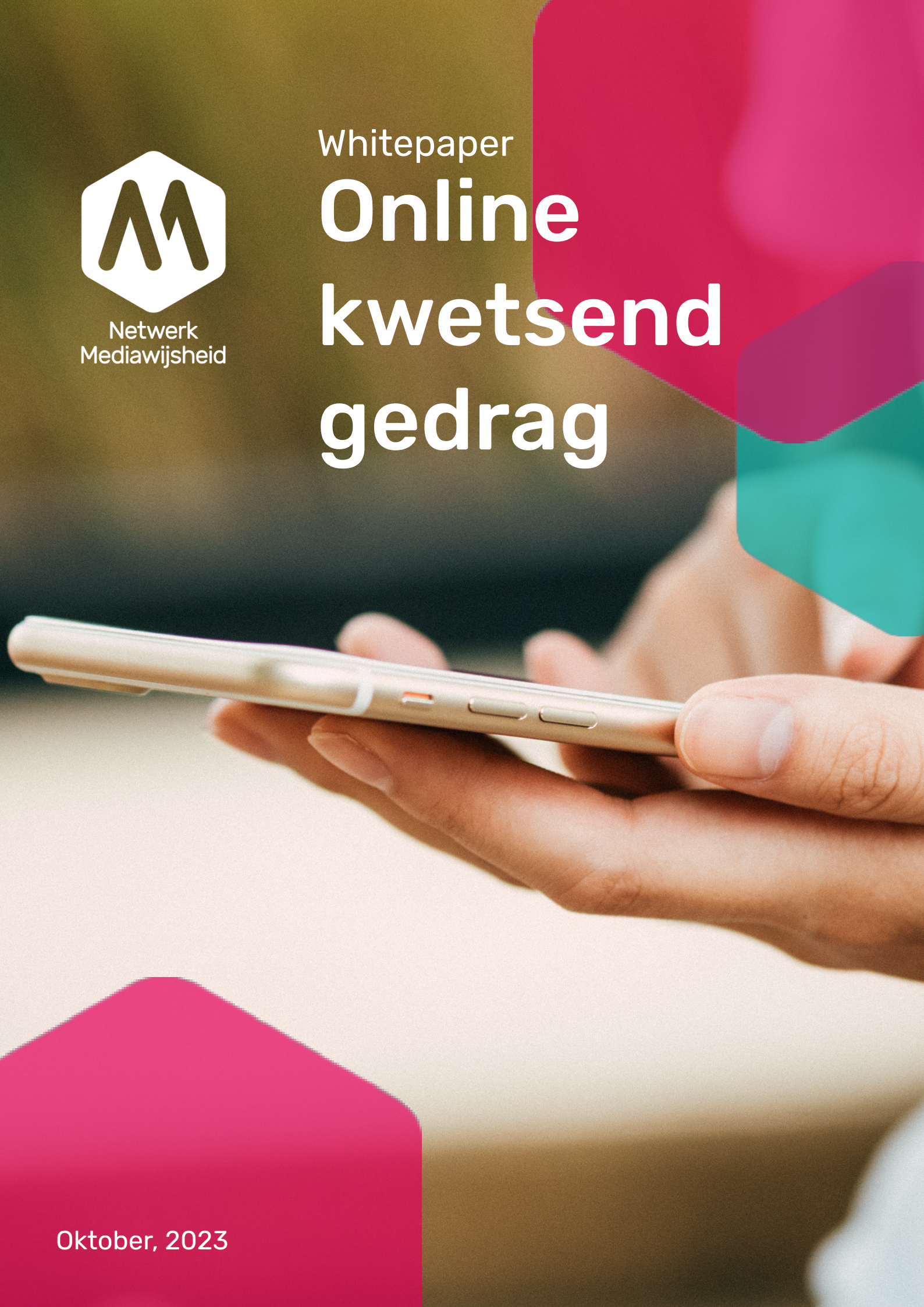
Netwerk Mediawijsheid

Whitepaper

Online kwetsend gedrag



Oktober, 2023

Deze whitepaper is opgesteld met input van en in samenwerking met:

Colofon

Tekstschrijver: Jurre Plantinga

Netwerk Mediawijsheid
e-mail: info@mediawijzer.net
website: NetwerkMediawijsheid.nl

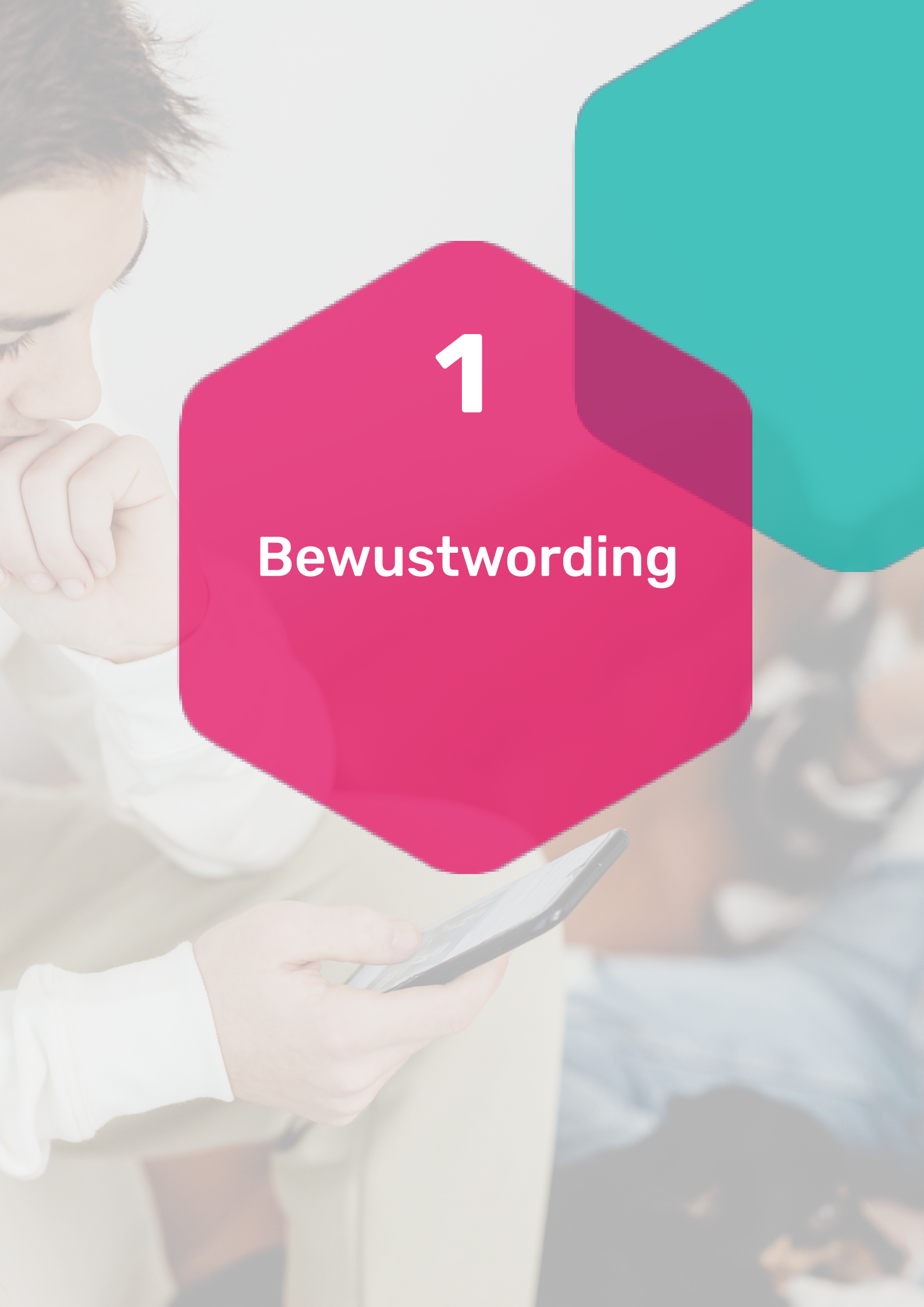
Inhoudsopgave

Inleiding

Online zijn we constant met elkaar in contact. Die voortdurende en laagdrempelige verbondenheid verrijkt onze levens, maar heeft ook een schaduwzijde. Van cyberpesten en cancelen tot haatzaaien en shaming: de lijst met vormen van online kwetsend gedrag die we inmiddels kennen, wordt steeds langer. Daarnaast ontstaan er steeds nieuwe vormen en tactieken om grensoverschrijdende content
te verspreiden. Dat is niet alleen schadelijk voor de individuen die hiermee te maken krijgen, maar ook voor de samenleving als geheel. Denk bijvoorbeeld aan het gemak waarmee politici en wetenschappers tegenwoordig online worden bedreigd. Online lijken andere regels en normen te gelden dan offline het geval is.

Veel mensen herkennen deze problematiek: 70% van de Nederlanders vindt dat het anders moet. Maar hoe? Om die vraag te beantwoorden is het allereerst belangrijk om te weten waar we het eigenlijk over hebben. Daartoe dient deze whitepapwer, waarin Netwerk Mediawijsheid stilstaat bij wat we eigenlijk onder online kwetsend gedrag verstaan, wat de juridische aspecten hiervan zijn en wat het handelingsperspectief is voor burgers. Deze whitepaper is gebaseerd op relevant onderzoek en bestaande maatschappelijke initiatieven.

Netwerkpartners en andere professionals kunnen deze whitepaper als basisdocument gebruiken om educatief materiaal of lessen te ontwikkelen. Ook kunnen online platformen de whitepaper gebruiken als basis voor het vormgeven van gedragsregels.



1

Bewustwording

Allereerst is het belangrijk om duidelijk te maken wat precies bedoeld wordt met online kwetsend gedrag en wat de omvang van de problematiek is. Daarom wordt in dit hoofdstuk onder meer besproken welke vormen van online kwetsend gedrag bekend zijn, wie bepaalt wanneer iets kwetsend is, de mogelijke gevolgen voor het slachtoffer en hoe vaak het voorkomt.

1.1 Wat is online kwetsend gedrag?

Er zijn veel verschillende vormen van online kwetsend gedrag. Het is daarom lastig om een overkoepelende definitie te geven. Wetenschappelijke literatuur naar cyberagressie gebruikt vaak de volgende definitie die ook op online kwetsend gedrag van toepassing is: “Het opzettelijk toebrengen van schade via ICT aan een persoon of een groep personen die deze handelingen als beledigend, denigrerend, schadelijk of ongewenst ervaren.”[1] Een kanttekening bij deze definitie is dat er uit wordt gegaan van een bewuste handeling van de zender, terwijl er ook vormen van grensoverschrijdend gedrag bestaan waarbij het slachtoffer iets als kwetsend ervaart terwijl dit niet de intentie van de zender was.

Een andere manier om online kwetsend gedrag te definiëren is door eerst bij het tegenovergestelde, gewenst gedrag, stil te staan. Gewenst gedrag voldoet vaak tenminste aan deze drie voorwaarden:

1. Toestemming: Er is van iedereen toestemming, bijvoorbeeld voor het maken van een foto, hetversturen van de foto of het plaatsen van de post.
2. Vrijwillig: Alle betrokkenen kiezen er vrijwillig voor om iets te doen. Er is geen sprake vanmanipulatie, druk, straf of beloning.
3. Gelijkwaardige relatie: Alle betrokkenen hebben evenveel macht over elkaar.

Er is eerder sprake van grensoverschrijdend gedrag wanneer een of meerdere van dezevoorwaarden ontbreken.

1.2 Welke vormen van online kwetsend gedrag bestaan er?

In de bijlage van deze whitepaper staat een uitgebreide lijst van verschillende vormen van online kwetsend gedrag. In deze whitepaper gaat het specifiek over een aantal varianten die aansluiten bij de thematiek van de Week van de Mediawijsheid 2023. Het betreft de volgende vormen van online kwetsend gedrag: cyberpesten, cancelen, doxing, online haat, seksueel grensoverschrijdend gedrag en shaming. Voor sommige vormen geldt dat er enige overlap bestaat en de grenzenwat fluïde zijn. Zo kan doxing een vorm van intimidatie zijn en leiden tot online haat. En kan shaming zowel een
vorm van seksueel grensoverschrijdend gedrag zijn als een manier om te cyberpesten. In de bijlage staan overige vormen van online kwetsend gedrag en de bijbehorende definities.

[1] Grigg, D.W. (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. Australian Journal of Guidance and Counselling 20(2), 143–56. https://doi.org/10.1375/ajgc.20.2.143

1. Cyberpesten

Onder cyberpesten, ook wel online pesten of cyberbullying genoemd, verstaan we het pesten via digitale media. Het Cyberbullying Research Center definieert cyberpesten als 'opzettelijke en herhaaldelijke schade die wordt toegebracht door het gebruik van computers, mobiele telefoons en andere elektronische apparaten.' Toch zijn er ook situaties denkbaar waarbij de ontvanger iets als cyberpesten ervaart, terwijl de zender dit niet zo heeft bedoeld.

Het Kenniscentrum Online Pesten wijst erop dat cyberpesten vaak een aanvulling is op ander pestgedrag en kinderen en jongeren in hun sociale interacties geen onderscheid meer zien tussen de fysieke en digitale wereld. Het grootste verschil tussen offline en online pesten is dat die laatste variant 24/7 door kan gaan. Hierdoor hebben ontvangers het gevoel nergens meer veilig te zijn en kan de impact nog groter zijn dan bij 'regulier' pesten al het geval is.

Het kenniscentrum onderscheidt drie kenmerken van online pesten:

1. Het pesten houdt nooit op en kan op elk moment doorgaan, wat de kwetsbaarheid van het slachtoffer vergroot. Digitale bestanden zoals foto's en video's kunnen breed verspreid worden en zijn moeilijk te verwijderen, zelfs als het pesten stopt.
2. Het vindt op afstand plaats, waardoor de impact minder zichtbaar is en het pesten ernstiger kan worden. Als het pesten ook op openbare platforms gebeurt, kan het een groot publiek bereiken.
3. Het kan anoniem gebeuren via nepaccounts, wat pesters het gevoel kan geven dat er minder toezicht is. Sommige pesters blijven bewust anoniem, ook al kennen ze hun doelwit in het echte leven.

Netwerkpartner VPNgids.nl heeft een uitgebreid artikel over wat cyberpesten is en wat je eraan kan doen.

Roddelaccounts

Steeds meer scholen hebben te maken met zogenoemde Gossip Girl-accounts waarmee roddels en compromitterende beelden van leerlingen (of docenten) online worden verspreid. Vaak gebeurt dit via TikTok. Netwerkpartner Kennisnet publiceerde een artikel over dit fenomeen met tips voor scholen om hier mee om te gaan.

2. Cancelen

Van cancelen bestaan meerdere definities. In het rapport 'Online ontspoord' spreekt het Rathenau Instituut van 'online shaming waarbij wordt opgeroepen om iemand uit te sluiten uit diens community bij wijze van sociale straf'. Deze definitie van cancelen kan voor sommige gevallen te beperkt zijn. Soms wordt er ook gesproken van een 'culturele boycot' die is gericht tegen bedrijven of beroemde personen.

Bij het verschijnsel cancelen hoort ook het begrip cancelcultuur. Hierover schrijft Richard Rogers, verbonden aan de afdeling Mediastudies van de Universiteit van Amsterdam, bijvoorbeeld: “Cancelcultuur is een hedendaagse term die het grotere fenomeen beschrijft van publieke belastering van aanstootgevende uitingen of acties, grotendeels in sociale media, maar ook via andere vormen van *deplatforming*, zoals het afzeggen van een spreekbeurt.”

In media is cancelen vaak onderwerp van gesprek, zoals hier in een artikel over hoe radiostations stoppen met het draaien van muziek van artiesten die met grensoverschrijdend gedrag in het nieuws zijn geweest. Of hier in een stuk over een boycot van Bud Light vanuit conservatieve kringen nadat het Amerikaanse biermerk samenwerkte met een transgenderactiviste. Het idee van cancelen en het bestaan van een cancelcultuur roept regelmatig felle kritiek op, dat vaak in lijn ligt met kritiek op wat met een containbegrip als ‘woke’ wordt omschreven. Ook is er een link tussen de #MeToo- beweging en cancelen te maken. Diverse mensen zijn gecanceld na het uitkomen van een #MeToo-affaire.

3. Doxing

Onder doxing wordt het openbaar delen van andermans persoonsgegevens verstaan, met de bedoeling om diegene te intimideren. Het gaat hier vaak om persoonlijke, sensitieve en privéinformatie zoals adres, telefoonnummer, paspoort, werkgever, gegevens van familie en foto’s van iemands kinderen. De informatie die wordt gedeeld is vaak via openbare bronnen beschikbaar, zodat er geen hacking nodig is. De term doxing is een samenvoeging van de Engelse woorden ‘dropping dox’, wat zoveel betekent als ‘documenten publiceren’. Doxing komt vaak voor bij bekende politici, journalisten of opiniemakers, maar kan zeker ook ‘gewone’ burgers overkomen. Doordat er gevoelige persoonlijke gegevens worden gedeeld, kan doxing ook leiden tot offline geweld.

Tijdens de coronapandemie heeft boosheid over de overheidsmaatregelen voor een toename van doxing gezorgd, zo laat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) weten. Er zijn in die periode diverse voorbeelden van doxing, zoals het delen van persoonsgegevens van mensen die – al dan niet als undercoveragent – bij de politie werken of de huisadressen van ‘linkse’ journalisten en bewindspersonen die in radicaal-rechtse Telegramgroepen zijn rondgegaan. Doxing kan ook een vorm zijn van digitaal vigilantisme: collectieve actie tegen personen die ongewenst sociaal gedrag vertonen.

In dit uitgebreide artikel gaat netwerkpartner VPNgids.nl uitgebreid in op (de gevolgen van) doxing. Ook bij netwerkpartner Kliksafe.nl lees je meer over (voorbeelden) van doxing. En in dit bericht lees je waarom doxing vanaf 1 januari 2024 strafbaar wordt.

Outing
Ook het ongevraagd openbaar maken van iemands seksuele voorkeur, genderidentiteit of geloofsovertuiging valt onder doxing. Dit is een vorm van online kwetsend gedrag waar vooral de LHBTIQ+-gemeenschap mee te maken heeft en wat een grote impact op hun leven kan hebben. Dit wordt ook wel 'outing' genoemd.

4. Online haat

Binnen deze grote categorie vallen meerdere vormen van online kwetsend gedrag: haatzaaien, discriminatie, bedreiging en intimidatie. In het rapport 'Online ontspoord' van het Rathenau Instituut is een uitgebreide paragraaf over online haat opgenomen, waarvan we hieronder enkele (ingekorte) passages overnemen.

Online haat richt zich op individuen, maar is vaak ook bedoeld om achterliggende groepen te schaden. Bij online haat is een vorm van xenofobie (afkeer van alles wat vreemd is) de belangrijkste drijfveer. Online haat komt voort uit afkeer tegen bepaalde groepen mensen, ook als het zich richt op individuen. Slachtoffers van online haat worden veroordeeld op basis van een of meer kenmerken van hun identiteit. Iemand die bijvoorbeeld zowel zwart, vrouw, als lesbisch is, kan online haat ervaren die zowel racistisch, seksistisch als homofoob van aard is. Dit wordt in de sociologie, genderstudies en rechtsgeleerdheid 'intersectionaliteit' of 'kruispuntdenken' genoemd: als ongelijkheid zich voordoet langs verschillende assen die elkaar snijden. Dit speelt een grote rol bij
online haat.[2]

Haatzaaien

Een uniforme definitie van haatzaaien (hate speech in het Engels) ontbreekt. De Raad van Europa definieert het als volgt: 'haatzaaien omvat alle uitingsvormen die zorgen voor verspreiding, aanstichting, aanmoediging of legitimering van raciale haat, xenofobie, antisemitisme of andere vormen van haat gebaseerd op intolerantie' (Council of Europe, 2021). Online haatzaaien is zowel schadelijk voor slachtoffers als voor de maatschappij in de breedte, omdat het zorgt voor een onveilige omgeving voor iedereen. Mensen kunnen voorzichtiger worden in hun online uitspraken uit angst om slachtoffer te worden van online haat. Haatzaaien op internet verschilt op vier belangrijke manieren van haatzaaien op straat, zo blijkt uit onderzoek van UNESCO (2015):

1. Online kan haatzaaiende content erg lang beschikbaar blijven op verschillende platformen.
2. De haatzaaiende content kan snel weer opduiken op een ander platform, ook als de content elders verwijderd is.
3. Anonimiteit op internet zorgt voor handhavingsproblemen, al heeft de politie vaak wel mogelijkheden tot identificatie maar niet genoeg capaciteit.
4. Het internationale karakter van het internet zorgt ervoor dat het moeilijk is om 'nationaal' op te treden tegen haatzaaien dat in andere landen gehost wordt.[3]

[2]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op hetinternet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)
[3]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het iinternet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)

In 2021 werd een man door de rechtbank Midden-Nederland veroordeeld voor online haatzaaien. De man plaatste in een half jaar tijd verschillende haatzaaiende, discriminerende en gewelddadige berichten op social media. Die berichten waren gericht tegen Joden, moslims en mensen met een andere huidskleur dan hijzelf.

Discriminatie

Drie veelvoorkomende vormen van online discriminatie zijn seksisme, racisme en homofobie:

- **Seksisme** omvat gedrag of houdingen die discrimineren puur op basis van ge slacht.Online is seksisme vaak verbonden met andere vormen van online immo reel en schadelijk gedrag, zoals bedreiging en cyberpesten. Vaak zijn vrouwen hiervan het slachtoffer. Volgens Amnesty International (2018) zijn online seksis me en misogynie (vrouwenhaat) vaak bedoeld om vrouwen te intimideren of te kleineren. Circa 7,1% van de tweets die vrouwen ontvangen, is problematisch of schimpend (Amnesty International, 2017). Ook passieve en indirecte seksisti sche opmerkingen verpakt als grapje kunnen schadelijk zijn voor het welzijn van vrouwen, zo blijkt uit onderzoek van Harvard uit 2015 (Fox et al., 2015). Atria, het Kennisinstituut voor Emancipatie en Vrouwengeschiedenis, schrijft in dit artikel meer over misogynie (een ander woord voor vrouwenhaat) en de haat waar vrouwen online mee te maken krijgen.
- **Racisme** draait om de opvatting dat mensen op basis van een verondersteld 'ras' in groepen zijn onderverdeeld en dat de ene groep superieur is aan de andere. Online racisme, ook wel cyber-racisme genoemd, onderscheidt zich van offline racisme doordat de racistische uitingen online plaatsvinden, en doordat racistische mensen elkaar online gemakkelijk kunnen vinden en zich zo kunnen verenigen (Bliuc et al., 2018). Mensen met racistische denkbeelden gebruiken het internet om hun denkbeelden te valideren en zichzelf het gevoel te geven dat ze ergens bij horen. Mensen die zich racistisch gedragen, kunnen online gemak kelijk hun denkbeelden delen, onder andere door de anonimiteit die het internet biedt. De motivatie achter online racisme ligt vaak in het schaden van mensen van kleur, het uitlokken van conflict en het normaliseren van racistisch gedachte goed in het publieke debat.[4]
- **Homofobie** is een angst voor, of haat tegenover, personen die zich emotioneel of seksueel aangetrokken voelen tot personen van dezelfde sekse, maar bij uitbreiding wordt de term ook gebruikt voor angst of haat ten aanzien van bij voorbeeld mensen met andere dan cisgenderidentiteiten. Er is sprake van discriminatie als iemands handelen door homofobie is ingegeven. Een vorm van ho mofoob immoreel en schadelijk gedrag online is 'outing'. Outing is het bekend maken van iemands genderidentiteit of seksuele voorkeur zonder zijn of haar toestemming. De schade daarvan kan enorm zijn, bijvoorbeeld in landen waar LHBTIQ+'s vervolgd worden of in families waarin zij niet geaccepteerd worden.[5] Outing kan daarnaast ook als een vorm van doxing worden gezien.

[4]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)

[5]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)

Bedreiging en intimidatie
Doordat groepen zich online gemakkelijk kunnen mobiliseren, kan bepaald gedrag al snel escaleren. Groepen mensen kunnen zich daardoor op één individu gaan richten, die het groepsgedrag als intimiderend kan ervaren (Blackwell et al., 2017). De intimidatie kan dan vormen aannemen variërend van het herhaaldelijk sturen van berichten, bellen met iemands werkgever tot het dreigen bepaalde foto's of informatie openbaar te maken. Alleen al het gevolgd worden door bepaalde accounts op sociale media, kan als intimiderend worden ervaren. Het dreigen met seksueel geweld is iets waar vooral jonge vrouwen online mee te maken krijgen (Plan International, 2020).[6] Van diverse politici is bekend dat ze met online bedreigingen te maken hebben. Ook zien we dat het aantal online (en offline) bedreigingen tegen journalisten toeneemt.

5. Seksueel grensoverschrijdend gedrag

Naast het hierboven al genoemde seksisme bestaan er verschillende vormen van online kwetsend gedrag met een seksuele component. Hieronder zetten we er een aantal op een rij:

- **Grooming:** het proces waarbij een volwassene iemand die jonger is dan 16 jaar verleidt tot (online) contact en vaak ook een vertrouwensband opbouwt, met als uiteindelijke doel om (al dan niet online) af te spreken en seksueel misbruik te plegen. In oktober 2023 werd bekend dat de rechtbank van Amsterdam een man tot vijf jaar cel en tbs met dwangverpleging heeft opgelegd nadat hij jonge meisjes online manipuleerde door zich voor te doen als een 14-jarige en hen verleidde tot het sturen van naaktfoto's en filmpjes. De zaak kwam aan het licht nadat een meisje aangifte deed na het zien van een aflevering van het televisieprogramma Klokhuis waarbij grooming ter sprake kwam. Online grooming verschilt van offline grooming, omdat volwassenen veel gemakkelijker (anoniem) contact kunnen leggen met kinderen. Ook blijkt uit onderzoek dat jongeren online sneller risicovol gedrag vertonen.[7]
- **Sexting en shame sexting:** onder sexting verstaan we het verspreiden of delen van seksueel getinte berichten, foto's of video's van zichzelf via mobiele telefoons of andere media. Het is belangrijk om te benadrukken dat sexting op zichzelf niet schadelijk of strafbaar is en past bij gezond experimenteergedrag van jongeren. Volgens Rutgers, het Nederlandse kenniscentrum seksualiteit, wordt sexting pas schadelijk als anderen ongevraagd met die seksueel getinte beelden aan de haal gaan. Dan noemen we het shame sexting. In combinatie met andere fenomenen als hacking en phishing en door versterking van online mechanismen (viraliteit, schaalbaarheid) kan shame-sexting leiden tot schade die veel groter is dan offline mogelijk zou zijn.[8]
- **Sextorion** een vorm van afpersing waarbij een zender dreigt om zonder toestemming seksueel beeldmateriaal van het slachtoffer te openbaren, om deze te dwingen om meer van dit soort materiaal te sturen, te betalen of om (al dan niet seksueel getinte) opdrachten uit te voeren.[9] Er zijn ook vormen van sextortion waarbij iemand wordt afgeperst om mee te werken aan criminele activiteiten

[6]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)
[7]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)
[8]Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)
[9] Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)

zoals het openstellen van een bankrekening, of het verstrekken van betaalmiddelen als crypto of cadeaukaarten.

- **Wraakporno:** het zonder toestemming bezitten en openbaar maken/verspreiden van (gestolen) seksueel beeldmateriaal door bijvoorbeeld hackers, (ex)partners, kindermisbruikers, verkrachters en mensenhandelaren. Anders dan bij sextortion gaat het hier niet om afpersing, maar over doelbewust schade toebrengen aan slachtoffers door het naar buiten brengen van de beelden.

6. Shaming

Er zijn veel verschillende vormen van online shaming. Het Rathenau Instituut omschrijft shaming als een vorm van digitaal vigilantisme waarbij publieke morele kritiek online wordt geuit als reactie op het overschrijden van sociale normen. Het ziet shaming als een tactiek om sociaal geldende normen duidelijk te maken, bijvoorbeeld door iemand online te wijzen op het racistische karakter van zijn of haar uitspraken. Dat maakt het ook lastig om te beoordelen of shaming 'gerechtvaardigd' is, en wanneer morele grenzen overschreden worden. Mensen die aan online shaming doen, hebben niet altijd tot doel dat iemand zich gaat schamen. Vaker willen ze aandacht voor een sociale gewoonte of norm vragen, die ter discussie stellen en anderen mobiliseren voor hun doel – bijvoorbeeld het tegengaan van racisme of seksisme. Shaming kan uitgroeien tot cancelen. [10]

Er zijn ook vormen van shaming waarbij de doelen minder nobel zijn. Zo valt het ongewenst digitaal verspreiden van seksueel getint beeldmateriaal bijvoorbeeld ook onder online shaming. Het televisieprogramma Pointer heeft hier onderzoek naar gedaan en een dossier over samengesteld. Hieruit blijkt dat een kwart van de basisscholen te maken heeft met online shaming door het verspreiden van digitale naaktfoto's van leerlingen. In hetzelfde onderzoek geeft negen van de tien ondervraagde zorgcoördinatoren aan dat er op hun middelbare school sprake is van online shaming. Er wordt dan ook voor gepleit om lessen over dit onderwerp te gaan geven, maar dit is nog niet verplicht.

Het internet maakt shaming gemakkelijker doordat groepen mensen zich eenvoudig kunnen verenigen en doordat gemeenschappen online gemakkelijker aan zelfregulering kunnen doen. Stel dat iemand in een community op Facebook iets zegt dat als racistisch wordt ervaren, dan kan een veroordelende opmerking van één persoon ervoor zorgen dat alle leden zich tegen hem of haar keren. Het internet zorgt er bovendien voor dat shaming erg moeilijk te controleren en in de hand te houden is.[11]

1.3 Waar vindt online kwetsend gedrag plaats?

Online kwetsend gedrag kan overal online plaatsvinden, wanneer er een interactie is tussen twee of meerdere personen of entiteiten zoals bedrijven of organisaties. Dit kan zowel in de privésfeer zijn tussen mensen die elkaar kennen en via privéberichten of -kanalen met elkaar communiceren, als in de openbare sfeer tussen mensen die elkaar al dan niet persoonlijk kennen op platforms, apps en websites. Je komt online kwetsend gedrag onder meer tegen op berichtenapps (o.a. WhatsApp of Telegram), socialmedia-

[10] Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)
[11] Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland.

apps of -sites (o.a. Instagram, Facebook, Snapchat of Twitter), video-apps of -sites (o.a. YouTube of TikTok), blogs en fora (o.a. Reddit of Dumpert), online nieuwssites met reactiemogelijkheid (o.a. Nu.nl), online games (o.a. League of Legends of Fortnite), online streamingplatforms (o.a. Twitch of Discord), datingapps (o.a. Tinder, Grindr of Bumble) en buurt- en wijkplatforms of -apps.[12]

1.4 Wie bepaalt wanneer we spreken over online kwetsend gedrag?

Wat we precies onder online kwetsend gedrag verstaan, kan per individu verschillen. Het hangt er bijvoorbeeld van af hoe iemand die met potentieel grensoverschrijdend gedrag te maken krijgt, dat specifieke gedrag zelf ervaart. Dit terwijl een rechter bijvoorbeeld over concrete kaders beschikt om te bepalen wat wel en niet toelaatbaar is, omdat die zich op bestaande wet- en regelgeving baseert. In theorie dan: niet voor al het grensoverschrijdend gedrag dat we kennen bestaat al wet- en regelgeving, omdat de online wereld zich nu eenmaal sneller ontwikkelt dan wetgevers kunnen bijbenen. Mede daarom blijft het in veel gevallen lastig om te beoordelen wat wel of niet grensoverschrijdend is. Daarbij speelt ook mee dat de normen per online community kunnen verschillen en daarmee ook wat deelnemers aan die community als aanvaardbaar zien. De online omgeving is niet per se wettelozer of grenzelozer dan de offline wereld, maar wordt wel sneller zo ervaren.[13]

Naast de vormen van online kwetsend gedrag die volgens wet- en regelgeving strafbaar zijn, is het goed om de ontvanger zelf te laten bepalen wat diegene als grensoverschrijdend ervaart. Hierbij is het belangrijk om te beseffen dat zenders lang niet altijd bewust grensoverschrijdend gedrag vertonen. Juist daarom is het cruciaal dat ontvangers hun grenzen aangeven en dat dit serieus wordt genomen. Ook zijn er manieren om zelf sociale normen te stellen, bijvoorbeeld binnen een organisatie, en zo een omgeving te creëren waarin het duidelijk is dat discriminatie niet door de beugel kan. In dit artikel geeft Movisie daar een aantal tips voor.

1.5 Hoe herken je online kwetsend gedrag?

Online kwetsend gedrag is onder meer te herkennen aan hoe de ontvanger reageert (of niet reageert) en aan reacties van omstanders die het gedrag bijvoorbeeld afkeuren, als zenders (veronderstelde) identiteitskenmerken zoals iemands ‘ras’, seksuele geaardheid of uiterlijk misbruiken om het slachtoffer te schaden, of als de context duidelijk maakt dat het gedrag expres kwetsend bedoeld is. Een grote uitdaging bij het herkennen van online kwetsend gedrag is het ontbreken van duidelijke normen in de online omgeving. Dit heeft als gevolg dat gedrag dat we in de offline wereld onacceptabel vinden, online veel lastiger kunnen herkennen. [14] Als er sprake is van online kwetsend gedrag, is de kans in ieder geval groot dat degene over wie het gaat het als kwetsend ervaart.

[12] https://www.vpngids.nl/privacy/apps/buurtpreventie/-apps
[13] Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)
[14] Rathenau Instituut (2021). Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Den Haag (auteurs: Huijstee, M. van, W. Nieuwenhuizen, M. Sanders, E. Masson en P. van Boheemen)

1.6 Wat zijn de mogelijke gevolgen van online kwetsend gedrag?

Omdat de vormen van online kwetsend gedrag nogal uiteenlopen, kunnen de gevolgen de ontvanger ook sterk verschillen. In deze whitepaper spreken we in plaats van ontvanger ook vaak over 'slachtoffer'. Om de negatieve gevolgen ervan te ondervinden, hoef je namelijk niet altijd ontvanger van kwetsend online gedrag te zijn. Je kan ook het onderwerp zijn, onder meer bij cancelen, doxing of shame texting.

Discriminerende en hatelijke online reacties online kunnen ernstige gevolgen hebben op zowel de korte als de lange termijn. Denk bijvoorbeeld aan een negatieve impact op de mentale gezondheid, zoals stress, maar ook aan sociale uitsluiting, pesten en slechtere werk- of schoolprestaties. Haatberichten op sociale media voeden bovendien de tegenstelling tussen verschillende groepen in de samenleving en dragen zo bij aan polarisatie.[15] Daarbij is het belangrijk om te beseffen dat bepaalde vormen van online kwetsend gedrag, zoals doxing, zich verder kunnen ontwikkelen tot offline geweld. Bij 20 procent van de vrouwelijke journalisten die met online kwetsend gedrag te maken krijgen, is dit bijvoorbeeld het geval.[16]

Onderzoek naar de langetermijngevolgen van (cyber)pesten laat zien dat volwassenen die tijdens de kindertijd of als tiener met online en/of offline pesten te maken hebben gehad een verhoogd risico op mentale gezondheidsproblemen hebben. Voormalige slachtoffers hebben vaak minder zelfvertrouwen, meer sociale angst en zijn minder tevreden over hun leven in vergelijking met volwassenen die vroeger niet zijn gepest. Bij (cyber) pesten zien onderzoekers diverse gevolgen voor slachtoffers. Het is aannemelijk dat deze gevolgen ook deels van toepassing zijn op slachtoffers van
andere vormen van online kwetsend gedrag:

- Minderwaardigheidsgevoel en weinig zelfvertrouwen en eigenwaarde;
- Onzeker gedrag;
- Terugtrekken in zichzelf, in hun (gekozen) eenzaamheid en terechtkomen in een isolement;
- Geen of moeilijk sociale contacten kunnen leggen;
- Niet voor zichzelf op durven komen;
- Wantrouwen of argwaan tegenover andere mensen;
- Fobieën zoals pleinvrees, claustrofobie;
- Angsten waaronder faalangst;
- Zich machteloos voelen;
- Zich buitengesloten voelen;
- Opgejaagd en angstig voelen;
- Wantrouwen ervaren naar mensen, zelfs als deze goede bedoelingen hebben;
- Zelf geen kinderen durven nemen uit angst voor herhaling bij eigen kind;
- Moeite hebben met het aangaan van relaties;
- Nachtmerries;
- Het hebben van (zware) depressies;

[15] https://www.kis.nl/sites/default/files/2022-12/Online-Discriminatie-Rapport.pdf
[16] ttps://www.icfj.org/sites/default/files/2023-02/ICFJ%20Unesco_TheChilling_OnlineViolence.pdf

- Het hebben van (ernstige) gezondheidsproblemen;
- Een einde willen maken aan hun leven, zelfs al bij heel jonge kinderen.[17]

Expertisecentrum voor seksualiteit Rutgers heeft onderzoek gedaan naar online seksueel geweld, waarin ze ook dieper ingaan op de gevolgen. In het rapport 'Wat bepaalt de impact van online seksueel geweld? Verkennend onderzoek onder slachtoffers en hulpverleners' zeggen de onderzoekers hier het volgende over: "De gevolgen van online seksueel geweld lopen uiteen, maar op de korte termijn hebben veel slachtoffers last van paniek en angst, van schaamte en schuldgevoelens, van zich vies en minderwaardig voelen, van eenzaamheid en verdriet en van machteloosheid. Ook is hun vertrouwen in mensen geschaad en worden slachtoffers soms negatief behandeld door anderen (pesten op school, victim blaming, uitlachen, reputatieschade). Sommige slachtoffers krijgen zelfs te maken met intimiderende of gewelddadige acties vanuit de familie en vanuit mannen die ze niet kennen, die hun gegevens hebben uit app- en telegramgroepen. Op de lange termijn kunnen deze gevoelens leiden tot mentale klachten, depressies, suïcidaliteit en posttraumatische stress. Ook kan online seksueel geweld, zeker in de adolescentie, leiden tot een verstoorde romantische en seksuele ontwikkeling."[18]

In dit artikel vertelt een vrouw hoe ze als tiener met shame sexting te maken had en wat de gevolgen voor haar waren.

Verschillende vormen van online kwetsend gedrag kunnen ook gevolgen hebben in de offline wereld. Dit is bijvoorbeeld bij doxing het geval. Zo kreeg de Groningse journalist Willem Groeneveld een molotovcocktail door het raam gegooid nadat zijn adresgegevens online waren gedeeld door een ondernemer die boos was na een artikel van Groeneveld. Een ander bekend voorbeeld is het bedreigen van D66-leider Sigrid Kaag door een man die met een fakkel bij haar huis stond.

1.7 Hoe vaak komt online kwetsend gedrag voor?

Het is lastig om een realistisch beeld van deze problematiek te schetsen. Dit komt onder meer doordat veel slachtoffers van online kwetsend gedrag hier geen melding van doen. Of dit nu uit schaamte is, of omdat ze niet weten bij welke instantie ze terechtkunnen, het gevolg is in ieder geval dat het daadwerkelijke aantal slachtoffers (significant) hoger is dan het aantal meldingen of aangiftes. Ook speelt mee dat er naar veel vormen van online kwetsend gedrag (nog) geen grote studies bestaan die inzicht kunnen bieden in de problematiek. Dit kan bijvoorbeeld komen doordat het relatief nieuwe fenomenen betreft en er verschillende definities in omloop zijn die zich daardoor moeilijk laten vergelijken. Ook kan de aard van sommige vormen van online kwetsend gedrag nogal verschillen, door de mate waarin slachtoffers dit al dan niet als kwetsend ervaren.

[17] Handboek voor Sta Sterk trainers - Sta Sterk training - Kenniscentrum Omgaan met Pesten
[18] https://rutgers.nl/wp-content/uploads/2022/06/Rapport-Wat-bepaalt-de-impact-van-online-seksueel-geweld.pdf

Al is het op dit moment dus vrijwel onmogelijk om de totale omvang van online kwetsend gedrag in kaart te brengen, er zijn wel diverse losstaande statistieken die inzicht bieden in de problematiek:

- Uit een wereldwijd onderzoek (2020) naar de veiligheid van vrouwelijke journalisten bleekdat 73 procent van de respondenten met online misbruik te maken heeft gehad. Twintigprocent liet weten slachtoffer te zijn geweest van offline aanvallen of misbruik gerelateerdaan online misbruik.[19]
- De organisatie Helpwanted, een anonieme hulplijn die praktische hulp en persoonlijk adviesbiedt bij online seksueel misbruik, kreeg in 2022 24 procent meer adviesvragen dan het jaarervoor. In totaal kreeg de organisatie 7.727 adviesaanvragen. De hulplijn is 24/7 bereikbaaren krijgt dagelijks meldingen van online kwetsend gedrag. Van 1 januari tot en met 30 juli2022 ging dit bijvoorbeeld om 5479 hulpvragen. [20]
- De Anti-Defamation League (ADL), een Amerikaanse NGO die antisemitisme enonverdraagzaamheid tegengaat, onderzocht in 2022 in hoeverre gamers last hebben vanonline intimidatie. Van de 2000 respondenten gaf 66 procent aan tijdens het online gamenweleens met een vorm van intimidatie te maken hebben gehad.
- Uit onderzoek van het CBS naar online veiligheid en criminaliteit (2022) blijkt dat 2 procentvan de Nederlanders van 15 jaar of ouder zich in de afgelopen 12 maanden weleens onlinegediscrimineerd heeft gevoeld. Dat zijn bijna 340 duizend mensen. Jongeren van 15 tot 25jaar gaven dit met 5 procent relatief vaak aan. Biseksuele vrouwen (9 procent) enhomoseksuele mannen (7 procent) hadden er vaker mee te maken dan personen met een andere seksuele oriëntatie.[21]
- In een enquête die Movisie uitzette rond online discriminatie in de voetbalwereld gaf 92procent van de respondenten, betaald voetbal-spelers in de Eredivisie en Eerste Divisie, aanwel eens discriminerende berichten over collega's op sociale media te zien. 44 procentontvangt zelf discriminerende berichten, waarvan een deel dagelijks. De berichten dierespondenten ontvangen, zijn veelal van racistische aard en komen grotendeels binnen viaprivéberichten op Instagram.
- Het aantal meldingen van bedreigde politici is de afgelopen jaren flink toegenomen. HetTeam Bedreigde Politici houdt cijfers bij van bedreigingen van onder meer ministers enstaatssecretarissen, maar ook bijvoorbeeld de voorzitter van de Raad van State en deNationale Ombudsman. Waar het in 2015 nog om 200 meldingen ging, was dit aantal in2020 gestegen naar 600 meldingen. [22]
- Uit onderzoek van het CBS blijkt dat in 2020 bijna 30% van de 16 tot 18-jarige vrouwen en 23% van de 18 tot 24-jarige vrouwen aangeeft in de afgelopen 12 maanden online te zijn geconfronteerd met ongewenst seksueel gedrag. Daarnaast gaat het respectievelijk om 9% en 8% van hun mannelijke leeftijdgenoten. Ruim een derde (36%) heeft deze ervaring van seksuele intimidatie voor zich gehouden.[23]

[19] https://www.freepressunlimited.org/en/current/press-freedom-digital-age-impact-digital-services-act
[20] https://jaarverslag2022.offlimits.nl/
[21] https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022/8-online-discriminatie
[22] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5285292/sociale-asociale-media-sigrid-kaag-beau
[23] https://www.rathenau.nl/sites/default/files/2021-07/Rathenau_Instituut_Rapport_Online_ontspoord.pdf

2

Wet- en regelgeving

Voor veel nieuwe technologieën geldt dat wet- en regelgeving vaak achterloopt op de impact die mensen in de praktijk ervaren. Dit is goed te verklaren: het kost veel tijd om wet- en regelgeving op te stellen en in werking te laten treden. Alles vooraf regelen is ook lastig, omdat de (negatieve) impact die een nieuwe technologie heeft niet altijd te voorspellen is. Dit gaat ook op voor online kwetsend gedrag. In dit hoofdstuk wordt ingegaan op wat er in Nederlandse én Europese wet- en regelgeving op het gebied van online kwetsend gedrag is vastgelegd.

2.1. Nederlandse wetgeving

Voor online kwetsend gedrag is het uitgangspunt dat wat offline verboden is, online ook niet mag. In artikel 1 van de Grondwet is bijvoorbeeld vastgelegd dat discriminatie op basis van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook verboden isn. Rond een flink aantal voorbeelden van online kwetsend gedrag bestaan relevante artikelen in het Wetboek van Strafrecht, zoals discriminatie en haatzaaien, sextortion, wraakporno, grooming, hacking, phishing, identiteitsfraude en cryptofraude.

Bij het opleggen van straffen wordt er door de rechter in principe geen onderscheid gemaakt tussen offline en online. Wel bestaan er bij online kwetsend gedrag soms aanvullende regels ten opzichte van het offline vergrijp. Zo zijn bij een aangifte van online discriminatie een aantal regelsvastgelegd en moet bijvoorbeeld de politie onder meer beschikken over de accountnaam waar de uiting mee is geplaatst en de periode waarin de uiting online heeft gestaan.[24]

De afgelopen jaren is er in de rechtszaal steeds vaker aandacht voor online kwetsend gedrag, zoals het bedreigen van politici. Zo kregen personen die Tweede Kamerlid Sylvana Simons online met de dood bedreigden door de rechter taakstraffen opgelegd in een rechtszaak die veel media-aandacht kreeg.[25] Bedreigers van kinderboekenschrijver Pim Lammers kregen onlangs ook taakstraffen opgelegd. De politierechter benadrukte hierbij dat gebruikers van sociale media vaak de ogen sluiten voor de gevolgen van het grove woordgebruik waarmee zij hun onvrede uiten. De rechter wil met het vonnis het signaal afgeven dat het strafrecht grenzen stelt aan wat men, bijvoorbeeld via sociale media, tegen anderen kan zeggen.[26]

In oktober 2023 werd bekend dat de rechtbank van Amsterdam een man tot vijf jaar cel en tbs met dwangverpleging heeft opgelegd nadat hij jonge meisjes online manipuleerde door zich voor te doen als een 14-jarige en hen verleidde tot het sturen van naaktfoto's en filmpjes. De zaak kwam aan het licht nadat een meisje aangifte deed na het zien van een aflevering van het televisieprogramma Klokhuis waarbij grooming ter sprake kwam.

Een uitdaging bij het aanpakken van online bedreigingen is dat veel van de bedreigingen al dan niet opzettelijk wat vaag en algemeen blijven. Dan schrijft iemand bijvoorbeeld "Ik hoop dat je een ongeluk krijgt". Zulke vormen van wensdenken zijn in Nederland niet

[24] https://www.kis.nl/sites/default/files/2022-12/Online-Discriminatie-Rapport.pdf
[25] https://www.ad.nl/binnenland/doodsbedreiger-sylvana-simons-krijgt-taakstraf-van-veertig-uur~a69027ce/
[26] https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Midden- Nederland/Nieuws/Paginas/Online-bedreiging-schrijver-Pim-Lammers-levert-taakstraffen-op.aspx

direct strafbaar. Het is daardoor vaak lastig om te bepalen waar de grenzen van de vrijheid van meningsuiting liggen en wanneer iets strafbaar is.

Als wetgevende macht debatteert het Nederlandse parlement regelmatig over online omgangsvormen en de gevolgen van online kwetsend gedrag. Hierbij komt ook de verantwoordelijkheid van de platforms waarop het gedrag plaatsvindt aan bod. Zo is onlangs een motie aangenomen[27] die socialemediabedrijven onder meer verplicht om continu bereikbare escalatiekanalen te faciliteren. Hier moeten slachtoffers zich kunnen melden en hulp krijgen van medewerkers die de Nederlandse taal spreken en de culturele context van de content begrijpen.

Voor de eerder in deze whitepaper genoemde vormen van online kwetsend gedrag geldt de volgende wet- en regelgeving:[28]

Cyberpesten: Hoewel de gevolgen groot kunnen zijn, is pesten zowel offline als online niet strafbaar.
Cancelen: Over cancelen bestaat geen relevante wet- en regelgeving.
Doxing: Doxing is vanaf 1 januari 2024 strafbaar. De wet die dit regelt, is onlangs door de Eerste Kamer aangenomen.[29]
Online haat: In het Wetboek van Strafrecht zijn drie artikelen opgenomen over haatzaaien: Artikel 137c, Artikel 137d en Artikel 137e. Discriminatie is strafbaar onder Artikel 137c, 137d en 137e van het Wetboek van Strafrecht. In Nederland is seksisme niet expliciet opgenomen in het Wetboek van Strafrecht, in tegenstelling tot bijvoorbeeld in België en Frankrijk. Wel is seksisme strafbaar onder discriminatie in Artikel 137c, 137d en 137e van het Wetboek van Strafrecht.
Grooming: Sinds 2010 is grooming strafbaar in Nederland onder artikel 248e van het Wetboek van Strafrecht. Voor de strafbaarheid is het noodzakelijk dat de dader een ‘voorstel tot ontmoeting’ heeft gedaan richting het slachtoffer.
Sextortion: Sextortion kan als chantage strafbaar zijn onder artikel 318 van het Wetboek van Strafrecht (afpersing en afdreiging).
Wraakporno: Sinds 1 januari 2020 is wraakporno strafbaar onder artikel 139h van het Wetboek van Strafrecht. Zowel het bezitten als het verspreiden van seksueel beeldmateriaal zonder toestemming is hierdoor strafbaar gesteld. Ook wordt onderzocht of het creëren en verspreiden van met behulp van kunstmatige intelligentie gemaakte ‘deepnudes’ strafbaar kan worden gesteld.
Shaming: Sinds 1 januari 2020 is online shaming verboden. Er mogen geen beelden worden verspreid als het aannemelijk is dat dat nadelig is voor degene die erop staat.[30]

Dat sommige vormen van online kwetsend gedrag (nog) niet strafbaar zijn, wil natuurlijk niet zeggen dat het gedrag daarmee automatisch gepast en wenselijk is of minder grote gevolgen voor de ontvanger heeft.

[27] https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2023Z10027&did=2023D24072
[28] https://www.rathenau.nl/sites/default/files/2021-07/Rathenau_Instituut_Rapport_Online_ontspoord.pdf
[29] https://www.rijksoverheid.nl/actueel/nieuws/2023/07/12/gebruik-van-persoonsgegevens-met-als-doel-intimidatie-wordt strafbaar#:~:text=Het%20wordt%20strafbaar%20om%20persoonsgegevens,doxing%20genoemd%20-%20strafbaar%20te%20stellen
[30] ttps://nos.nl/artikel/2403930-anonieme-daders-online-shaming-vaak-onbestraft-zijn-moeilijk-te-achterhalen

2.2. Europese wet- en regelgeving

Op Europees niveau zijn de afgelopen jaren flinke stappen gezet door onder meer afspraken te maken met socialemediabedrijven zoals Facebook, X (voorheen Twitter), YouTube, Instagram, TikTok en Snapchat. Hierbij gaat het bijvoorbeeld over het tegengaan van online haatzaaien. Er is een 'Code of Conduct' opgesteld waarin is vastgelegd dat platforms haatzaaiende content die via zogenoemde 'trusted flaggers' is gemeld binnen 24 uur evalueren en indien nodig verwijderen. In de gedragscode zijn verder de volgende verzoeken aan sociale mediabedrijven opgenomen, zo somt het Kennisplatform Inclusief Samenleven (KIS) op in een eind vorig jaar uitgebracht rapport over de aanpak van online discriminatie:

- Het hebben van regels en normen die het aanzetten tot haatspraak verbieden en systemen en teams hebben om haatzaaiende content te evalueren en te melden
- Content die als haatzaaiend wordt aangegeven binnen 24 uur te evalueren en indien gegrond te verwijderen.
- Regelmatig trainingen te geven aan hun personeel met betrekking tot online haatzaaien.
- Het aangaan van samenwerkingen en opleidingsactiviteiten met het maatschappelijke middenveld om betrouwbare netwerken van verslaggevers te vergroten.
- Contactpunten vanuit de nationale autoriteiten aanwijzen om informatie ter kennisgeving te ontvangen.
- Bevorderen van transparantie zowel naar gebruikers als naar het grote publiek toe. [31]

Nieuwe wetgeving: Digital Services Act

De grootste verandering die op het gebied van wet- en regelgeving op komst is in het online domein, is de Digital Services Act (DSA). Deze nieuwe Europese wet is erop gericht om een veiligere online omgeving voor gebruikers te creëren waar hun fundamentele rechten beter zijn beschermd. De wet is verbonden aan de Digital Market Act (DMA), die erop toeziet dat er in het digitale domein meer sprake is van een gelijk speelveld met eerlijke concurrentie en ruimte voor innovatie. Voor het tegengaan van online kwetsend gedrag is vooral de DSA van belang.

In de DSA zijn onder meer de volgende verplichtingen opgenomen die relevant zijn voor de bestrijding van online kwetsend gedrag:

1 Het verwijderen van informatie of gebruikersaccounts moeten digitale aanbieders gaan onderbouwen en uitleggen. Gebruikers kunnen verwijdering aanvechten.

2 Een verbod op ingebouwde 'paden' die bezoekers naar illegale content of desinformatie leiden.

[31] https://www.kis.nl/sites/default/files/2022-12/Online-Discriminatie-Rapport.pdf

3 Voor bijzondere omstandigheden, zoals de oorlog in Oekraïne of de coronacrisis, heeft de Europese Commissie een noodprocedure opgesteld waarbij aanvullende maatregelen van techbedrijven geëist kunnen worden. Zij worden dan verplicht om tijdelijk hun algoritmesaan te passen om de verspreiding van desinformatie (of specifieke oorlogspropaganda) tegen te houden.

4 De grootste online platforms – de sites met meer dan 45 miljoen actieve Europese gebruikers per maand, dit zijn vooral de bekende platforms als Facebook, Instagram, YouTube en TikTok – worden het strengst gereguleerd. Hiervoor gelden extra verplichtingen zoals verplichte onafhankelijke audits. Onder de extra verplichtingen valt ook een risicobeoordelingsexercitie waarbij het platform moet kijken naar in hoeverre gebruikers worden blootgesteld aan illegale goederen of content. Ook moeten zij openbaar maken hoeveel personeel zij inzetten om schadelijke content op te sporen en te verwijderen.

5 Maatschappelijke (zelf)organisaties (de ngo's) kunnen een 'trusted flagger' worden. Dit houdt in dat de meldingen van illegale content met prioriteit door socialemediabedrijven worden behandeld. De organisaties kunnen die status aanvragen bij de nieuwe nationale 'digitaledienstencoördinatoren'.[32]

De Europese Commissie houdt toezicht op de naleving van de DSA door de grootste online platforms en zoekmachines. Via een heffing betalen deze bedrijven zelf voor dit toezicht. Wanneer de bedrijven niet aan de verplichtingen uit de DSA voldoen, riskeren zij hoge geldboetes tot maximaal zes procent van de wereldwijde jaaromzet.

De nieuwe Europese wet treedt stapsgewijs in werking. Vanaf 25 augustus is de DSA actief voor een select aantal zeer grote onlineplatforms en zoekmachines. Het gaat hierbij om platforms met meer dan 45 miljoen dagelijkse gebruikers in de EU, waaronder de Apple App Store, Meta's Facebook en Instagram, en Microsofts LinkedIn en Bing. De overige veertien platforms die met onmiddellijke ingang onder de DSA vallen, zijn Alphabets Google Maps, Play, Search, Shopping, YouTube, AliExpress, Amazon Marketplace, Booking.com, Pinterest, Snapchat, TikTok, X, Wikipedia en Zalando. Op 1 januari 2024 wordt de wet actief voor andere platforms, en op 17 februari 2024 voor alle online dienstverleners.[33]

[32] https://www.kis.nl/sites/default/files/2022-12/Online-Discriminatie-Rapport.pdf
[33] https://tweakers.net/nieuws/212948/digital-services-act-geldt-vanaf-vrijdag-voor-eerste-grote-onlineplatforms.html

Diverse partijen zijn enthousiast over de DSA, waaronder Amnesty International. “Concluderend kan worden gesteld dat de DSA een mijlpaal is in de wetgeving om onze rechten in het digitale tijdperk te versterken. Hoewel de reikwijdte ervan beperkt is tot de Europese Unie, wordt verwacht dat het rimpeleffecten zal veroorzaken die veel verder gaan dan haar grondgebied”, zo reageert de organisatie. Daarbij benadrukt Amnesty ook wat het belang van de wetgeving is: “We kunnen niet nog meer tijd verspillen en kunnen niet langer overgeleverd worden aan de genade van Big Tech en schadelijke, op surveillance gebaseerde bedrijfsmodellen. Onze rechten in de digitale wereld moeten nu worden beschermd.”

De DSA vervangt nationale wetgeving. Wel blijft nationale wetgeving leidend in het bepalen van wat illegale content is en of dit strafbaar is. Dit zorgt ervoor dat er, naast de eerder genoemde lof die de nieuwe wet krijgt, ook kanttekeningen worden geplaatst. Zo is Free Press Unlimited bezorgd dat de maatregelen niet de volledige reikwijdte van online geweld dekken, aangezien ze geen betrekking hebben op schadelijke inhoud. Dit is volgens de NGO problematisch omdat het meeste online geweld (nog) niet als illegaal is gedefinieerd in nationale wetgeving, ook al is het ontzettend schadelijk en kan het resulteren in offline aanvallen. Dit is bijvoorbeeld bij doxing het geval, dat in veel EU lidstaten nog niet in wetgeving is opgenomen.[34]

[34] https://www.freepressunlimited.org/en/current/press-freedom-digital-age-impact-digital-services-act

3

Handelings perspectief

Wanneer je slachtoffer of getuige bent van online kwetsend gedrag is het belangrijk om te weten wat je kan ondernemen om het gedrag te stoppen of – wanneer dat niet mogelijk is – er zo goed mogelijk mee om te gaan. Zoals je in het vorige hoofdstuk kon lezen, zijn verschillende vormen van online kwetsend gedrag strafbaar of is er wetgeving op komst die dit regelt. Via het initiatief Meldknop.nl[35] kom je eenvoudig in contact met de organisatie die jou verder kan helpen, ook om bijvoorbeeld aangifte te doen. Op de website zijn voor een groot aantal vormen van online kwetsend gedrag tips, adviezen en hulpbronnen te vinden. In dit hoofdstuk staan we mede op basis van dit soort tips en adviezen verder stil bij het handelingsperspectief dat je als slachtoffer of omstander hebt. We delen tips en adviezen voor zowel slachtoffers als omstanders, behandelen theoretische modellen die kunnen helpen bij het ontwerpen van gedragsinterventies en zetten organisaties op een rij waarbij je terechtkunt met vragen over online kwetsend gedrag.

3.1. Wat kun je doen als je slachtoffer bent van online kwetsend gedrag?

Zoals eerder in deze handreiking is benadrukt, komt online kwetsend gedrag voor in alle soorten en maten. Je kan dan ook op veel verschillende manieren slachtoffer worden van dit gedrag. Lang niet in alle gevallen is er sprake van een vergrijp waarvan je aangifte kan doen. Dan is het belangrijk om naar andere manieren te zoeken om je te wapenen en de situatie zo goed mogelijk op te lossen. Ook zijn er verschillende instanties waar je na online kwetsend gedrag terecht kan. Hierover staat meer informatie bij 3.3.

Hieronder zetten we voor verschillende vormen van online kwetsend gedrag op een rij wat het handelingsperspectief is om ermee om te gaan of te voorkomen.

Cyberpesten

- Veel soorten online kwetsend gedrag vertonen overeenkomsten met pestgedrag. Het Kenniscentrum Omgaan met Pesten zet in hun werkboek ‘Feel Fine Online’[36] een aantal tips op een rij die slachtoffers helpen om te gaan met grensoverschrijdend gedrag. Deze tips zijn met name gericht op kinderen en jongeren:

- Weet dat er in berichten vaak nare woorden geschreven worden die helemaal niet zijn bedoeld om jou te kwetsen. Deze kunnen zijn geschreven uit verveling of boosheid over iets anders. Als de afzender een onbekende is, is de kans dat de woorden echt voor jou zijn bedoeld kleiner. Ook kunnen woorden op zichzelf niet naar zijn, maar door de ontvanger wél zo worden geïnterpreteerd en ervaren. Bijvoorbeeld omdat diegene iets traumatisch heeft meegemaakt.
- Ga niet steeds opnieuw lezen of kijken naar wat over jouw grens is gegaan.
- Stop het contact of blokkeer de ander.
- Zet je apparaat uit, zodat je rust krijgt.
- Bewaar bewijsmateriaal.
- Kijk of je een melding kunt doen bij de beheerder van de website of de app waar de ander(en) over je grens is (zijn) gegaan.

[35] Meldknop.nl is een initiatief van Veilig Internetten en wordt ondersteund door de politie. De website wordt mede mogelijk gemaakt door: Helpwanted.nl, Pestweb, Vraaghetdepolitie.nl, Meld.Online Discriminatie en medegefinancierd door de Europese Unie.
[36] Feel Fine Online Kinderen & Jongeren – Kenniscentrum Omgaan met Pesten

- Begin opnieuw online: maak een nieuw profiel of account. Kies opnieuw met wie je dit wilt delen.
- Verwijder je eerdere account (bewaar wel bewijs als je dat nog nodig hebt). Online gepest worden is nooit jouw schuld. Je kunt ook chatten of bellen met www.pestweb.nl of www.kindertelefoon.nl.
- **Ook anderen kunnen je helpen:**

    - Praat erover met vrienden, ouders, iemand van school. Dat lucht vaak op.
    - Vraag hulp aan iemand die je vertrouwt: een leeftijdgenoot of een volwassene. Dit isgeen klikken. Als iemand online over je grens gaat, is dat moeilijk om in je eentje op te lossen.
    - Kies iemand die je kan helpen om voor jezelf op te komen en samen met jou kan praten met degene die online over je grens is gegaan.
    - Lees (samen) over online pesten, speel een spel, verzamel tips en praat erover. Zo ontdek je dat anderen dit ook meemaken. Dat kan je helpen.
    - Schrijf of teken over wat je meemaakt. Dit kun je voor jezelf houden of juist met eenander delen. Dit kan voor opluchting zorgen of troost geven.

Doxing

Dit zijn drie tips waarmee je de kans verkleint om zelf slachtoffer van doxing te worden:

Controleer regelmatig of je contact- of adresgegevens makkelijk te vinden zijn. Wees ook terughoudend met het delen van deze informatie.

Ga na wie jouw gegevens op sociale media kunnen zien. Staat je profiel op openbaar of privé? Dit kun je instellen via de privacyinstellingen.

Zorg dat je je wachtwoorden geheim houdt en op een veilige plek bewaart.[37]

[37] https://www.mediawijsheid.nl/veelgestelde-vraag/wat-is-doxing/

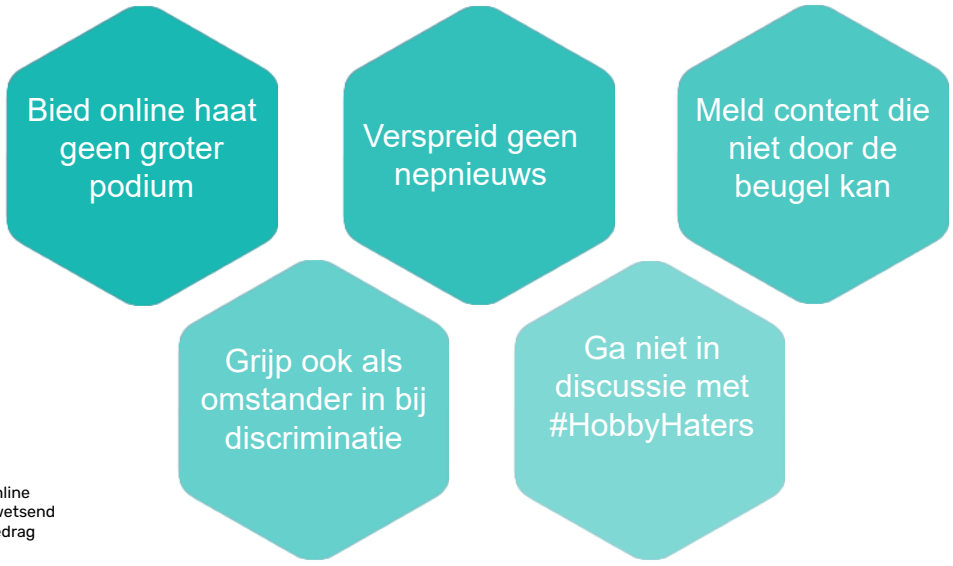
Helpwanted.nl, een organisatie die hulp biedt bij online kwetsend gedrag, geeft ook tips voor wat je kan doen als iemand jouw privégegevens online deelt:

- Praat erover: Blijf niet alleen met je zorgen rondlopen, maar neem iemand in vertrouwen. Samen zoeken jullie naar een oplossing. Anderen begrijpen jouw vervelende situatie dan ook beter.
- Rapporteer en blokkeer: Verzamel bewijs van de doxing-aanval. Meld de doxing-aanval aan de platforms waarop je persoonlijke informatie is geplaatst. Blokkeer degene die jouw gegevens online heeft gezet via sociale media.
- Zoek jezelf op: Stel Google Alerts in op jouw volledige naam, telefoonnummer, woonadres of andere privégegevens. Zo krijg je een melding wanneer deze worden gebruikt op het internet.
- Laat het verwijderen: Laat je persoonlijke informatie verwijderen van de sociale-media- platforms waar ze op staan. Of stuur een verwijderverzoek naar de beheerder van de website waarop het staat.
- Bescherm je financiën: Meld het direct aan je bank als doxers je bankrekening- of creditcardnummers online hebben gedeeld. Wijzig direct ook je wachtwoorden voor je online bank- en creditcardrekeningen.
- Pas je privacy-instellingen aan: Pas je privacy-instellingen aan en scherm al jouw sociale-media-accounts af.
- Overweeg een melding of aangifte: Je kunt melding of aangifte doen bij de politie. Doe dit als de doxer jou (ook) bedreigt, oplicht of online lastigvalt. Hierbij is het belangrijk om eerst zo veel mogelijk informatie voor de politie te verzamelen. [38]

Online haat

Onder online haat vallen diverse vormen van online kwetsend gedrag. Er zijn dan ook verschillende bronnen met tips om online haat tegen te gaan of ermee om te gaan. Op Mediawijsheid.nl wordt dieper ingegaan op dreigtweets en haatberichten en wat je hier tegen kan doen.

Dare to be Grey, een beweging tegen polarisatie, geeft de volgende tips om online haat tegen te gaan:



[38] https://www.helpwanted.nl/onderwerpen/doxing

Op de website Eerste hulp bij online haat, een initiatief van DeGoedeZaak, staat een stappenplan om erachter te komen hoe serieus een online haataanval is, hoe je het beste jezelf kan beschermen en wat voor actie je kan onernemen.

PEN America, een Amerikaanse non-profitorganisatie die zich richt op het beschermen van de vrijheid van schrijvers, geeft meerdere tips over hoe op online haat, en dan met name online intimidatie, kan reageren. Hierbij komen de volgende adviezen aan bod:

- Documenteren, onder meer door het maken van screenshots en het bewaren van berichten
- Blokkeren, muten en beperken, en de mogelijkheden die verschillende platforms hiertoe bieden
- Rapporteren aan platforms, en wat hierbij per platform de mogelijkheden zijn

In dit artikel geeft Atria, het Kennisinstituut voor Emancipatie en Vrouwengeschiedenis, diverse tips om om te gaan met online haat tegen politici.

Grooming

De politie heeft de volgende tips om je online veiligheid te vergroten en grooming tegen te gaan:

- Bedenk vooraf goed wat jouw grenzen zijn. Wat laat je wel en niet toe op internet? En wat laat je wel en niet zien van jezelf? Dat geldt trouwens niet alleen voor contact met vreemden. Ook bekenden kunnen je dingen vragen die je misschien liever niet wilt
- Accepteer niet zomaar vriendenverzoeken van vreemden.
- Voel je niet verplicht om contact te houden met een onbekende.
- Luister naar je gevoel: als je het niet vertrouwt, doe het dan niet.
- Twijfel je over iets? Praat er eens over met vrienden of je ouders/verzorgers.[39]

Shame sexting

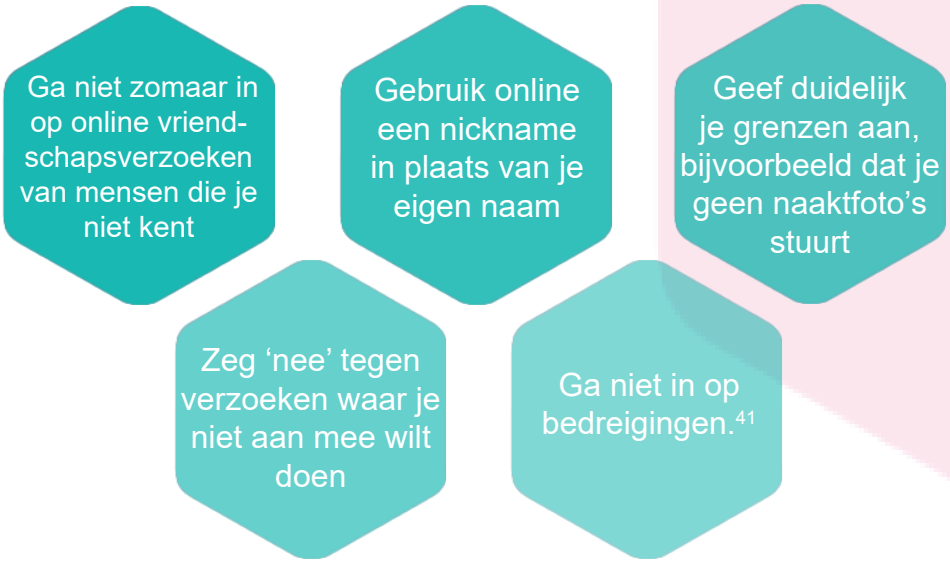
De politie adviseert om snel iemand in vertrouwen te nemen als je met shame sexting te maken hebt. Dit kan een vriend of vriendin zijn, je ouders, een mentor of een organisatie als Helpwanted.nl of de politie zelf. Samen kan je vervolgens kijken welke stappen te ondernemen. Als je aangifte wilt doen, is het verstandig om het verwijderen van de foto in overleg met de politie te doen. Wanneer het materiaal al verwijderd is voordat je aangifte hebt gedaan, is namelijk ook een belangrijk deel van het bewijsmateriaal verdwenen. Wanneer je bewijsmateriaal verzamelt, doe dat dan zoveel mogelijk vanaf een computer of laptop. Bij screenshots vanuit een app ontbreekt de URL vaak en die is van cruciaal belang, omdat deze uniek is. [40]

En in dit artikel deelt het televisieprogramma Pointer vijf tips om slachtoffers van shame sexting te helpen.

[39] https://www.vraaghetdepolitie.nl/dwang-en-seks/misbruik/hoe-voorkom-ik-grooming.html
[40] https://www.vraaghetdepolitie.nl/dwang-en-seks/naaktfotos-en-filmpjes/wat-kan-ik-doen-als-mijn-naaktfoto-verspreid-is.html

Sextortion

Slachtofferhulp Nederland geeft verschillende adviezen om de kans te verkleinen dat je te maken krijgt met sextortion:



Ook Helpwanted.nl geeft informatie over wat te doen bij sextortion.

Wraakporno

Op de website Meldknop.nl staan diverse tips rond wraakporno:

- Als je weet wie de beelden online heeft gezet, benader hem of haar en verzoek de beelden offline te halen.
- Praat erover met je vrienden, ouders, leraar of vertrouwenspersoon.
- Verzamel zoveel mogelijk bewijs. Dit kan helpen wanneer je nu of later naar de politie gaat.Staat er ook iets vervelends van je online? Maak ook daar screenshots van en zorg ervoor dat de URL ook in beeld is.
- Zoek jezelf op internet via zoekmachines. Mocht hij of zij de foto of video online zetten, neem dan zo snel mogelijk contact op met die website. Vaak vind je onderaan een site een link naar 'help', 'abuse' of 'contact'. Leg in je mail uit dat je erop te zien bent en voor de plaatsing ervan geen toestemming hebt gegeven.

Ook is het mogelijk om bij Helpwanted.nl melding te doen van wraakporno. Een medewerker kijkt dan mee om te bepalen hoe de beelden offline kunnen worden gehaald. Ook is het mogelijk om aangifte te doen bij de politie.

[41] https://www.slachtofferhulp.nl/gebeurtenissen/seksueel-misbruik-geweld/sextortion/

3.2. Wat kun je als omstander doen wanneer je online kwetsend gedrag bij anderen ziet?

Om online kwetsend gedrag een halt toe te roepen is het ingrijpen van omstanders heel belangrijk. Met omstanders bedoelen we individuen die getuige zijn van kwetsend gedrag, maar niet direct als zender of ontvanger bij het voorval betrokken zijn. Het slachtoffer krijgt hierdoor steun en zeker als meerdere omstanders ingrijpen, bevestigt dit de sociale norm van wat wel en niet acceptabel gedrag is. Toch blijkt in de praktijk dat mensen vaak wel willen ingrijpen, maar niet goed weten hoe ze dit moeten doen. Dit heeft extra negatieve gevolgen voor het slachtoffer: doordat omstanders passief blijven, lijkt het alsof ze het gedrag van de zender stilzwijgend goedkeuren.

Media-empowerment model

Tijdens de Week van de Mediawijsheid 2022 is uitgebreid onderzoek[42] gedaan naar het stimuleren van online prosociaal omstandergedrag. Een van de conclusies is dat het momenteel 'vrij onwaarschijnlijk' is dat omstanders in actie komen tegen zaken als online shaming en cancelen, ongeacht tot welke generatie zij behoren. Ook concluderen de opstellers van het rapport dat het ingrijpen van omstanders meestal uit persoonlijke steun bestaat en zelden door een melding te maken bij de politie of een meldpunt.

Om het online ingrijpen van omstanders – in dit onderzoek ook wel 'upstandergedrag' genoemd – te kunnen voorspellen, maakt het rapport gebruik van het Media-empowerment model. Dit model is gebaseerd op wetenschappelijke theorieën op het gebied van mediawijsheid, gedragsverandering en zelfregulatie. Het geeft inzicht in de factoren die bepalen of mensen in actie komen tegen online kwetsend gedrag. De belangrijkste factoren hierbij zijn **1.** Kennis; **2.** Vaardigheden; **3.** Motivatie; en **4.** Gelegenheid. Een omstander grijpt volgens dit model waarschijnlijk pas in als diege de kennis en vaardigheden heeft die nodig zijn om dat gedrag te vertonen, gemotiveerd is om het gedrag te vertonen en de gelegenheid heeft om het gedrag te vertonen.

Tijdens het onderzoek is het Media-empowerment model in de praktijk getoetst. Hieruit blijkt dat met name automatische motivatie en sociale gelegenheid de belangrijkste factoren zijn die upstandergedrag voorspellen. Dat betekent dat voor alle generaties de kans dat ze in actie komen groter is wanneer het een gewoonte voor hen is én het hen een goed gevoel geeft om dat te doen én wanneer zij het gevoel hebben dat hun sociale omgeving hen aanmoedigt om dat te doen. Kennis en vaardigheden lijken volgens het onderzoek een minder grote rol te spelen in het voorspellen van upstandergedrag.

[42] https://netwerkmediawijsheid.nl/wp-content/uploads/2022/11/Onderzoeksrapportage-Netwerk-Mediawijsheid-2022.pdf

Bystander Intervention Model

Het uit de psychologie afkomstige Bystander Intervention Model[43] is ook zeer relevant om te benoemen. De verschillende stappen uit dit model laten zien wat omstanders nodig hebben om adequaat in te kunnen grijpen wanneer zij getuige zijn van grensoverschrijdend gedrag online. Dit zijn de vijf stappen: **1.** Grensoverschrijdend gedrag herkennen; **2.** De ernst van de situatie inzien; **3.** Verantwoordelijkheid nemen; **4.** Weten hoe in te grijpen; en **5.** Beslissen om in te grijpen. Een interventie gericht op het toerusten van omstanders, neemt al deze stappen idealiter mee.

Tips en adviezen

In een recent artikel[44] zetten adviseurs van Movisie een aantal tips op een rij over wat je als omstander kan doen:

1. **De zender aanspreken op positieve normen en waarden en eigenschappen.** Ook mensen die openlijk discrimineren, hebben vaak normen en waarden die ervan uitgaan dat jeanderen gelijk en respectvol moet behandelen. Het is raadzaam om deze normen en waarden 'te activeren' bij de zender. Een voorbeeld is: 'Ik ben verbaasd dat je dat zegt/doet, aangezien ik dacht dat jij gelijkwaardigheid belangrijk vindt.' Of: 'Je zegt nu dit maar eigenlijk ken ik jou zo niet. Sta je nog steeds achter je opmerking?'.

2. **Geef ruimte aan de gevoelens van het slachtoffer.** Zenders staan namelijk vaak niet stil bij wat hun gedrag veroorzaakt bij slachtoffers. Vooral online blijven de gevolgen van racisme en discriminatie onzichtbaar voor zenders doordat ze geen fysieke reactie zien bij het slachtoffer. Ook kan het helpen om aan de zender te vragen om zich in te leven in het slachtoffer. Bijvoorbeeld door te vragen: 'Kan je je voorstellen dat je je misschien minder fijn op het werk voelt, als je met regelmaat dit soort opmerkingen over je afkomst hoort?'

3. **Geef ruimte aan de gevoelens van het slachtoffer.** Omdat mensen eerder iemand zullen helpen die op hem of haar lijkt, kan het helpen om de zender aan te spreken op diens groepsidentiteit. Bijvoorbeeld als beide bij hetzelfde bedrijf werken, of als beide voetbalfans of buurtbewoners zijn. Als je wat deelt met elkaar, is het makkelijker om elkaar aan te spreken:'Zo willen we hier toch niet met elkaar omgaan?' Als iemand een professionele rol heeft, kun je hem of haar daar ook op aanspreken. Bijvoorbeeld: 'Jij hebt hier een voorbeeldrol als **professional.** Daarom vind ik het juist belangrijk dat jij je realiseert dat dit soort opmerkingen niet door de beugel kunnen.'

[43] https://www.movisie.nl/sites/movisie.nl/files/2021-06/Omstanders-activeren-stappenplan.pdf
[44] https://www.movisie.nl/artikel/ingrijpen-omstander-discriminatie-heeft-echt-zin

Helpwanted, een initiatief van Offlimits, het Expertisecentrum Online Misbruik[45] , geeft ook adviezen over wat je als omstander kan doen:

1. **Zoek andere omstanders die willen ingrijpen.** Er is moed en lef nodig om je uit te spreken tegen online grensoverschrijdend gedrag. Het helpt om eerst steun te zoeken bij andere upstanders, of vrienden, klasgenoten, familie, een collega of docent. Dan kun je samen bedenken hoe je het beste kunt opkomen voor het slachtoffer. Bied steun en luister

2. **Steun de persoon die grensoverschrijdend gedrag meemaakt door diegene een privébericht te sturen.** Vraag daarin hoe het gaat en luister. Zeg ook dat het niet de schuld is van diegene. Dat het meer mensen overkomt, en dat diegene zich niet hoeft te schamen. Zeg liever niet: 'Het komt wel goed' of: 'Het is niet zo erg', want daarmee erken je de gevoelens van de ander niet. Je kunt ook vragen hoe je kunt helpen. Soms weet iemand zelf nog niet dat er een foto/video online staat. Het kan lastig zijn om dit te vertellen. Maar hoe eerder iemand het weet, hoe sneller diegene actie kan ondernemen.

3. **Stop victim blaming.** Let erop dat je niet (onbedoeld) aan victim blaming doet. Dat is dat je de schuld van wat er gebeurd is bij het slachtoffer legt. Wat zeg je wél tegen iemand die iets naars heeft meegemaakt? • 'Ik geloof je' • 'Dit had die persoon jou nooit mogen aandoen' • 'Jij hebt niets verkeerd gedaan' • 'Of je aan sexting doet is jouw keuze, niemand mag daar misbruik van maken' • 'Wat naar dat je dit meemaakt, en dat je zo hard oordeelt over jezelf' • 'Wat jij nu voelt is normaal' • 'Het voelt nu misschien alsof je geen kant uit kunt, maar er zijn stappen die je kunt zetten'.

4. **Spreek je uit in het openbaar.** Bijvoorbeeld via een reactie onder een bericht. Doe dit ook wanneer je iets krijgt doorgestuurd, of als je een naar bericht leest in een groepsapp. Let erop dat je je op een respectvolle manier uit. Zeg bijvoorbeeld alleen: 'Dit is **niet oké'.** Ongevraagd (naakt)foto's/video's van iemand delen is strafbaar. Daar kun je iemand op wijzen**.**

[45] https://offlimits.nl/

5. **Stuur niets door en verwijder het.** Als jij een foto/video van iemand krijgt doorgestuurd, stuur deze dan zelf niet door. Ook een vervelend bericht over iemand anders stopt bij jou! Verwijder de foto/video of het bericht van je telefoon, tablet of computer. Vraag anderen dit ook te doen. Deel de nare berichten niet en doe niet mee met uitlachen, pesten en shamen.

6. **Meld en rapporteer.** Meld het online grensoverschrijdend gedrag bij het platform waarop het plaatsvindt. Rapporteer de persoon en/of het account dat zich hier schuldig aan maakt. Hoe meer mensen grensoverschrijdend gedrag melden en rapporteren, hoe groter de kans dat er iets tegen gedaan wordt. Meld het ook wanneer je ziet dat er online wordt gediscrimineerd. Dit kan bij Meld.Online Discriminatie. Meld foto's/video's van seksueel misbruik van minderjarigen bij het Meldpunt Kinderporno.

Of je nu getuige bent van online kwetsend gedrag of niet, het is natuurlijk altijd goed om zelf online het juiste voorbeeld te geven. Goed gedrag, zoals iets aardigs doen voor een ander of iemand troosten die ontvanger is van online kwetsend gedrag, werkt aanstekelijk. Dit geldt ook voor het bieden van online hulp en steun door omstanders. In het tegengaan van online kwetsend gedrag zijn rolmodellen als leraren, ouders of influencers daarom belangrijk. Wees je daarom bewust van je rol als voorbeeld én potentiële omstander en de impact die je online met je gedrag kan hebben.

3.3 Welke instanties kun je inschakelen als je slachtoffer bent van online kwetsend gedrag of meer informatie of advies wil?

Er zijn in Nederland tal van organisaties die zich bezighouden met verschillende soorten online kwetsend gedrag en waarvan je de websites en andere kanalen kan raadplegen om meer informatie over het onderwerp te vinden. Hieronder vind je een (niet uitputtende) lijst van deze organisaties en initiatieven:

113 | Zelfmoordpreventie, mogelijkheid om te bellen of chatten met hulpverleners
De Kindertelefoon | Bellen, chatten en een forum voor kinderen, informatie voor volwassenen en leerkrachten
Helpwanted | Hulp bij online kwetsend gedrag, met onder meer een chat voor eerste hulp
Slachtofferhulp | Hulp en advies voor slachtoffers van uiteenlopende gebeurtenissen
Fraudehelpdesk | Hulp bij fraude, zoals online oplichting of gegevensdiefstal
Fier | Expertisecentrum op het terrein van geweld in afhankelijkheidsrelaties
Centrum Seksueel Geweld (CSG) | Hulp voor slachtoffers van seksueel geweld

The Safe Space Club | Ervaringsdeskundigen bieden hulp aan slachtoffers van seksueel geweld
Meld.Online Discriminatie | Meldpunt ter bestrijding van online discriminatie
MIND Korrelatie | Anoniem advies voor mensen met psychische klachten en hun omgeving
Pestweb | Informatie en advies over pesten op school, onderdeel van de Stichting School en Veiligheid
Veilig Internetten | Tips, tricks en praktische uitleg over veilig internetten
Meldknop | Een door de politie ondersteund initiatief van Veilig Internetten voor het melden van onder meer pesten en oplichting
Het Juridisch loket | Eerste hulp bij juridische vragen
Stichting School & Veiligheid | Stichting die werkt aan sociale veiligheid op scholen
Vraag het de politie | Op jongeren gericht informatieportal over veiligheid, met ook aandacht voor pesten en online

Bijlagen

1. Begrippenlijst Rathenau Instituut

In het rapport 'Online ontspoord. Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland' (2021)[46] geeft het Rathenau Instituut een handige (maar niet volledige) begrippenlijst, waar veel vormen van online kwetsend gedrag voorbijkomen:

Cancelen: online shaming waarbij wordt opgeroepen om iemand uit te sluiten uit diens community bij wijze van sociale straf.

Catfishing: het opzettelijk misleiden van anderen door delen van je eigen identiteit te verbergen of te veranderen, meestal in de context van online dating en soms zonder de intentie om iemand ooit in het echt te ontmoeten.

Complotdenken: de overtuiging dat bepaalde gebeurtenissen of situaties geen toeval zijn, maar in het geheim zijn gemanipuleerd door machtige groepen met verkeerde bedoelingen.

Cyberverslaving: excessieve en ongecontroleerde online activiteit met langdurig gebruik van internet in het algemeen en sociale media, gaming en pornosites in het bijzonder.

Cyberchondrie: excessief of herhaaldelijk zoeken naar informatie over gezondheid leidend tot onnodige paniek of zorgen over de gezondheid.

Cryptofraude: oplichting waarbij mensen worden aangemoedigd cryptomunten te (ver) kopen, soms in de vorm van een piramidespel, bijvoorbeeld om de beurswaarde van cryptomunten te manipuleren.

Cyberbullying: herhaaldelijk online pesten door een groep of individu van een slachtoffer dat zichniet gemakkelijk kan verdedigen.

Challenges: het aanmoedigen van mensen om bepaalde (gevaarlijke) opdrachten uit te voeren en vervolgens online te delen.

Desinformatie: het verspreiden van informatie die 'onjuist' of 'misleidend' is met de intentie om kwaadwillend te handelen of schade te berokkenen.

Digitaal vigilantisme: een vorm van collectieve actie, morele afkeuring of terechtwijzing (bijvoorbeeld via online shaming, intimidatie of doxing) gericht aan personen die ongewenst sociaal gedrag vertonen.

Doxing: het openbaar maken van iemands persoonlijke, sensitieve en privéinformatie zoals adres, telefoonnummer, paspoort, werkgever, gegevens van familie en foto's van iemands kinderen.

Extreme pranks: een vorm van vernedering en voor de gek houden (plagerige grap) die plaatsvindt tussen dader, slachtoffer en omstanders. Online nemen pranks vaak de vorm aan van gefilmde "offline" pranks, waarbij de reactie van slachtoffers (verwarring, verbijstering, ongemak of schaamte) breed wordt uitgemeten.

Griefing: doelbewust irriteren van andere spelers in online games door bepaalde spelelementen zo te manipuleren dat andere spelers daar last van hebben.

Grooming: een proces waarbij een volwassene een relatie van seksueel misbruik ontwikkelt door middel van technologie, zoals op sociale media. In dit verband wordt ook gesproken van 'digitale kinderlokkerij'.

Haatzaaien: alle uitingsvormen die zorgen voor de verspreiding, aanstichting, aanmoediging of legitimering van raciale haat, xenofobie, antisemitisme of andere vormen van haat gebaseerd op intolerantie.

Hacking: alle soorten activiteiten rondom het ongeautoriseerd toegang (proberen te) verkrijgen tot computersystemen.

Kwakzalverij: onbevoegd uitoefenen van de geneeskunst door iemand die beweert ziekten te kunnen genezen met een nutteloos of zelfs schadelijk geneesmiddel.

Pedojagen: vorm van digitaal vigilantisme waarbij burgers zich voordoen als kind om pedofielen 'in de val' te lokken en ze vervolgens zelf te straffen of ze aan te geven bij de politie.

Phishing: manier om via het internet allerlei soorten informatie te ontfutselen over personen, bijvoorbeeld via valse e-mails of websites.

Pro-ana coach: persoon die jonge meisjes met een eetstoornis aanmoedigt om verder af te vallen, veelal met als doel seksueel expliciet materiaal van (minderjarige) meisjes te bemachtigen.

Sexting: verspreiden of delen van seksueel getinte berichten, foto's of video's van zichzelf via mobiele telefoons of andere media.

Sextortion: een vorm van afpersing waarbij een dader dreigt om zonder toestemming seksueel beeldmateriaal te openbaren van een slachtoffer om deze te dwingen om meer van dit soort foto's te sturen, geld te betalen of om (seksueel getinte) opdrachten uit te voeren.

Shaming: vorm van digitaal vigilantisme waarbij publieke morele kritiek online wordt geuit als reactie op het overschrijden van sociale normen.

Shame sexting: het zonder toestemming maken en/of verspreiden van seksueel getinte beelden of video's.

Stalking: het herhaaldelijk intimideren, lastigvallen en soms bedreigen van slachtoffers.

Sock puppet: een valse identiteit (sokpop) die wordt aangenomen om anderen te misleiden. Een sock puppet kan op sociale media bijvoorbeeld worden ingezet voor catfishing of trolling.

Trolling: het opzettelijk dwars zitten van mensen in online gemeenschappen met gedrag dat niet als acceptabel wordt gezien, zoals mensen uitschelden, ruzie zoeken of zich negatief uitlaten over anderen. Daarnaast bestaat tegenwoordig ook een bredere interpretatie van het begrip trolling, namelijk het gebruik van nepaccounts om desinformatie te verspreiden en het publieke debat te beïnvloeden.

Wraakporno: zonder toestemming bezitten, openbaar maken en verspreiden van (gestolen) seksueel beeldmateriaal door bijvoorbeeld hackers, (ex)partners, kindermisbruikers, verkrachters en mensenhandelaren.

Verstoord eetgedrag (eetstoornissen): psychische stoornissen die worden gekenmerkt door verstoord eetgedrag en/of inadequaat compensatiegedrag (braken, laxeren). Mensen met een eetstoornis hebben een verstoord lichaamsbeeld, zijn veel bezig met hun gewicht of lichaamsvorm en zijn erg bang om aan te komen.

2. Overige vormen van online kwetsend gedrag

Naast de vormen van online kwetsend gedrag uit de begrippenlijst van het Rathenau Instituut kennen we ook nog onderstaande soorten:

DDos-aanval: met een (Distributed) Denial-of-Service-aanval (DDoS-aanval) wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur aangevallen. Het resultaat van deze aanval is dat diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten. Dit kan leiden tot grote (imago)schade. Het vormt een reële dreiging voor alle organisaties met onlinedienstverlening, zoals websites, waarvan de continuïteit van belang is.[47]

Deepfakes: een verzamelnaam voor software waarmee je nepvideo's kunt maken die bijna niet van echt te onderscheiden zijn. Met deze software kun je iemand dingen laten zeggen of doen die hij of zij in werkelijkheid nooit gezegd of gedaan heeft. Deepfake is een vorm van wat we synthetische media noemen: media die zijn gemaakt of bewerkt met behulp van een kunstmatige intelligentie. [48]

Flaming: Het bewust plaatsen van kwetsende of beledigende berichten, veelal op forums, social media platforms of via direct messages. Hate raids: hierbij bezoeken grote groepen mensen livestreams en zetten ze massaal ongewenste berichten in de chat. [49]

Swatting: een levensgevaarlijke grap die vaak wordt uitgehaald door gamers, hackers of andere kwaadwillenden. Ze zoeken hun slachtoffer uit en doen vervolgens een noodoproep bij de hulpdiensten. De politie of andere handhavingsinstanties worden bewust op het verkeerde been gezet, met als doel te reageren op een vals dreigement op de locatie van het doelwit.[50]

Netwerk Mediawijsheid

Online kwetsend gedrag