pdf.

- Woman's Aid, 'Submission to the Committee on Justice and Equality on Online Harassment, Harmful Communications and Related Offences, september 2019, https://www.womensaid.ie /assets/files/pdf/submission_to_the_committee_on_justice_and_equality_on_online_harassment _harmful_communications_and_related_offences.pdf.

- Zheng, Z., e.a., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", *2017 IEEE International Congress on Big Data (BigData Congress)* 2017, p. 557-564, Honolulu, HI, USA 2017, p. 557-564, doi: 10.1109/BigDataCongress.2017.85.

Parlementaire stukken

- *Kamerstukken II* 2005/06, 30392, 3.

- *Kamerstukken II* 2013/14, 33662, 6

- *Kamerstukken II* 2017/18, 34851, 3.

- Kamerbrief Burgerinitiatief 'Internetpesters aangepakt', *Kamerstukken II* 2018/19, 34602, 2.

- *Kamerstukken II* 2019/20, 35263, 21.

Jurisprudentie

- EHRM 21 februari 1975, ECLI:NL:XX:1975:AB5466 (*Golder/Verenigd Koninkrijk*).
- EHRM 7 december 1976, ECLI:CE:ECHR:1976:1207JUD000549372 (*Handyside/Verenigd Koninkrijk*).
- EHRM 26 april 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (*Sunday Times/Verenigd Koninkrijk*).
- EHRM 9 oktober 1979, appl. No 6289/73 (*Airey/Ierland*).
- EHRM 11 oktober 1979, appl. nos. 8348/78 & 8406/78 (*Glimmerveen en Hagenbeek/Nederland*).
- EHRM 8 juli 1986, ECLI:CE:ECHR:1986:0708JUD000981582 (*Lingens/Oostenrijk*).
- EHRM 4 december 1995 ECLI:CE:ECHR:1995:1204JUD002380594 (Bellet/Frankrijk).
- EHRM 18 februari 1997 appl. no. 18990/91 (*Nideröst-Huber/Zwitserland*).
- EHRM 19 juni 2001, appl. no. 28249/95 (*Kreuz/Polen*)
- EHRM 7 mei 2002, appl. no. 46311/99 (McVicar v Verenigd Koninkrijk)
- EHRM 24 juni 2003, ECLI:CE:ECHR:2003:0624DEC006583101 (*Garaudy/Frankrijk*).
- EHRM 24 juni 2004, ECLI:CE:ECHR:2004:0624JUD005932000 (*Von Hannover/Duitsland 1*).
- EHRM 16 november 2004, ECLI:CE:ECHR:2004:1116DEC002313103 (*Norwood/Verenigd Koninkrijk*).
- EHRM 15 februari 2005 appl. no .68416/01, ECLI:CE:ECHR:2004:0406DEC006841601 (*Steel and Morris v Verenigd Koninkrijk*)
- EHRM 9 januari 2007 ECLI:CE:ECHR:2007:0109JUD005174499 (*Kwiecién/Polen*).
- EHRM 2 december 2008 ECLI:CE:ECHR:2008:1202JUD000287202 (*K.U./Finland*).
- EHRM 15 oktober 2009, appl. no. 17056/06 (*M. v Malta*)
- EHRM 14 september 2010, appl. no. 38224/03 (*Sanoma/Nederland*).
- EHRM 10 mei 2011 ECLI:CE:ECHR:2011:0510JUD004800908 (*Mosley/Verenigd Koninkrijk*).
- EHRM 7 februari 2012 ECLI:NL:XX:2012:BW0603 (*Springer/Germany*).
- EHRM 20 oktober 2015, ECLI:CE:ECHR:2015:1020DEC002523913 (*M'Bala M'Bala/Frankrijk*).
- EHRM 7 februari 2017 ECLI:CE:ECHR:2017:0207DEC007474214 (*Pihl/Sweden*).
- EHRM 7 november 2017 ECLI:CE:ECHR:2017:1107JUD002470315 (Egeill Einarsson/IJsland).

- EHRM 6 december 2018, appl. no. 68924/12 (*Słomka/Polen*).
- EHRM 30 april 2019, appl. nos. 48310/16 en 59663/17 (*Kablis/Rusland*).
- EHRM 25 juli 2019, 47542/07 (*Brzeziński/Polen*).
- EHRM 10 oktober 2019 ECLI:CE:ECHR:2019:0110JUD006528613 (*Khadija Ismayilova/Azerbeidzjan*).
- EHRM 14 januari 2020 ECLI:CE:ECHR:2020:0114JUD004128815 (*Beizaras en Levickas/Litouwen*).
- HvJEU 16 december 2008, ECLI:EU:C:2008:727 (*Satamedia*).
- HvJEU 17 november 1998, ECLI:EU:C:1998:543 (*Van Uden/Deco-Line*).
- HvJEU 18 maart 2010, ECLI:EU:C:2010:146 (*Alassini/Telecom Italia*).
- HvJEU 25 oktober 2011, ECLI:EU:C:2011:685 (*eDate/Martinez*).
- HvJEU 22 december 2010 ECLI:EU:C:2010:811 (*DEB v Bondsrepubliek Duitsland*)
- HC (QB) 6 oktober 2017, HQ17M03348 (AI-KO Kober Ltd & Anor/Balvinder Sambhi).
- Hof 's-Hertogenbosch 1 februari 2018, ECLI:NL:GHSHE:2018:363.
- Hof Amsterdam 5 november 2019, ECLI:NL:GHAMS:2019:3966.
- Hof Den Haag 15 december 2015, ECLI:NL:GHDHA:2015:3815.
- Hof Den Haag 29 januari 2013, ECLI:NL:GHDHA:2013:BZ0458.
- HR 14 juni 2013, ECLI:NL:HR:2013:CA2788 (Cruijff/Tirion Uitgevers).
- HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers).
- HR 29 juni 2001, ECLI:NL:HR:2001:AB2391 (Impag/Hasbor).
- HR 7 januari 2006, ECLI:NL:HR:2006:AU5787.
- Rb. 's-Gravenhage 4 mei 2011, ECLI:NL:RBSGR:2011:BQ3525 (Nadia Plesner Joensen/Louis Vuitton Malletier).
- Rb. Amsterdam 15 juni 2012, ECLI:NL:RBAMS:2012:BW9838.
- Rb. Amsterdam 25 juni 2015, ECLI:NL:RBAMS:2015:3984.
- Rb. DeHaag 26 maart 2010, B9 8722 (Vlisco/V&D).
- Rb. Den Haag 14 december 2009, B9 8453 (Kruidvat/Adventure Bags).
- Rb. Den Haag 18 december 2009, B9 8486 (Ten Berg/Bodum).

- Rb. Den Haag 19 december 2008, B9 7519 (Go Fast Sports/Lucky Times c.s.).
- Rb. Den Haag 28 juni 2019, ECLI:NL:RBDHA:2019:6302.
- Rb. Den Haag 31 augustus 2018, ECLI:NL:RBDHA:2018:10449.
- Rb. Den Haag 4 mei 2011, ECLI:RBSGR:2011:BQ3525 (Nadia Plesner Joensen/Louis Vuitton Malletier).
- Rb. Haarlem 31 augustus 2007, ECLI:NL:RBHAA:2007:BB3561.
- Rb. Noord-Nederland 16 september 2016, ECLI:NL:RBNO:2016:7720.
- Rb. Rotterdam 27 augustus 2018, ECLI:NL:RBROT:2018:7070.
- RvS 21 februari 2018, ECLI:NL:RVS:2018:590.

Regelgeving

- Artikel 1:2 jo. Artikel 7:1 jo. Artikel 8:1 van de Algemene wet bestuursrecht.
- Artikel 1:3 lid 3 van de Algemene wet bestuursrecht.
- Artikel 1019g van Rechtsvordering.
- Artikel 1019i lid 1 van Rechtsvordering.
- Artikel 12 lid 4 jo. Artikel 13 lid 2 sub d jo. Artikel 14 lid 2 sub e jo. Artikel 15 sub f van de Algemene Verordening Gegevensbescherming.
- Artikel 12 van de 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 (“Richtlijn inzake elektronische handel”).
- Artikel 12-15 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 (“Richtlijn inzake elektronische handel”).
- Artikel 139h van het Wetboek van Strafrecht.
- Artikel 15-21 van de Algemene Verordening Gegevensbescherming jo. Artikel 35 van de Uitvoeringswet Algemene Verordening Gegevensbescherming en Artikel 79 Algemene Verordening Gegevensbescherming.
- Artikel 18 lid 2 jo. Overweging 67 Algemene Verordening Gegevensbescherming.
- Artikel 2 lid 2 van het besluit van de Autoriteit Persoonsgegevens van 20 september 2018, houdende de vaststelling van beleidsregels met betrekking tot de prioritering van klachtenonderzoek (Beleidsregels prioritering klachtenonderzoek AP), www.wetten.overheid.nl.

- Artikel 2 Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking)Voor de EER relevante tekst.

- Artikel 2 van de Richtlijn 2004/48/EG van het Europees Parlement en De Raad van 29 april 2004 betreffende de handhaving van intellectuele-eigendomsrechten (PbEU 2004, L 195/16).

- Artikel 285 onderdeel b van het Wetboek van Strafrecht.

- Artikel 3 lid 4 van de 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 (“Richtlijn inzake elektronische handel”).

- Artikel 32 van de Algemene Verordening inzake Gegevensbescherming.

- Artikel 33 van de Algemene Verordening inzake Gegevensbescherming.

- Artikel 34 van de Algemene Verordening inzake Gegevensbescherming.

- Artikel 36 van de Uitvoeringswet Algemene Verordening Gegevensbescherming.

- Artikel 43 van de Uitvoeringswet Algemene Verordening Gegevensbescherming ter implementatie van Artikel 85 Algemene Verordening Gegevensbescherming.

- Artikel 4 lid 1 jo. Artikel 77 van de Algemene Verordening Gegevensbescherming.

- Artikel 57 lid 1 sub f jo. Artikel 57 lid 3 jo. Artikel 56 lid 2 van de Algemene Verordening Gegevensbescherming.

- Artikel 57 lid 1 sub f van de Algemene Verordening Gegevensbescherming.

- Artikel 58 lid 1 van de Algemene Verordening Gegevensbescherming jo. Hoofdstuk 5 van de Algemene wet bestuursrecht.

- Artikel 58 lid 2 van de Algemene Verordening Gegevensbescherming jo. Artikel 5:32 van de Algemene wet bestuursrecht.

- Artikel 6 lid 1 sub e-f Algemene Verordening Gegevensbescherming.

- Artikel 6 van de Algemene Verordening inzake Gegevensbescherming.

- Artikel 6:4 jo. Artikel 7:1 jo. Artikel 8:104 jo. Artikel 8:5 jo. Bijlage 2 van de Algemene wet bestuursrecht.

- Artikel 60 ev. van de Algemene Verordening Gegevensbescherming.

- Artikel 77 jo. Artikel 57 lid 2 jo. Overweging 116 van de Algemene Verordening Gegevensbescherming.

- Artikel 77 jo. Artikel 80 jo. Overweging 141 tot 142 van de Algemene Verordening Gegevensbescherming.

- Artikel 77 lid 2 van de Algemene Verordening Gegevensbescherming.

- Artikel 77-78 van de Algemene Verordening Gegevensbescherming.

- Artikel 78 lid 2 jo. Artikel 57 lid 1 sub f jo. Artikel 77 lid 2 van de Algemene Verordening Gegevensbescherming.

- Artikel 78 lid 2 van de Algemene Verordening Gegevensbescherming.

- Artikel 78 van de Algemene Verordening Gegevensbescherming.

- Artikel 80 jo. Overweging 142 van de Algemene Verordening Gegevensbescherming.

- Artikel 8sexies van het Wetboek van Strafrecht.

- Besluit van 4 juli 2001, houdende nadere regels inzake de ambtshandelingen van gerechtsdeurwaarders en de tarieven (Besluit tarieven ambtshandelingen gerechtsdeurwaarders).

- Besluit van de Autoriteit Persoonsgegevens van 20 september 2018, houdende de vaststelling van beleidsregels met betrekking tot de prioritering van klachtenonderzoek (Beleidsregels prioritering klachtenonderzoek AP), www.wetten.overheid.nl.

- Considerans 40 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 (“Richtlijn inzake elektronische handel”).

- Hoofdstuk 3 van de Algemene Verordening inzake Gegevensbescherming.

- LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l’information (1).

- Notice and Takedown 2018, *Gedragscode Notice-and-Take-Down,* 13 december 2018, https://noticeandtakedowncode.nl/ntd-code/.

- Overweging 65 Algemene Verordening Gegevensbescherming.

- Richtlijn (EU) 2018/1808 van het Europees Parlement en de Raad van 14 november 2018 tot wijziging van Richtlijn 2010/13/EU betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten) in het licht van een veranderende marktsituatie.

- Richtlijn 2010/13/EU van het Europese Parlement en de Raad van 10 maart 2010 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake het aanbieden van audiovisuele mediadiensten (richtlijn audiovisuele mediadiensten).

- Richtlijn 2012/29/EU van het Europees Parlement en de Raad van 25 oktober 2012 tot vaststelling van minimumnormen voor de rechten, de ondersteuning en de bescherming van slachtoffers van strafbare feiten, en ter vervanging van Kaderbesluit 2001/220/JBZ.

- Wet ter verbetering van de handhaving van de wet op de sociale netwerken (wet op de netwerkhandhaving) 2017, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren /Dokumente/NetzDG_engl.pdf?__ blob=publicationFile=2.

Annex i
Begeleidingscommissie

- prof. dr. mr. G.J. Zwenne (voorzitter) - advocaat en hoogleraar Law and Digital Technologies, Universiteit Leiden
- dr. S.B.L. Leferink - senior onderzoeker Provincie Overijssel
- drs. L.F. Heuts - onderzoeker WODC
- mr. N. ten Kate - wetgevingsjurist DWJZ, Ministerie van Justitie en Veiligheid
- mr. P.V.F.L. Breitbarth - Director EU Policy & Strategy, TrustArc Inc.

Annex ii
Verkorte leidraad expert workshop

i. Probleemanalyse

- Onrechtmatige en schadelijke online content wordt in Nederland ervaren als een maatschappelijk probleem. Uit de afgenomen survey blijkt dat 15% van de Nederlanders (in)direct ervaring heeft met schadelijke online content en uit de expertinterviews blijkt dat er een maatschappelijke noodzaak gevoeld wordt tot de verbetering van de mogelijkheden om onrechtmatige online content verwijderd te krijgen;
- Onrechtmatige online content kan zeer schadelijk zijn vanwege de potentieel grote schaal en snelheid waarop het verspreid kan worden. Het open en decentrale karakter van het internet maakt, daarnaast, dat online content soms moeilijk definitief verwijderd kan worden;
- Het wereldwijde karakter van het internet staat ook in contrast met het nationale karakter van wet- en regelgeving, wat op punten spanningen oplevert;
- Tegelijkertijd is juist dit open en decentrale karakter van groot maatschappelijk belang, ook vanuit het perspectief van de vrijheid van meningsuiting;
- Het verwijderd krijgen van content kan moeilijker zijn bij kleine, ongrijpbare, websites en hosting providers ten opzichte van de grote sociale media platforms die hiervoor een eigen mechanisme hebben en vatbaarder zijn voor maatschappelijke druk. Capaciteit speelt hierbij een belangrijke rol.

ii. Specifieke knelpunten

Vanuit de rechtszoekende

- Veelal ervaart de rechtszoekende problemen met het vinden van de juiste partij om aan te spreken. Afhankelijk van de situatie kan de hostingprovider, het sociale media platform of degene die de uiting doet aangesproken worden. Verder kan de hostingprovider moeilijk te contacteren zijn of in het buitenland gevestigd, of is onbekend wie de uiting geplaatst heeft;
- Het verwijderen van onrechtmatige online content betreft juridisch gezien specialistische problematiek waardoor veel gebruikte laagdrempelige instanties zoals wetwinkels of het juridisch loket niet altijd even goed kunnen helpen;
- In voorkomende gevallen is niet zozeer het verwijderd krijgen van de content, de take-down, problematisch, maar zit het knelpunt in het verwijderd houden, de stay-down. Dezelfde onrechtmatige content kan via andere partijen weer terugkomen.

Procedurele problemen

- Wanneer een partij, bijvoorbeeld de hostingprovider, in het buitenland gevestigd is, kan dat betekenen dat deze in de praktijk onbereikbaar is voor rechtszoekenden. In dit kader is door sommigen voorgesteld om, naar Amerikaans voorbeeld, tegen een anonieme partij te kunnen procederen om de uitspraak te verkrijgen dat bepaalde content onrechtmatig is;
- In een civiele zaak de betekening van internationale partijen zoals Google of Facebook een vertragende en kostenverhogende factor zijn;
- De beschikbare procedurele en technische mogelijkheden voor het verwijderen van onrechtmatige content moeten mede afhankelijk zijn van het type onrechtmatigheid. Zo vergt de problematiek van wraakporno een andere behandeling dan online pesten;
- Het vaststellen van de onrechtmatigheid van online content die mensen in hun persoon raakt is complex en vereist vaak een uitgebreide afweging van belangen en grondrechten. De impact op de vrijheid van meningsuiting en de ruimte voor interpretatie bij het vaststellen van de onrechtmatigheid maakt dat een rechterlijk oordeel vanuit dat oogpunt de voorkeur heeft;

- De doorlooptijd en complexiteit van een civiele procedure is een belangrijke drempel, ook in kort geding.

Rechtssysteem

- In hoeverre is een aparte procedure voor deze specifieke problematiek gerechtvaardigd in het licht van andere situaties waar rechtszoekende problemen ervaren met de toegang tot het recht?
- In voorkomende gevallen is de verhouding tussen de beschikbare routes niet helder (vanuit het perspectief van rechtszoekenden).

iii. Mogelijke oplossingsrichtingen

- Verbetering van de informatievoorziening voor rechtszoekenden over de beschikbare juridische en technische routes om onrechtmatige online content verwijderd te krijgen;
- Uitbreiding van bestaande procedurele mogelijkheden, zoals de verzoekschriftprocedure, ex parte-procedure of een kantonrechterskortgeding (zonder verplichte procesvertegenwoordiging) met korte doorlooptijd voor spoedeisende gevallen.
- Een centraal meldpunt (met directe ingangen bij o.a. de Autoriteit Persoonsgegevens en de politie om snel te kunnen schakelen) waar mensen terechtkunnen voor informatie en advies over de routes die ze kunnen bewandelen.

Annex iii
Verkorte leidraad expert interviews

Algemene vragen

1. Kunt u toelichten wat uw eigen ervaring is met verzoeken tot verwijdering van onrechtmatige online content en de bestaande mogelijkheden daartoe?
2. In welke mate en in welk opzicht denkt u dat onrechtmatige online content een maatschappelijk probleem vormt?
3. In hoeverre kunt u een inschatting geven van de maatschappelijke behoefte aan een voorziening voor verzoeken tot snelle verwijdering van online content?
4. Meer specifiek, waar zou naar uw oordeel het zwaartepunt moeten liggen bij de vormgeving van een nieuwe of aangepaste voorziening?

Knelpuntanalyse

Valorisatie

1. Kunt u zich vinden in het beeld dat uit de knelpuntanalyse rijst?
2. Waar ziet u de grootste obstakels voor de snelle verwijdering van onrechtmatige online content?
3. Welke criteria zijn in de context van de geschetste problematiek het meest relevant in uw optiek?
4. In hoeverre maakt het type onrechtmatige content uit voor de wijze van verwijdering?

Toevoeging

1. Welke aanvullende criteria en/of gezichtspunten kunt u nog noemen in dit verband?
2. Zijn er nog procedurele of andere aspecten die in de knelpuntenanalyse tot nu toe onderbelicht zijn gebleven?
3. Hebt u nog andere opmerkingen of toevoegingen?

Specifieke onderwerpen

- Kunt u vanuit uw eigen ervaring aangeven tegen welke problemen rechtszoekenden aan lopen in de context van de geschetste problematiek?
- Zou de ex parte-procedure zich volgens u lenen voor het soort verwijderverzoeken waar dit onderzoek op is gericht? Waarom wel of niet?
- Op welke manier zou in uw visie rekening gehouden moeten worden met de belangen van de betrokken partijen bij zowel de (procedurele) vormgeving van een nieuwe of aangepaste voorziening als de (materiële) beoordeling van een verwijderverzoek?
- Hoe beoordeelt u de rol van de internettussenpersoon in de snelle verwijdering van onrechtmatige online content, en indien mogelijk, kunt u aangeven waar de uitdagingen liggen?
- Hoe beoordeelt u de rol van de Autoriteit Persoonsgegevens in de verwijdering van onrechtmatige online content?
- Wat is uw visie op de rechtsbescherming die het gegevensbeschermingsrecht individuen biedt?
- Wat zijn de problemen waar de politie en het OM tegenaan lopen bij de opsporing en vervolging van strafbare feiten die verband houden met deze problematiek?
- Hoe beoordeelt u de ruimte voor Nederland ten opzicht van Europese wetgeving en (internationale) zelfregulering om een nieuwe procedure voor de snelle verwijdering van online content te creëren?

Annex iv
Deelnemers expert interviews en workshop

i. Overzicht deelnemers expertinterviews

Naam	Organisatie
Milica Antic	Head of Legal Netherlands, Google
Christiaan Alberdingk Thijm	Advocaat, Bureau Brandeis
Marleen Balk	Stafjurist, Rechtbank Amsterdam
Jacqueline Bonnes	Officier van justitie Cybercrime en Digitaal Bewijs
Rainier Braat	Senior jurist, DAS Rechtsbijstand
Remy Chavannes	Advocaat, Brinkhof Advocaten
Quirine Eijkman	Ondervoorzitter, College voor de Rechten van de Mens en lector Toegang tot het Recht, Hogeschool Utrecht
Arjan El Fassed	Head of Public Policy Netherlands, Google
Herman van Harten	Rechter, Rechtbank Den Haag
Edo Haveman	Head of Public Policy Netherlands, Facebook
Sikke Kingma	Advocaat, Pels Rijcken & Droogleever Fortuijn
Willem Korthals Altes	Senior rechter en lid VMC Studiecommissie Uitingsdelicten
Alex de Joode	Public Policy Manager, NL Digital (ten tijde van interview)
Gijs van der Linden	Teamleider Landelijk Meldpunt Internetoplichting
Chantal Malfeyt	Head of Government Relations eBay Classifieds Group
Esther Mieremet	Projectadviseur Platform voor de Informatie Samenleving
Sjoera Nas	Senior Privacy Adviseur, Privacy Company
Peter van der Veen	Coördinator internationaal onderzoek, Autoriteit Persoonsgegevens
Dirk Visser	Advocaat Visser Schaap & Kreijger en hoogleraar IE-recht, Universiteit Leiden
Mirjam van Walraven	Rechter en teamvoorzitter kort geding, Rechtbank Amsterdam
Bastiaan Winkel	Beleidsadviseur Criminaliteit en Veiligheid, Ministerie van Justitie en Veiligheid
Rejo Zenger	Beleidsadviseur, Bits of Freedom
Parketsecretaris	Kennis- en Expertisecentrum Cybercrime, Openbaar Ministerie

ii. Overzicht deelnemers expertworkshops

Naam	Organisatie
Peter Blok	Raadsheer, Gerechtshof Den Haag en hoogleraar Octrooirecht en Privacy, Universiteit Utrecht
Ruth de Bock	Advocaat-generaal bij de Hoge Raad en deeltijdhoogleraar Civiele rechtspleging, Universiteit van Amsterdam
Thomas Bruning	Algemeen secretaris, Nederlandse Vereniging van Journalisten
Carina van Eck	Vicevoorzitter, Stichting Stop Online Shaming
Stefan Kulk	Universitair hoofddocent, Universiteit Utrecht

Ron Lamme	Advocaat, Boekx Advocaten
Cyril van der Net	Raadadviseur/Projectmanager Auteursrecht, Ministerie van Justitie en Veiligheid
Justine Pardoen	Oprichter Bureau Jeugd & Media
Remco Pijpers	Strategisch adviseur digitale geletterdheid, Stichting Kennisnet
Maurice Schellekens	Universitair docent, Tilburg University
Paul Tjiam	Advocaat, Simmons & Simmons
Folkert Wilman	Legal Service, Europese Commissie (op persoonlijke titel)
Otto Volgenant	Advocaat, Boekx Advocaten

Annex v
Survey

In deze vragenlijst vragen we naar uw mening over schadelijke informatie op internet en uw eigen ervaringen met dit onderwerp.

Vraag 1 Hebt u ooit te maken gehad met voor u schadelijke informatie op internet?

- ☐ Ja
- ☐ Nee

Vraag 2 Heeft een lid van uw huishouden ooit te maken gehad met voor hem of haar schadelijke informatie op internet?

- ☐ Ja
- ☐ Nee

Misschien zijn er vormen van schadelijke informatie waar u bij voorgaande vragen niet aan hebt gedacht.

Vraag 3 Met welke van onderstaande vormen van schadelijke informatie op internet hebt u of hebben uw huishoudleden wel eens te maken gehad?

Het gaat om inhoud die voor u of een lid van uw huishouden schadelijk is/was. Meerdere antwoorden mogelijk. Als u met geen van deze vormen te maken hebt gehad, kiest u dan voor 'Geen van bovenstaande'.

- ☐ Ongewilde publicatie van privé-informatie
- ☐ Publicatie van onjuiste of verouderde gegevens
- ☐ Publicatie van foto's en video's die inbreuk maken op uw privacy of reputatie
- ☐ Verspreiding van seksueel beeldmateriaal, bv. Door een ex-partner
- ☐ Pesten
- ☐ Bedreiging
- ☐ Stalking
- ☐ Belediging
- ☐ Valse beschuldigingen of verdachtmakingen
- ☐ Discriminatie
- ☐ Commercieel gebruik van uw informatie zonder toestemming
- ☐ Datalekken
- ☐ Geen van bovenstaande

Vraag 4 Waar kwam u of uw huishoudlid de schadelijke inhoud tegen?

Meerdere antwoorden mogelijk.

- ☐ Op een sociaal medium, zoals Facebook, Twitter, Instagram
- ☐ Op een app als SnapChat of TikTok
- ☐ Op een videodienst zoals YouTube, Twitch, Dumpert
- ☐ Op een messaging dienst, zoals Whatsapp of Facebook messenger
- ☐ Op een datingsite of app
- ☐ Op een internetforum
- ☐ Een zoekmachine zoals Google, Bing
- ☐ Op een nieuwssite of blog
- ☐ Op een online marktplaats voor de verkoop van tweedehands goederen
- ☐ Anders, namelijk

Vraag 5 Welke drie vormen van schadelijke informatie op internet vindt u het grootste probleem?

Geeft u een 1 aan wat volgens u het grootste probleem is, een 2 aan het daarna grootste probleem en een 3 aan het volgens u daarna grootste probleem.

Ongewilde publicatie van privé-informatie	☐
Publicatie van onjuiste of verouderde gegevens	☐
Publicatie van foto's en video's die inbreuk maken op uw privacy of reputatie	☐
Verspreiding van seksueel beeldmateriaal, bv. Door een ex-partner	☐
Pesten	☐
Bedreiging	☐
Stalking	☐
Belediging	☐
Valse beschuldigingen of verdachtmakingen	☐
Discriminatie	☐
Commercieel gebruik van uw informatie zonder toestemming	☐
Datalekken	☐

Vraag 6 In het algemeen, hebt u wel eens gebruik gemaakt van een mogelijkheid om schadelijke informatie te rapporteren (voor uzelf of iemand anders)?

Het gaat hier om een mogelijkheid die door de betreffende dienst zelf, bv. Facebook of Youtube, wordt aangeboden.

- ☐ Ja
- ☐ Nee

Vraag 7 Hoe bekend bent u met de mogelijkheden om schadelijke informatie te rapporteren?

Het gaat hier om een mogelijkheid die door de betreffende dienst zelf wordt aangeboden.

helemaal niet bekend	1	2	3	4	5	6	7	heel goed bekend
	☐	☐	☐	☐	☐	☐	☐	

Vraag 8 Hoe vaak maakt u gebruik van de aangeboden mogelijkheid om schadelijke informatie te rapporteren?

☐ Nog nooit gebruik van gemaakt
☐ Hoogstens eens per jaar
☐ Een aantal keer per jaar
☐ Ongeveer één keer per maand
☐ Meerdere keren per maand

Vraag 9 Hoe tevreden bent u over de aangeboden mogelijkheden om schadelijke informatie te rapporteren?

heel erg ontevreden	1	2	3	4	5	6	7	heel erg tevreden
	☐	☐	☐	☐	☐	☐	☐	

Vraag 10 Wat vindt u belangrijk als u de mogelijkheid krijgt om schadelijke informatie te rapporteren?

Noemt u hierbij uw top drie van belangrijkste eigenschappen. Geeft u een 1 aan de eigenschap die u het belangrijkst vindt, een 2 aan de eigenschap die u daarna het belangrijkst vindt en een 3 aan de eigenschap die u daarna het belangrijkst vindt.

Dat deze makkelijk vindbaar is.	☐
Dat deze gebruiksvriendelijk is.	☐
Dat deze begrijpelijk is.	☐
Dat deze anoniem te gebruiken is.	☐
Dat ik iemand persoonlijk kan spreken.	☐
Dat rapportering snel wordt afgehandeld.	☐
Dat er sprake is van een grondige toetsing van de rapportering.	☐
Dat de gerapporteerde inhoud ook echt verwijderd wordt.	☐
Dat u na afloop een gemotiveerde reactie op de rapportering krijgt.	☐
Dat de vrijheid van meningsuiting wordt beschermd.	☐

Vraag 11 Hebt u wel eens informatie op internet gezet, die werd verwijderd na een klacht over deze informatie?

☐ Ja
☐ Nee

Vraag 12 Hebt u wel eens juridische stappen overwogen met betrekking tot voor u schadelijke informatie op internet?

- ☐ Ja
- ☐ Nee

Vraag 13 Hebt u wel eens juridische stappen ondernomen met betrekking tot voor u schadelijke informatie op internet?

- ☐ Ja
- ☐ Nee

Vraag 14 Welke soort juridische stappen hebt u wel eens overwogen of ondernomen met betrekking tot voor u schadelijke informatie op internet?

Meerdere antwoorden mogelijk.

- ☐ Zoeken van informatie over uw rechten en het juridisch kader
- ☐ Informeren bij een rechtswinkel
- ☐ Zoeken van een advocaat
- ☐ Contact met rechtsbijstandsverzekering
- ☐ Een juridische procedure bij de rechter
- ☐ Klacht bij de Autoriteit Persoonsgegevens
- ☐ Aangifte bij de politie
- ☐ Anders, namelijk _____

Vraag 15 In welke mate zouden onderstaande zaken u tegenhouden om juridische stappen te ondernemen?

	Dit houdt mij helemaal niet tegen	1	2	3	4	5	6	7	Dit houdt mij erg tegen
Het kost geld									
Het kost moeite									
Ik ben niet bekend met de relevante wetten en regels									
Het is moeilijk om een juridische procedure te beginnen									
Een juridische procedure kan lang duren									
Ik heb weinig vertrouwen dat er een onafhankelijke en onpartijdige rechter naar mijn zaak zal kijken									
Het is onzeker of ik een positieve uitkomst krijg									
Ik heb weinig vertrouwen dat er een rechtvaardig oordeel komt									

Afsluitende vragen:

NB: Maakt u alstublieft de vragenlijst af totdat u weer bij het beginscherm komt. Pas dan registreert het systeem de vragenlijst als volledig ingevuld.

Tot slot. Wat vond u van deze vragenlijst:

1 = beslist niet 5 = beslist wel

	1	2	3	4	5
Vond u het moeilijk om de vragen te beantwoorden?	☐	☐	☐	☐	☐
Vond u de vragen duidelijk?	☐	☐	☐	☐	☐
Heeft de vragenlijst u aan het denken gezet?	☐	☐	☐	☐	☐
Vond u het onderwerp interessant?	☐	☐	☐	☐	☐
Vond u het plezierig om de vragen in te vullen?	☐	☐	☐	☐	☐

Hebt u nog opmerkingen over deze vragenlijst?

☐ Ja
☐ Nee

Annex vi
Resultaten survey

i. Algemene info

Totale steekproefgrootte: 1576 respondenten

Leeftijd	Minimum Leeftijd	Maximum Leeftijd	Gemiddelde	Std. deviatie
Leeftijd van respondents	16	102	53,65	18,553
Valid N (listwise)				

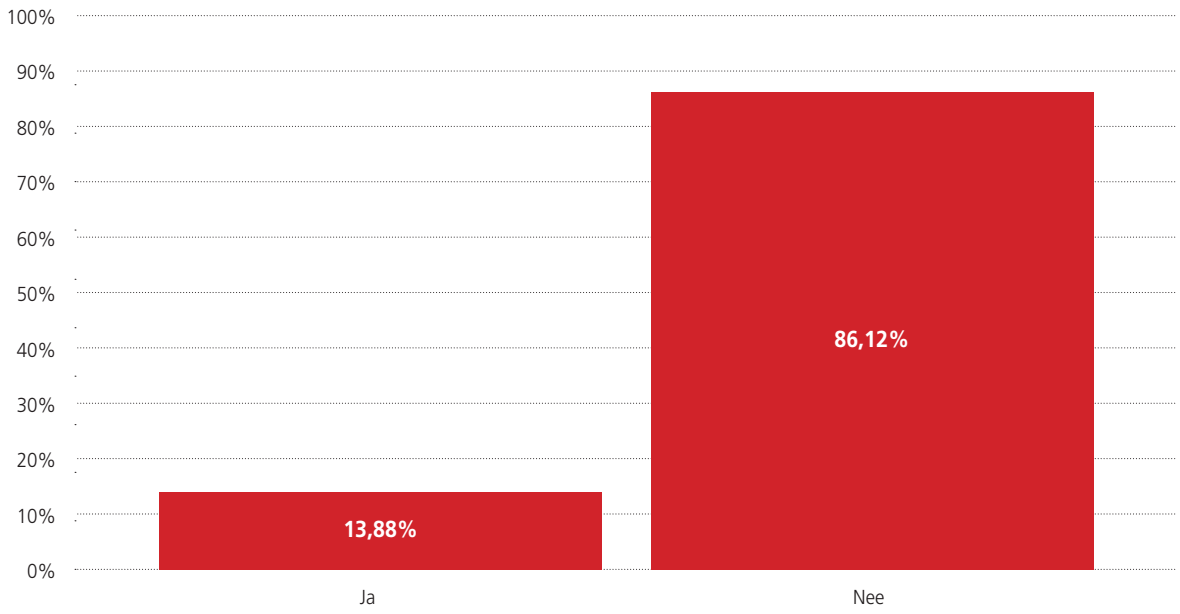
Leeftijdcategorie		Frequency	Percent
Valid	15 - 24 jaar	136	8,6
	25 - 34 jaar	194	12,3
	35 - 44 jaar	153	9,7
	45 - 54 jaar	239	15,2
	55 - 64 jaar	309	19,6
	65 jaar en ouder	545	34,6
	Total	1576	100,0

Gender		Frequency	Percent
Valid	Man	731	46,4
	Vrouw	845	53,6
	Total	1576	100,0

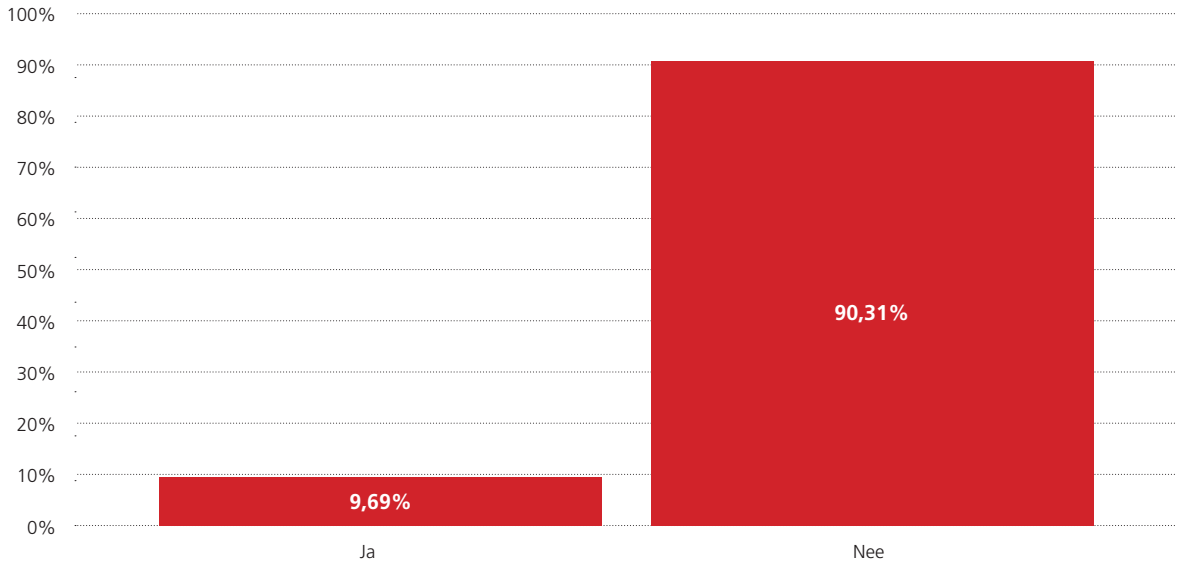
Opleiding		Frequency	Percent
Valid	basisonderwijs	121	7,7
	vmbo	312	19,8
	havo/vwo	176	11,2
	mbo	391	24,8
	hbo	379	24,0
	wo	194	12,3
	Total	1573	99,8

ii. Surveyresultaten

Vraag 1 **Hebt u ooit te maken gehad met voor u schadelijke informatie op internet?**



Vraag 2 **Heeft een lid van uw huishouden ooit te maken gehad met voor hem of haar schadelijke informatie op internet?**



Vraag 3 Met welke van onderstaande vormen van schadelijke informatie op internet hebt u of hebben uw huishoudleden wel eens te maken gehad?

Ongewilde publicatie van privé-informatie		Frequency	Percent
Valid	Nee	1515	96,1
	Ja	61	3,9
	Total	1576	100,0

Publicatie van onjuiste of verouderde gegevens		Frequency	Percent
Valid	Nee	1525	96,8
	Ja	51	3,2
	Total	1576	100,0

Publicatie van foto's en video's die inbreuk maken op uw privacy of reputatie		Frequency	Percent
Valid	Nee	1522	96,6
	Ja	54	3,4
	Total	1576	100,0

Verspreiding van seksueel beeldmateriaal, bv. door een ex-partner		Frequency	Percent
Valid	Nee	1566	99,4
	Ja	10	,6
	Total	1576	100,0

Pesten		Frequency	Percent
Valid	Nee	1520	96,4
	Ja	56	3,6
	Total	1576	100,0

Stalking		Frequency	Percent
Valid	Nee	1541	97,8
	Ja	35	2,2
	Total	1576	100,0

Bedreiging		Frequency	Percent
Valid	Nee	1539	97,7
	Ja	37	2,3
	Total	1576	100,0

Belediging		Frequency	Percent
Valid	Nee	1508	95,7
	Ja	68	4,3
	Total	1576	100,0

Valse beschuldigingen of verdachtmakingen		Frequency	Percent
Valid	Nee	1542	97,8
	Ja	34	2,2
	Total	1576	100,0

Discriminatie		Frequency	Percent
Valid	Nee	1550	98,4
	Ja	26	1,6
	Total	1576	100,0

Commercieel gebruik van uw informatie zonder toestemming		Frequency	Percent
Valid	Nee	1475	93,6
	Ja	101	6,4
	Total	1576	100,0

Datalekken		Frequency	Percent
Valid	Nee	1534	97,3
	Ja	42	2,7
	Total	1576	100,0

Geen van bovenstaande		Frequency	Percent
Valid	Nee	304	19,3
	Ja	1272	80,7
	Total	1576	100,0

Vraag 4 Waar kwam u of uw huishoudlid de schadelijke inhoud tegen?

Meerdere antwoorden mogelijk

Op een sociaal medium, zoals Facebook, Twitter, Instagram		Frequency	Percent
Valid	Nee	200	12,7
	Ja	176	11,2
	Total	376	23,9

Op een app als SnapChat of TikTok		Frequency	Percent
Valid	Nee	356	22,6
	Ja	20	1,3
	Total	376	23,9

Op een videodienst zoals YouTube, Twitch, Dumpert		Frequency	Percent
Valid	Nee	353	22,4
	Ja	23	1,5
	Total	376	23,9

Op een messaging dienst, zoals Whatsapp of Facebook messenger		Frequency	Percent
Valid	Nee	312	19,8
	Ja	64	4,1
	Total	376	23,9

Op een datingsite of app		Frequency	Percent
Valid	Nee	358	22,7
	Ja	18	1,1
	Total	376	23,9

Op een internetforum		Frequency	Percent
Valid	Nee	346	22,0
	Ja	30	1,9
	Total	376	23,9

Een zoekmachine zoals Google, Bing		Frequency	Percent
Valid	Nee	308	19,5
	Ja	68	4,3
	Total	376	23,9

Op een nieuwssite of blog		Frequency	Percent
Valid	Nee	360	22,8
	Ja	16	1,0
	Total	376	23,9

Op een online marktplaats voor de verkoop van tweedehands goederen		Frequency	Percent
Valid	Nee	352	22,3
	Ja	24	1,5
	Total	376	23,9

Anders, namelijk		Frequency	Percent
Valid	Nee	285	18,1
	Ja	91	5,8
	Total	376	23,9

Vraag 5 Welke drie vormen van schadelijke informatie op internet vindt u het grootste probleem?

1 = het grootste probleem, 2 = het daarna grootse probleem, 3 = het daarna grootste probleem.

Ongewilde publicatie van privé-informatie		Frequency	Percent
Valid	1	391	24,8
	2	192	12,2
	3	210	13,3
	Total	793	50,3

Publicatie van onjuiste of verouderde gegevens		Frequency	Percent
Valid	1	32	2,0
	2	57	3,6
	3	48	3,0
	Total	137	8,7

Publicatie van foto's en video's die inbreuk maken op uw privacy of reputatie		Frequency	Percent
Valid	1	161	10,2
	2	320	20,3
	3	181	11,5
	Total	662	42,0

Verspreiding van seksueel beeldmateriaal, bv. door een ex-partner		Frequency	Percent
Valid	1	351	22,3
	2	193	12,2
	3	157	10,0
	Total	701	44,5

Pesten		Frequency	Percent
Valid	1	139	8,8
	2	176	11,2
	3	127	8,1
	Total	442	28,0

Bedreiging		Frequency	Percent
Valid	1	159	10,1
	2	193	12,2
	3	174	11,0
	Total	526	33,4

Stalking		Frequency	Percent
Valid	1	37	2,3
	2	81	5,1
	3	107	6,8
	Total	225	14,3

Belediging		Frequency	Percent
Valid	1	17	1,1
	2	28	1,8
	3	34	2,2
	Total	79	5,0

Valse beschuldigingen of verdachtmakingen		Frequency	Percent
Valid	1	65	4,1
	2	127	8,1
	3	193	12,2
	Total	385	24,4

Discriminatie		Frequency	Percent
Valid	1	43	2,7
	2	57	3,6
	3	81	5,1
	Total	181	11,5

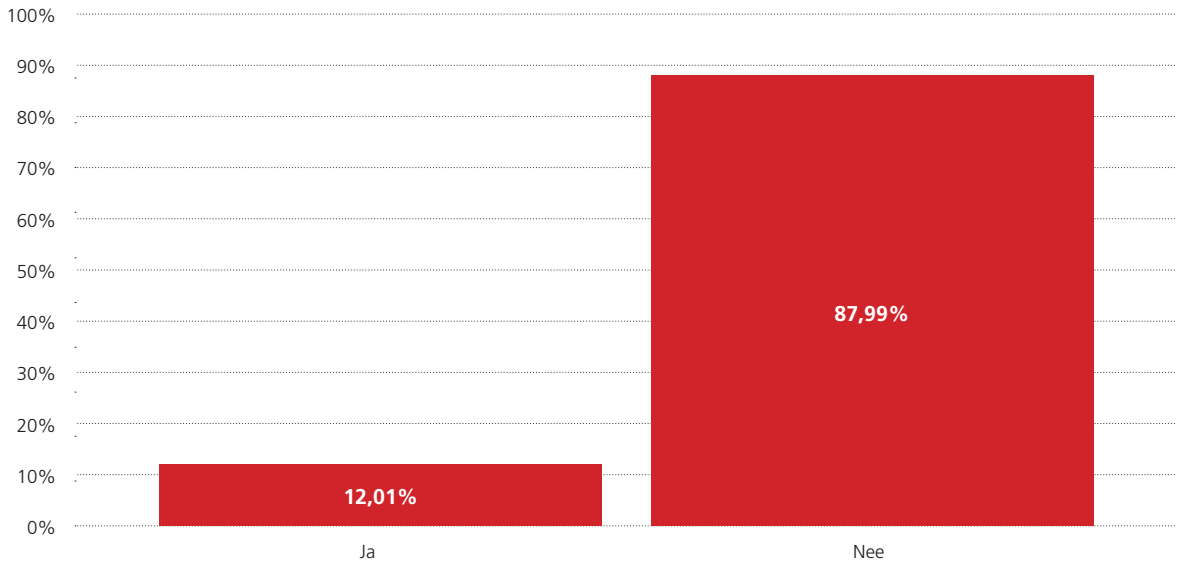
Commercieel gebruik van uw informatie zonder toestemming		Frequency	Percent
Valid	1	61	3,9
	2	76	4,8
	3	112	7,1
	Total	249	15,8

Datalekken		Frequency	Percent
Valid	1	113	7,2
	2	69	4,4
	3	144	9,1
	Total	326	20,7

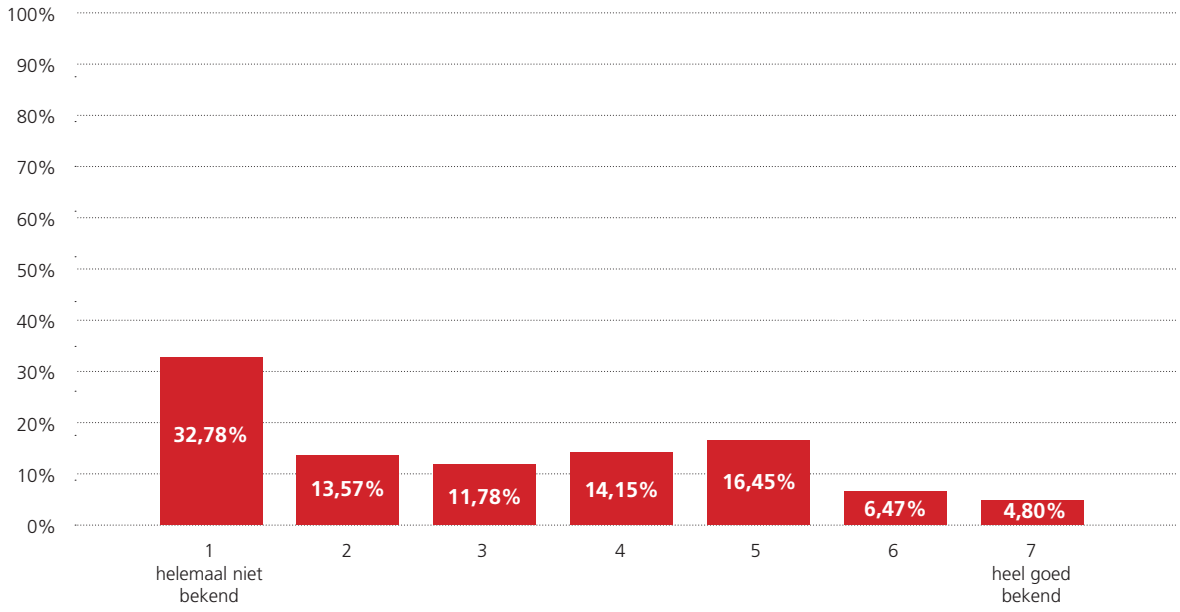
Discriminatie		Frequency	Percent
Valid	1	43	2,7
	2	57	3,6
	3	81	5,1
	Total	181	11,5

Vraag 6 **In het algemeen, hebt u wel eens gebruik gemaakt van een mogelijkheid om schadelijke informatie te rapporteren (voor uzelf of iemand anders)?**

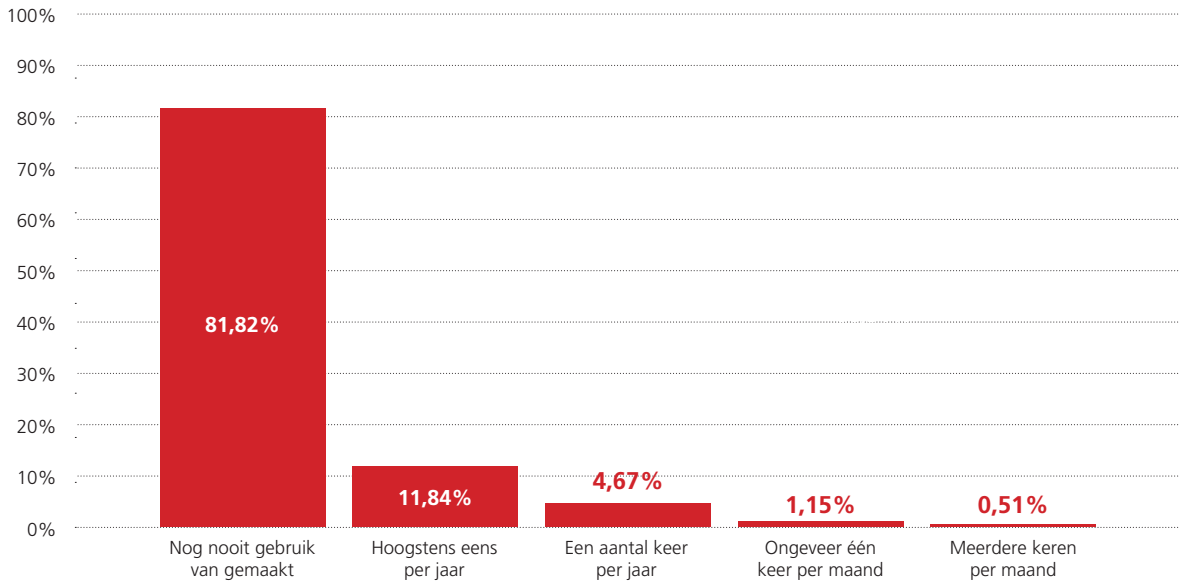
Het gaat hier om een mogelijkheid die door de betreffende dienst zelf, bv. Facebook of Youtube, wordt aangeboden.



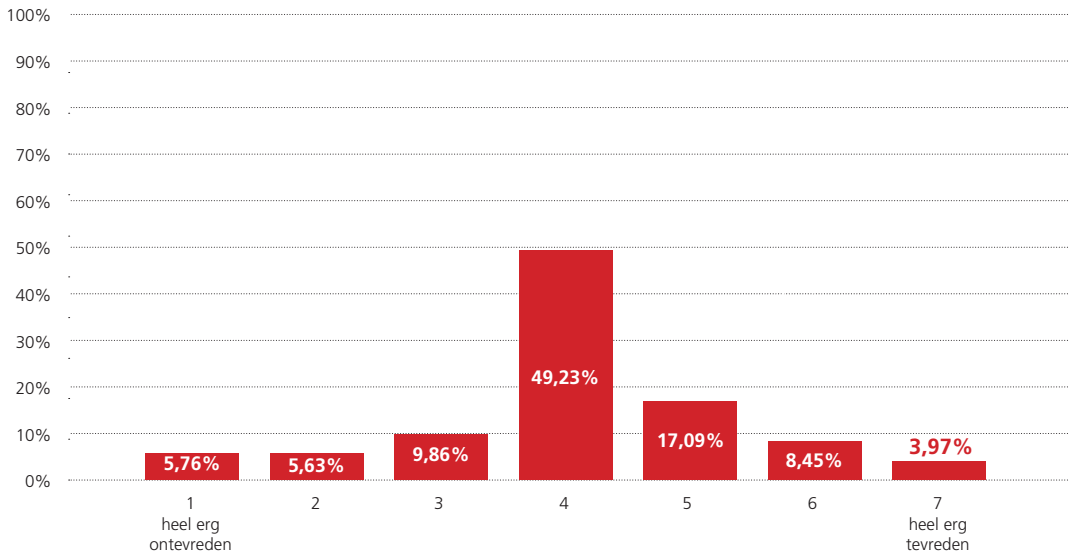
Vraag 7 **Hoe bekend bent u met de mogelijkheden om schadelijke informatie te rapporteren? Het gaat hier om een mogelijkheid die door de betreffende dienst zelf wordt aangeboden.**



Vraag 8 **Hoe vaak maakt u gebruik van de aangeboden mogelijkheid om schadelijke informatie te rapporteren?**



Vraag 9 **Hoe tevreden bent u over de aangeboden mogelijkheden om schadelijke informatie te rapporteren?**



Vraag 10 Wat vindt u belangrijk als u de mogelijkheid krijgt om schadelijke informatie te rapporteren?

Noemt u hierbij uw top drie van belangrijkste eigenschappen. Geeft u een 1 aan de eigenschap die u het belangrijkst vindt, een 2 aan de eigenschap die u daarna het belangrijkst vindt en een 3 aan de eigenschap die u daarna het belangrijkst vindt.

Dat deze makkelijk vindbaar is.		Frequency	Percent
Valid	1	677	43,0
	2	133	8,4
	3	123	7,8
	Total	933	59,2

Dat deze gebruiksvriendelijk is.		Frequency	Percent
Valid	1	128	8,1
	2	287	18,2
	3	99	6,3
	Total	514	32,6

Dat deze begrijpelijk is.		Frequency	Percent
Valid	1	84	5,3
	2	169	10,7
	3	161	10,2
	Total	414	26,3

Dat deze anoniem te gebruiken is.		Frequency	Percent
Valid	1	163	10,3
	2	197	12,5
	3	149	9,5
	Total	509	32,3

Dat ik iemand persoonlijk kan spreken.		Frequency	Percent
Valid	1	75	4,8
	2	93	5,9
	3	88	5,6
	Total	256	16,2

Dat rapportering snel wordt afgehandeld.		Frequency	Percent
Valid	1	72	4,6
	2	211	13,4
	3	212	13,5
	Total	495	31,4

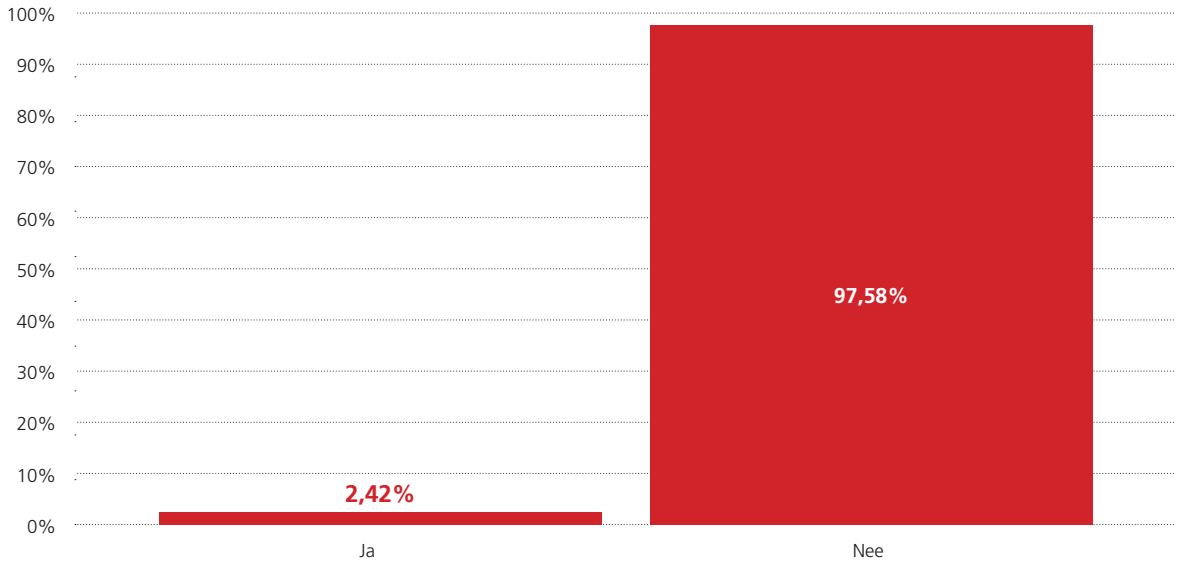
Dat er sprake is van een grondige toetsing van de rapportering.		Frequency	Percent
Valid	1	76	4,8
	2	137	8,7
	3	104	6,6
	Total	317	20,1

Dat de gerapporteerde inhoud ook echt verwijderd wordt.		Frequency	Percent
Valid	1	207	13,1
	2	209	13,3
	3	275	17,4
	Total	691	43,8

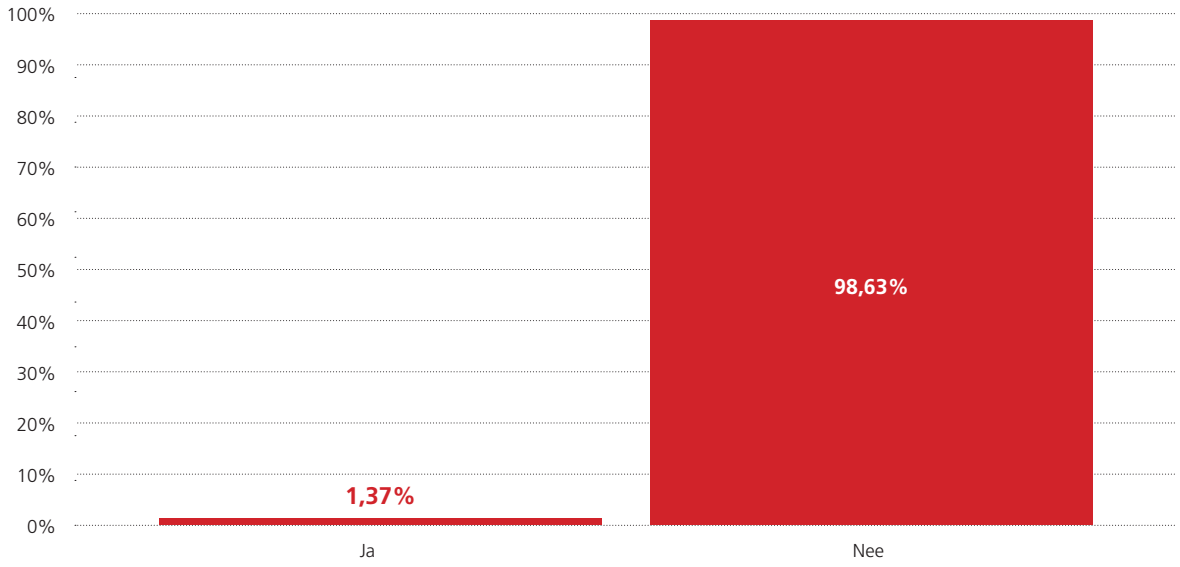
Dat u na afloop een gemotiveerde reactie op de rapportering krijgt.		Frequency	Percent
Valid	1	17	1,1
	2	74	4,7
	3	187	11,9
	Total	278	17,6

Dat de vrijheid van meningsuiting wordt beschermd.		Frequency	Percent
Valid	1	60	3,8
	2	49	3,1
	3	161	10,2
	Total	270	17,1

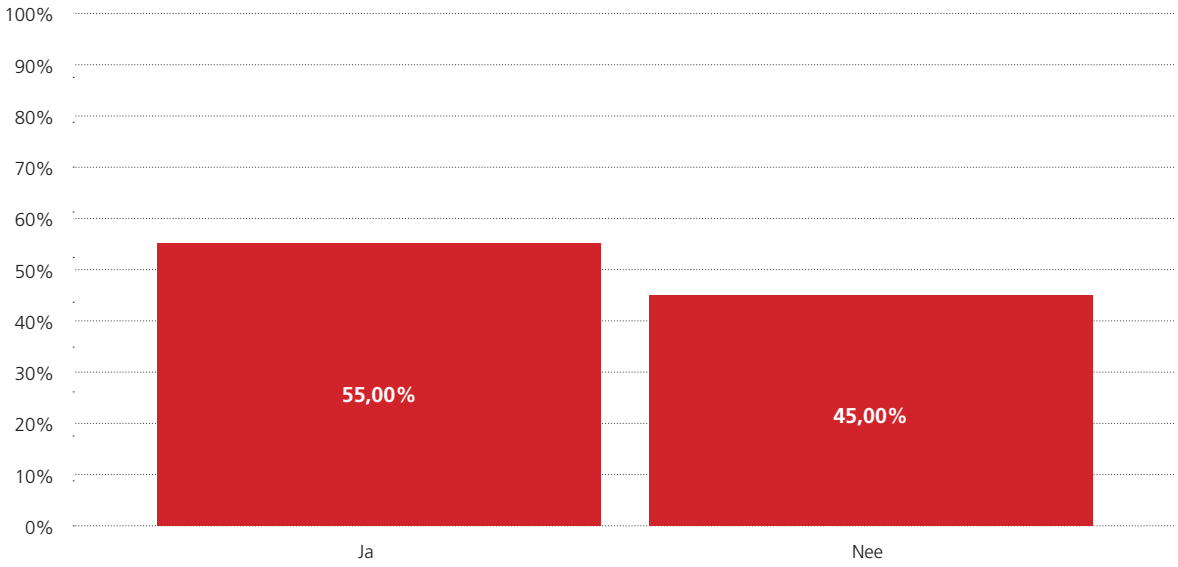
Vraag 11 **Hebt u wel eens informatie op internet gezet, die werd verwijderd na een klacht over deze informatie?**



Vraag 12 **Hebt u wel eens juridische stappen overwogen met betrekking tot voor u schadelijke informatie op internet?**



Vraag 13 (voor wie 'ja' antwoordde op vraag 12). Hebt u wel eens juridische stappen ondernomen met betrekking tot voor u schadelijke informatie op internet?



Vraag 14 Welke soort juridische stappen hebt u wel eens overwogen of ondernomen met betrekking tot voor u schadelijke informatie op internet?

Meerdere antwoorden mogelijk.

Zoeken van informatie over uw rechten en het juridisch kader		Frequency	Percent
Valid	Nee	15	1,0
	Ja	6	,4
	Total	21	1,3

Informeren bij een rechtswinkel		Frequency	Percent
Valid	Nee	18	1,1
	Ja	3	,2
	Total	21	1,3

Zoeken van een advocaat		Frequency	Percent
Valid	Nee	16	1,0
	Ja	5	,3
	Total	21	1,3

Contact met rechtsbijstandsverzekering		Frequency	Percent
Valid	Nee	17	1,1
	Ja	4	,3
	Total	21	1,3

Een juridische procedure bij de rechter		Frequency	Percent
Valid	Nee	18	1,1
	Ja	3	,2
	Total	21	1,3

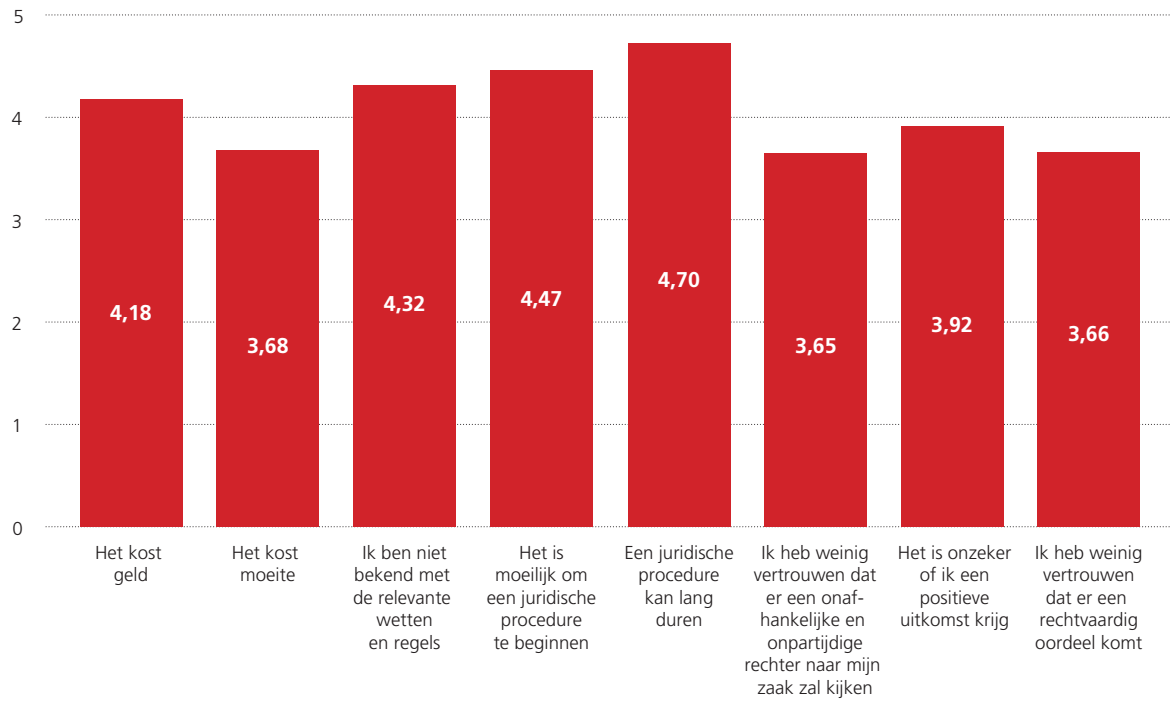
Klacht bij de Autoriteit Persoons-gegevens		Frequency	Percent
Valid	Nee	19	1,2
	Ja	2	,1
	Total	21	1,3

Aangifte bij de politie		Frequency	Percent
Valid	Nee	11	,7
	Ja	10	,6
	Total	21	1,3

Anders		Frequency	Percent
Valid	Nee	19	1,2
	Ja	2	,1
	Total	21	1,3

Vraag 15 In welke mate zouden onderstaande zaken u tegenhouden om juridische stappen te ondernemen?

Schaal van 1 t/m 7 waarbij 1 helemaal niet tegenhoudt en 7 erg tegenhoudt.



iii. Nadere analyse

Direct of Indirecte ervaring (vraag 1 en 2 van de survey) en juridische stappen genomen

De focus van de analyse komt te liggen op de groep mensen die (direct of indirect) ervaring hebben met schadelijke online content (gecombineerde groep uit vraag 1 en 2). Hiermee komen we uit op 240 respondenten (ofwel, 15% van de totale steekproef). Hier zijn de demografische gegevens van deze subsample.

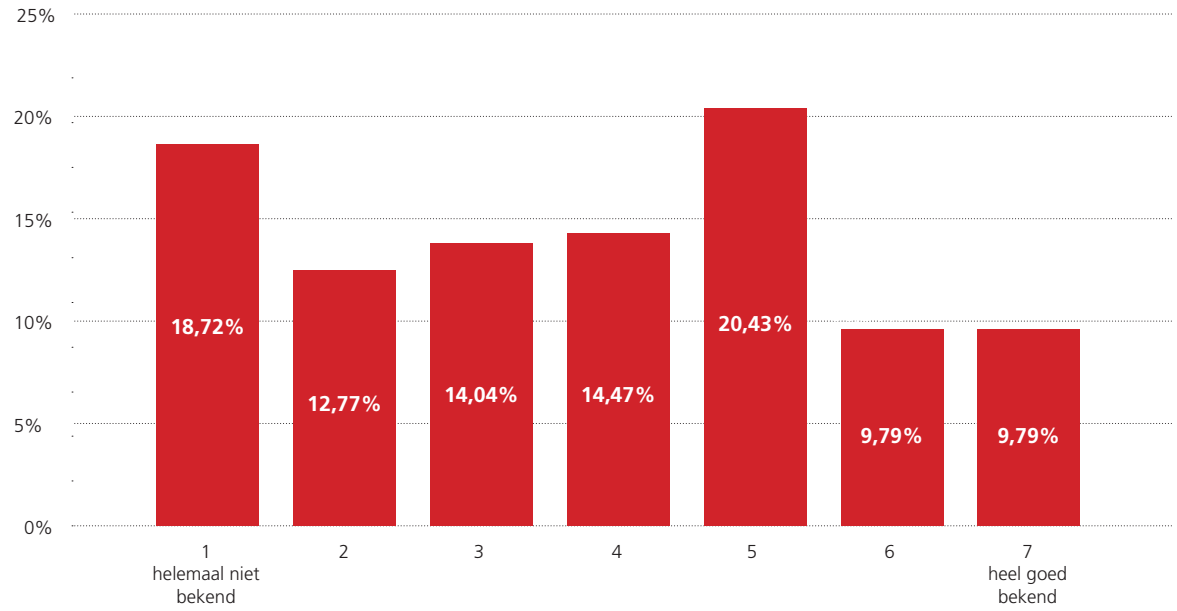
Leeftijd in CBS-categorieën		Frequency	Percent	Cumulative Percent
Valid	15 - 24 jaar	24	10,0	10,0
	25 - 34 jaar	32	13,3	23,3
	35 - 44 jaar	22	9,2	32,5
	45 - 54 jaar	25	10,4	42,9
	55 - 64 jaar	59	24,6	67,5
	65 jaar en ouder	78	32,5	100,0
	Total	240	100,0	

Geslacht		Frequency	Percent	Cumulative Percent
Valid	Man	147	61,3	61,3
	Vrouw	93	38,8	100,0
	Total	240	100,0	

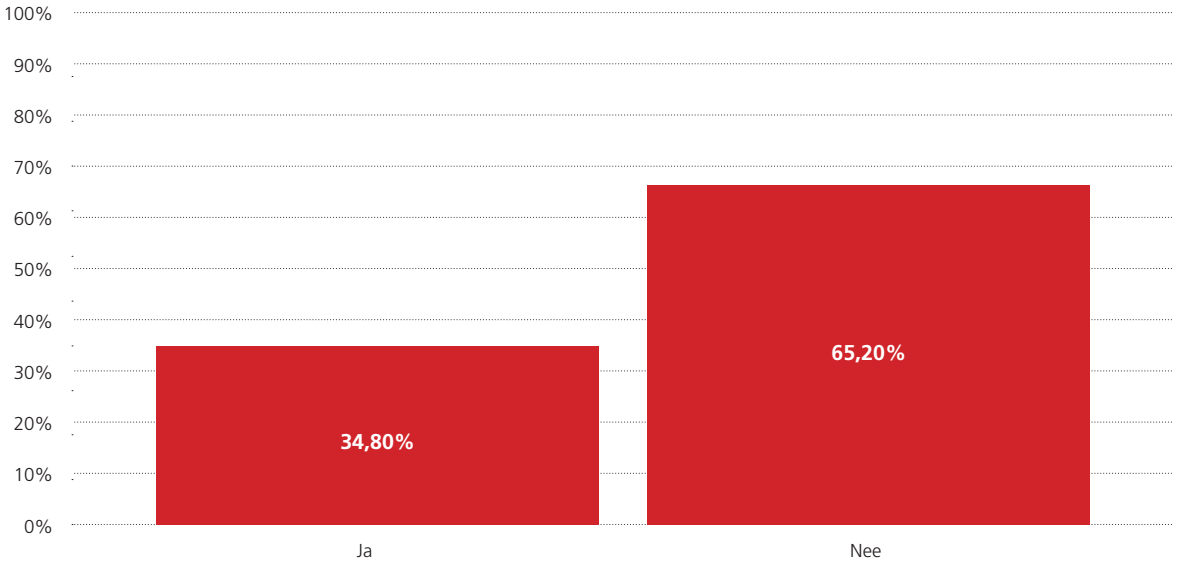
Opleiding in CBS-categorieën		Frequency	Percent	Cumulative Percent
Valid	basisonderwijs	11	4,6	4,6
	Vmbo	32	13,3	17,9
	havo/vwo	30	12,5	30,4
	Mbo	58	24,2	54,6
	Hbo	63	26,3	80,8
	Wo	46	19,2	100,0
	Total	240	100,0	

Vervolgens: in welke mate is voor deze groep de extra-juridische route een oplossing?

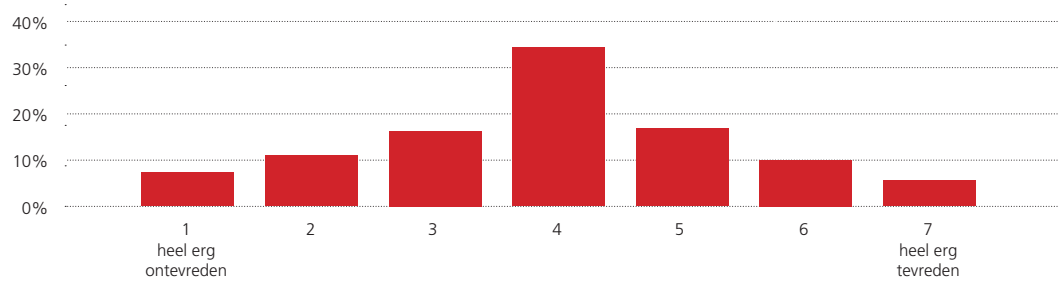
Vraag 1 Zijn zij bekend met de rapporteer mogelijkheid van de dienst zelf



Vraag 2 Hebben zij gebruik gemaakt van de rapporteer mogelijkheid van de dienst zelf?



Vraag 3 Hoe tevreden zijn zij met de rapporteer mogelijkheden bij de dienst zelf?



Vraag 4 Wat vinden zij belangrijk bij het rapporteren van schadelijke informatie?

Noemt u hierbij uw top drie van belangrijkste eigenschappen. Geeft u een 1 aan de eigenschap die u het belangrijkst vindt, een 2 aan de eigenschap die u daarna het belangrijkst vindt en een 3 aan de eigenschap die u daarna het belangrijkst vindt.

Dat deze makkelijk vindbaar is.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	98	40,8	67,1	67,1
	2	22	9,2	15,1	82,2
	3	26	10,8	17,8	100,0
	Total	146	60,8	100,0	
Missing	System	94	39,2		
Total		240	100,0		

Dat deze gebruiksvriendelijk is.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	16	6,7	19,3	19,3
	2	40	16,7	48,2	67,5
	3	27	11,3	32,5	100,0
	Total	83	34,6	100,0	
Missing	System	157	65,4		
Total		240	100,0		

Dat deze begrijpelijk is.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	2,1	8,9	8,9
	2	31	12,9	55,4	64,3
	3	20	8,3	35,7	100,0
	Total	56	23,3	100,0	
Missing	System	184	76,7		
Total		240	100,0		

Dat deze anoniem te gebruiken is.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	24	10,0	34,8	34,8
	2	22	9,2	31,9	66,7
	3	23	9,6	33,3	100,0
	Total	69	28,7	100,0	
Missing	System	171	71,3		
Total		240	100,0		

Dat ik iemand persoonlijk kan spreken.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	3,3	26,7	26,7
	2	10	4,2	33,3	60,0
	3	12	5,0	40,0	100,0
	Total	30	12,5	100,0	
Missing	System	210	87,5		
Total		240	100,0		

Dat rapportering snel wordt afgehandeld.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	11	4,6	16,2	16,2
	2	31	12,9	45,6	61,8
	3	26	10,8	38,2	100,0
	Total	68	28,3	100,0	
Missing	System	172	71,7		
Total		240	100,0		

Dat er sprake is van een grondige toetsing van de rapportering.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	17	7,1	32,1	32,1
	2	22	9,2	41,5	73,6
	3	14	5,8	26,4	100,0
	Total	53	22,1	100,0	
Missing	System	187	77,9		
Total		240	100,0		

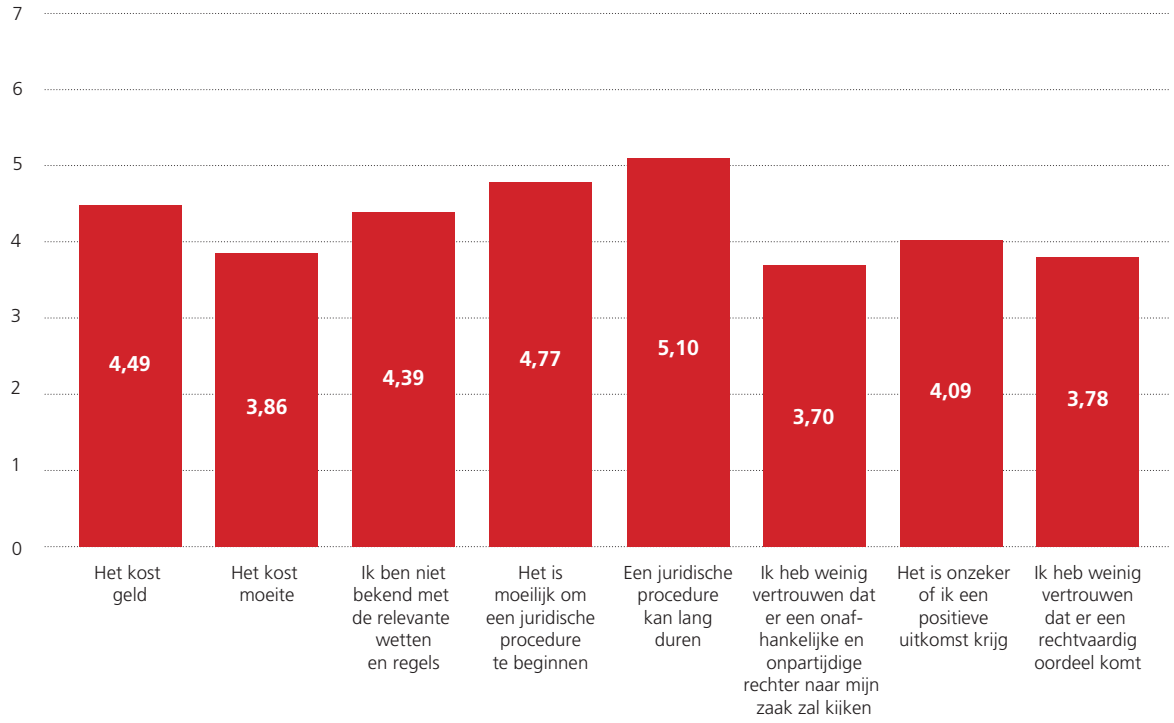
Dat de gerapporteerde inhoud ook echt verwijderd wordt.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	46	19,2	40,7	40,7
	2	35	14,6	31,0	71,7
	3	32	13,3	28,3	100,0
	Total	113	47,1	100,0	
Missing	System	127	52,9		
Total		240	100,0		

Dat u na afloop een gemotiveerde reactie op de rapportering krijgt.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	,4	2,4	2,4
	2	16	6,7	38,1	40,5
	3	25	10,4	59,5	100,0
	Total	42	17,5	100,0	
Missing	System	198	82,5		
Total		240	100,0		

Dat de vrijheid van meningsuiting wordt beschermd.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	9	3,8	20,0	20,0
	2	6	2,5	13,3	33,3
	3	30	12,5	66,7	100,0
	Total	45	18,8	100,0	
Missing	System	195	81,3		
Total		240	100,0		

Vraag 5 Wat houdt hen tegen bij het ondernemen van juridische stappen?

Gemiddelden op een schaal van 7.



Directe of indirecte ervaring (vraag 1 en 2 van de survey) en geen juridische stappen ondernomen

De gecombineerde groep uit vraag 1 en 2 die ervaring hebben met schadelijke informatie, maar géén stappen hebben overwogen of ondernomen. Bij toepassing van de selectie wordt op 219 respondenten uitgekomen.

Vraag 1 Welk type schadelijke informatie hebben zij ervaring mee?

Ongewilde publicatie van privé-informatie		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	188	85,8	85,8	85,8
	Ja	31	14,2	14,2	100,0
	Total	219	100,0	100,0	

Publicatie van onjuiste of verouderde gegevens		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	191	87,2	87,2	87,2
	Ja	28	12,8	12,8	100,0
	Total	219	100,0	100,0	

Publicatie van foto's en video's die inbreuk maken op uw privacy		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	188	85,8	85,8	85,8
	Ja	31	14,2	14,2	100,0
	Total	219	100,0	100,0	

Verspreiding van seksueel beeld-materiaal, bv. door een ex-partner		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	213	97,3	97,3	97,3
	Ja	6	2,7	2,7	100,0
	Total	219	100,0	100,0	

Pesten		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	194	88,6	88,6	88,6
	Ja	25	11,4	11,4	100,0
	Total	219	100,0	100,0	

Bedreiging		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	200	91,3	91,3	91,3
	Ja	19	8,7	8,7	100,0
	Total	219	100,0	100,0	

Stalking		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	204	93,2	93,2	93,2
	Ja	15	6,8	6,8	100,0
	Total	219	100,0	100,0	

Belediging		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	185	84,5	84,5	84,5
	Ja	34	15,5	15,5	100,0
	Total	219	100,0	100,0	

Valse beschuldigingen of verdacht-makingen		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	200	91,3	91,3	91,3
	Ja	19	8,7	8,7	100,0
	Total	219	100,0	100,0	

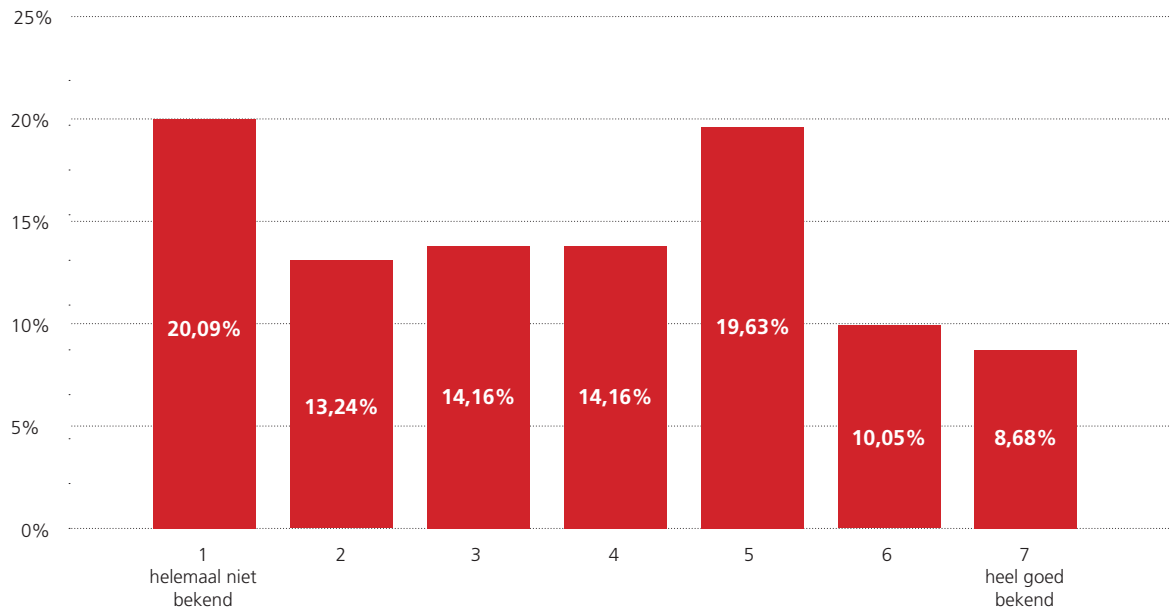
Discriminatie		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	208	95,0	95,0	95,0
	Ja	11	5,0	5,0	100,0
	Total	219	100,0	100,0	

Commercieel gebruik van uw informatie zonder toestemming		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	155	70,8	70,8	70,8
	Ja	64	29,2	29,2	100,0
	Total	219	100,0	100,0	

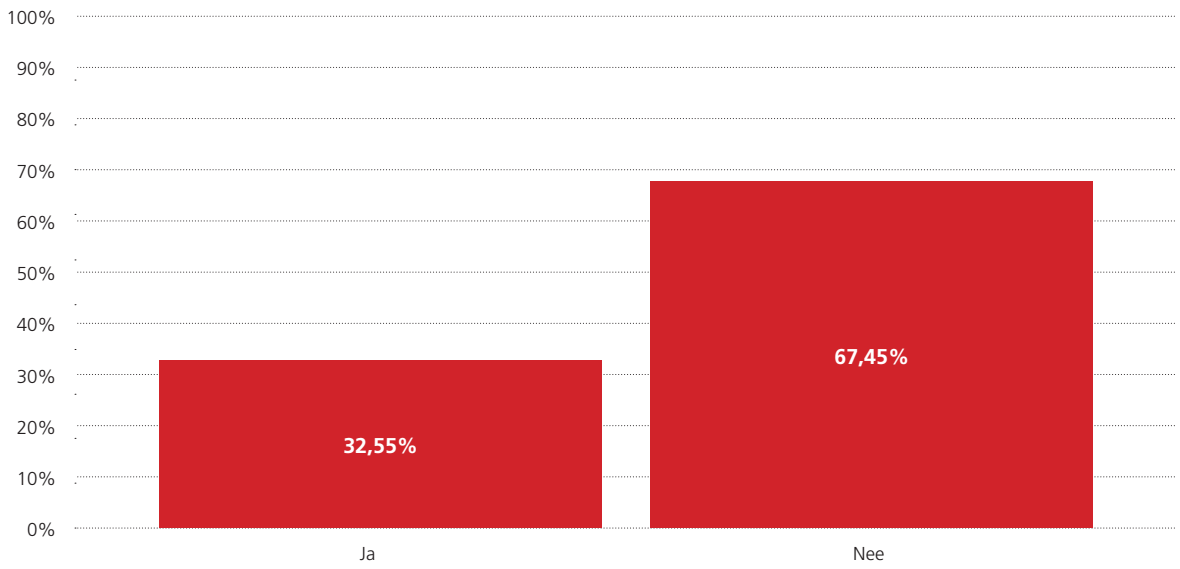
Datalekken		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	194	88,6	88,6	88,6
	Ja	25	11,4	11,4	100,0
	Total	219	100,0	100,0	

Geen van bovenstaande		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	150	68,5	68,5	68,5
	Ja	69	31,5	31,5	100,0
	Total	219	100,0	100,0	

Vraag 2 Hoeveel is bekend met de rapporteer mogelijkheid?



Vraag 3 Hoeveel gebruikt de rapporteer mogelijkheid?



Vraag 4 Wat vinden zij belangrijk aan de rapporteer mogelijkheden (vraag 10)?

Dat deze makkelijk vindbaar is.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	92	42,0	67,6	67,6
	2	20	9,1	14,7	82,4
	3	24	11,0	17,6	100,0
	Total	136	62,1	100,0	
Missing	System	83	37,9		
Total		219	100,0		

Dat deze gebruiksvriendelijk is.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	16	7,3	20,5	20,5
	2	37	16,9	47,4	67,9
	3	25	11,4	32,1	100,0
	Total	78	35,6	100,0	
Missing	System	141	64,4		
Total		219	100,0		

Dat deze begrijpelijk is.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	2,3	9,3	9,3
	2	30	13,7	55,6	64,8
	3	19	8,7	35,2	100,0
	Total	54	24,7	100,0	
Missing	System	165	75,3		
Total		219	100,0		

Dat deze anoniem te gebruiken is.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	21	9,6	33,3	33,3
	2	20	9,1	31,7	65,1
	3	22	10,0	34,9	100,0
	Total	63	28,8	100,0	
Missing	System	156	71,2		
Total		219	100,0		

Dat ik iemand persoonlijk kan spreken.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	8	3,7	27,6	27,6
	2	10	4,6	34,5	62,1
	3	11	5,0	37,9	100,0
	Total	29	13,2	100,0	
Missing	System	190	86,8		
Total		219	100,0		

Dat rapportering snel wordt afgehandeld.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	11	5,0	17,7	17,7
	2	30	13,7	48,4	66,1
	3	21	9,6	33,9	100,0
	Total	62	28,3	100,0	
Missing	System	157	71,7		
Total		219	100,0		

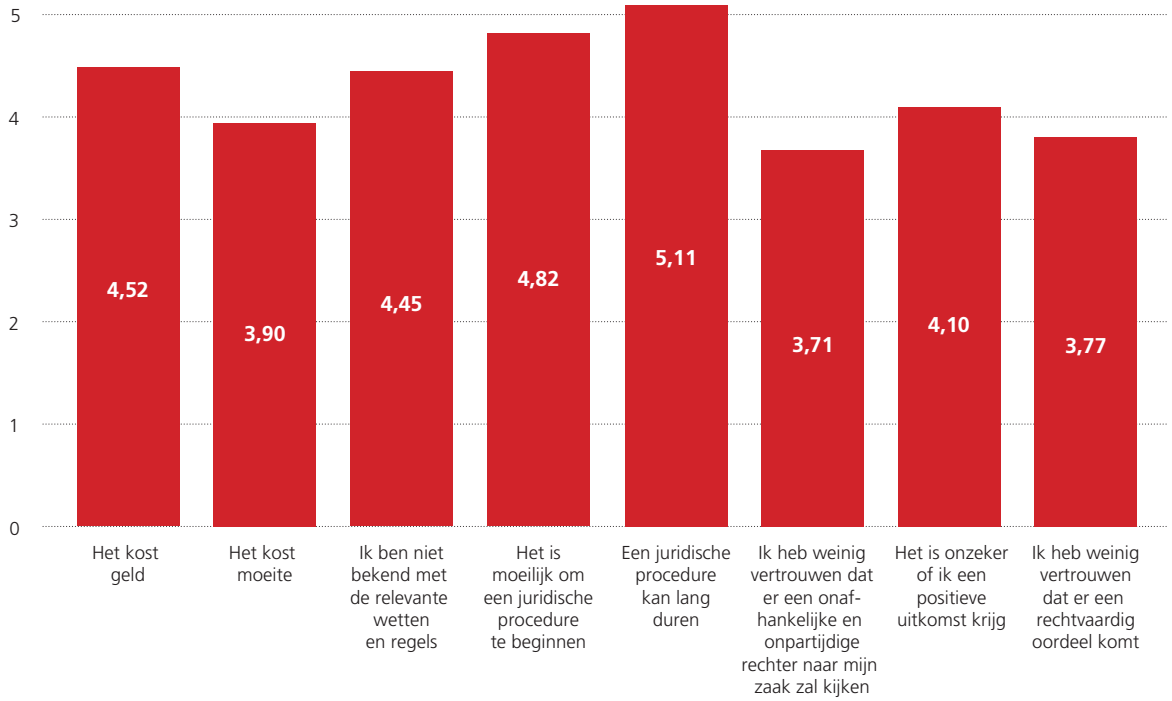
Dat er sprake is van een grondige toetsing van de rapportering.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	16	7,3	32,0	32,0
	2	20	9,1	40,0	72,0
	3	14	6,4	28,0	100,0
	Total	50	22,8	100,0	
Missing	System	169	77,2		
Total		219	100,0		

Dat de gerapporteerde inhoud ook echt verwijderd wordt.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	42	19,2	38,9	38,9
	2	34	15,5	31,5	70,4
	3	32	14,6	29,6	100,0
	Total	108	49,3	100,0	
Missing	System	111	50,7		
Total		219	100,0		

Dat u na afloop een gemotiveerde reactie op de rapportering krijgt.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	,5	2,6	2,6
	2	14	6,4	35,9	38,5
	3	24	11,0	61,5	100,0
	Total	39	17,8	100,0	
Missing	System	180	82,2		
Total		219	100,0		

Dat de vrijheid van meningsuiting wordt beschermd.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	7	3,2	18,4	18,4
	2	4	1,8	10,5	28,9
	3	27	12,3	71,1	100,0
	Total	38	17,4	100,0	
Missing	System	181	82,6		
Total		219	100,0		

Vraag 5 Welke drempels ervaren zij om juridische stappen te ondernemen?



Vraag 1 **Waar men de schadelijke informatie tegenkwam: wat hebben mensen ingevuld bij 'anders'**
Vraag 4 van de survey

Bij deze analyse is weer de volledige steekproef gebruikt (N = 1576). De "anders" categorie is een "open veld". De antwoorden staan hieronder en de kolom 'frequency' geeft aan hoe vaak dit antwoord gegeven is geweest (heel vaak is dit gewoon 1 keer).

Dat er sprake is van een grondige toetsing van de rapportering.		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No answer	1485	94,2	94,2	94,2
	bank app	1	,1	,1	94,3
	Databank met datalekken	1	,1	,1	94,4
	datalek bij autoverzekeraar	1	,1	,1	94,4
	Datalek bij een verhuurmakelaar waarmee ik samen werk.(die had mijn privégegevens)	1	,1	,1	94,5
	door het zenden van een email, zonder dat ik mijn adres gaf	1	,1	,1	94,5
	e-mail	6	,4	,4	94,9
	Een andere krant beweerde rechten op mijn tekst te hebben.	1	,1	,1	95,0
	email	3	,2	,2	95,2
	Email	3	,2	,2	95,4
	fishing	1	,1	,1	95,4
	Fishing bankgegevens	1	,1	,1	95,5
	Foute mail. Met link waar je niet op moet klikken	1	,1	,1	95,6
	geen	1	,1	,1	95,6
	Geen	1	,1	,1	95,7
	Geen van allen	1	,1	,1	95,7
	Gmail	1	,1	,1	95,8
	het kraken van de computer	1	,1	,1	95,9
	ik ben gehackt zonder dat ik dit wist	1	,1	,1	95,9
	Ik kreeg een melding dat een wachtwoord was gelekt	1	,1	,1	96,0
	Ik werd geconfronteerd met de inhoud van mails en whats app	1	,1	,1	96,1
	In de mailbox	1	,1	,1	96,1
	in mailverkeer naar derden	1	,1	,1	96,2
	in mijn mailbox	1	,1	,1	96,3
	indirect: werd dagelijks gebeld omdat een overheidsinstantie per abuis ons telefoon-nummer had ingevuld voor een lagere school	1	,1	,1	96,3
	Ingeligd door bedrijf met datalek	1	,1	,1	96,4
	internet	1	,1	,1	96,4
	kanker	1	,1	,1	96,5
	Klacht.nl	1	,1	,1	96,6
	laptop	1	,1	,1	96,6
	lokale website	1	,1	,1	96,7
	mail	4	,3	,3	97,0
	Mail	1	,1	,1	97,0
	mail pishing	1	,1	,1	97,1
	Mailbox	1	,1	,1	97,1
	met iets kopen werd gelijk op facesbook gezet	1	,1	,1	97,2
	mijn emailadres	1	,1	,1	97,3
	mijn laptop raakte geblokkeerd. Ik moest betalen. Ik heb alle software verwijderd. dit is ook bij mijn man gebeurd	1	,1	,1	97,3

	Msn	1	,1	,1	97,4
	msn bij de chat dat vroeger nog was	1	,1	,1	97,5
	niet	2	,1	,1	97,6
	Niet aan de orde	1	,1	,1	97,7
	onbekend, een trojan horse is de computer binnengekomen.	1	,1	,1	97,7
	ongevraagde advertenties	1	,1	,1	97,8
	Op de maill	1	,1	,1	97,8
	Op een andere website	1	,1	,1	97,9
	Op een site van de overheid	1	,1	,1	98,0
	Op school	1	,1	,1	98,0
	Op website van fotograaf	1	,1	,1	98,1
	per brief	1	,1	,1	98,2
	per post	1	,1	,1	98,2
	phishing bij bank	1	,1	,1	98,3
	phishing mail	1	,1	,1	98,4
	phishing mails in grote getalen.	1	,1	,1	98,4
	Phising mail	1	,1	,1	98,5
	Serieus via wordfeud/ruzzle	1	,1	,1	98,5
	skype	1	,1	,1	98,6
	telefonisch	1	,1	,1	98,7
	telemarketing	1	,1	,1	98,7
	Ticketmaster	1	,1	,1	98,8
	Tool om te kijken of je gegevens buit gemaakt zijn bij een data lek	1	,1	,1	98,9
	valse berichten van mijn bank.	1	,1	,1	98,9
	Via de gemeente	1	,1	,1	99,0
	via de mail	1	,1	,1	99,0
	via de website (contactformulier) van mijn eenmanszaak	1	,1	,1	99,1
	via e-mail	1	,1	,1	99,2
	Via e-mail	1	,1	,1	99,2
	Via een email	1	,1	,1	99,3
	via kennissen	1	,1	,1	99,4
	via mail	2	,1	,1	99,5
	via mail die door de spam geglipt was.	1	,1	,1	99,6
	via sms en email	1	,1	,1	99,6
	via spam in de mailbox kwam ik erachter dat deze gebruikt is zonder toestemming	1	,1	,1	99,7
	virus via en gedownload bestand	1	,1	,1	99,7
	Website	1	,1	,1	99,8
	Website (rijschool)	1	,1	,1	99,9
	website universiteit	1	,1	,1	99,9
	weet ik niet	1	,1	,1	100,0
	Total	1576	100,0	100,0	
Missing	System	169	77,2		
Total		219	100,0		

Waar kwam u of uw huishoudlid de schadelijke inhoud tegen?

Meerdere antwoorden mogelijk

Hercodering van vraag 4 van de surveyresultaten in de categorieën ‘open’ en ‘gesloten’ internet. Sociale media, apps zoals Snapchat en Tiktok, videodiensten, internetfora, zoekmachines, blogs en marktplaatsen horen bij het open internet. Direct messaging, datingapp en e-mail behoren daarentegen bij het gesloten internet.

open_internet		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	1361	86,4	86,4	86,4
	Ja	215	13,6	13,6	100,0
	Total	1576	100,0	100,0	

gesloten_internet		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	1471	93,3	93,3	93,3
	Ja	105	6,7	6,7	100,0
	Total	1576	100,0	100,0	

De gecombineerde groep uit vraag 1 en 2 die ervaring hebben met schadelijke informatie, én die wel stappen hebben overwogen of ondernomen:

Bij toepassing van deze selectie wordt uitgekomen op 13 respondenten. Merk op dat dit aantal vreemd lijkt, want de groep die met schadelijke inhoud te maken kreeg was 240, waarvan 219 géén stappen hadden ondernomen. Je zou dus denken dat 21 respondenten al stappen hebben ondernomen. Dit klopt echter niet, want er zijn ook enkele mensen die op die vraag 'weet niet' hebben geantwoord, en daarom zijn er slecht 13 die volmondig 'ja' hebben geantwoord op de vraag of ze al dan niet stappen hebben overwogen of ondernomen.

Geslacht		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	7	53,8	53,8	53,8
	Ja	6	46,2	46,2	100,0
	Total	13	100,0	100,0	

Opleiding in CBS-categorieën		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	basisonderwijs	2	15,4	15,4	15,4
	vmbo	3	23,1	23,1	38,5
	havo/vwo	2	15,4	15,4	53,8
	mbo	2	15,4	15,4	69,2
	hbo	3	23,1	23,1	92,3
	wo	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Leeftijd in CBS-categorieën		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	basisonderwijs	2	15,4	15,4	15,4
	vmbo	4	30,8	30,8	46,2
	havo/vwo	1	7,7	7,7	53,8
	mbo	3	23,1	23,1	76,9
	hbo	3	23,1	23,1	100,0
	wo	13	100,0	100,0	
	Total	13	100,0	100,0	

Vraag 1 Met welke van onderstaande vormen van schadelijke informatie op internet hebben ze al te maken gehad?

Ongewilde publicatie van privé-informatie		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	9	69,2	69,2	69,2
	Ja	4	30,8	30,8	100,0
	Total	13	100,0	100,0	

Publicatie van onjuiste of verouderde gegevens		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	11	84,6	84,6	84,6
	Ja	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Publicatie van foto's en video's die inbreuk maken op uw privacy		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	11	84,6	84,6	84,6
	Ja	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Verspreiding van seksueel beeldmateriaal, bv. door een ex-partner		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	12	92,3	92,3	92,3
	Ja	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Pesten		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	10	76,9	76,9	76,9
	Ja	3	23,1	23,1	100,0
	Total	13	100,0	100,0	

Bedreiging		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	7	53,8	53,8	53,8
	Ja	6	46,2	46,2	100,0
	Total	13	100,0	100,0	

Stalking		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	11	84,6	84,6	84,6
	Ja	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Belediging		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	9	69,2	69,2	69,2
	Ja	4	30,8	30,8	100,0
	Total	13	100,0	100,0	

Valse beschuldigingen of verdachtmakingen		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	8	61,5	61,5	61,5
	Ja	5	38,5	38,5	100,0
	Total	13	100,0	100,0	

Discriminatie		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	9	69,2	69,2	69,2
	Ja	4	30,8	30,8	100,0
	Total	13	100,0	100,0	

Commercieel gebruik van uw informatie zonder toestemming		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	9	69,2	69,2	69,2
	Ja	4	30,8	30,8	100,0
	Total	13	100,0	100,0	

Datalekken		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	10	76,9	76,9	76,9
	Ja	3	23,1	23,1	100,0
	Total	13	100,0	100,0	

Geen van bovenstaande		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nee	13	100,0	100,0	100,0

IViR - Instituut voor Informatierecht
Postbus 15514, 1001 NA Amsterdam, Nederland

https://www.ivir.nl/