STOP ONLINE GRENSOVER-SCHRIJDEND GEDRAG

EEN VEILIGE WERKVLOER VOOR IEDEREEN

Januari 2025

INHOUDSOPGAVE

INLEIDING

In de moderne digitale werkomgeving is de manier van communicatie en interactie tussen werknemers drastisch veranderd. Dit is mede door het coronavirus versneld. Terwijl technologieën de efficiëntie en flexibiliteit op de werkvloer hebben vergroot, hebben ze ook nieuwe uitdagingen en psychosociale risico's met zich meegebracht. Een van deze risico's is de toename van online grensoverschrijdend gedrag, ook wel cybergeweld genoemd.[1]
Online grensoverschrijdend gedrag lijkt laagdrempeliger dan offline grensoverschrijdend gedrag.

Online grensoverschrijdend gedrag op de werkvloer omvat verschillende vormen van ongewenst, schadelijk, intimiderend of beledigend gedrag dat via digitale kanalen plaatsvindt. Dit kan variëren van cyberpesten, cyberstalking, online intimidatie en andere vormen van digitale agressie. In tegenstelling tot offline, kan online grensoverschrijdend gedrag vaak onzichtbaar blijven voor anderen. Dit maakt het moeilijker om incidenten te detecteren en aan te pakken.[2]

Onderzoek van de European Trade Union Confederation laat zien dat er geen gegevens zijn die de blootstelling van werknemers aan cybergeweld op de werkplek meten. De meerderheid van de geïnterviewde vakbonden hebben bevestigd dat cybergeweld wordt gezien als een toenemend probleem, vooral onder vrouwen, op de werkvloer. Tegelijkertijd verklaarden ze dat hun vakbond momenteel geen cybergeweld aanpakt, voornamelijk vanwege het gebrek aan kennis, bewustzijn en expertise over hoe dit probleem op de werkplek moet worden aangepakt. We mogen het belang van het probleem echter niet onderschatten. Online grensoverschrijdend gedrag heeft het potentieel om een belangrijke vorm van geweld en intimidatie op de werkplek te worden. Daarom heeft de FNV onderzoek gedaan naar deze vorm van grensoverschrijdend gedrag.

[1] P. Baranska, S. Picard, & European Trade Union Confederation (ETUC). 'Safe at work, safe at home, safe online: Tackling gender-based violence and harassment in a changing world of work, januari 2024. https://www.etuc.org/sites/default/files/publication/file/2024-10/Report%20-%20EN%20-%20151024%20-%20WEB.pdf

[2] P. Baranska, S. Picard, & European Trade Union Confederation (ETUC). 'Safe at work, safe at home, safe online: Tackling gender-based violence and harassment in a changing world of work, januari 2024. https://www.etuc.org/sites/default/files/publication/file/2024-10/Report%20-%20EN%20-%20151024%20-%20WEB.pdf

SAMENVATTING

De online werkvloer is verre van veilig. Dat is de conclusie uit het **rapport 'horen zien en zwijgen'** dat de FNV in oktober 2023 publiceerde. Dit onderzoek laat zien in hoeverre er online grensoverschrijdend gedrag op de werkvloer is en wat er tegen te doen is. Er is gekeken naar de frequentie en de verschillende vormen van online grensoverschrijdend gedrag. Uit de resultaten blijkt dat online seksuele intimidatie vaak voorkomt, vooral bij vrouwen, die dit acht keer vaker meemaken dan mannen. Mannen ervaren juist vaker online intimidatie en cyberpesten. Cyberstalking treft vrouwen weer meer, terwijl doxing vaker voorkomt bij mannen.

Online grensoverschrijdend gedrag heeft grote negatieve invloed op werknemers. Maar liefst 95% van de respondenten die dit hebben ervaren, rapporteert negatieve gevolgen. Dat is vooral stress of angst: 22%. De impact op de loopbaan en financiële zekerheid van slachtoffers is groot.

De oorzaak ligt vaak in machtsdynamieken en een gebrek aan sancties en toezicht binnen organisaties. Dat creëert een cultuur waarin grensoverschrijdend gedrag kan blijven bestaan. Veel medewerkers melden incidenten niet uit wantrouwen tegenover HR of het management. Van de meldingen die wél worden gedaan, wordt een groot deel onbeantwoord gelaten, wat het vertrouwen in de aanpak ondermijnt en het probleem normaliseert.

Daarnaast ontbreekt vaak beleid rond online grensoverschrijdend gedrag, en waar dit wel bestaat, is het vaak slecht gecommuniceerd. Bijna 60% van de respondenten vindt de maatregelen van hun werkgever tegen online grensoverschrijdend gedrag onvoldoende. Er is een duidelijke noodzaak voor werkgevers om zichtbare en transparante stappen te nemen, zodat werknemers zich veilig voelen op de online werkvloer.

Deze uitkomsten laten zien dat er echt nog stappen moeten worden gezet. Online grensoverschrijdend gedrag wordt nu nog te vaak vergeten in de discussie over grensoverschrijdend gedrag, met grote gevolgen voor de samenleving en het individu. Samen moeten we ervoor zorgen dat ook de online werkvloer een veilige plek wordt.

VERANTWOORDING

De enquête, die tussen 10 september en 29 oktober 2024 is uitgevoerd, had als doel inzicht te krijgen in de aard en omvang van online grensoverschrijdend gedrag op de werkvloer in Nederland. Het onderzoek is verspreid via de FNV-nieuwsbrieven, de FNV-website en via sociale media. In totaal namen 752 mensen deel, 361 respondenten hadden zelf of via anderen te maken met online grensoverschrijdend gedrag.

Van deze 361 respondenten meldden 164 zelf slachtoffer te zijn geweest, terwijl 102 alleen incidenten hadden gezien of gehoord bij collega's. Nog eens 95 respondenten gaven aan dat zowel zijzelf als een of meer collega's ermee te maken hadden.

1. WAT IS ONLINE GRENSOVERSCHRIJDEND GEDRAG?

Grensoverschrijdend gedrag is een verzamelterm voor alle vormen van gedrag waarbij iemand over de grenzen van een andere persoon gaat. Of als het gedrag de grenzen overgaat die zijn vastgelegd in de wet of binnen organisaties. Grensoverschrijdend gedrag kan verschillende vormen aannemen: pesten, intimidatie, seksuele intimidatie, discriminatie, lichamelijke agressie.[3]

Naast de vormen van grensoverschrijdend gedrag die offline kunnen voorkomen, zijn er ook een aantal vormen specifiek voor online grensoverschrijdend gedrag.

CYBERPESTEN

Wanneer pesten online gebeurt, wordt dit vaak cyberpesten genoemd. Dat is de 'opzettelijke en herhaaldelijke schade die wordt toegebracht door het gebruik van computers, mobiele telefoons en andere elektronische apparaten.'[4] Ook als het niet opzettelijk is, kan het wel pesten zijn. Ook het uitsluiten van online groepen is een vorm van grensoverschrijdend gedrag.

De drie kenmerken van cyberpesten zijn:

1. Het pesten houdt nooit op en kan op elk moment doorgaan. Foto's en video's kunnen makkelijk worden verspreid op het internet en zijn moeilijk te verwijderen, zelfs als het pesten stopt.
2. Het vindt op afstand plaats, hierdoor is de impact minder zichtbaar. Als het pesten ook op openbare platforms gebeurt, kan dit een groter publiek bereiken.
3. Het kan anoniem gebeuren via nepaccounts. Dit kan daders het gevoel kan geven dat er minder toezicht is. Sommige pesters zijn bewust anoniem, ook als ze het slachtoffer in het echte leven kennen.

ONLINE INTIMIDATIE

Intimidatie is een vorm van manipulatie. Iemand kan angst aangejaagd worden en bedreigd worden met negatieve gevolgen. Online intimidatie kan bijvoorbeeld het herhaaldelijk sturen van berichten zijn, bellen met iemands werkgever of 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.[5]

VELE MANIEREN VAN SEKSUELE INTIMIDATIE

Online seksuele intimidatie is het ontvangen van ongewenste, beledigende, seksueel getinte e-mails of sms-berichten of het meemaken van ongepaste seksuele toenaderingen via sociale media of online chatrooms.[6]

Vormen van online seksuele intimidatie zijn:

- Sexting
- Sextortion
- Wraakporno

[3] SER. 'Dossier Grensoverschrijdend Gedrag'. https://www.ser.nl/nl/thema/arbeidsomstandigheden/dossiers/grensoverschrijdend-gedrag
[4] Netwerk Mediawijsheid. 'Online kwetsend gedrag', oktober 2023.
[5] Rathenau Instituut. 'Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', 2021.
[6] Atria. 'Factsheet Online seksuele intimidatie', november 2018. https://prod-cdn.atria.nl/wp-content/uploads/sites/3/2018/11/20174731/online-seksuele-intimidatie-20181101.pdf

Sexting

Ongewenste sexting is het doorsturen van seksueel getint materiaal zonder toestemming van de afgebeelde persoon. Het ongewenst ontvangen van seksueel getint materiaal valt hier ook onder, zoals het ontvangen van dickpics.[7]
Dan is er ook shame sexting. Tussen ongewenste sexting en shame sexting bestaat een belangrijk verschil. Wanneer de seksueel getinte beelden in de verkeerde handen vallen en zonder toestemming verspreid worden, is sprake van 'shame sexting'. De beelden worden doorgestuurd uit bijvoorbeeld wraak of na een ruzie. Dit kan ernstige gevolgen hebben voor het slachtoffer. De problemen ontstaan in dat geval dus pas wanneer de beelden met de verkeerde intenties worden doorgestuurd.[8]

Sextortion

Sextortion is een vorm van afpersing waarbij de dader dreigt om zonder toestemming seksueel beeldmateriaal te openbaren, om het slachtoffer te dwingen meer van dit soort foto's te sturen, te betalen of om (seksueel getinte) opdrachten uit te voeren.[9] De afperser kan dreigen de naaktbeelden te verspreiden onder vrienden, familieleden of op het werk wanneer je niet doet wat de afperser vraagt. In veel gevallen van sextortion gaat het om geld en dit wordt ook wel 'financial sextortion' genoemd.[10]

Wraakporno

Wraakporno is het zonder toestemming bezitten, openbaar maken en 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 om doelbewust schade toebrengen aan slachtoffers door het naar buiten brengen van de beelden.
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.[11]

Deepfakes

Deepfake is de verzamelnaam voor beelden, geluiden of teksten die door kunstmatige intelligente software worden gemaakt. Vaak gaat het over nepvideo's of nepfoto's die van een persoon zijn gemaakt, waarin iemand iets zegt of doet die in werkelijkheid nooit zijn gebeurd.[12]
De meeste deepfakes zijn te vinden binnen de internetporno. Uit een rapport van Deeptrace blijkt dat 96% van alle deepfakes mensen ongewild te zien zijn in pornografisch materiaal. De gezichten van de actrices worden vervangen door gezichten van andere vrouwen die daar geen toestemming voor hebben gegeven. In dit geval spreken we ook wel van 'deep nudes'. Dit overkomt niet alleen bekende mensen, maar ook doodgewone vrouwen.[13]
Tientallen bekende Nederlanders, Tweede Kamerleden en leden van het Koninklijk Huis figureren in deepfake porno-video's die vaak tienduizenden keren zijn bekeken, blijkt uit onderzoek van het AD.[14]

Deepfakes zijn strafbaar als het gaat om:[15]

- Smaad of laster: iemand probeert je goede naam te schaden.
- Seksuele exposing: het verspreiden van seksueel getint materiaal zonder jouw toestemming.
- Kinderporno: als het slachtoffer minderjarig is.

[7] Nederlands Jeugdinstituut. 'Van Ongewenste Sexting Tot Wraakporno: Wat Is Online Seksueel Overschrijdend Gedrag?', https://www.nji.nl/seksueel-grensoverschrijdend-gedrag/van-ongewenste-sexting-tot-wraakporno-wat-is-online-seksueel-overschrijdend-gedrag
[8] Slachtofferwijzer. 'Wat Is Sextortion: Van Hulp en Aangifte Tot Voorkomen', 2024, https://slachtofferwijzer.nl/artikelen/sextortion-seksuele-afpersing-betekenis
[9] Rathenau Instituut. 'Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', 2021.
[10] Slachtofferwijzer. 'Wat Is Sextortion: Van Hulp en Aangifte Tot Voorkomen', 2024, https://slachtofferwijzer.nl/artikelen/sextortion-seksuele-afpersing-betekenis
[11] Rathenau Instituut. 'Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', 2021.
[12] Nederlands Jeugdinstituut. 'Van Ongewenste Sexting Tot Wraakporno: Wat Is Online Seksueel Overschrijdend Gedrag?', https://www.nji.nl/seksueel-grensoverschrijdend-gedrag/van-ongewenste-sexting-tot-wraakporno-wat-is-online-seksueel-overschrijdend-gedrag
[13] Slachtofferwijzer. 'Betekenis Deepfakes: Wat Zijn Het?', 2024, https://slachtofferwijzer.nl/artikelen/wat-zijn-deepfakes-gevaar
[14] AD. 'Deepfake pornovideo's schokken medialandschap: BN'ers en politici doen aangifte', 19-03-24, https://www.ad.nl/tech/deepfake-pornovideos-schokken-medialandschap-bners-en-politici-doen-aangifte~aecdc584/
[15] Slachtofferhulp Nederland. 'Deepfake', https://www.slachtofferhulp.nl/gebeurtenissen/deepfake/

Exposen

Exposen is het ongevraagd online delen van privéfoto's en -filmpjes met daarbij persoonlijke gegevens als namen en adresgegevens. Dit gebeurt meestal om een goede naam van iemand te beschadigen. Soms wordt de foto of video ook naar bijvoorbeeld de familieleden, vrienden of werkgever gestuurd.[16]
De app Telegram wordt hier veel voor gebruikt. De 'exposers' gebruiken chatgroepen waarbij mensen zich anoniem kunnen aansluiten om mensen die zich in hun ogen onzedelijk gedragen, openbaar te vernederen. Het gaat vaak over vrouwen van Turkse of Marokkaanse afkomst.[17]

DRIE VORMEN VAN ONLINE DISCRIMINATIE

Bij discriminatie is er sprake van een ongelijke behandeling: het benadelen of buitensluiten van mensen op basis van persoonlijke kenmerken. Er is sprake van discriminatie wanneer je een bepaald stereotypische gedachte hebt en deze uitspreekt of wanneer je gedrag vertoont gebaseerd op deze stereotypische gedachtes.[18]
Voor discriminatie is een wettelijk begrip vastgelegd in de Grondwet.[19] Deze is voor de werkvloer uitgewerkt in de Algemene wet gelijke behandeling. Deze wet verbiedt discriminatie op de werkvloer wegens een aantal gronden, zoals godsdienst, ras, geslacht, nationaliteit, handicap, gerichtheid of leeftijd.[20]
De drie veelvoorkomende vormen van online discriminatie zijn seksisme, racisme en homofobie.

Online seksisme

Seksisme is gedrag dat discrimineert op basis van geslacht. Online is seksisme vaak verbonden met andere vormen van online immoreel en schadelijk gedrag, zoals bedreiging, doxing of cyberpesten. Het International Center For Research On Women gebruikt de term "technologisch gefaciliteerd gender-gerelateerd geweld" voor alle vormen van cyberpesten, intimidatie en (verbaal) geweld waarbij seksisme een rol speelt. Vaak zijn vrouwen hiervan het slachtoffer.[21]

Online Racisme

Mensen die zich racistisch gedragen, kunnen online gemakkelijk hun denkbeelden delen en zich verenigen, 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 ideeën.[22] Een voorbeeld kan zijn het delen van racistisch getinte 'grapjes' in WhatsApp groepen.

Homofobie

Homofobie is een angst voor of haat tegen mensen die zich seksueel en/of romantisch tot hun eigen gender aangetrokken voelen. Een vorm van online homofobie is 'outing'. Outing is het bekendmaken van iemands genderidentiteit of seksuele oriëntatie zonder zijn of haar toestemming. De schade daarvan kan enorm zijn, bijvoorbeeld in landen waar LGBTIQ+-mensen vervolgd worden of in families waarin zij niet geaccepteerd worden.[23]

[16] Slachtofferwijzer. 'Online Seksueel Misbruik: Betekenis, Vormen en Voorbeelden', 2024, https://slachtofferwijzer.nl/artikelen/online-seksueel-misbruik-betekenis
[17] Fonds Slachtofferhulp. ' Eerste Hulp na Online Seksueel Grensoverschrijdend Gedrag', 04-2023, https://fondsslachtofferhulp.nl/files/uploads/2023/04/FSH-Interventie-EHOSGG.pdf
[18] FNV. 'Pesten, Intimidatie, Discriminatie', https://www.fnv.nl/werk-inkomen/veilig-gezond-werken/pesten-intimidatie-discriminatie#/
[19] Rijksoverheid. 'Non-discriminatiegronden Grondwet uitgebreid met handicap en seksuele gerichtheid', 18-01-2023. https://www.rijksoverheid.nl/actueel/nieuws/2023/01/17/non-discriminatiegronden-grondwet-uitgebreid-met-handicap-en-seksuele-gerichtheid
[20] Regeringscommissariaat seksueel grensoverschrijdend gedrag en seksueel geweld. 'Handreiking voor cultuurverandering op de werkvloer: Over preventie en de aanpak van seksueel grensoverschrijdend gedrag', 13 maart 2024.
[21] Rathenau Instituut. 'Online ontspoord - Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', 2021.
[22] Idem.
[23] Idem.

CYBERSTALKING

Cyberstalking is wanneer iemand expres, en steeds weer, online lastiggevallen, bespioneert, bang gemaakt en/of bedreigd wordt. Een cyberstalker probeert zoveel mogelijk informatie via internet te verzamelen. Sociale media zijn voor cyberstalkers vaak een bron van informatie. Daar ontdekken ze wie jouw contacten zijn of waar je kort geleden bent geweest. Een cyberstalker is meestal iemand die je persoonlijk kent, zoals een (ex-)partner, schoolgenoot, collega, of een vriend. De cyberstalker wil contact afdwingen door je bang te maken of onder druk te zetten.[24]

DOXING

Doxing is het openbaar maken van persoonsgegevens om iemand lastig te vallen of te intimideren. Bijvoorbeeld adresgegevens, telefoonnummer, werkgever, of gegevens van familieleden of foto's van kinderen. De informatie die wordt gebruikt om iemand te doxen, is vaak openbaar online beschikbaar zonder dat je daarvoor gehackt hoeft te worden. Bijvoorbeeld als iemand zijn werkgever op LinkedIn heeft vermeld, dan kan dit in combinatie met andere publieke gegevens gebruikt worden.
Doordat persoonlijke informatie op straat komt te liggen, lopen slachtoffers na doxing ook offline risico op schadelijk gedrag. Doxing is schadelijk omdat privé-informatie van slachtoffers online gemakkelijk misbruikt kan worden, bijvoorbeeld om iemand te bedreigen of iemands werkgever lastig te vallen.[25]
Sinds 1 januari 2024 is doxing strafbaar. Voor doxing staat maximaal 2 jaar gevangenisstraf of een geldboete van € 22.500. De maximale gevangenisstraf kan met een derde verhoogd worden, als de doxing gericht is tegen personen met een specifiek beroep, zoals politici, rechters, journalisten of hulpverleners.[26]

HAATZAAIEN

Haatzaaien of haatspraak is het aanvallen van een persoon of groep op grond van godsdienst, seksuele oriëntatie of discriminatie.
Haatzaaien op internet verschilt van haatzaaien op straat doordat haatzaaiende content online erg lang beschikbaar blijven op verschillende platformen. Het kan ook snel weer opduiken op een ander platform, ook als content elders verwijderd is. Het internationale karakter van het internet zorgt ervoor dat het moeilijk is om op te treden tegen haatzaaien dat vanuit andere landen komt.[27]

Haatzaaien valt volgens het VN-verdrag niet onder de bescherming van de vrijheid van meningsuiting omdat het, door op te roepen tot geweld en discriminatie, geldt als een misbruik van dat recht. Haatzaaien is strafbaar volgens Artikel 137d van het Nederlands Wetboek van Strafrecht.[28]

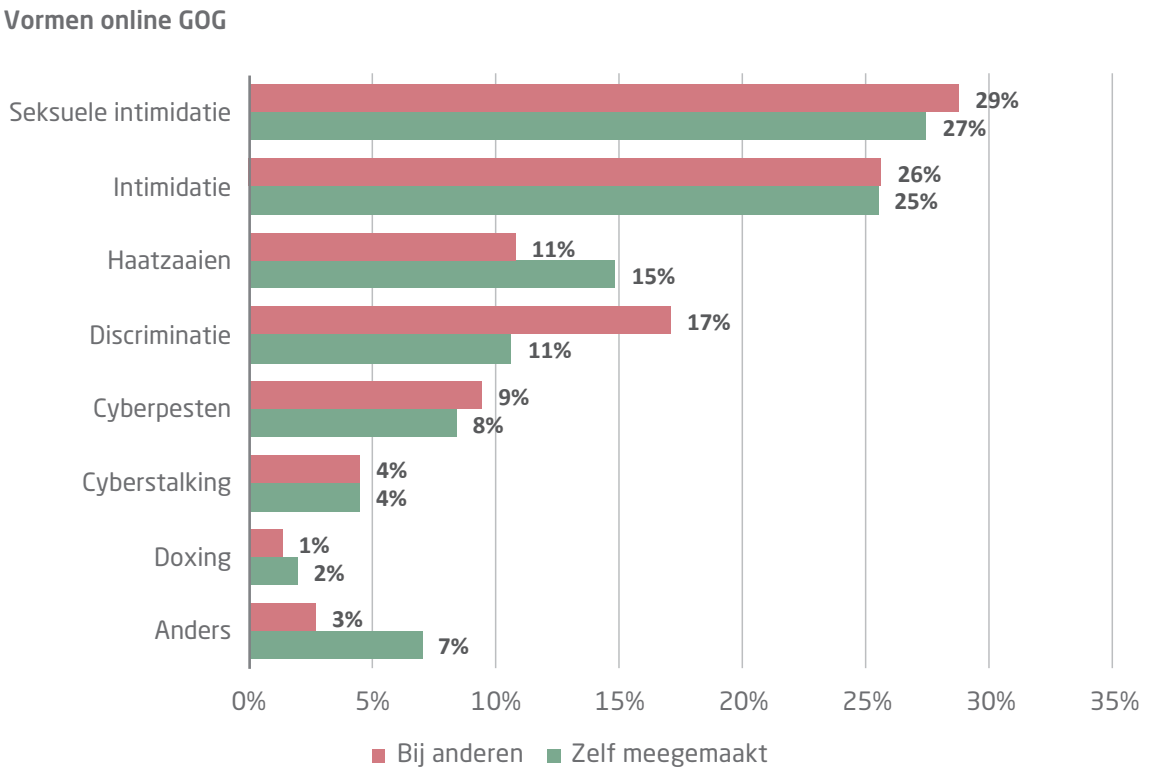
Sommige vormen van grensoverschrijdend gedrag komen ook online voor, zoals pesten intimidatie, discriminatie, stalking en haatzaaien. Maar het internet biedt ook plek aan nieuwe vormen van grensoverschrijdend gedrag, zoals ongewenste sexting, wraakporno, sextortion, deepfakes, exposen en doxing. Al deze vormen van grensoverschrijdend gedrag kunnen voorkomen op de werkvloer en in dit digitale tijdperk moeten wij ons daar bewust van zijn en maatregelen met elkaar te treffen om werknemers te beschermen.

[24] Helpwanted. 'Cyberstalking', https://www.helpwanted.nl/onderwerpen/cyberstalking
[25] Rathenau Instituut. 'Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', 2021.
[26] Rijksoverheid. 'Doxing', 2024. https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/doxing
[27] Rathenau Instituut. 'Online ontspoord – Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland', 2021.
[28] Amnesty International. 'Haatzaaien en haatspraak', https://www.amnesty.nl/encyclopedie/haatzaai-haatspraak-hate-speech

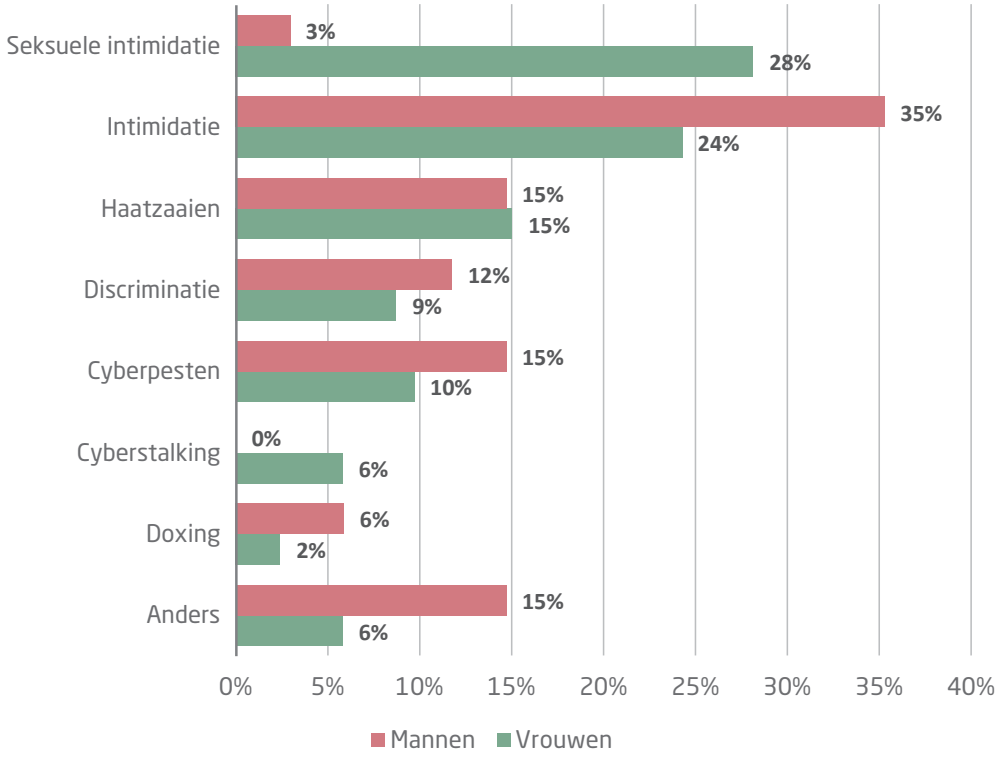
2. WELKE VORMEN KOMEN HET VAAKST VOOR OP DE WERKVLOER?

In dit hoofdstuk richten we ons op de verschillende vormen van online grensoverschrijdend gedrag (GOG) die het meest voorkomen op de werkvloer. Deze zijn gerangschikt op basis van de frequentie waarin de respondenten ze hebben gerapporteerd.
Van de **752** mensen die de enquête hebben ingevuld, geeft bijna de helft aan te maken te hebben gehad met online grensoverschrijdend gedrag. De percentages die hieronder genoemd worden betreffen respondenten die te maken hebben gehad met online grensoverschrijdend gedrag. **22%** hiervan geeft aan er zelf mee te maken hebben gehad en 14% heeft het gezien of gehoord bij een of meer collega's. **13%** geeft aan dat zowel zijzelf als een of meer collega's met online grensoverschrijdend gedrag te maken hebben gehad.

VORMEN:



Vormen online GOG man/vrouw



Seksuele intimidatie

Seksuele intimidatie is de meest gerapporteerde vorm van online grensoverschrijdend gedrag op de werkvloer, met **27%** van de respondenten die aangaven hiermee te maken te hebben gehad. Vrouwen hebben acht keer zo vaak hiermee te maken dan dat mannen dat hebben.

Uit de enquête komt naar voren dat mensen vooral te maken hebben gehad met ongewenste sexting. Er werden bijvoorbeeld seksueel getinte opmerkingen gemaakt door een collega die 35 jaar ouder was. Of iemand kreeg WhatsApp berichten en foto's van een ontbloot bovenlijf terwijl die persoon een partner had. Daarnaast werd er één deepfake gerapporteerd in de enquête.

Intimidatie

Direct na seksuele intimidatie is intimidatie de tweede meest voorkomende vorm van online grensoverschrijdend gedrag, gerapporteerd door **25%** van de respondenten. Mannen geven vaker aan hier mee te maken te hebben dan vrouwen.

Als voorbeelden uit de enquête komen naar voren dat er denigrerende opmerkingen en grof taalgebruik plaatsvonden.

Een persoon gaf aan te maken hebben gehad met gaslighten. Dit is een vorm van emotionele manipulatie. Een gaslighter voedt zijn of haar zelfvertrouwen door de waarheid te verdraaien. Door de twijfel die dit zaait gaat het slachtoffer meer en meer op de gaslighter leunen, waardoor deze zich steeds belangrijker voelt.[29]

Haatzaaien

Haatzaaien, dat verwijst naar het verspreiden van discriminerende of beledigende taal gericht op een individu of groep, werd door 15% van de respondenten gemeld als een vorm van online grensoverschrijdend gedrag op de werkvloer. Dit gedrag wordt vaker zelf meegemaakt dan gesignaleerd bij anderen.

[29] Slachtofferwijzer. 'Gaslighting: betekenis, symptomen en voorbeelden', 2024. https://slachtofferwijzer.nl/artikelen/gaslighting-betekenis-symptomen-voorbeelden

Discriminatie

Discriminatie via onlinekanalen is gerapporteerd door 11% van de respondenten. Het wordt vaker gesignaleerd bij anderen dan dat respondenten er zelf mee te maken hebben.
Dit gedrag kan variëren van expliciete opmerkingen die gericht zijn op iemands ras, geslacht, seksuele gerichtheid, leeftijd of religie, tot subtielere vormen van uitsluiting of neerbuigende communicatie. Als voorbeeld werd er gegeven dat die persoon gediscrimineerd is vanwege zijn/haar seksuele gerichtheid.

Cyberpesten

Cyberpesten werd door 8% van de respondenten genoemd en verwijst naar herhaaldelijk ongewenst, kwetsend gedrag dat bedoeld is om het slachtoffer te vernederen, kleineren of uitsluiten. Hierbij geven mannen iets vaker aan er mee te maken te hebben dan vrouwen.
Als voorbeelden uit de enquête kwam naar voren dat iemand was buitengesloten van systemen tijdens ziekte. Of het expres weigeren van vakantiedagen in het systeem. Iemand werd genegeerd en had geen toegang tot de werkomgeving terwijl andere collega's hier wel inzicht in hadden.

Cyberstalking

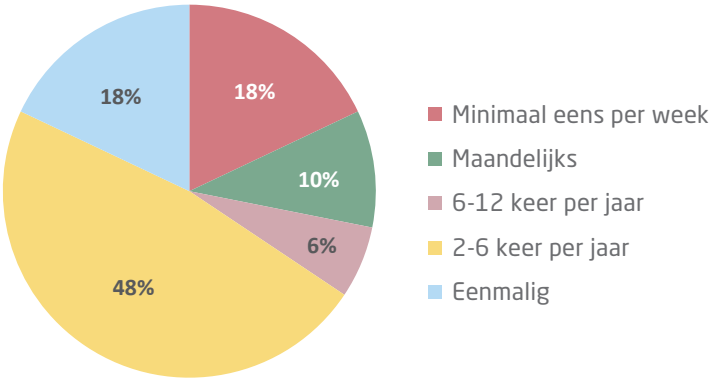
Cyberstalking, waarbij een persoon via digitale kanalen continu wordt gevolgd of lastiggevallen, werd door 4% van de respondenten gerapporteerd. Dit kan gaan om het ongewenst en herhaaldelijk sturen van berichten, het volgen van online activiteiten, of zelfs het dreigen om persoonlijke informatie openbaar te maken.
Mannen geven aan niet te maken hebben gehad met cyberstalking terwijl vrouwen in 6% van de gevallen hiermee te maken kreeg.

Doxing

Doxing, waarbij persoonlijke informatie van iemand zonder toestemming openbaar wordt gedeeld met de intentie om schade toe te brengen, werd door 2% van de respondenten genoemd. Hierbij geven mannen iets vaker aan er mee te maken te hebben dan vrouwen.
Hoewel dit de minst gerapporteerde vorm van online grensoverschrijdend gedrag is, kan doxing vergaande gevolgen hebben voor het slachtoffer. Dit kan bijvoorbeeld gaan om het publiceren van privégegevens zoals adressen of telefoonnummers, wat kan leiden tot ernstige veiligheidsrisico's.

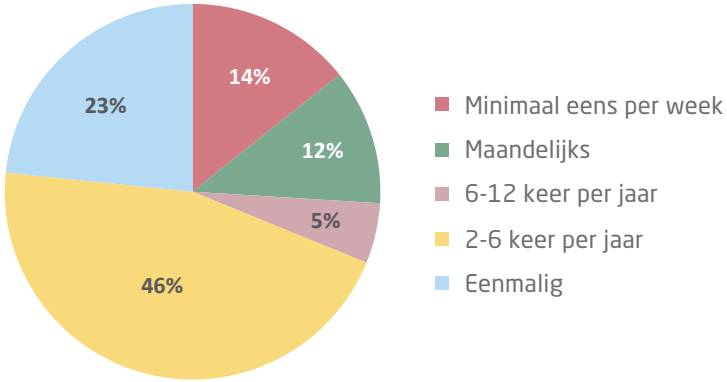
HOE VAAK KWAM DIT GEDRAG VOOR?

Frequentie online GOG afgelopen jaar



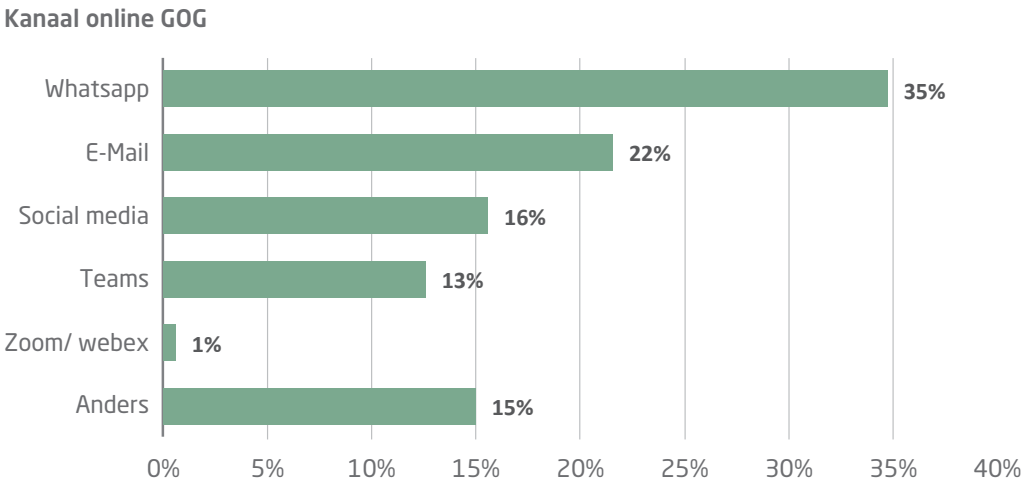
In de enquête zijn de respondenten gevraagd hoe vaak dit gedrag is voorgekomen. **38%** gaf aan dat het online grensoverschrijdende gedrag meer dan een jaar geleden is voorgekomen. Van de groep die het afgelopen jaar heeft meegemaakt geeft ruim een kwart (**28%**) aan dit minimaal maandelijks mee te maken. Ruim **80%** geeft aan dit meerdere keren per jaar mee te maken.

Frequentie collega's online GOG afgelopen jaar



21% van de respondenten wist niet hoe vaak het bij collega's was voorgekomen het afgelopen jaar. **24%** gaf aan dat het langer dan een jaar geleden was. Van de groep die het afgelopen jaar heeft meegemaakt, geldt dat **26%** dit minimaal maandelijks meemaakt. Ruim driekwart (**77%**) maakt het meerdere keren per jaar mee.

VIA WELK KANAAL?



De digitalisering van werkprocessen en communicatie heeft ervoor gezorgd dat er verschillende platforms zijn waar werknemers met elkaar in contact komen. Deze platforms kunnen ook worden gebruikt voor grensoverschrijdend gedrag.
Uit het onderzoek blijkt dat het online grensoverschrijdend gedrag het meest voorkomt via WhatsApp. Daarna komt e-mail en sociale media zoals Facebook, Instagram, Twitter en Snapchat. Via Teams komt het online grensoverschrijdend gedrag ook vaak voor.

1. WhatsApp

WhatsApp wordt steeds vaker gebruikt voor werk gerelateerde communicatie, zeker nu de scheidslijn tussen werk en privé door thuiswerken verder vervaagd. Voor veel werknemers die te maken hadden met online grensoverschrijdend gedrag, werd WhatsApp met 35% genoemd als meest gebruikte kanaal.

Voorbeelden:

- Ik heb te maken gehad met het uitsluiten van een appgroep (zogenaamd per ongeluk)
- Een onschuldig flirterige App. Maar daardoor durfde ik niet meer het initiatief te nemen om alleen met die persoon af te spreken voor werk.
- Ik ontving een dickpic, toen ik hem er op aan sprak zei hij dat zijn broertje aan zijn telefoon had gezeten.

2. E-mail

Hoewel e-mail vaak als een formeel communicatiemiddel wordt beschouwd, blijkt uit het onderzoek dat ook dit kanaal wordt gebruikt voor grensoverschrijdend gedrag. In 22% van de gevallen was dit zo.

Voorbeelden:

- Vernederende mail naar groep collega's gestuurd
- Een manlijke medewerker die een ietwat te dikke vrouwelijke leidinggevende in een mail laat weten dat ze 'toch al niet zo smakelijk is'

3. Sociale media

Sociale media platforms, zoals Facebook, Instagram, Twitter en LinkedIn, worden steeds vaker gebruikt voor werk gerelateerde contacten. Echter, deze platforms bieden ook ruimte voor grensoverschrijdend gedrag, zeker wanneer collega's elkaar volgen of vriendschapsverzoeken accepteren. In het onderzoek werd sociale media in 16% van de gevallen genoemd als een kanaal waar grensoverschrijdend gedrag plaatsvindt. Een respondent gaf aan dat het grensoverschrijdend gedrag plaatsvond via Snapchat en bij een respondent was dit via SMS.

4. Teams

Microsoft Teams, evenals andere vergader- en chatplatforms zoals Zoom, of Webbex, is een veelgebruikt middel voor communicatie op de werkvloer, vooral sinds de toename van thuiswerken tijdens de pandemie. In 14% van de gevallen werd deze manier van communiceren gebruikt voor grensoverschrijdend gedrag.

CONCLUSIE FREQUENTIE

De resultaten van de enquête schetsen een verontrustend beeld van het aantal slachtoffers van online grensoverschrijdend gedrag op de werkvloer. Bijna de helft van de respondenten geeft aan zelf of bij collega's online grensoverschrijdend gedrag meegemaakt te hebben.
Seksuele intimidatie, zoals ongewenste sexting, blijkt de meest voorkomende vorm te zijn. Zowel bij mensen die het zelf hebben meegemaakt en mensen die het bij anderen hebben gezien, scoort dit hoog. Het verschil tussen mannen en vrouwen die te maken hebben met seksuele intimidatie is erg groot. Vrouwen hebben acht keer zo vaak hiermee te maken dan dat mannen dat hebben. Mannen hebben dan weer meer te maken met intimidatie en cyberpesten. Mannen geven aan niet te maken hebben gehad met cyberstalking terwijl vrouwen in 6% van de gevallen hiermee te maken kreeg. Doxing komt daarentegen weer vaker voor bij mannen ten opzichte van vrouwen.
Bij haatzaaien wordt aangegeven dat het vaker zelf wordt meegemaakt dan dat het bij anderen wordt gezien, bij discriminatie is dit juist andersom.

De frequentie waarmee het online grensoverschrijdend gedrag plaatsvindt, is ook zorgelijk.
Meer dan een kwart geeft aan hier zowel zelf als bij anderen het vaak mee te maken. In beide groepen geeft bijna de helft aan hier twee tot zes keer per jaar mee geconfronteerd te worden. Meer dan driekwart, die het afgelopen jaar met online GOG te maken heeft gehad, heeft dit meer dan eens meegemaakt.

Wat betreft de gebruikte communicatiekanalen springt WhatsApp er in negatieve zin uit. Misschien niet verassend maar wel zorgelijk gezien het enorme gebruik van WhatsApp groepen van werknemers en het snelle verspreiden van schadelijke informatie. Het lastige is dan ook de groepsnormen die gezet worden in deze groepen.
De groepsdynamiek kan zorgen voor een cultuur waarin ongepast gedrag stilzwijgend wordt geaccepteerd.
Als schadelijke berichten niet worden tegengesproken, kan dit bijdragen aan een bredere normalisering van grensoverschrijdend gedrag binnen de organisatie.

Daarnaast spelen ook andere kanalen een rol. E-mail en persoonlijke berichten kunnen worden gebruikt voor directe intimidatie of ongewenste communicatie, terwijl sociale media een platform bieden voor gedrag dat buiten de directe controle van de werkgever valt, maar toch ernstige gevolgen kan hebben. Teams, hoewel meestal gemonitord door de werkgever, blijkt eveneens niet gevrijwaard van ongewenste interacties.

Voor werkgevers ligt hier een belangrijke verantwoordelijkheid. Zij moeten zich bewust zijn van de specifieke risico's die elk digitaal platform met zich meebrengt en passende beleidsmaatregelen ontwikkelen om de digitale werkomgeving zo veilig mogelijk te maken. Dit vraagt om een aanpak die niet alleen gericht is op het creëren van bewustwording en bespreekbaarheid, maar ook op concrete preventie- en handhavingsstrategieën.

3. WIE ZIJN DE MEEST VOORKOMENDE SLACHTOFFERS EN DADERS?

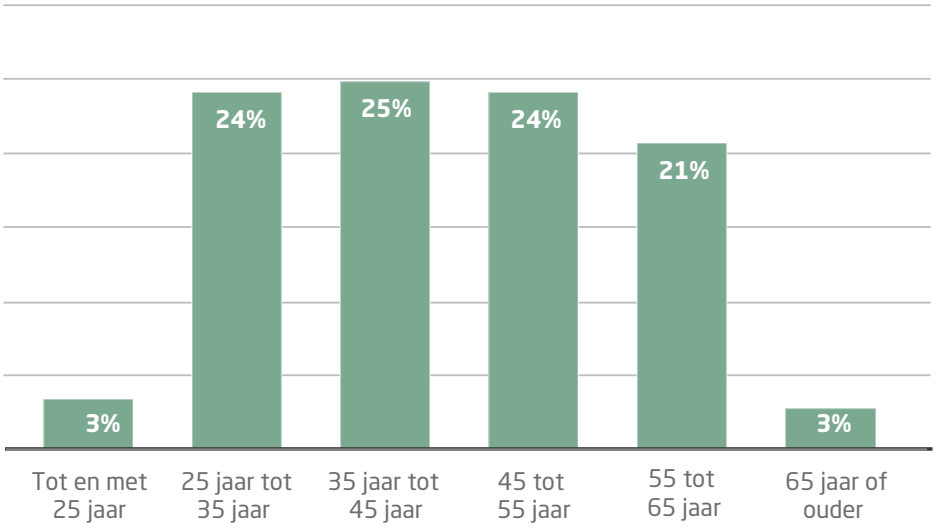
Nu er bekend is welke vormen, de frequentie en kanalen van online grensoverschrijdend gedrag voorkomen, blijft een belangrijke vraag onbeantwoord: wie zijn de mensen die dit gedrag het vaakst ervaren en wie zijn degenen die het veroorzaken?

SLACHTOFFERS

Het onderzoek toont aan dat online grensoverschrijdend gedrag een probleem vormt in de werkomgeving, waarbij een deel van de werknemers te maken krijgt met ongewenst gedrag via digitale kanalen. Van de respondenten gaf **34%** aan zelf slachtoffer te zijn geweest van online grensoverschrijdend gedrag, terwijl **14%** getuige is geweest van dergelijke voorvallen richting collega's. Deze cijfers laten zien dat online grensoverschrijdend gedrag niet alleen de slachtoffers zelf raakt, maar ook een impact heeft op omstanders. Dit kan bijdragen aan een negatief werkklimaat en gevoelens van onveiligheid onder collega's.

Een belangrijke conclusie van dit onderzoek is dat vrouwen aanzienlijk vaker het slachtoffer zijn van online grensoverschrijdend gedrag dan mannen. **84%** van de meldingen betreft vrouwelijke slachtoffers, tegenover **14%** mannelijke slachtoffers. Deze ongelijke verdeling wijst op een bredere maatschappelijke tendens waarin vrouwen vaak kwetsbaarder zijn voor grensoverschrijdende interacties op het werk, zowel online als offline.
Dit blijkt ook uit de Nationale Enquête Arbeidsomstandigheden (NEA). 21% van de vrouwelijke werknemers geven daar aan dat zij in de afgelopen twaalf maanden met ongewenst gedrag te maken hebben gehad, tegenover 13% van de mannelijke werknemers. Dit speelt mee bij het relatief hoge percentage ongewenst gedrag in bedrijfstakken waar veel vrouwen werken, zoals de zorg en het onderwijs. In die twee bedrijfstakken was in 2023 respectievelijk 82 en 65 procent van de werknemers vrouw. In de bouw was dit 14 procent.[30]

Leeftijdsverdeling mensen die OGOG hebben meegemaakt

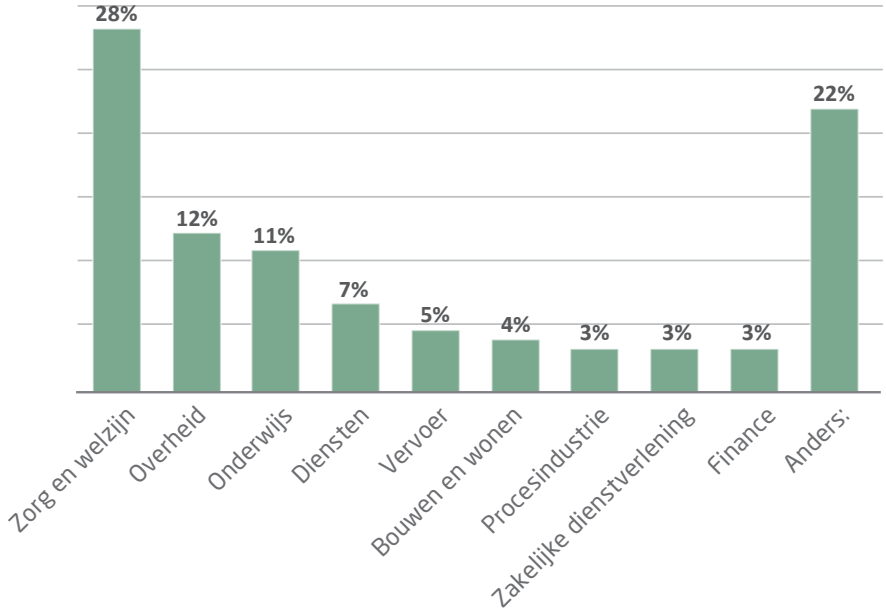


[30] Centraal Bureau voor de Statistiek. 'Werknemers in zorg en horeca ervaren vaakst ongewenst gedrag', 11 november 2024. https://www.cbs.nl/nl-nl/nieuws/2024/46/werknemers-in-zorg-en-horeca-ervaren-vaakst-ongewenst-gedrag

Verder wijst dit onderzoek uit dat online grensoverschrijdend gedrag in alle leeftijdsgroepen voorkomt.

Verder valt op dat het merendeel van de respondenten een contract voor onbepaalde tijd heeft: **80%** van de ondervraagden beschikt over een vast dienstverband. Voor medewerkers met een tijdelijk contract (**8%**) of uitzendcontract (**3%**) is er wellicht sprake van een verhoogde kwetsbaarheid, doordat zij zich in een afhankelijkere positie bevinden, en mogelijk minder vaak melding maken van ongewenst gedrag.

Sectoren



Uit het onderzoek naar online grensoverschrijdend gedrag op de werkvloer blijkt dat de mate waarin werknemers hiermee worden geconfronteerd sterk verschilt tussen sectoren. Ongewenst gedrag komt ook vaker voor als het werk meer contact met collega's, klanten, patiënten of leerlingen met zich meebrengt.[31]

Zorg en Welzijn steekt er met 28% van de meldingen bovenuit. Deze sector omvat een breed scala aan beroepen, waaronder Ambulancezorg, Geestelijke Gezondheidszorg, Gehandicaptenzorg, Jeugdzorg, Kinderopvang, Kraamzorg, Verpleeg- en Verzorgingshuizen & Thuiszorg, en Ziekenhuizen. Professionals in deze sectoren werken vaak intensief met cliënten en hun families, wat hun blootstelling aan grensoverschrijdend gedrag verhoogt.
Uit onderzoek van de NEA blijkt dat deze sector sowieso het meest te maken heeft met ongewenst gedrag (online en offline), 30% heeft daarmee te maken.

[31] Centraal Bureau voor de Statistiek. 'Werknemers in zorg en horeca ervaren vaakst ongewenst gedrag', 11 november 2024. https://www.cbs.nl/nl-nl/nieuws/2024/46/werknemers-in-zorg-en-horeca-ervaren-vaakst-ongewenst-gedrag

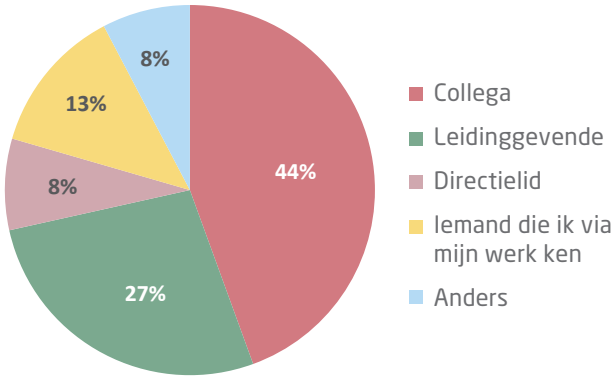
De Overheidssector volgt met 12% van de meldingen. Hier zijn vooral publieke functies kwetsbaar, aangezien deze professionals regelmatig te maken hebben met lastige beslissingen en handhavingstaken. Vaak worden ze geconfronteerd met online kritiek of intimidatie, vooral wanneer burgers het niet eens zijn met bepaalde beleidsmaatregelen. In de Nationale Enquête Arbeidsomstandigheden staat het openbaar bestuur op vierde plek met 17,4%.[32] Uit onderzoek van de FNV naar het ministerie van VWS blijkt ook dat grensoverschrijdend gedrag daar een groot probleem is.[33]

Onderwijs staat op de derde plaats, met 11% van de meldingen. Docenten en andere onderwijsprofessionals werken regelmatig digitaal samen met studenten en hun ouders.

Hierdoor is de kans groter dat zij via sociale media of e-mail met grensoverschrijdend gedrag worden geconfronteerd, vooral in situaties waarin zij corrigerende of lastige beslissingen moeten nemen. In de NEA staat onderwijs op de zesde plek met 16,9%.[34]

DADERS

Veroorzaker online GOG



Uit het onderzoek komt naar voren de daders zijn meestal personen binnen de eigen organisatie. In **44%** van de incidenten gaat het om collega's. Wanneer online grensoverschrijdend gedrag plaatsvindt binnen de directe werkomgeving, kan dat de veiligheid en het vertrouwen in collega's ernstig onder druk zetten.

Dat directieleden en leidinggevenden in **35%** van de gevallen de daders zijn, is bijzonder kwalijk, omdat zij de verantwoordelijkheid dragen voor een veilige werkomgeving en zelf een voorbeeldfunctie hebben. Wanneer leidinggevenden echter zelf de grens overschrijden, kan dat niet alleen de werkervaring van de betrokken werknemers negatief beïnvloeden, maar ook de drempel om incidenten te melden aanzienlijk verhogen.
Dit zagen we ook in eerdere FNV onderzoeken.[35]

Wanneer grensoverschrijdend gedrag uit de top van de organisatie komt, ondermijnt dit het vertrouwen in het leiderschap en kan het de effectiviteit van beleid en protocollen tegen grensoverschrijdend gedrag verzwakken.

[32] Centraal Bureau voor de Statistiek. 'Werknemers in zorg en horeca ervaren vaakst ongewenst gedrag', 11 november 2024. https://www.cbs.nl/nl-nl/nieuws/2024/46/werknemers-in-zorg-en-horeca-ervaren-vaakst-ongewenst-gedrag
[33] FNV. 'Onderzoeksrapport omgangsvormen op de werkvloer ministerie van VWS', 2024.
[34] Centraal Bureau voor de Statistiek. 'Werknemers in zorg en horeca ervaren vaakst ongewenst gedrag', 11 november 2024. https://www.cbs.nl/nl-nl/nieuws/2024/46/werknemers-in-zorg-en-horeca-ervaren-vaakst-ongewenst-gedrag
[35] FNV. 'Horen, zien en zwijgen: omgangsvormen op de werkvloer', oktober 2023.

Externe partijen, zoals klanten, passagiers of patiënten, zijn in **13%** van de gevallen de daders van online grensoverschrijdend gedrag. Hoewel deze groep een kleiner aandeel heeft, blijft het een aandachtspunt, omdat werknemers hierbij te maken krijgen met gedrag waar ze zelf weinig controle over hebben. Voor veel organisaties vormt dit een uitdaging, omdat sommige van deze interacties door de aard van het werk vaak onvermijdelijk zijn.

Deze bevindingen maken duidelijk dat online grensoverschrijdend gedrag niet alleen plaatsvindt tussen collega's onderling, maar ook te maken heeft met hiërarchische en externe invloeden. Dit benadrukt de complexiteit van het probleem en wijst op de noodzaak van een breed gedragen aanpak om een respectvolle, digitale werkomgeving te creëren.

CONCLUSIE SLACHTOFFERS EN DADERS

Er zijn significante verschillen in frequentie van online grensoverschrijdend gedrag tussen man/vrouw, leeftijdsgroepen en sectoren. Met 34% van de respondenten die aangaven zelf slachtoffer te zijn geweest en nog eens 14% die dergelijk gedrag bij collega's hebben waargenomen, heeft bijna de helft van de respondenten direct of indirect met online grensoverschrijdend gedrag te maken. Dit onderstreept de urgentie om deze problematiek binnen organisaties aan te pakken. Vooral vrouwen lijken hierin kwetsbaar: 84% van de gemelde incidenten betrof vrouwelijke slachtoffers.

Sectorniveau-analyse toont aan dat grensoverschrijdend gedrag het vaakst voorkomt in de sectoren Zorg en Welzijn, Overheid en Onderwijs. In deze sectoren hebben medewerkers veel interactie met derden, zoals patiënten, klanten of leerlingen, wat mogelijk bijdraagt aan verhoogde risico's voor grensoverschrijdend gedrag. Deze sectoren hebben ook offline een hoog risico op grensoverschrijdend gedrag. De interactie met derden en de hoge werkdruk in deze sectoren kunnen bijdragen aan extra spanning en daarmee aan een toename van incidenten tussen collega's onderling.

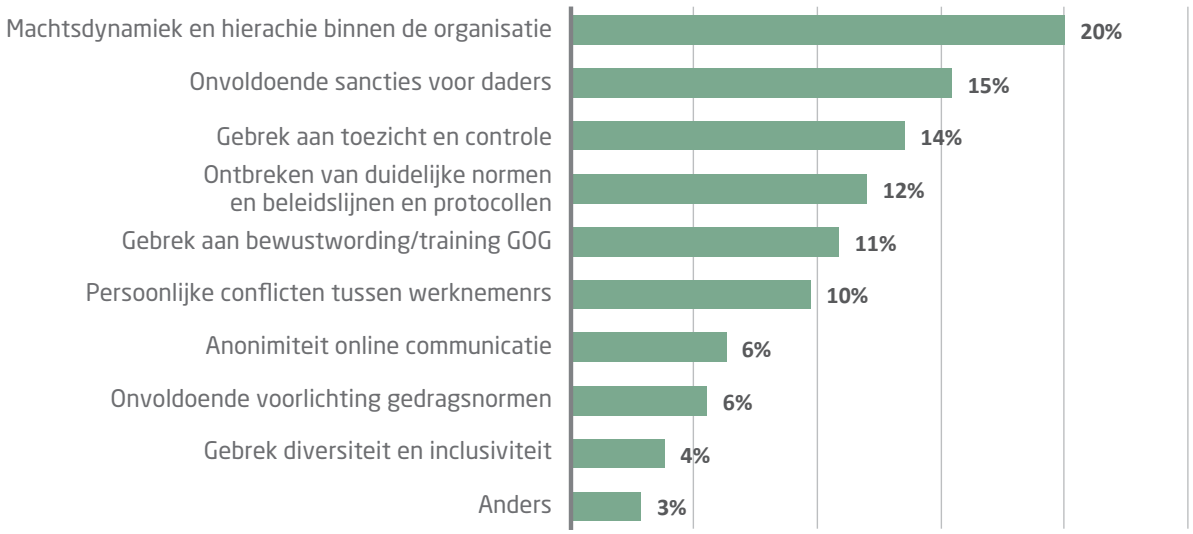
44% van de daders zijn collega's, maar liefst 35% werd door leidinggevenden en directieleden gedaan. 13% door derden (patienten, passagiers e.d..).

4. DE OORZAKEN

Online grensoverschrijdend gedrag op de werkvloer is een nieuwe vorm van een bekend probleem dat grote gevolgen kan hebben voor werknemers en hun werkomgeving. Maar wat veroorzaakt dit gedrag? En hoe zit het met het melden? Hoe vaak wordt het gemeld, bij wie en wat wordt er met de meldingen gedaan? In dit hoofdstuk gaan we in op die vragen.

OORZAKEN

Oorzaken online GOG



Uit het onderzoek naar de oorzaken van online grensoverschrijdend gedrag op de werkvloer blijkt dat de onderliggende factoren vaak te maken hebben met de interne structuur, cultuur en het management binnen organisaties. Machtsdynamiek en hiërarchie binnen de organisatie werd door **20%** van de respondenten genoemd als de belangrijkste oorzaak.

De tweede meest genoemde oorzaak, met **15%**, betreft het gebrek aan sancties voor daders. Dit wijst op een tekort aan effectieve maatregelen binnen organisaties om grensoverschrijdend gedrag aan te pakken en te ontmoedigen. Wanneer overtreders niet worden geconfronteerd met consequenties, kan dit gedrag blijven voortduren, wat het gevoel van veiligheid onder werknemers negatief beïnvloedt.

14% gaf aan dat er een gebrek aan toezicht en controle de oorzaak was. Omdat online communicatie vaak buiten het directe gezichtsveld van leidinggevenden of collega's plaatsvindt, kunnen incidenten onopgemerkt blijven. De afwezigheid van voldoende controlemaatregelen verhoogt het risico op grensoverschrijdend gedrag.
Daarnaast gaven **12%** van de respondenten aan dat het ontbreken van duidelijke normen, beleidslijnen en protocollen bijdraagt aan online grensoverschrijdend gedrag. Wanneer bedrijven geen heldere richtlijnen hebben, ontbreekt een basis om werknemers effectief te beschermen en op een respectvolle manier te communiceren. Dit zijn niet direct oorzaken voor online grensoverschrijdend gedrag maar faciliteren het wel.

Gebrek aan bewustwording en training was voor **11%** van de respondenten een belangrijke factor. Veel werknemers en leidinggevenden zijn zich onvoldoende bewust van de risico's en gevolgen van online grensoverschrijdend gedrag. Verder gaf 10% aan dat persoonlijke conflicten tussen werknemers vaak escaleren in online omgevingen, vooral zonder direct toezicht.

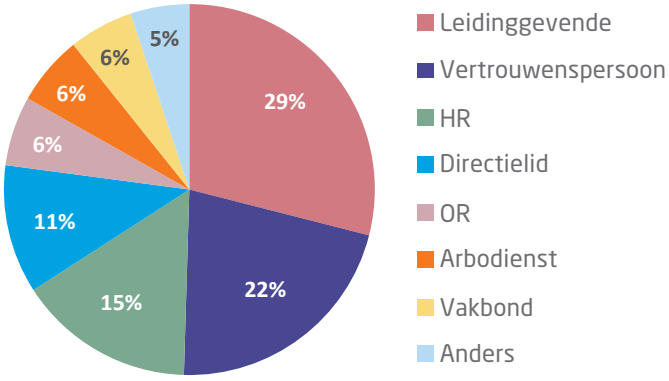
De laatste oorzaken van online grensoverschrijdend gedrag hebben te maken met de aard van digitale communicatie en de normen binnen de organisatie. Anonimiteit in online communicatie en een gebrek aan voorlichting over gedragsnormen scoorden beide **6%**. Anonimiteit kan ervoor zorgen dat werknemers zich minder verantwoordelijk voelen voor hun acties, terwijl onvoldoende voorlichting bijdraagt aan een gebrek aan inzicht in wat wel of niet acceptabel is. Ten slotte werd gebrek aan diversiteit en inclusiviteit als oorzaak door **4%** van de respondenten genoemd. Een diverse en inclusieve werkomgeving kan bijdragen aan het verminderen van grensoverschrijdend gedrag door meer begrip en acceptatie tussen werknemers te bevorderen.

In de categorie "anders" gaven respondenten voorbeelden als het ontbreken van sociale kaders en een gebrek aan normbesef bij de daders zelf. Respondenten merkten op dat daders vaak niet inzien dat hun gedrag onprofessioneel is en niet thuishoort in een werkomgeving, wat volgens hen meer zegt over het karakter van de dader dan de werksituatie.
Kortom de resultaten wijzen erop dat grensoverschrijdend gedrag op de werkvloer niet alleen voortkomt uit persoonlijk conflict of digitale anonimiteit, maar vooral samenhangt met de machtsstructuren, cultuur en het management binnen een organisatie.

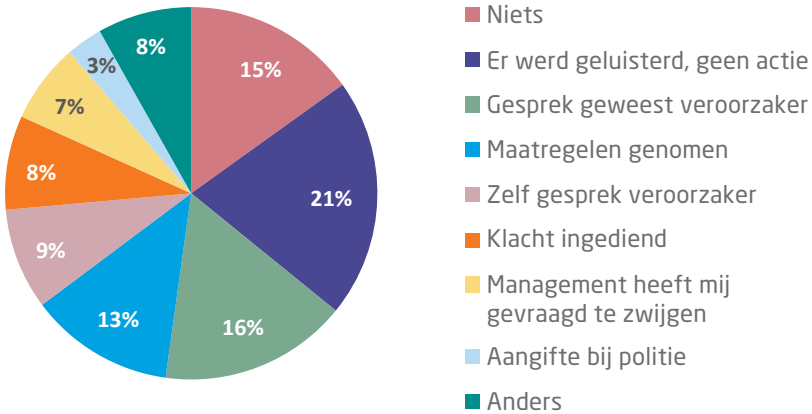
MELDINGEN

Uit het onderzoek blijkt dat online grensoverschrijdend gedrag op de werkvloer in veel gevallen wel gemeld wordt, maar dat een aanzienlijk deel van deze meldingen zonder concrete actie blijft. Hoewel meer dan de helft van de respondenten melding maakte van online grensoverschrijdend gedrag, koos **47%** ervoor dit niet te melden. De meeste meldingen werden gedaan bij een leidinggevende (**29%**), gevolgd door vertrouwenspersonen (**22%**) en Personeelszaken/HR (**15%**). Bij anders gaf bijvoorbeeld een respondent aan het College voor de Rechten van de Mens ingeschakeld te hebben.

Bij wie gemeld



Wat is er met de melding gebeurd?



Op de vraag "Wat is er gebeurd met jouw melding van grensoverschrijdend gedrag?" blijkt dat in **15%** van de gevallen niets werd gedaan. Bij **21%** werd er geluisterd maar geen actie ondernomen. In ruim een derde van de gevallen is er dus niets gedaan met de melding van online grensoverschrijdend gedrag. Dit kan een demotiverend effect hebben op slachtoffers, die mogelijk het gevoel krijgen dat hun ervaringen niet serieus worden genomen.

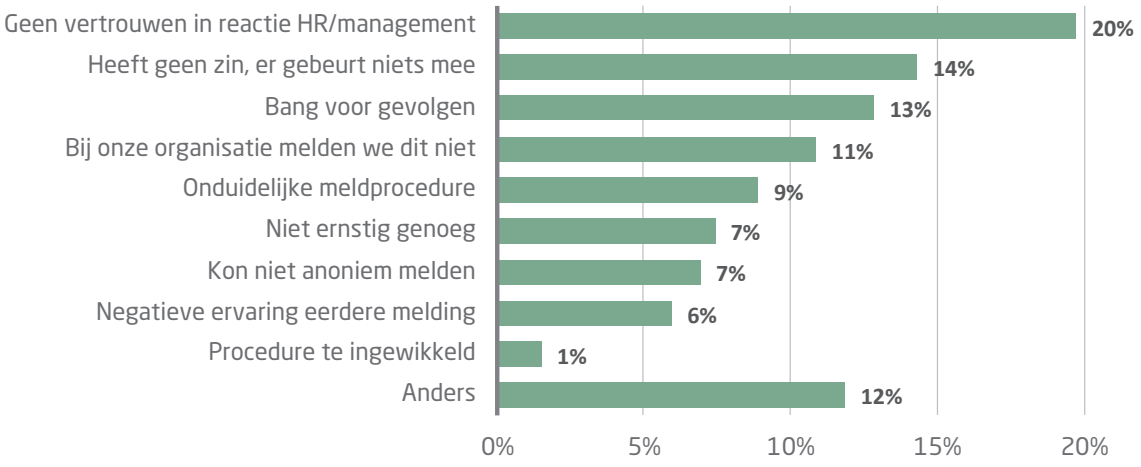
Bij de meldingen waarbij wél actie werd ondernomen, vond in **16%** van de gevallen een gesprek plaats met de dader en in **13%** van de gevallen werden concrete maatregelen genomen. Enkele van deze maatregelen omvatten: het op non-actief stellen van de collega, het beëindigen van een arbeidsovereenkomst, het opleggen van een waarschuwing en het uitvoeren van een extern onderzoek. Andere, minder voorkomende maatregelen omvatten bijvoorbeeld de herindeling van roosters en veiligheidsmaatregelen zoals het instellen van een noodknop op werktelefoon.

9% van de respondenten gaf aan zelf een gesprek te hebben gehad met de dader en 8% heeft een formele klacht ingediend. Opvallend en zorgwekkend is dat **7%** van de respondenten te maken kreeg met het verzoek van het management om te zwijgen over het incident.
Uiteindelijk is in **3%** van de gevallen aangifte gedaan bij de politie.

Bovendien meldden respondenten enkele bijzondere, vaak negatieve ervaringen met de aanpak van hun meldingen. Zo werden ze geconfronteerd met bedreigingen om aangeklaagd te worden voor laster, of zelfs gevraagd om te vertrekken uit de organisatie. In één geval werd er verwezen naar de vertrouwenspersoon maar die was juist de persoon die het online grensoverschrijdend gedrag vertoonde.

Deze bevindingen onderstrepen de noodzaak van een duidelijke en goed gedefinieerde aanpak voor online grensoverschrijdend gedrag op de werkvloer. Organisaties moeten niet alleen heldere meldingsprocedures en ondersteuningsmechanismen opzetten maar ook zorgen voor een cultuur waarin meldingen serieus worden genomen en slachtoffers zich gesteund voelen.

Reden om niet te melden



47% van de respondenten heeft het online grensoverschrijdende gedrag op de werkvloer niet gemeld. De redenen hiervoor bieden inzicht in de uitdagingen die slachtoffers ervaren bij het aankaarten van dit soort gedrag binnen hun organisatie. De meest voorkomende reden was een gebrek aan vertrouwen in HR of het management, met **20%** van de respondenten die dit aangaf. Deze uitkomst wijst erop dat veel werknemers het gevoel hebben dat hun melding niet serieus wordt genomen of dat de juiste stappen niet worden gezet, wat een belangrijke belemmering vormt voor het melden van incidenten.

Een andere reden die frequent genoemd werd, met **14%**, is het gevoel dat melden ''toch geen zin heeft'' omdat er naar hun verwachting geen actie wordt ondernomen. Dit wijst op een bredere perceptie dat organisaties tekortschieten in het aanpakken van grensoverschrijdend gedrag, wat kan leiden tot een cultuur waarin incidenten niet worden gerapporteerd en daarmee onbestraft blijven.
Daarnaast gaf **13%** aan dat ze bang waren voor de mogelijke gevolgen van het melden. Ook wordt grensoverschrijdend gedrag vaak niet actief besproken binnen organisaties: **11%** gaf aan dat dergelijke kwesties niet gemakkelijk worden besproken of gemeld, wat suggereert dat in sommige werkomgevingen een cultuur heerst waarin dergelijke problemen eerder worden genegeerd dan aangepakt.
Andere obstakels die door respondenten werden genoemd zijn onder meer onduidelijkheid over de meldprocedure (**9%**), het gevoel dat de kwestie niet ernstig genoeg was (**7%**) of de angst voor het gebrek aan anonimiteit bij het melden (**7**%). Eerdere negatieve ervaringen met meldingen ontmoedigden **6%** van de respondenten en een ingewikkelde procedure werd als reden genoemd door **1%**.
Andere redenen die werden genoemd waren:

- Situaties waarin het gedrag slechts eenmalig plaatsvond of waarin de leidinggevende reeds op de hoogte was.
- Sommige medewerkers gaven er de voorkeur aan om zelf grenzen aan te geven, bijvoorbeeld door direct te reageren op het gedrag.
- De perceptie dat het gedrag nog relatief onschuldig was, zoals een collega die hen steeds 'schat' noemde in de chat, wat wel irritatie veroorzaakte maar geen aanleiding gaf tot officiële melding.

CONCLUSIE OORZAKEN EN MELDINGEN

De bevindingen van dit onderzoek tonen aan dat online grensoverschrijdend gedrag op de werkvloer sterk verweven is met structurele organisatorische factoren en een cultuur die onvoldoende preventief en corrigerend optreedt tegen dergelijke incidenten. Machtsdynamiek en hiërarchie binnen de organisatie worden door 20% van de respondenten als de grootste oorzaak genoemd. Dit benadrukt hoe een gebrek aan gelijkwaardigheid en transparantie bijdraagt aan een omgeving waarin online grensoverschrijdend gedrag kan floreren. Het tweede vaakst genoemde probleem is het ontbreken van sancties voor daders, wat aangeeft dat veel organisaties tekortschieten in het opleggen van consequenties bij grensoverschrijdend gedrag. Daarnaast wijzen respondenten op een gebrek aan toezicht en controle, evenals het ontbreken van duidelijke normen en protocollen, wat bijdraagt aan een onduidelijke gedragslijn voor medewerkers.

De onderzoeksresultaten laten zien dat werknemers om uiteenlopende redenen aarzelen om online grensoverschrijdend gedrag op de werkvloer te melden. De belangrijkste redenen zijn een gebrek aan vertrouwen in de reactie van HR en management, de verwachting dat er geen actie zal worden ondernomen, en angst voor mogelijke gevolgen. Daarnaast wijzen deze bevindingen op structurele uitdagingen binnen organisaties, zoals het gebrek aan heldere meldprocedures, het ontbreken van een cultuur waarin grensoverschrijdend gedrag openlijk besproken kan worden en negatieve ervaringen met eerdere meldingen.

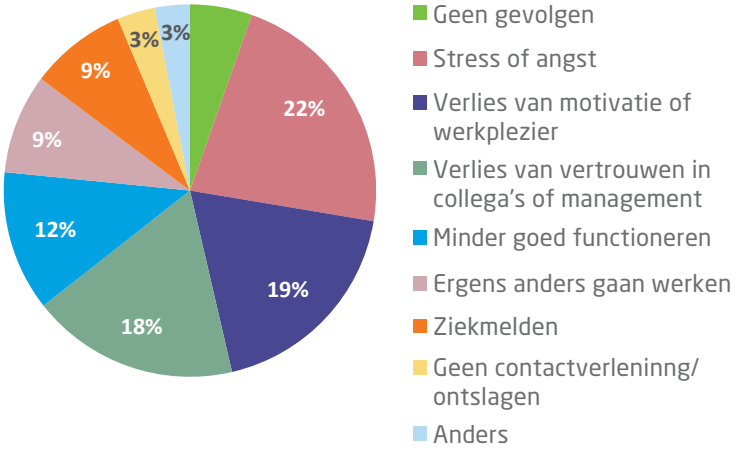
De meldingen die wél zijn opgepakt, resulteerden in een aantal van de gevallen in een gesprek met de dader vanuit de organisatie en slechts in 13% van de gevallen in daadwerkelijke maatregelen. Opvallend is dat 7% van de respondenten zelfs te horen kreeg dat zij moesten zwijgen over het incident, wat lijkt op het verdoezelen van incidenten in plaats van het aanpakken ervan. Bovendien werd in sommige gevallen gedreigd met rechtszaken wegens laster of gevraagd om de organisatie te verlaten.

Voor organisaties is het cruciaal om bewustwording te creëren over de beschikbaarheid en toegankelijkheid van meldingsprocedures, ervoor te zorgen dat meldingen serieus worden behandeld, en het vertrouwen te versterken dat medewerkers veilig en zonder repercussies melding kunnen maken van ongewenst gedrag.

5. DE GEVOLGEN

Uit eerder onderzoek van de FNV naar grensoverschrijdend gedrag uit 2023[36] blijkt dat de gevolgen heel ernstig kunnen zijn, niet alleen voor het slachtoffer zelf, maar ook voor de omgeving. Wanneer het slachtoffer uit dezelfde organisatie komt als de dader, zijn de gevolgen vaak groter dan wanneer de dader van buiten komt.

Gevolgen online GOG zelf meegemaakt

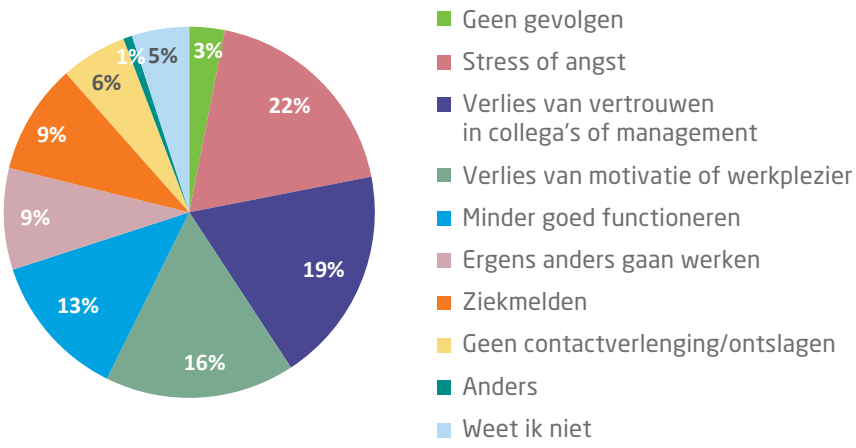


Uit de verzamelde gegevens van dit onderzoek blijkt dat online grensoverschrijdend gedrag niet alleen een effect heeft op het welzijn van medewerkers maar ook op hun carrière en werkprestaties. Van de respondenten die met dergelijke incidenten te maken kregen, geeft **95%** aan negatieve gevolgen te ervaren. De meest voorkomende reactie is stress of angst. Dit geeft een duidelijk signaal af over de impact van grensoverschrijdend gedrag op de mentale gezondheid van werknemers.

De tweede meest voorkomende impact is minder werkplezier en motivatie, gerapporteerd door **19%** van de respondenten. Daarnaast geeft **18%** van de respondenten aan dat hun vertrouwen in collega's of management hierdoor is aangetast. Dit verlies van vertrouwen kan verregaande gevolgen hebben voor de werksfeer en de samenwerking. Bovendien geeft 12% aan dat zij door de ervaring minder goed functioneren in hun rol.
Dit belemmert niet alleen hun persoonlijke groei en prestaties, maar heeft ook invloed op het functioneren van de organisatie als geheel.
Bijna **een op de 10** respondenten gaf aan dat hun negatieve ervaring hen ertoe aanzette om een andere functie te zoeken. Dit kan voor organisaties een signaal zijn dat grensoverschrijdend gedrag niet alleen invloed heeft op het huidige werkklimaat maar ook leidt tot verloop en het verlies van getalenteerde medewerkers. Verder heeft hetzelfde percentage zich ziekgemeld als gevolg van de ervaren incidenten, wat onderstreept hoe grensoverschrijdend gedrag de gezondheid en inzetbaarheid van medewerkers aantast.
Andere gevolgen, zoals ontslag of het niet verlengen van een contract (**3%**), laten zien hoe ernstig de impact kan zijn op loopbanen en inkomenszekerheid. Tevens geven respondenten aan door deze ervaringen aan zichzelf te twijfelen of in aanzien bij collega's te dalen. Voor een aantal was het online grensoverschrijdend gedrag de reden om op zoek te gaan naar een andere baan.

[36] FNV. 'Horen, zien en zwijgen: omgangsvormen op de werkvloer', oktober 2023.

Gevolgen online GOG bij anderen



Naast de groep die dit gedrag zelf heeft ervaren, is ook gekeken naar de gevolgen voor collega's die getuige zijn geweest van online grensoverschrijdend gedrag. Zij gaven aan welke gevolgen zij hebben gezien bij hun collega's. Hierbij geeft **3%** aan dat er geen gevolgen waren en **5%** weet het niet. Bij **92%** van de respondenten die het bij collega's zien, heeft dit gevolgen op de werkvloer.
De effecten die het vaakst worden genoemd door de getuigen komen overeen met die van de slachtoffers zelf.

Het overgrote deel van de mensen die te maken krijgen met online grensoverschrijdend gedrag ervaren hier negatieve gevolgen van. De effecten zoals stress, verminderde motivatie, minder goed functioneren en uiteindelijk zelfs ziekteverzuim en personeelsverloop, zorgen ervoor dat dit een probleem wordt dat de hele organisatie raakt. Het is dan ook van cruciaal belang dat werkgevers deze problemen serieus nemen.

CONCLUSIE GEVOLGEN

Uit de onderzoeksresultaten blijkt dat online grensoverschrijdend gedrag op de werkvloer een aanzienlijke negatieve impact heeft op de betrokken werknemers. Van de respondenten die dit soort incidenten hebben ervaren, rapporteert bijna iedereen negatieve gevolgen.
De meest voorkomende reactie onder respondenten is stress of angst. Dit wordt gevolgd door verminderde motivatie en werkplezier en het verlies van vertrouwen in collega's of management. Deze psychologische en sociale effecten laten zien dat grensoverschrijdend gedrag het gevoel van veiligheid en samenwerking ernstig kan aantasten.

Daarnaast blijkt uit de resultaten dat grensoverschrijdend gedrag een directe invloed heeft op de prestaties en het functioneren van medewerkers: zo kan het vermogen om goed te presteren verminderen of besluiten respondenten om een andere baan te zoeken. Bovendien heeft bijna een op de 10 zich ziekgemeld na online grensoverschrijdend gedrag. Dit heeft niet alleen gevolgen voor de betrokken individuen maar ook voor de organisaties waarin zij werkzaam zijn.
Ten slotte wijzen de resultaten op mogelijke carrière-impact, zo zijn er een aantal respondenten die gemeld hebben dat zij hun baan verloren of dat hun contract niet werd verlengd door de nasleep van grensoverschrijdend gedrag. Dat illustreert hoe ernstig de effecten kunnen zijn op zowel de loopbaan als de financiële zekerheid van slachtoffers.

6. WAT WORDT ER NU AL GEDAAN?

Nu er een duidelijk beeld is van wat online grensoverschrijdend gedrag is, hoe vaak en bij wie het voorkomt en wat de oorzaken en gevolgen zijn, kijken we nu naar welke maatregelen er al zijn om het tegen te gaan.

In de Arbeidsomstandighedenwet staat dat werkgevers de zorgplicht hebben om werknemers zoveel mogelijk te beschermen tegen psychosociale arbeidsbelasting (PSA). Onder deze arbeidsbelasting valt grensoverschrijdend gedrag. Werkgevers moeten dus beleid maken om PSA te voorkomen of te beperken. De wet schrijft voor dat werkgevers arbeidsrisico's gedetailleerd in kaart brengen in een risico-inventarisatie en -evaluatie (RI&E). In het bijbehorende plan van aanpak komen vervolgens de maatregelen te staan.[37]

Een belangrijk onderdeel van dit plan is het aanstellen van één of meerdere vertrouwenspersonen, waar werknemers veilig en in vertrouwen meldingen kunnen doen. Ook kan een klachtencommissie worden ingesteld om klachten onafhankelijk en serieus te behandelen. Het is bovendien essentieel dat medewerkers geïnformeerd worden over deze mogelijkheden, zodat ze weten waar ze terecht kunnen en welke stappen ze kunnen verwachten als ze een melding maken.

De zorgplicht van de werkgever verplicht hen om in te grijpen bij bekendheid van grensoverschrijdend gedrag. Als de werkgever op de hoogte is, of redelijkerwijs had moeten zijn, van grensoverschrijdend gedrag dan moet deze passende maatregelen treffen. Voor gevallen waarbij een leidinggevende betrokken is, ligt de verantwoordelijkheid direct bij de werkgever, die verplicht is deze situatie adequaat aan te pakken om de veiligheid op de werkvloer te herstellen en te waarborgen.

Naast het voorkomen en verhelpen van grensoverschrijdend gedrag, hebben werkgevers ook de verplichting om klachten hierover zorgvuldig te behandelen. Dit betekent dat een klacht snel, vertrouwelijk en met hoor- en wederhoor moet worden afgehandeld. De klager moet eveneens worden geïnformeerd over de uitkomst van het onderzoek en de genomen acties. Transparante communicatie over de voortgang en resultaten van klachtenprocedures is daarbij cruciaal om het vertrouwen van werknemers in het beleid te behouden.

Werknemers die melding maken van grensoverschrijdend gedrag hebben recht op bescherming tegen benadeling. Dit staat bekend als het verbod op victimisatie. Dit houdt in dat een werknemer geen negatieve gevolgen mag ondervinden als die een klacht heeft ingediend. Er kan bijvoorbeeld sprake zijn van victimisatie als een contract van een klager niet wordt verlengd of diegene na een melding wordt gepest op de werkvloer.[38]

Uit het FNV-onderzoek naar grensoverschrijdend gedrag van 2023[39] komt duidelijk naar voren dat er grote gebreken zijn in het beleid op het gebied van sociale veiligheid in veel organisaties. Bijna de helft van de respondenten geeft aan ontevreden te zijn over de huidige maatregelen. Dit wijst erop dat werkgevers er nog onvoldoende in slagen een veilige werkomgeving te bieden, vooral in het licht van online grensoverschrijdend gedrag.

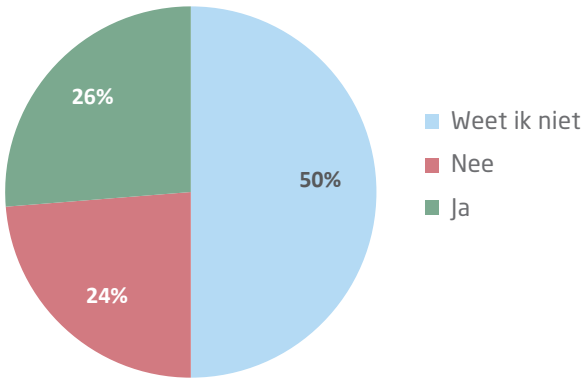
Daarnaast blijkt dat **57%** van de werknemers nooit voorlichting heeft ontvangen over sociale veiligheid, terwijl het verstrekken hiervan wettelijk verplicht is. Dit tekort aan basisvoorlichting maakt medewerkers kwetsbaarder omdat ze vaak niet weten hoe ze online grensoverschrijdend gedrag kunnen herkennen, voorkomen of melden. Wanneer zich binnen een organisatie daadwerkelijk grensoverschrijdend gedrag voordoet, blijkt bovendien dat in **47%** van de gevallen niet of onvoldoende wordt opgetreden. Dit tekort in de aanpak versterkt het gevoel van onveiligheid en kan het risico op herhaling van ongewenst gedrag vergroten.

[37] SER. 'Dossier Grensoverschrijdend Gedrag'.
[38] College Voor de Rechten van de Mens. 'Zorgplicht werkgevers bij seksuele intimidatie: wat houdt het in en wat kan er beter?', 20-12-2023. https://www.mensenrechten.nl/actueel/toegelicht/toegelicht/2023/zorgplicht-werkgevers-bij-seksuele-intimidatie-wat-houdt-het-in-en-wat-kan-er-beter
[39] FNV. 'Horen, zien en zwijgen: omgangsvormen op de werkvloer', oktober 2023.

BELEID ONLINE GRENSOVERSCHRIJDEND GEDRAG

Wat betreft specifiek beleid tegen online grensoverschrijdend gedrag, zijn de uitkomsten uit dit onderzoek eveneens zorgwekkend. De helft van de respondenten weet niet of hun werkgever over een beleid beschikt voor online grensoverschrijdend gedrag. Dit geeft aan dat er vaak geen heldere communicatie is over dergelijke protocollen. Bij iets meer dan een kwart van de werknemers blijkt dit beleid wel aanwezig, maar iets minder dan een kwart geeft ook aan dat hun werkgever geen enkel beleid heeft om online grensoverschrijdend gedrag te voorkomen of aan te pakken.

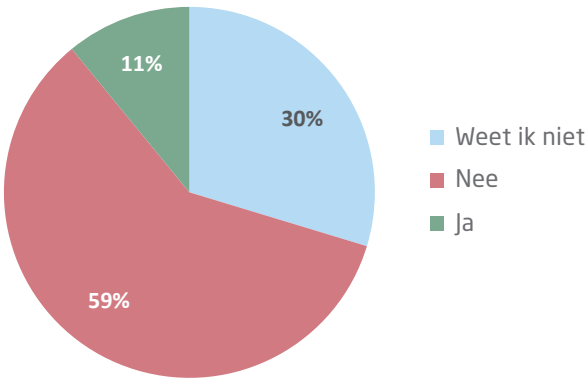
Beleid online GOG



Uit de antwoorden op de open vraag naar bestaand beleid tegen online grensoverschrijdend gedrag blijkt dat organisaties verschillende maatregelen hanteren. Veelvoorkomende beleidsstukken en maatregelen zijn onder meer een gedragscode, sanctiebeleid, een protocol psychosociale arbeidsbelasting (PSA) en een stappenplan met preventieve en reactieve maatregelen. Ook zien we bij sommige organisaties een dossieropbouw van daders en een zero-tolerance-beleid, wat aangeeft dat grensoverschrijdend gedrag direct en serieus wordt aangepakt. Daarnaast worden een onafhankelijke vertrouwenspersoon en een intern HR-onderzoek genoemd die werknemers kunnen ondersteunen en klachten kunnen onderzoeken.

Toch blijkt uit de respons op de vraag of werkgevers voldoende maatregelen nemen dat er nog veel ruimte voor verbetering is. Meer dan de helft van de respondenten gaf aan dat hun werkgever volgens hen niet genoeg doet om online grensoverschrijdend gedrag tegen te gaan. Daarnaast weet bijna eenderde niet precies wat hun werkgever doet om dit probleem aan te pakken, wat kan duiden op gebrekkige communicatie over bestaande maatregelen. Slechts een op de tien respondenten ervaart dat hun werkgever voldoende maatregelen neemt.

Maatregelen voldoende?



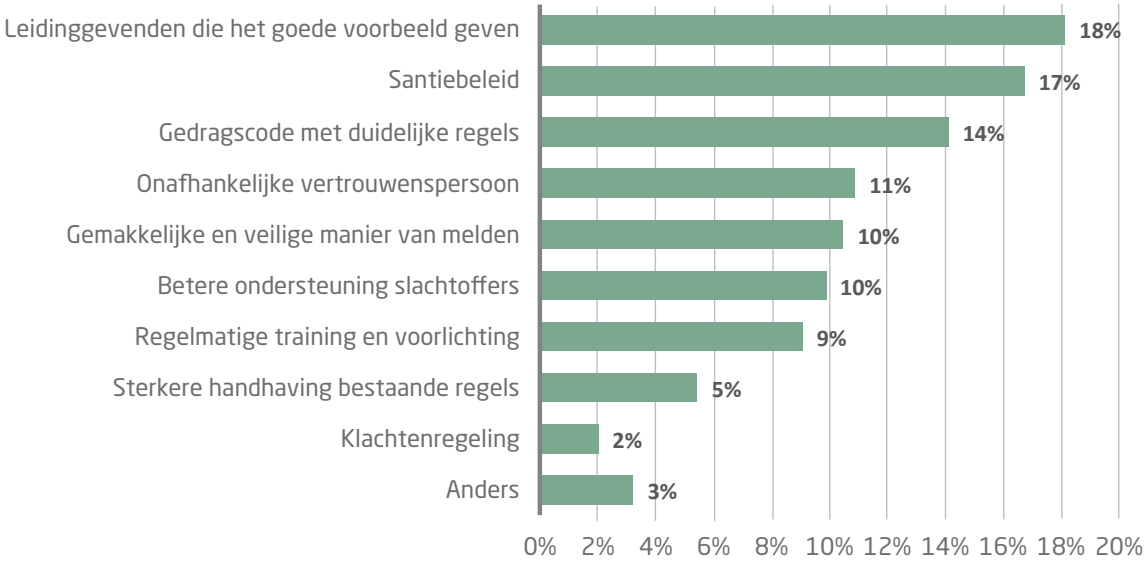
CONCLUSIE HUIDIG BELEID

De uitkomst van dit onderzoek wijst dus aanzienlijke verbeterpunten aan. Een groot deel van de werknemers voelt zich onvoldoende beschermd tegen online grensoverschrijdend gedrag. Opvallend is dat de helft van de deelnemers niet weet of hun werkgever überhaupt beleid heeft op dit gebied. Dit wijst op een gebrek aan communicatie over bestaande maatregelen en protocollen, wat de effectiviteit van het beleid sterk kan ondermijnen.
Werkgevers kunnen daarom nog veel winst behalen door niet alleen hun beleid en protocollen te verbeteren, maar ook door medewerkers beter te informeren en bewust te maken van de bestaande middelen en steun die beschikbaar is.

7. MAATREGELEN TEGEN ONLINE GRENSOVERSCHRIJDEND GEDRAG

Met de opkomst van thuiswerken en digitale werkvormen zijn niet alleen nieuwe manieren van samenwerken ontstaan, maar ook nieuwe vormen van grensoverschrijdend gedrag. Dit online grensoverschrijdend gedrag vormt een toenemende uitdaging op de werkvloer, met duidelijke gevolgen voor de mentale gezondheid en het welzijn van werknemers. Maar wat kunnen we eraan doen? En welke maatregelen zien werknemers zelf graag om dit probleem aan te pakken? Dit onderzoek geeft inzicht in de ervaringen en wensen van werknemers, en biedt aanknopingspunten voor bedrijven om een veilige, respectvolle digitale werkomgeving te creëren.

GEWENSTE MAATREGELEN



Uit het onderzoek blijkt dat respondenten verschillende maatregelen belangrijk vinden om online grensoverschrijdend gedrag op de werkvloer te voorkomen. De meest gekozen maatregel, door **18%** van de respondenten, is dat leidinggevenden een actieve rol nemen door zelf het goede voorbeeld te geven en effectief op te treden tegen grensoverschrijdend gedrag. Deze bevinding benadrukt het belang van een positieve voorbeeldfunctie en proactieve aanpak door leidinggevenden, die essentieel worden geacht om een veilige online werkomgeving te bevorderen.
Daarnaast geeft **17%** van de respondenten aan behoefte te hebben aan een helder sanctiebeleid waarin de consequenties voor grensoverschrijdend gedrag duidelijk staan beschreven. Dit geeft aan dat medewerkers behoefte hebben aan structurele en consequente handhaving van gedragsnormen, waarbij duidelijk is welke acties worden ondernomen bij overtredingen.
De top drie wordt afgesloten met de wens voor een duidelijke gedragscode (**14%**), waarin concrete gedragsregels staan vastgelegd. Dit wijst op een behoefte aan richtlijnen die helder communiceren wat acceptabel en onacceptabel gedrag is in de online werksfeer.

Andere maatregelen die in het onderzoek werden genoemd.

- Toegang tot een onafhankelijke vertrouwenspersoon (11%). Dit biedt medewerkers een veilige plek om grensoverschrijdend gedrag te melden zonder angst voor repercussies.
- Gemakkelijke en veilige meldingsprocedures (10%). Deze maatregel laat zien dat medewerkers meer mogelijkheden willen om incidenten te rapporteren.
- Betere ondersteuning voor slachtoffers (10%). Naast preventie vinden respondenten het ook belangrijk dat slachtoffers goede ondersteuning ontvangen.

- Regelmatige trainingen en voorlichting (9%). Dit wijst op de noodzaak van bewustwording en gedragsverandering om een respectvolle digitale cultuur te bevorderen.
- Sterkere handhaving van bestaande regels (5%). Hieruit blijkt dat men soms twijfelt aan de huidige naleving van bestaande regels.
- Een klachtenregeling (2%). Hoewel minder vaak genoemd, geeft dit aan dat sommigen een formeel kanaal willen om klachten te uiten.

Verder werden enkele specifieke suggesties aangedragen, waaronder het verbieden van het gebruik van mobiele telefoons tijdens werktijd, het implementeren van een 'zero tolerance'-beleid bij recidive, extra begeleiding voor slachtoffers en meer toezicht op leidinggevenden.

OPLOSSINGSRICHTINGEN

De respondenten is ook gevraagd naar wat zij goede oplossingsrichtingen vonden. Daar kwamen sterke aanbevelingen uit. Er is behoefte aan meer en duidelijke, toegankelijke en structurele maatregelen tegen online grensoverschrijdend gedrag. Daarbij is een proactieve houding van leidinggevenden en heldere richtlijnen in de vorm van sanctiebeleid en gedragscodes een voorwaarde om te zorgen dat ook de online werkvloer veilig is. Andere oplossingsrichtingen die worden aangegeven zijn goed te benaderen vertrouwenspersonen, trainingsprogramma's en ondersteuning. De combinatie van zowel preventieve als ondersteunende maatregelen kunnen bijdragen aan een veilige en respectvolle online werkomgeving.

Uit de antwoorden van de respondenten blijkt ook dat vakbonden belangrijk zijn in het aanpakken van online grensoverschrijdend gedrag op de werkvloer. Dat kan de vakbond doen door zich nadrukkelijk uit te spreken voor een veilige online werkvloer en het onderwerp hoog op de agenda te plaatsen van sociale partners. Zoals ook is gebleken bij onderzoeken door de FNV naar grensoverschrijdend gedrag kan het openbaar maken van incidenten, het creëren van aandacht en het maken van afspraken in cao's door vakbonden essentieel zijn om te zorgen dat een werkvloer veiliger wordt.

Omdat deze vormen van grensoverschrijdend gedrag nog zo onbekend zijn, is het nodig om bewustwordingscampagne te voeren over wat je moet doen als je het overkomt of opmerkt in bijvoorbeeld Whatsappgroepen waar je lid van bent. Er wordt verder gepleit voor een versterkte ondersteuning voor werknemers die hiermee te maken hebben. Vakbonden kunnen hun leden bijstaan in gesprekken met leidinggevenden, zodat de meldingen serieus genomen worden. Er is ook behoefte aan een hulplijn, waar werknemers discreet hun verhaal kunnen doen en advies kunnen krijgen over vervolgstappen. De FNV biedt de vertrouwenstelefoon aan, waar iedereen die te maken heeft met grensoverschrijdend gedrag op de werkvloer terecht kan, zowel leden als niet-leden.[40]

Daarnaast geven respondenten aan dat het bijhouden van incidenten per bedrijf zou kunnen helpen bij het inzichtelijk maken van de omvang en frequentie van grensoverschrijdend gedrag. Een onafhankelijk onderzoek zou op basis van deze gegevens een goed beeld kunnen geven van patronen en structurele knelpunten binnen verschillende organisaties en sectoren. Specifieke onderzoeken naar onveilige werkculturen worden als een belangrijk aandachtspunt genoemd.

Tot slot benadrukken respondenten dat grensoverschrijdend gedrag vaak subtiel en op het eerste gezicht onbeduidend kan lijken, maar dat de impact op de lange termijn ernstig kan zijn voor zowel de slachtoffers als de organisatiecultuur. Kleine, onopgemerkte incidenten kunnen escaleren en bijdragen aan een onveilige werkomgeving. Daarom is het belangrijk dat er bij de eerste signalen meteen een streep wordt getrokken door leidinggevenden en collega's; zo kunnen we samen werken aan een veilige werkcultuur in Nederland voor iedereen.

[40] FNV. 'Vertrouwenstelefoon', https://www.fnv.nl/service-contact/vertrouwenstelefoon

CONCLUSIE GEWENSTE MAATREGELEN

Uit het onderzoek blijkt dat werknemers duidelijk gedefinieerde en proactieve maatregelen verwachten om online grensoverschrijdend gedrag op de werkvloer tegen te gaan. De meest gekozen maatregel is dat leidinggevenden een actieve rol oppakken. Dit houdt in dat zij niet alleen als voorbeeld moeten dienen maar ook daadkrachtig moeten optreden bij grensoverschrijdend gedrag. Dit onderstreept de behoefte aan een cultuur waarin leiderschap niet alleen regels stelt maar deze ook zichtbaar naleeft en handhaaft.

Daarnaast geven respondenten aan dat een helder en goed gestructureerd sanctiebeleid nodig is. Door duidelijke consequenties vast te leggen voor grensoverschrijdend gedrag kan een afschrikwekkend effect worden gecreëerd en ontstaat er een klimaat waarin duidelijk is dat dergelijk gedrag niet wordt getolereerd. Ook is er de wens voor een concrete gedragscode, waarin gedetailleerde gedragsregels worden opgenomen. Deze code helpt niet alleen werknemers te informeren over wat wel en niet acceptabel is, maar fungeert ook als een referentiekader voor de hele organisatie.

Naast deze drie prioriteiten, zien de respondenten ook graag toegang tot een onafhankelijke vertrouwenspersoon om vertrouwelijke gesprekken te kunnen voeren. Gemakkelijke en veilige meldingsprocedures werden eveneens hoog gewaardeerd, omdat hiermee de drempel om incidenten te rapporteren wordt verlaagd. Betere ondersteuning voor slachtoffers is ook een noodzakelijke maatregel.
Bovendien zijn er oproepen voor regelmatige trainingen en voorlichting om het bewustzijn te vergroten en medewerkers te informeren over grensoverschrijdend gedrag en hoe dit te voorkomen. Tot slot noemden respondenten de handhaving van bestaande regels en een klachtenregeling als aanvullende maatregelen.

Uit de antwoorden van de respondenten blijkt dat proactieve actie vanuit de vakbond om online grensoverschrijdend gedrag op de werkvloer onder de aandacht brengen gewenst is. Dit omvat initiatieven om incidenten publiekelijk te maken, aandacht en bewustwording te creëren en de bespreekbaarheid van grensoverschrijdend gedrag actief te bevorderen.

Daarnaast is er vraag naar cursussen en trainingen, die niet alleen werknemers maar ook leidinggevenden ondersteunen bij het herkennen en effectief aanpakken van online grensoverschrijdend gedrag, met speciale aandacht voor de subtiele vormen die via digitale kanalen plaatsvinden.

AANBEVELINGEN

De FNV wil dat een veilige werkvloer en gelijke behandeling voor iedereen de standaard wordt. Sociale en fysieke veiligheid en gelijke kansen moeten gegarandeerd en verankerd zijn in beleid.
Werkgevers zijn wettelijk verplicht de sociale en fysieke veiligheid van werknemers te garanderen. Uit tal van onderzoeken weten we dat dit nog lang geen realiteit is.
Het kabinet is van plan het Nationaal Actieprogramma Aanpak grensoverschrijdend gedrag uit te voeren, wat de FNV ondersteunt. Hierin is online grensoverschrijdend gedrag ook opgenomen.
De FNV pleit onder andere voor het verplichten van een gedragscode met sanctiebeleid, klachtenregeling en onafhankelijke en deskundige vertrouwenspersoon. De FNV maakt zich hier hard voor; bij de politiek in Den Haag, bij werkgevers en bij werknemers. Ook biedt de FNV een luisterend oor voor slachtoffers door de vertrouwenstelefoon. En heeft de FNV gezorgd voor omstanderstrainingen zodat werkenden beter in staat zijn om zelf in te grijpen bij het zien van grensoverschrijdend gedrag. De FNV heeft ook gezorgd voor OR scholing over sociale veiligheid.

Aanvullend daarop zijn er nog een aantal aanbevelingen voor werkgevers als het gaat om online grensoverschrijdend gedrag tegen te gaan. Het is de verantwoordelijkheid van de werkgever om te zorgen voor een veilige werkomgeving. Uit de uitkomsten van het onderzoek blijkt dat dit onvoldoende lukt. Daarom zes concrete aanbevelingen aan werkgevers om (online) grensoverschrijdend gedrag op de werkvloer tegen te gaan.

1. Ontwikkel en implementeer sanctiebeleid

- Zorg voor een helder beleid tegen grensoverschrijdend gedrag, met duidelijke definities en protocollen. Hierin moet ook aandacht worden besteed aan online grensoverschrijdend gedrag. Grensoverschrijdend gedrag mag niet worden getolereerd en de organisatie moet zich inzetten voor het creëren van een omgeving waarin iedereen zich gerespecteerd en gewaardeerd voelt. Daarnaast moet dit beleid actief worden gecommuniceerd met alle werknemers.
- Zorg dat directies en leidinggevenden goed worden getraind als verantwoordelijken voor het uitdragen en uitvoeren van het beleid. Neem disciplinaire maatregelen tegen leidinggevenden die zich schuldig maken aan grensoverschrijdend gedrag en niet optreden tegen grensoverschrijdend gedrag.

2. Het opnemen van online grensoverschrijdend gedrag in de RI&E en PvA

Werkgevers zijn verplicht een risico-inventarisatie en -evaluatie en plan van aanpak te maken. Nadat de werkgever heeft vastgesteld welke risico's werknemers lopen op de werkvloer wordt er een lijst van maatregelen opgesteld om die risico's aan te pakken. Online grensoverschrijdend gedrag moet als risico worden gezien en hier moet beleid op worden ontwikkeld. Maak het concreet en neem maatregelen om deze zoveel mogelijk bij de bron aan te pakken in het eveneens verplichte plan van aanpak.

3. Een onafhankelijk klachtencommissie

Elke melding van grensoverschrijdend gedrag moet worden onderworpen aan een onpartijdig onderzoek. Er moeten toepasselijke sancties zijn. De ernst van de sancties moet voldoende zijn om toekomstig wangedrag af te schrikken.

4. Versterk meldprocedures en vertrouwensmechanismen

- Zorg voor deskundige en onafhankelijke vertrouwenspersonen in alle organisaties, ongeacht de grootte. Kleine organisaties zouden dit branchegewijs kunnen organiseren.
- Introduceer daarnaast laagdrempelige en veilige meldkanalen, zoals anonieme hulplijnen. Neem werkenden die melding maken van grensoverschrijdend gedrag altijd serieus en bied hun een luisterend oor en zorg voor effectieve opvolging van de melding.
- Bied training aan HR, leidinggevenden en vertrouwenspersonen om meldingen professioneel en empathisch te behandelen. Zorg altijd voor opvolging.

5. Stimuleer bewustwording en voorlichting

Voorlichting is wettelijk verplicht maar veel werknemers geven aan die nooit te ontvangen. Werkgevers moeten campagnes voeren om de impact van (online) grensoverschrijdend gedrag zichtbaar te maken. Organiseer workshops en trainingen om werknemers en leidinggevenden te leren hoe ze grensoverschrijdend gedrag kunnen herkennen en aanpakken.

6. Bevorder een veilige werkcultuur

Implementeer een systeem van sancties om grensoverschrijdend gedrag effectief aan te pakken.
Volg meldingen consequent op en geef transparantie over de genomen maatregelen. Dit zorgt er ook voor dat het vertrouwen in meldingen omhoog gaat.
Creëer een omgeving waarin het bespreekbaar maken van grensoverschrijdend gedrag wordt aangemoedigd. Richt aandacht op machtsdynamieken en diversiteit binnen de organisatie om een inclusieve cultuur te bevorderen. Zorg voor opvang en nazorg bij slachtoffers.
Voor zowel de cultuuraanpak als de meldprocedure kan gebruik worden gemaakt van de Handreiking Meldingen van seksueel grensoverschrijdend gedrag op de werkvloer.[42]

Als werknemer zijn er ook een aantal dingen die je kan doen. Hierbij kan je onderscheid maken tussen omstander, slachtoffer en OR-lid. Zie hiervoor de stappenplannen op onze **pagina grensoverschrijdend gedrag**.
Omstander: herken grensoverschrijdend gedrag, spreek degene aan die grensoverschrijdend gedrag vertoont, steun je collega die grensoverschrijdend gedrag overkomt, bespreek het grensoverschrijdend gedrag met collega's, bespreek het gedrag met leidinggevende en/of de OR.
Slachtoffer: trek een grens, bespreek het grensoverschrijdend gedrag dat jou is overkomen, leg alle gebeurtenissen vast, doe een melding, dien een klacht in, achterhaal het werkgeversbeleid, zet juridische stappen.
OR: initiatief nemen preventief beleid, werkwijze RI&E beïnvloeden, meebeslissen bedrijfsbeleid (klachtenprocedure, sanctiebeleid, gedragscode) invloed benoeming vertrouwenspersoon, toezicht houden naleving cao.

[42] Regeringscommissariaat seksueel grensoverschrijdend gedrag en seksueel geweld. 'Handreiking voor cultuurverandering op de werkvloer: Over preventie en de aanpak van seksueel grensoverschrijdend gedrag', 13 maart 2024.

241634