

Vrijheid van online-meningsuiting?



LISA Law & ICT
Students' Association

Brinkhof

ADVOCATEN

**Hogan
Lovells**

NORD

ADVOCATEN

HOOFDREDACTEUR
Patrick van de Wetering

**REDACTEUR/
VORMGEVER**
Lisa Celine Helfrich

**REDACTEUR/
SECRETARIS**
Luuk Wassink

REDACTEUR
Marit Jeeninga

REDACTEUR
Daniel Colenbrander



v.l.n.r. Luuk, Marit, Patrick, Lisa Celine, Daniel

VOORWOORD

HOOFDREDACTEUR

Beste lezer,

Voor u ligt het laatste wat de redactiecommissie 2018/2019 heeft geschreven. Het vierde en laatste e-magazine van dit jaar. Na vele artikelen, blogs en verslagen komt ons jaar ten einde.

Ook voor dit blad kan ik weer met gepaste trots dit magazine inluiden. Dit keer zijn we het uiten online gaan verkennen. Mag alles zomaar geuit worden online? Zijn er grenzen? Kunnen platforms aansprakelijk zijn? Heeft een werkgever houvast als zijn werknemer zich negatief uit?

Stuk voor stuk interessante onderwerpen die wij de afgelopen tijd hebben uitgespit en op papier hebben gezet.

Zoals altijd wil ik iedereen bedanken voor zijn of haar inzet bij het totstandbrengen van het vierde en laatste e-magazine van het jaar 2018/2019.

Als laatste wil ik mijn commissiegenoten bedanken die het hele jaar door interessante stukken hebben weten neer te zetten!

Veel leesplezier.

Namens de redactiecommissie,

Patrick van de Wetering
Hoofdredacteur Redactiecommissie 2018/2019

5	Uiten op het internet en moderne delicten
11	Verantwoordelijkheden van platformen
19	Ontslagen wegens Facebook bericht?
24	Interview redactie
26	Nawoord

Uiten op het internet en moderne delicten



Alles gaat tegenwoordig snel en het liefst ook nog digitaal. Contact vindt plaats in een fractie van een seconde via Whatsapp, een foto is zo geüpload op Instagram, symptomen van een infectie worden zo opgezocht en die vervelende buurman van je maak je online met een simpel getikt bericht even flink zwart. Hij besloot namelijk gisternacht nog doodleuk het gras te gaan maaien. Vrijheid van meningsuiting toch?

Dit doet natuurlijk niet iedereen. Sterker nog, het lijkt mij de normaalste zaak van de wereld om dit niet te doen. Toch komt het vaker voor dan je verwacht. De cijfers op het gebied van discriminatie op het internet waren in 2018 uitdrukkelijk lager dan de jaren ervoor. Echter, ook werd bekend dat dit een gevolg was van

online platformen die steeds actiever discriminerende uitingen weren of verwijderen.¹ Dat het vaker voorkomt dan verwacht kan veel oorzaken hebben. Wat een vanzelfsprekende oorzaak is, is mijns inziens de gemakkelijkerheid die erbij komt kijken. Via de smartphone of achter de computer voel je je al snel 'veilig' in die zin dat je de consequenties niet overziet. Wanneer gaat het te ver? Zijn er specifieke beledigingen waar echt actie voor ondernomen moet worden? Wat zegt de wet hier momenteel over?

¹ Discriminatiecijfers in 2018. Een rapport over registraties van discriminatie-incidenten door de politie, en meldingen bij antidiscriminatievoorzieningen en andere organisaties in Nederland, 2019, p. 49.

Strafbaar uiten

We uiten ons vrijwel allemaal via het internet. Of we nou een reactie achterlaten op een foto of een product, een bericht liken of zelfs onze teamgenoot uitschelden in een online spel, we uiten ons allemaal. Er zijn genoeg variaties denkbaar. Een paar variaties van strafbare uitingen zijn de volgende:

Smaad en laster:

Allereerst hebben we smaad en laster uit de artikelen 261 en 262 van het wetboek van strafrecht (Sr). Smaad houdt in dat je iemands eer of goede naam aanrandt met het kennelijke doel om daaraan ruchtbaarheid te geven. Dat komt neer op iemand zijn goede naam aantasten met als doel dat in het openbaar te doen. Laster komt op vrijwel hetzelfde neer, alleen bestaat bij laster een extra component, namelijk het bewust zijn van het feit dat wat je verspreidt, in strijd met de waarheid is. In het verleden is er op het gebied van smaad al een arrest gewezen door de Hoge Raad met betrekking tot wanneer het nou 'in het openbaar is' op het internet.² Het ging in dat arrest om het platform Hyves, en dan specifiek een Hyves-pagina waar 20 á 25 mensen lid van waren. Op die pagina waren uitingen gedaan die vielen onder smaad en de Hoge Raad besliste dat er, ondanks dat het een besloten groep was, voldaan was aan het gedeelte 'ruchtbaarheid'.

² HR 5 juli 2011, ECLI:NL:HR:2011:-BQ2009 (Ruchtbaarheid via Hyves)

Belediging en bedreiging:

In de wet zijn belediging en bedreiging strafbaar gesteld. Belediging kan online, om het zo maar te zeggen, eenvoudig worden toegepast. Wat ik daarmee bedoel is dat het 'oude' (oorsprong 1881)³ artikel 266 Sr erg goed mee gaat in de digitale wereld. Het omschrijft namelijk elke opzettelijke belediging in het openbaar of persoonlijk, mondeling, bij geschrift of afbeelding. De praktijk heeft uitgewezen dat dit in een online context ook toepasbaar kan zijn. Nog niet zo heel lang geleden zijn er veroordelingen geweest van eenvoudige belediging. Voorbeelden zijn het beledigen van Sylvana Simons op Facebook⁴ en een veroordeling omtrent de Zwarte Pietendiscussie waarbij er ook werd beledigd via Facebook.⁵

Bedreiging, artikel 285 Sr, is in de online context ook goed toepasbaar en kent hierbij ook genoeg voorbeelden. Iemand die hier veelvuldig gebruik van maakt is politicus Geert Wilders. In 2011 kreeg hij nog gelijk toen iemand een bericht had getweet en kwam het tot een veroordeling wegens bedreiging.⁶ Een aantal jaar later lukte dat

³ A.L.J.M. Janssens, De ontwikkeling van de strafbare belediging in het WvSr van 1881 (diss. Groningen RUG; Strafbare belediging) (online publiek); zie ook art. 266 Wetboek van Strafrecht.

⁴ Rb. Amsterdam 18 mei 2017, ECLI:NL:RBAMS:2017:3393.

⁵ Rb. Amsterdam 22 november 2018, ECLI:NL:RBAMS:2018:8299.

⁶ Rb. Den Haag 9 juni 2011, ECLI:N-

echter niet. In 2014 werd er door de Hoge Raad gezegd dat er meer is vereist dan dat een verdachte een bedreiging op Twitter heeft gezet. Het verweer van de verdachte kwam erop neer dat deze niet had verwacht dat Geert Wilders de tweet ook daadwerkelijk zou lezen en dat bij hem de daadwerkelijke vrees zou ontstaan dat hij zijn leven zou verliezen. Dat was namelijk niet de bedoeling van de verdachte.⁷

Problemen online

Dat uitingsdelicten tegenwoordig makkelijk te plegen zijn via het internet is eenieder vast bekend. Het probleem ermee is dat het niet onderschat moet worden. Dit beschrijven prof. dr. B.J Koops en mr. dr. J.J. Oerlemans in Strafrecht en ICT.⁸ Zo wordt uiteengezet dat in 2013

L:RBSGR:2011:BQ7588.

7 HR 7 oktober 2014, ECLI:N-L:HR:2014:2916.

8 B.J Koops en J.J. Oerlemans, Strafrecht en ICT. (Monografieën en Recht en Informatietechnologie), Den Haag: SDU 2019.

er dagelijks ongeveer 35.000 bedreigingen via twitter worden geuit en dat de politie ongeveer 200 daarvan natrekt.⁹ Dit aantal zal naar mijn mening de laatste tijd alleen maar zijn gestegen, maar wellicht tegelijkertijd ook zijn verminderd, gezien de actieve houding van platformen. Steeds meer platformen hanteren namelijk een zogenoemd 'notice-and-takedown'-beleid (NTD). Dit houdt in dat wanneer er onrechtmatige informatie, misbruik van copyright of discriminatie op een bepaald platform staat, degene die zich daartegen wil gaan verzetten, gebruik kan maken van NTD.¹⁰ De verzetter doet een melding bij diegene die de onrechtmatige informatie op een platform heeft gezet. Als niet bekend is wie dat is (wat natuurlijk vaak voorkomt op het internet) dan wordt de tussenpersoon, het platform zelf bijvoorbeeld, 'genoticed' en zal via het platform

9 NOS, "200 ernstige dreigtweets per dag", 31 oktober 2013, online via: <https://nos.nl> (laatst geraadpleegd op 17 mei 2019).

10 NTD, Veel gestelde vragen, online via: <https://noticeandtakedowncode.nl> (laatst geraadpleegd op 17 mei 2019).



Brinkhof

ADVOCATEN

Hogan
Lovells

N O R D

ADVOCATEN

E-MAGAZINE 7

de onrechtmatige informatie worden verwijderd. Naast het NTD heb je ook een notice-and-staydown (NSD) beleid. Dit gaat nog een stap verder dan NTD. Nadat iets van het internet af is gehaald (takedown), zal het in de toekomst niet meer geüpload mogen worden (staydown).¹¹

Veel kritiek wordt ergeuit op notice-and-takedown en voornamelijk op NSD. De problemen die geschetst worden zijn dat het recht op privacy wordt geschonden, maar ook dat de vrijheid van meningsuiting ernstig wordt ingeperkt.¹² De angst bestaat dat het uiten van je mening aan banden wordt gelegd. Romero-Moreno legt uit dat keuzes van NSD-systemen gebaseerd zijn op software en database matches in plaats van menselijke interactie. Oftewel als een systeem in zijn software/database heeft staan dat een bepaalde uitspraak 'niet kan', dan kan het zo zijn dat dit direct naar beneden wordt gehaald of zelfs het platform niet haalt. Als iemand uitleg of voorbeelden wilt geven in een bepaalde context, zonder daarmee beledigend of discriminerend te zijn, dan kan een systeem dat opvatten als een belediging of iets discriminerends en zal deze het niet toelaten op het platform. Dat lijkt mij natuurlijk niet de

bedoeling, maar is wel een reëel beeld. Automatische systemen missen namelijk nog steeds dat stukje 'menselijkheid' om de juiste keuzes te maken.

Terug naar het onderwerp. Er kleeft immers nog een groot probleem aan de uitingsdelicten online, namelijk de anonimiteit. Zoals al eerder gezegd voelen mensen zich al snel 'veilig' achter hun scherm. Met name de oproep omtrent het privacyvraagstuk om meer aan je privacy te denken en zo anoniem mogelijk te zijn speelt een rol. Aan de ene kant is het natuurlijk heel mooi, en je goed recht, om een Virtual Private Network (VPN) aan te schaffen, die ervoor zorgt dat je anoniem op het web kan surfen. Het zorgt er namelijk voor dat je een tijdelijk ip-adres krijgt zodat je echte ip-adres verborgen blijft. Dat is erg handig, maar heeft ook een keerzijde. Online criminelen gebruiken het ook¹³ en het lijkt me niet ondenkbaar dat mensen die de intentie hebben om te beledigen, te discrimineren of haat te zaaien dit ook gebruiken. Ze hebben doorgaans niet de intentie om er ook nog voor opgepakt te worden. Dit is een groot probleem voor opsporingsambtenaren. Ze krijgen meldingen binnen van bijvoorbeeld discriminerende uitingen, maar kunnen vervolgens lastig achterhalen wie de dader is. Eén ding weten ze meestal wel, waar het

13 What is My IPAddress, The Internet Isn't Safe. That's Why You Need a VPN., online via: <https://whatismyipaddress.com> (laatst geraadpleegd op 17 mei 2019).

11 Wikipedia, Notice and take down, 10 april 2019, online via: <https://en.wikipedia.org> (laatst geraadpleegd op 17 mei 2019).

12 Filipe Romero-Moreno, "Notice and staydown' and social media: amending Article 13 of the Proposed Directive on Copyright', International Review of Law, Computers & Technology 2019/33, afl. 2, p.189-190.

gebeurt. Denk aan een platform, kunnen ze deze dan aansprakelijk stellen? Een interessante vraag die ik aan de lezer overlaat. Met een knipoog verwijs ik naar een ander artikel in dit magazine die de aansprakelijkheid van platformen centraal heeft staan. (**Verantwoordelijkheden van platformen**)

Nieuwe wetten

Nog enkele onbelichte onderwerpen, waar de opsporing het ook lastig mee heeft, zijn andere varianten van afpersing online. Ik ga hier voornamelijk in op wraakporno. Daarvoor leg ik dan eerst sexting uit om een beter beeld te krijgen.

Sexting:

Sexting, zoals de naam wellicht al zegt, is het verzenden van seksueel getinte beelden of tekstberichten door middel van een telefoon of een online platform als WhatsApp, Facebook, YouTube etc.¹⁴ Al een tijd lang wordt er erg voor gewaarschuwd dat sexting onuitwisbaar is. Zo snel als een afbeelding is gestuurd, zo snel kan deze ook worden verspreid. Op zich is sexting zelf niet een zeer groot probleem, als het maar onder volwassenen gebeurt en er geen minderjarigen aan te pas komen. Het wordt echter een probleem als het materiaal in iemands handen valt die kwade bedoelingen heeft. Denk aan het dreigen met het pu-

14 Onuitwisbaar, Wat is sexting?, online via: <http://www.onuitwisbaar.nu> (laatst geraadpleegd op 17 mei 2019).

bliceren op social media van het materiaal (afpersing) of het uit wraak verspreiden van beeldmateriaal (wraakporno).

Wraakporno:

Het algemeen Nederlands woordenboek heeft hier een mooie definitie voor: 'pornografische foto's of filmpjes van een ex-geliefde, die in principe voor privédoel-einden bedoeld zijn, die men op internet publiceert als wraak op degene die de relatie heeft verbroken'. Het fenomeen wraakporno is een modern probleem. Het woord duikt steeds vaker op, zaken die erover gaan duiken vaker op en de roep om modernisering van de wetten op het gebied van moderne afpersingsdelicten klinkt ook steeds luider. Dit is minister Grapperhaus ook niet ontgaan, die druk bezig is om in een apart wetsartikel wraakporno strafbaar te stellen. In het wetgevingsadvies van minister Grapperhaus over de herwaardering strafbaarstelling van actuele delictsvormen staat onder andere artikel 139h Sr dat wraakporno strafbaar moet gaan stellen.¹⁵ Al eerder zijn er alarmbellen afgegaan die niet vanuit de media maar vanuit de Raad voor de Rechtspraak kwamen, die stelden dat de eisen die het wetsvoorstel had te hoog zijn om in veel zaken tot een veroordeling te komen.¹⁶ De Raad vroeg zich terecht af waarom 'of redelij-

15 Kamerstukken II, 2018/2019, 35080, 2.

16 Rechtspraak, Raad: maak het makkelijker om wraakporno te bestraffen, 2 juli 2018, online via: <https://www.rechtspraak.nl> (laatst geraadpleegd op 17 mei 2019); zie ook T. Den Hartog, Wet te-

kerwijs moet vermoeden' ontbrak in de wetsomschrijving en waarom er niet was gekozen voor een variant met voorwaardelijk opzet.¹⁷ Daar heeft de minister naar geluisterd zodat ook voorwaardelijk opzet op het gebied van wraakporno voldoende is om voor strafbaarheid in aanmerking te kunnen komen. De hoop is dat het zo snel mogelijk ingevoerd wordt gezien de maatschappelijke problemen omtrent dit delict. De laatste nota van wijziging was vorige maand, er wordt dus nog hevig gewerkt aan de wet zelf.¹⁸

Conclusie

Je online uiten lijkt een hedendaags recht. Zodra je het ergens niet mee eens bent, kun je dat laten weten aan je online wereld. Iets wat tegenwoordig een, wellicht noodzakelijke, uitlaatklep is of kan zijn. Er zijn grenzen, de rechtspraak laat al af en toe zien wat deze grenzen zijn. We zijn er echter nog lang niet, want veel daders blijven onbestraft. Dat kan komen door de toenemende anonimiteit of door het uitblijven van een aangifte van het

gen wraakporno 'gaat tegenvallen', 2 juli 2018, online via:
<https://www.ad.nl> (laatst geraadpleegd op 17 mei 2019).

17 Advies Wetsvoorstel herwaardering strafbaarstelling actuele delictsvormen (Rvdr-advies van 13 juni 2018 aan de minister van Justitie en Veiligheid mr. F.B.J. Grapperhaus), Den Haag: Rvdr 2018 (online publiek).

18 Kamerstukken II, 2018/2019, 35080, 8.

slachtoffer. Toch zijn er oplossingen. Platformen doen al hun best om de omgeving zo netjes mogelijk te houden door middel van een NTD-systeem. Deze techniek zal zich ongetwijfeld blijven ontwikkelen en zal steeds beter zijn werk kunnen doen. Wellicht iets te goed. De opsporing kan namelijk bemoeilijkt worden als elke belediging verwijderd wordt. Het bericht met de belediging kan bijvoorbeeld gebruikt worden in de opsporing. Daar heb je echter weinig meer aan als het al verwijderd is. Naast de uitingsdelicten heb ik stilgestaan bij een ander modern probleem: wraakporno. De roep om strafbaarstelling bestaat al langer. De minister is daarom druk bezig om dit te verwezenlijken. Ik kan mij vinden in de wijziging tot verlaging van de bewijsdrempel, die zoals het er nu uitziet ook doorgevoerd zal worden. Het zal de strafbaarstelling van daders ten goede komen om met voorwaardelijk opzet te kunnen bewijzen dat het delict gepleegd is. Tot op heden is de wet nog niet van kracht geworden.

Namens de redactiecommissie,

Patrick van de Wetering

Brinkhof

ADVOCATEN

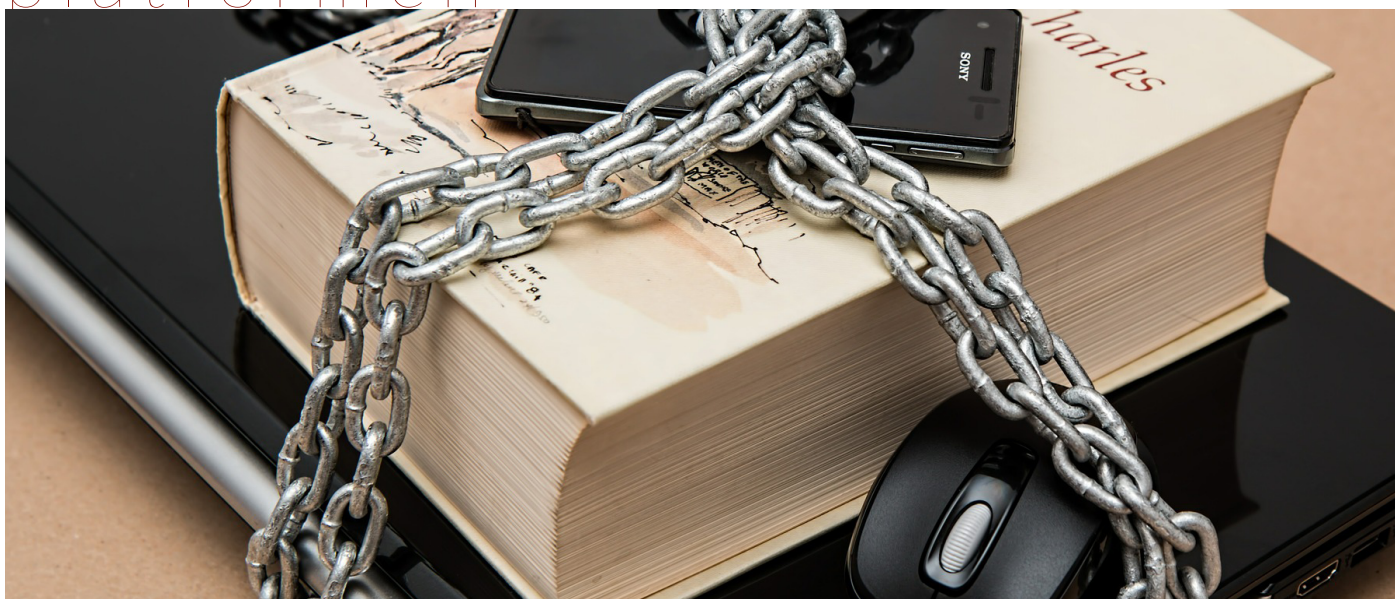
10 E-MAGAZINE

Hogan
Lovells

N O R D

ADVOCATEN

Verantwoordelijkheden van platformen



Het is momenteel ruim twee maanden geleden dat de hele wereld op 15 maart 2019 live mee kon kijken met de schietpartij in twee moskeeën in Christchurch. Het betrof een video waarin de schutter een bodycam droeg en zijn beelden streamde via zijn Facebookaccount. Facebook heeft de beelden zo snel mogelijk geprobeerd te verwijderen, maar via het internet verspreidden deze beelden zich razendsnel en via allerlei kanalen was te zien hoe de schutter tientallen mensen doodde. Een verschrikkelijke video die nooit online had mogen komen, maar het was zeker niet de eerste video waarin schokkende beelden naar voren kwamen. Al vaker verschenen er video's waarin moorden, zelfmoord of verkrachting te zien waren. Platformen zoals Facebook, Twitter en YouTube doen hun

best om deze video's zo snel mogelijk te verwijderen. Dit doen zij door middel van een algoritme dat geweld, seks en haatzaaien detecteert, waarna een controle achteraf plaats kan vinden door natuurlijke personen. Hoe deze video zomaar door het algoritme kon komen en met name niet eerder werd gedetecteerd, is niet bekend.¹

Dit soort livestreams of video's zijn niet de enige content waar een platform vandaag de dag mee te maken krijgt. Ook beledigingen in chatrooms, onrechtmatig geüploade auteursrechtelijk beschermde content en in het bijzonder de opkomst

¹ N. Klaassen, Live meekijken met massamoord: "Internetreuzen moeten ingrijpen", 15 maart 2019, online via: <https://hln.be/> (laatst geraadpleegd op 14 mei 2019).

van nepnieuws zijn zaken waar platformen rekening mee moeten houden. Door middel van nepnieuws werden de afgelopen jaren onder andere verkiezingen en referenda een bepaalde richting uitgestuurd.² Nepnieuws is soms zelfs de aanleiding tot racisme en geweld.³ De vraag is of platformen verantwoordelijk zijn voor de content die op hun site wordt geplaatst en of zij deze inhoud zo maar mogen of zelfs moeten verwijderen. Dit laatste met name wanneer het platform van mening is dat de content niet thuishoort op het net. Het is natuurlijk heel belangrijk dat video's, zoals hierboven beschreven, niet op internet belanden. Maar is het verwijderen van content, geplaatst door gebruikers van het platform, niet in strijd met de vrijheid van meningsuiting? Deze problematiek wordt in dit artikel verder toegelicht.

Platformen als tussenpersoon

Allereerst is het belangrijk om te weten wie er verantwoordelijk is voor de content die op een platform staat. De persoon die de content plaatst of het platform? Voor het antwoord hierop moet onderscheid gemaakt worden tus-

sen twee verschillende situaties. Ruwweg komt het erop neer dat personen zelf content kunnen creëren, of dat ze een platform bieden waarop de content gepubliceerd kan worden. In dit artikel zal verder worden ingegaan op de tweede situatie: het aanbieden van een platform waarop content kan worden gepubliceerd.⁴ Het platform treedt in dat geval in beginsel op als tussenpersoon.

Aansprakelijkheid platformen

De kern van de aansprakelijkheid voor platformen is in het Nederlandse recht geregeld in art. 6:196c van het Burgerlijk Wetboek (BW). Die bepaling geeft specifieke regels voor de aansprakelijkheid van dienstverleners op het internet.⁵ Dit gaat dan met name om zogeheten Internet Service Providers (ISP's). ISP's zijn ondernemingen die toegang tot het internet mogelijk maken of websites faciliteren, wat ook wel beter bekend staat als hosting. Voor het verschaffen van die diensten moet er informatie, al dan niet tijdelijk, worden opgeslagen. Die informatie kan echter onrechtmatig zijn jegens een derde, wegens privacyaantasting of auteursrechtinbreuk. In de beginjaren van het internet vonden

2 K. Hermans, Is Facebook verantwoordelijk voor nepnieuws?, 4 augustus 2018, online via: <https://www.metronieuws.nl/> (laatst geraadpleegd op 14 mei 2019).

3 M. Nijhuis, Facebook in Myanmar: een 'wild beest' dat etnisch geweld faciliteerde, 30 april 2018, online via: <https://www.vn.nl/> (laatst geraadpleegd op 15 mei 2019).

4 C. Meindersma, Wie is aansprakelijk voor de content op een website?, 10 juni 2015, online via: <https://www.charlotteslaw.nl/> (laatst geraadpleegd op 14 mei 2019).

5 S. Kulk, in: GS Onrechtmatige daad VI, commentaar op art. 6:196c, aant. 2 (online, bijgewerkt 6 december 2017).

er uitvoerige discussies plaats onder welke omstandigheden dienstverleners aansprakelijk zouden zijn.

Om zeker te stellen dat een dienstverlener niet aansprakelijk is als hij aan bepaalde eisen voldoet, zijn in art. 12 tot en met 15 van de e-commercerichtlijn regels gesteld voor de aansprakelijkheid van internetdienstverleners.⁶ De gedachte is dat een dienstverlener niet aansprakelijk is, zolang hij geen directe bemoeienis heeft gehad met de doorgegeven of opgeslagen informatie en geen weet heeft van het onrechtmatige karakter ervan. Volgens art. 15 lid 1 van de e-commerce richtlijn mag op de dienstverlener geen algemene verplichting worden gelegd tot actief onderzoek naar de legitimiteit van de doorgegeven informatie, al laat de richtlijn wel ruimte voor het opleggen van verplichtingen (art. 12 lid 3, 13 lid 2 en 14 lid 3). De mate van aansprakelijkheid van ISP's komt daarom met name neer op de reikwijdte van die verplichtingen. Art. 6:196c BW is een implementatie van bovengenoemde artikelen van de richtlijn. Art. 15 van de e-commercerichtlijn, dat algemene toezichtsverplichtingen verbiedt, is niet uitdrukkelijk door de Nederlandse wetgever geïmplementeerd. Deze bepaling dient echter wel gerespecteerd te worden.

Art. 6:196c BW is een *lex specialis* op de regels van onrechtmatige daad op grond

⁶ Richtlijn 2000/31/EG.

van art. 6:162 BW.⁷ Als de dienstverlener heeft voldaan aan de voorwaarden van de *lex specialis*, kan hij niet aansprakelijk worden gesteld uit hoofde van onrechtmatige daad. Daaruit volgt niet het tegenovergestelde dat de dienstverlener zonder meer aansprakelijk is indien niet aan deze voorwaarden is voldaan. Uit het arrest L'Oréal/eBay blijkt dat diens aansprakelijkheid in dat geval moet worden beoordeeld volgens de gewone regels van onrechtmatige daad, waar de nationale rechter over dient te oordelen.⁸ Bovendien doen de bepalingen van de AVG geen afbreuk aan de aansprakelijkheidsbeperkingen, wat blijkt uit art. 2 lid 4 van deze Verordening.

Diensten van de informatiemaatschappij

De bepalingen van art. 6:196c BW hebben betrekking op (rechts)personen die bepaalde diensten van de informatiemaatschappij (DIM) verrichten, zoals bepaald in art. 3:15d lid 3 BW.⁹ Onder DIM worden volgens dit artikel alle diensten verstaan die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer worden verricht.

⁷ S. Kulk, in: GS Onrechtmatige daad VI, commentaar op art. 6:196c, aant. 4 (online, bijgewerkt 6 december 2017).

⁸ HvJ EU 12 juli 2011, ECLI:EU:C:2011:474 (L'Oréal/eBay).

⁹ S. Kulk, in: GS Onrechtmatige daad VI, commentaar op art. 6:196c, aant. 5 (online, bijgewerkt 6 december 2017).

De diensten moeten ook worden verricht zonder dat partijen op dezelfde plaats aanwezig zijn. De omschrijving van DIM is erg breed, maar art. 6:196c BW geldt slechts voor een subcategorie van DIM: dienstverleners die DIM verlenen die bestaan uit het doorgeven of opslaan van informatie die van een ander afkomstig is. Zoals al eerder gezegd zijn dit primair internet- en hostingaanbieders, maar ook bijvoorbeeld beheerders van chatrooms vallen hieronder. Op het internet worden diensten vaak 'gratis' aangeboden. Vergoeding van dienstverlening vindt dan op indirecte wijze plaats, zoals door middel van advertenties. Volgens het arrest *Mc Fadden* is er in die gevallen ook sprake van DIM.¹⁰

Inhoud van 6:196c BW

De strekking van bovenstaand artikel is dat de dienstverlener niet aansprakelijk is voor zover hij zich niet actief met de doorgeven of opgeslagen informatie heeft bemoeid, oftewel alleen faciliterend heeft opgetreden.¹¹ Considerans nr. 42 van de e-commercerichtlijn stelt dat er sprake is van doorgeven en tijdelijk opslaan van informatie als het een activiteit betreft met een louter technisch, automatisch en passief karakter, wat in-

houdt dat de aanbieder van DIM noch kennis noch controle heeft over de informatie die wordt doorgegeven of opgeslagen.

Leden 1 tot en met 4 van art. 6:196c BW bevatten elk specifieke bepalingen voor verschillende vormen van ISP's. Zo gaan lid 1 en 2 respectievelijk over ISP's die als doorgeefluik deel uitmaken van het internet (mere conduit). Met name aanbieders als Ziggo vallen onder die bepaling, aangezien zij toegang verschaffen tot het internet door het afsluiten van een abonnement. Lid 3 ziet op ISP's die ervoor zorgen dat van een ander afkomstige informatie geautomatiseerd, tussentijds en tijdelijk wordt opgeslagen om het later doorgeven van die informatie aan anderen doeltreffender te maken. Dit wordt ook wel caching wordt genoemd. De meest interessante bepaling voor platformen is lid 4, die bedoeld is voor ISP's die DIM verrichten die bestaan uit het op verzoek opslaan van informatie die van een ander afkomstig is.¹² Veel platformen en websites bieden gelegenheid tot opslag van informatie, waardoor zij vaak onder de laatste bepaling zullen vallen. Voorbeelden van dit soort hosting providers zijn Google, eBay en Reddit.

Volgens art. 6:196c lid 4 sub a BW en considerans nr. 42 van de e-commercerichtlijn is een dergelijke ISP niet aansprakelijk voor de opgeslagen informatie als de opslagdienst louter technisch, automatisch

¹⁰ HvJ EU 15 september 2016, ECLI:EU:C:2016:689 (*Mc Fadden*).

¹¹ S. Kulk, in: *GS Onrechtmatige daad VI*, commentaar op art. 6:196c, aant. 6 (online, bijgewerkt 6 december 2017).

¹² S. Kulk, in: *GS Onrechtmatige daad VI*, commentaar op art. 6:196c, aant. 10 (online, bijgewerkt 6 december 2017).

en passief is, waarbij hij geen weet heeft van het onrechtmatige karakter van de informatie. Sub b voegt daaraan toe dat de ISP onverwijld de informatie moet verwijderen of de toegang daartoe onmogelijk maken, zodra hij kennis heeft of behoort te hebben van het onrechtmatige karakter van de informatie. Dit wordt ook wel een Notice & Take Down-verplichting (NTD) genoemd. Als de auteursrechthebbende of benadeelde een melding maakt van de onrechtmatige content aan de ISP, dient het platform die post of dat filmpje offline te halen of onbereikbaar te maken.

De platformen hebben dus nog steeds de verantwoordelijkheid om onrechtmatige content te weren, ook al zijn ze in beginsel niet aansprakelijk voor de informatie die door derden op hun site wordt geplaatst. Daar komt echter ook nog bij kijken dat de ISP's passief moeten zijn en het hangt per platform af welke gedragingen nog als passief worden gezien. In het arrest Google AdWords werd bepaald dat Google passief handelde, ondanks dat zij betaald werd na het aanklikken van een advertentie, ze het mogelijk maakte zoekwoorden op te geven en dat het algoritme van de zoekmachine

bepaalde advertenties hoger plaatste dan andere.¹³ Google zou niet passief hebben gehandeld als ze hadden geholpen met het schrijven van de reclameboodschappen of bij het vaststellen van trefwoorden. Google had in casu kennis noch controle, waardoor het geen actieve rol speelde.

In de zaak PVH/Facebook kwam naar voren dat Facebook zich niet mocht beroepen op art. 6:196c BW.¹⁴ Het ging in deze zaak om reclames van onder andere schoenen die niet werden verkocht door Tommy Hilfiger, maar wel het merk droegen. Door controle van Facebook op advertenties, vastgelegd in het advertentiebeleid, bepaalt zij mede de inhoud en speelt zij dus een actieve rol. Van Facebook wordt verwacht dat zij passende maatregelen treft om stelselmatige inbreuken op IE-rechten van derden zoals PVH te voorkomen. Voortaan moet Facebook niet wachten tot Tommy

13 HvJ EU 25 maart 2011, ECLI:EU:C:2011:685 (Google AdWords).

14 Rb Amsterdam 21 december 2018, ECLI:NL:RBAMS:2018:9362 (PVH/Facebook).



Hilfiger komt klagen over een nepwebshop, maar verdachte gebruikers die adverteren met Tommy Hilfiger-spullen zelf van Instagram en Facebook schoppen.

Artikel 17 DSM-richtlijn

Waar artikel 6:196c lid 4 BW de voorwaarden geeft voor de aansprakelijkheidsvrijstelling voor tussenpersonen bij de plaatsing van onrechtmatige content door gebruikers, stelt artikel 17 lid 3 van de nieuwe Digital Single Market-richtlijn (DSM) het eerdergenoemde artikel onder bepaalde omstandigheden buiten werking op het gebied van auteursrecht. Als aan deze voorwaarden wordt voldaan is het platform primair aansprakelijk voor openbaarmaking, niet secundair als tussenpersoon in de hoedanigheid van een hosting provider. Na de officiële bekendmaking van de richtlijn in het Publicatieblad van de EU op 22 mei 2019 hebben lidstaten 24 maanden lang de tijd om de richtlijn om te zetten in hun nationale wetgeving.¹⁵ Artikel 17 DSM-richtlijn, voorheen bekend als artikel 13, is van toepassing voor online content-sharing service providers (OCSSP's). OCSSP's zijn aanbieders van DIM die grote hoeveelheden auteursrechtelijk beschermde content openbaar maken, waarbij de content is geüpload door de gebruikers, met het voornaamste doel of een van de

voornaamste doelen om er winst mee te maken.

Deze platformen moeten ervoor zorgen dat ze vooraf toestemming hebben om door gebruikers geüpload content toe te mogen staan op het platform, bijvoorbeeld door het afsluiten van licenties (lid 1). Die toestemming moet niet alleen voor het platform gelden, maar ook voor de individuele gebruikers die geen commercieel doel hebben (lid 2). Mocht er onverhoopt geen toestemming zijn verkregen, moet het platform aantonen wel hun uiterste best te hebben gedaan om toestemming te krijgen, zorgen dat de door de auteursrechthebbenden aangegeven content niet op het platform beschikbaar kan zijn en moeten na melding van een inbreuk de desbetreffende content direct van het platform verwijderen en nieuwe uploads daarvan voorkomen (lid 4 sub a-c). Bij lid c is er sprake van een Notice and Stay Down-verplichting (NSD), die dus ook moet verzekeren dat inbreukmakende content niet terugkomt op het platform. Platformen hoeven geen toestemming of licentie van de auteursrechthebbenden te krijgen om het commerciële gebruik van de content te regelen. Een gebruiker met een commercieel doel, zoals een zakelijk Pinterest account, blijft zelf aansprakelijk voor de geüpload auteursrechtelijk beschermde content. Hij zal dan opmerkelijk genoeg wel opnieuw een licentie voor hetzelfde werk moeten afsluiten bij de rechthebbende.

¹⁵ Stichting Brein, Laatste horde genomen: de DSM richtlijn definitief aangenomen, 16 april 2019, online via: <https://stichtingbrein.nl/> (laatst geraadpleegd op 16 mei 2019).

Vrijheid van meningsuiting

Er is veel ophef ontstaan over de upload-filters die mogelijk nodig zijn om aan de vereisten van art. 17 DSM-richtlijn te voldoen. Deze zouden namelijk haaks staan op de vrijheid van meningsuiting. Het internet behoudt met deze richtlijn niet meer het vrije en open systeem wat het nu heeft. Content wordt voordat het openbaar wordt gemaakt gecontroleerd op auteursrechtelijk beschermde trekken, wat in beginsel goed is om auteursrechthebbers te beschermen. Het auteursrecht kent echter enkele uitzonderingen. In de Nijntje-zaak is bijvoorbeeld geoordeeld dat het is toegestaan om zonder toestemming van de auteur een humoristische parodie te maken.¹⁶ Ook mag er inhoudelijk gereageerd worden op auteursrechtelijke content door bijvoorbeeld een scène uit een film te laten zijn en daarbij kritiek te geven. Een filter kent deze uitzonderingen niet en kan niet bepalen wat wel en wat niet is toegestaan. 'Het filter heeft maar een beperkte intelligentie, laat staan gevoel voor humor', aldus Hugenholtz, professor Intellectueel Eigendomsrecht op de Universiteit van Amsterdam).¹⁷

Het uploadfilter zorgt ervoor dat content gecontroleerd wordt voordat het

16 Hof Amsterdam 13 september 2011, ECLI:NL:GHAMS:2011:BS7825.

17 B. Hulsen, *EU stemt voor 'uploadfilter': Wat is het en waarom is het omstreden*, 15 september 2018, online via: www.nu.nl (laatst geraadpleegd op 17 mei 2019).

openbaar mag worden gemaakt. YouTube werkt al met contentfilters om aan de beleidsregels van het platform te voldoen, waarmee bijvoorbeeld video's met kinderporno prompt worden verwijderd. De DSM-richtlijn heeft slechts betrekking op het filteren van auteursrechtelijk beschermde content. De hosting providers die daarbuiten vallen, zullen daardoor weinig merken van de nieuwe verplichtingen. Ze kunnen er uiteraard buiten vallen doordat ze niet te maken krijgen met auteursrechtelijke content. In art. 17 lid 6 is ook bepaald dat nieuwe OCCP's niet aansprakelijk zijn als ze minder dan 3 jaar bestaan en minder omzet draaien dan €10.000.000. OCCP's moeten dan nog wel trachten licenties te bemachtigen en hebben een NTP-verplichting. Met meer dan 5 miljoen maandelijkse gebruikers komt er bovendien een NSD-verplichting bij. Ook als ISP's buiten de DSM-richtlijn vallen, kan er sprake zijn van een onevenredige inbreuk op de vrijheid van meningsuiting. Bij een NTD-procedure kan ook overfiltering plaatsvinden, met name als de 'notices' ongefundeerd zijn. Het mag het platform niet worden verplicht om ook legaal gedrag te blokkeren.

Niet alleen voor het censureren van auteursrechtelijke content worden tegenwoordig afspraken gemaakt in Europa. Een aantal maanden geleden heeft het Europees Parlement ingestemd met regels die internetplatformen verplichten om terroristische content binnen een uur

ontoegankelijk te maken.¹⁸ Deze regelgeving gaat gepaard met enige kritiek. Een van deze kritiekpunten is dat de term 'terroristische content' in het huidige voorstel erg breed is. Er is in het voorstel geen duidelijke uitzondering opgenomen voor educatieve, journalistieke of onderzoeksdoeleinden. Volgens Berners-Lee van Wikipedia, een van de ondertekenaars van de brief met kritiekpunten, draagt dit bij aan het risico dat er te veel legale en belangrijke politieke uitingen worden verwijderd.¹⁹

Conclusie

Er zijn tegenwoordig verschillende regels en wetten die er voor zorgen dat content gefilterd en mogelijk zelfs verwijderd moet worden. Platformen hebben een grote verantwoordelijkheid voor het naleven van deze regels. Zo geldt voor plat-

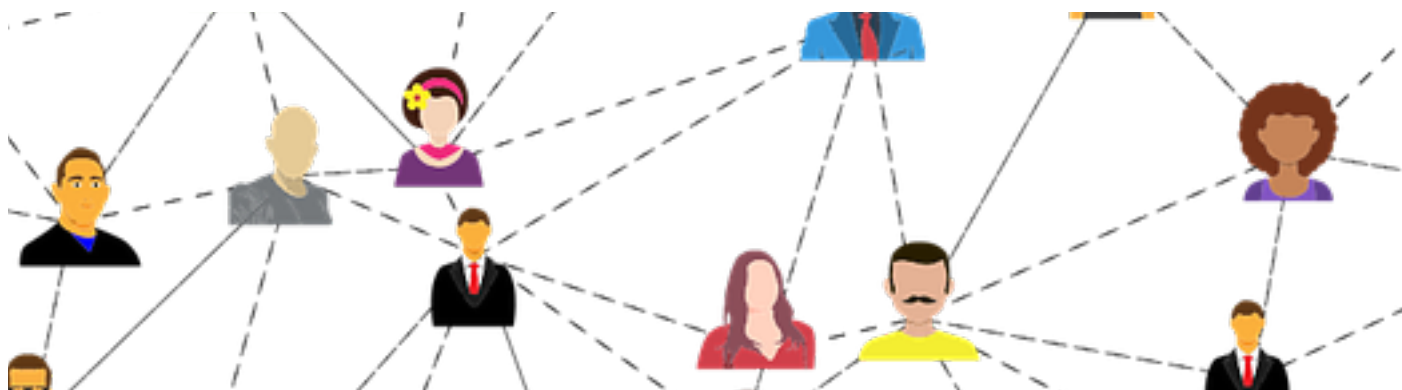
18 Proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, C8-0405/2018.

19 A. Wokke, EU-parlement stemt in met regels verwijderen terroristische content binnen een uur, 17 april 2019, online via: www.tweakers.net (laatst geraadpleegd op 17 mei 2019).

formen de NTD-verplichting bij het naleven van art. 6:196c BW en onder de nog te implementeren DSM-richtlijn toestemmings-, filter- en NSD-verplichtingen. De regelgeving blijft zich verder uitbreiden en ontwikkelen, zoals de nieuwe regelgeving vanuit het Europees Parlement met betrekking tot het verwijderen van terroristische content. De verantwoordelijkheid van platformen voor het verwijderen/filteren van content gaat mogelijk ook gepaard met de inperking van de vrijheid van meningsuiting. Er lijkt nog geen duidelijke scheidslijn te zijn tussen wat een filter wel en niet mag blokkeren. Uploadfilters en regelgeving over het verwijderen van terroristische content zijn een goede ontwikkeling, mits juist geïmplementeerd. Het heeft nog enige verbetering nodig voordat we onze grondrechten in grote mate overdragen aan algoritmes, met name de vrijheid van meningsuiting.

Namens de redactiecommissie,

Marit Jeeninga
Daniel Colenbrander



Brinkhof

ADVOCATEN

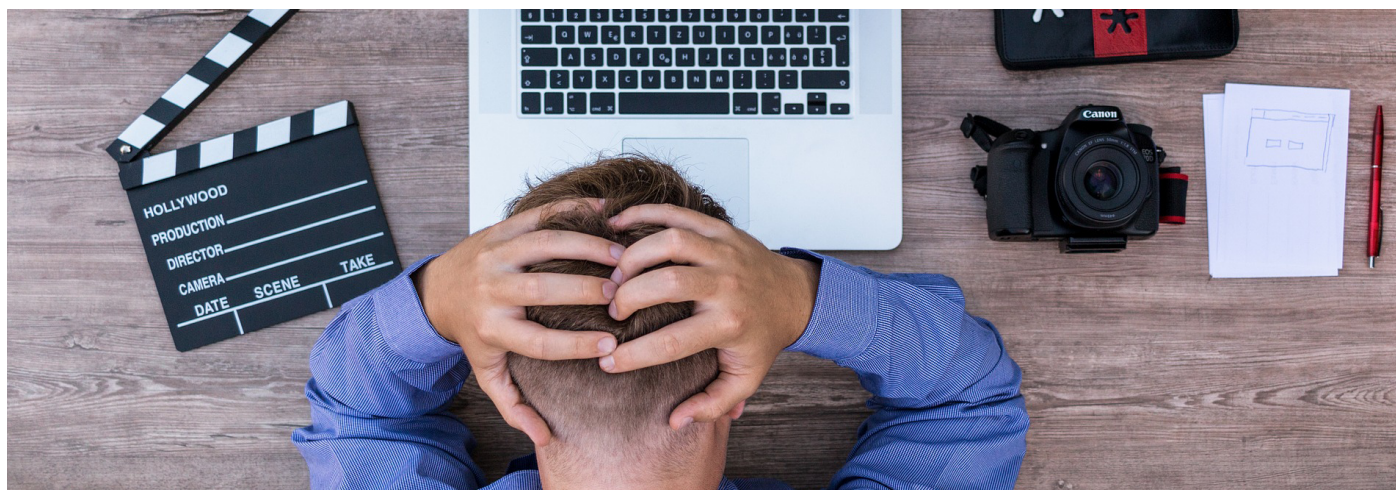
18 E-MAGAZINE

Hogan
Lovells

NORD

ADVOCATEN

Ontslagen wegens Facebook bericht?



Massaal delen we de details over ons dagelijkse leven op Facebook, Instagram of Twitter.¹ Deze kanalen worden ook veelvuldig gebruikt om een ongezouten mening te geven over uiteenlopende onderwerpen. We zijn vrij om overal iets van te vinden en deze mening mag ook worden geuit. Werkgevers worden hierdoor echter steeds meer geconfronteerd met werknemers die zich op sociale media uiten, op een manier die schadelijk kan zijn voor het bedrijf. Werkgevers houden hierdoor steeds vaker in de gaten wat hun werknemers op sociale media uitvoeren en sollicitanten worden voorafgaand aan de sollicitatie gegoogled.² Indien het

sociale media gedrag van de (kandidaat-) werknemer de werkgevers niet aanstaat, worden zij mogelijk afgewezen of ontslagen.³ In dit artikel zal worden ingegaan op de vraag of, en zo ja, in welke mate sollicitanten en werknemers mogen worden gescreend. Vervolgens wordt de bijzondere positie van ambtenaren besproken en de mogelijkheid van een sociale media code. Tot slot wordt uit het bovenstaande nog een conclusie getrokken.

Screenen van sollicitanten en werknemers

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Deze wet heeft consequenties voor de regels voor de screening (laatst geraadpleegd op 13 mei 2019).

1 J. Mooij, Kun je een werknemer ontslaan om zijn social media-gedrag?, 11 december 2017, te vinden op: www.legalmatters.com (laatst geraadpleegd op 13 mei 2019).

2 Werkgevers controleren steeds meer op social media, te vinden op: www.werken20.nl

3 Werkgever wijst kandidaat vaker af om sociale media, te vinden op: www.arro.nl (laatst geraadpleegd op 13 mei 2019).

van werknemers en sollicitanten.⁴ De Autoriteit Persoonsgegevens (AP) stelt dat screening inhoudt dat een werkgever informatie opvraagt over een werknemer of sollicitant om zo een inschatting te maken van zijn integriteit.⁵ Omdat screening zeer ingrijpend kan zijn voor de privacy van de sollicitant, is dit alleen onder bepaalde wettelijke voorwaarden toegestaan. De AVG en de uitvoeringswet AVG (UAVG) stellen de volgende eisen aan screening. Allereerst dient er sprake te zijn van een gerechtvaardigd belang.⁶ Dit belang moet rechtmatig, voldoende duidelijk verwoord en ook echt aanwezig zijn. Ten tweede dient de screening noodzakelijk te zijn. Hiermee wordt bedoeld dat het doel niet op een andere manier of door middel van een minder ingrijpend middel dan screening kan worden bereikt. Ten derde dient te worden voldaan aan de informatieplicht. De werkgever moet aan de betreffende sollicitant of werknemer vooraf laten weten dat de screening wordt uitgevoerd en achteraf wat de resultaten zijn. Ten vierde mogen de gegevens die uit de screening

4 J. de Nooij, Sollicitanten 'screenen' op social media, mag dat?, 6 augustus 2018, te vinden op: www.rechtblog.nl (laatst geraadpleegd op 13 mei 2019).

5 Autoriteit Persoonsgegevens, Screening, te vinden op: www.autoriteitpersoonsgegevens.nl (laatst geraadpleegd op 13 mei 2019).

6 Autoriteit Persoonsgegevens, Mag u persoonsgegevens verwerken?, te vinden op: www.autoriteitpersoonsgegevens.nl (laatst geraadpleegd op 13 mei 2019).

volgen niet voor een ander doel worden gebruikt en niet langer worden bewaard dan noodzakelijk. Tot slot moeten de gegevens goed worden beveiligd. Deze eisen zijn duidelijk genoeg en er kan geconcludeerd worden dat veel is toegestaan, zolang er maar van te voren over nagedacht is.

Tijdens de sollicitatieprocedure mag een werkgever dus onder de nodige voorwaarden toekomstige werknemers screenen. Maar hoe zit dit tijdens het dienstverband? Mag de werkgever een werknemer op staande voet ontslaan wegens gedragingen op sociale media? Om hier een goed antwoord op te kunnen geven, moet er eerst een belangrijk spanningsveld worden geschetst. Het recht op privacy en de vrijheid van meningsuiting staan op gespannen voet met elkaar. Uit twee arresten van het EHRM volgt een basislijn voor de controle van een werkgever op de werkplek van zijn werknemers.⁷ Het recht op privacy strekt ook uit tot de werkplek en dit betekent dat de werknemer een zekere mate van vrijheid heeft in zijn telefoongesprekken, e-mails en internetgebruik. Wanneer de werkgever besluit om hier een inbreuk op te maken, dan moet dit eerst worden medegedeeld aan de werknemer. Voor deze inbreuk is ook een gerechtvaardigd belang nodig.

7 EHRM 16 december 1992, NJ 1993/400, m.nt. E.J. Dommering, par. 32 (Niemiets) en EHRM 3 april 2007, JAR 2007/233 (Copland).

Deze noodzakelijkheid van een gerechtvaardigd belang geldt ook voor de gevallen waarin de werkgever bewijs wil gebruiken dat afkomstig is van sociale media. Hierbij moet een onderscheid worden gemaakt tussen de publieke en privésfeer. Een werknemer die zich bewust uit op openbare websites zoals Facebook, waarbij derden alles kunnen lezen, zorgt ervoor dat eenieder en dus ook de werkgever hier toegang tot krijgt.⁸ Standaardjurisprudentie is echter dat privé-uitlatingen van de werknemer die niks met zijn werk te maken hebben, in beginsel geen effect mogen hebben op de arbeidsrelatie. In beginsel zijn dan ook de uitlatingen van een werknemer via sociale media privé.⁹ In beginsel, want er zit een logische grens aan. Deze grens is neergelegd in artikel

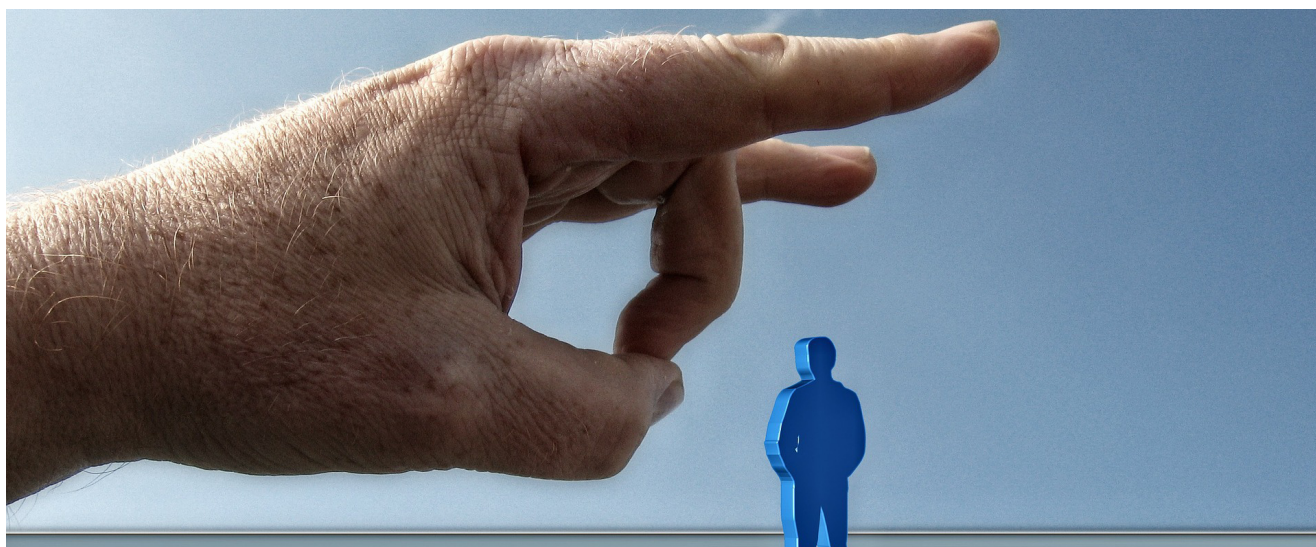
8 M.J. Aantjes, 'Werk vinden en verliezen door sociale media', TAP 2012, afl. 2, p. 62-68.

9 Rb. Maastricht (vzr.) 8 februari 2012, ECLI:NL:RBMAA:2012:BV3122.

7:678 lid 2 sub e BW. Beledigingen of ondeloos grievende uitlatingen die gericht zijn op de werkgever, diens familieleden of huisgenoten en op medewerkers zijn een voldoende grond voor ontslag op staande voet. Een werkgever moet dus een terughoudende positie innemen, maar bij uitingen die echt niet door de beugel kunnen, bestaat er de mogelijkheid om in te grijpen.

De bijzondere positie van de ambtenaar

Ambtenaren werken voor de overheid en vanwege deze speciale werkgever zijn er andere regels waaraan zij zich moeten houden. De belangrijkste in deze context is neergelegd in artikel 125a van de Ambtenarenwet. Hierin is voor ambtenaren een 'functioneringsnorm' opgenomen die ervoor zorgt dat een ambtenaar: "zich dient te onthouden van het openbaren van gedachten of gevoelens als daardoor de goede vervulling van zijn functie of



Brinkhof

ADVOCATEN

Hogan
Lovells

N O R D

ADVOCATEN

E-MAGAZINE 21

de goede functionering van de openbare dienst, voor zover deze in verband staat met zijn functievervulling, niet in redelijkheid zou zijn verzekerd”.¹⁰ Het gaat hierbij vooral om de goede functionering van de openbare dienst, oftewel het functioneren van de overheid. Een handeling in strijd met deze regeling kan leiden tot plichtsverzuim.

Een goed voorbeeld hiervan is de Facebook-uitspraak van 2017.¹¹ Een ambtenaar die als personenchauffeur in dienst is bij de overheid bezoekt in zijn vrije weekend in 2014 de voetbalwedstrijd ADO-Ajax. Wanneer hij na de wedstrijd terugloopt naar zijn auto, ziet hij daar een parkeerboete onder zijn ruitenwisser liggen. Hierop besluit de ambtenaar zijn ongenoegen te uiten en maakt hij de politieagenten via zijn Facebookpagina uit voor: “tering lafbekken”, “gore tyfusleijers”, “honden” en wenst hij ze het volgende toe: “rij jezelf maar te pletter op je motor”. Het moge duidelijk zijn dat dit gedrag een grens overschrijdt. De minister heeft dan ook geoordeeld dat er sprake is van plichtsverzuim en heeft hem een disciplinaire straf opgelegd die stand heeft gehouden bij de CRvB. Volgens deze rechter kunnen gedragingen in de privésfeer tot plichtsverzuim leiden, vooral wanneer er

10 K.P.D. Vermeulen, ‘Grenzen aan de meningsuiting van ambtenaren op social media’, TAR 2018, afl. 1/2, p. 3-9.

11 CRvB 10 augustus 2017, ECLI:NL:CR-VB:2017:2964.

sprake is van een representatieve functie.¹²

Sociale media code

Om ervoor te zorgen dat sociale media voornamelijk een waardevolle bijdrage leveren aan een organisatie kan een sociale media code of protocol worden opgesteld. Op deze manier kan een werkgever bij ongewenste uitingen op sociale media sneller corrigerend optreden als verwezen kan worden naar bestaande regels.¹³ Middels een set van gedragsregels op het gebied van sociale media worden duidelijke kaders aan zowel de werkgever als werknemer geboden. Desondanks hanteert momenteel nog geen 30% van de Nederlandse overheidsinstanties op dit moment een sociale mediabeleid, terwijl sociale media wel al veelvuldig worden ingezet. Zo blijkt uit onderzoek van Ernst & Young.¹⁴ De werknemer is verplicht zich te houden aan voorschriften die “de goede orde in de onderneming” bevorderen.¹⁵ Een sociale media code kan als een dergelijk voorschrift worden beschouwd

12 CRvB 10 augustus 2017, ECLI:NL:CR-VB:2017:2964, r.o. 4.4.

13 SocialMediaRecht, te vinden op: www.justitia.nl (laatst geraadpleegd op 13 mei 2019).

14 Richtlijnen voor gedrag sociale media, 19 augustus 2017, te vinden op: www.hr-kiiosk.nl (laatst geraadpleegd op 13 mei 2019).

15 Zie artikel 7:660 BW.

en mag dus eenzijdig door de werkgever worden opgelegd. Deze gedragsregels moeten wel binnen deze wettelijke instructiebevoegdheid vallen, indien dit niet het geval is kan de werkgever mogelijk nog een beroep doen op de norm van het “goed werknemerschap”.¹⁶ De werkgever kan ook nog overwegen de gedragsregels op te nemen in de arbeidsovereenkomst. Echter, kunnen deze regelingen in een arbeidsovereenkomst niet tussentijds worden aangepast en dienen werknemers die reeds in dienst zijn een nieuwe arbeidsovereenkomst of aanvulling op hun bestaande contract te tekenen.

16 Zie artikel 7:611 BW.

Conclusie

Het gebruik van sociale media is niet meer weg te denken uit onze samenleving, wat veel positieve gevolgen met zich meebrengt. Echter, veel mensen plaatsen inmiddels hun hele hebben en houden online zonder erbij na te denken. Dit geldt ook voor veel werknemers, waardoor het imago van een bedrijf kan worden geschaad. Wij raden jullie aan om eerst goed na te denken voordat je wat deelt via sociale media met de wereld. Zoals hierboven is gebleken, kan het namelijk van invloed zijn op zowel je toekomstige sollicitatiegesprekken als je huidige baan!

Namens de redactiecommissie,

Luuk Wassink
Lisa Celine Helfrich

Interview met de huidige redactie



Zouden jullie je als commissie eens willen voorstellen?

“Wij zijn de Redactie, mensen die af en toe wat zeggen in de chat. Je kunt dat klikken op de klink die we sturen en vervolgens onze stukken lezen. Het hele jaar schrijven we met veel plezier voor de vereniging.”
Daniel: ‘afnemend.’ Patrick: ‘Maar wel enthousiast.’

Hoe zijn jullie bij LISA terechtgekomen?

Patrick: ‘Jaren geleden. Dit is mijn 3de commissie. Drie jaar geleden heb ik gesolliciteerd op de BSR. Toen werd ik de commissaris promo en dat was hartstikke leuk. Nadat ik was aangenomen ben ik naar een borrel geweest en zo ben ik blijven plakken.’

Luuk: ‘Hallo ik ben Luuk en ik ben 21 jaar. Dit jaar was ik ook voor het eerst actief bij LISA. Ik heb de Redactie gedaan, wat ik overigens nog steeds doe en daar ben

ik erg blij mee. Dit is mijn derde jaar in Groningen. Ik kom oorspronkelijk uit de Achterhoek.’

Daniel: ‘Ik wist wel dat de vereniging bestond, maar ik deed er niks bij. Naar aanleiding van een collegepraatje twee jaar geleden solliciteerde ik, maar ik was helaas te laat. Via Patrick ben ik naar een symposium gepreparaat. Samen met hem heb ik besloten om bij de Redactie te gaan. We kennen elkaar sinds de eerste werkgroep.’

Lisa: ‘Ik was met Luzan in de stad en wist eigenlijk niet dat we naar een borrel gingen van de vereniging. Ik kwam met Rianne in gesprek over een commissie en dat leek me leuk. Uiteindelijk was het heel erg gezellig op de borrel en zo ben ik bij LISA gekomen.’

Marit: ‘Ik deed vorig jaar nog niets naast mijn studie, maar dat wilde ik wel graag

Brinkhof

ADVOCATEN

Hogan
Lovells

NORD

ADVOCATEN

gaan doen. Aangezien ik voor de richting IT-recht heb gekozen, was LISA een logische keuze. Ik solliciteerde en zo kwam ik bij de Redactie.'

Wat is jullie leukste commissie avontuur tot nu toe?

De winterfair! Op commissieweekend gingen we naar de ALDI en daar hing een bord met winterfair. We zeiden meteen "daar moeten we heen!"

Wat maakt de redactiecommissie nou de redactiecommissie?

Winterfair heeft ons gemaakt. Liefde voor ijsberen. Onze band is daar wel echt ontstaan.

Daniel: 'We hebben dit weekend helaas niet gevestigd, want we konden niet in het hokje waar de vishengels stonden.'

Dit maakt de redactiecommissie de redactiecommissie. We hebben zelfs vergaderd tijdens commissieweekend.

Hoe gaat een vergadering bij jullie?

We eten altijd eerst samen, daarna vergaderen we. We bespreken alle nodige punten, dat duurt meestal een uur tot anderhalf uur. Daarna blijven we nog even gezellig naborrelen.

Hoe is het om alleen maar over anderen te schrijven in plaats van over jezelf?

Daniel: 'Is wel fijn dat we er buiten kunnen vallen soms omdat dingen soms negatief naar buiten kunnen komen.'

Lisa: 'Je komt zelf met een onderwerp voor een blog en een schrijft een eigen conclusie dus op die manier maak je het wel persoonlijk.'

Daniel: 'Ja, dat klopt. Patrick schrijft over games en Luuk over gokken.'

Beschrijf de commissie eens in drie woorden.

Win-ter-fair.

Wat kunnen de leden nog verwachten van de redactiecommissie?

Helaas is dit het laatste wat de redactiecommissie van dit jaar zal doen. Kortom, niks meer.

Hoe vonden jullie het gaan om zelf geïnterviewd te worden?

Marit: 'Minder leuk dan ik dacht.'

Lisa: 'Ja, ik dacht soms wat zeggen sommige mensen weinig, maar ik snap ze nu wel.' Daniel: 'Ik vond het stiekem wel leuk om over vragen na te denken in plaats van ze zelf te stellen.'

Willen jullie nog iets kwijt aan de leden van LISA?

Daniel: 'Het is fijn als men zegt dat het wel gelezen wordt. Beetje waardering.'

Daniel: 'Het is leuk om op een laagdrempelige wijze te leren schrijven, maar een reactie is altijd leuk om te horen.'

Patrick wil de accie bedanken dat ze dit wilden doen.

Brinkhof

ADVOCATEN

Hogan
Lovells

N O R D

ADVOCATEN

E-MAGAZINE 25

Geachte lezer,

Aan al het moois komt een einde, zo ook aan dit collegejaar. Dit brengt met zich mee dat u het laatste e-magazine van dit collegejaar achter de kiezen heeft. Ik hoop allereerst dat u met veel plezier de afgelopen blogs en e-magazines heeft gelezen. De commissie heeft afgelopen jaar veel mooie, enerverende en interessante onderwerpen aangesneden, waarbij ze hun literaire kunsten konden laten zien.

Terugkijkend op het afgelopen jaar mag de commissie ontzettend trots zijn op zichzelf. Voor het vijfde jaar op rij is er een prachtig verenigingsblad uitgebracht, van hoge kwaliteit. Zo zijn veel vlakken van het IT-recht aan bod gekomen in de afgelopen magazines. De actuele onderwerpen e-health en The Internet of Things in afgelopen magazines en in dit magazine onder andere het cyberpesten.

De commissie heeft het hele jaar door hard gewerkt om de kwaliteit te behouden, daar zijn we trots op. Ik zou graag, namens het bestuur, de commissie willen bedanken voor hun inzet het afgelopen jaar. Zonder hen was het voortzetten van dit mooie verenigingsblad niet mogelijk geweest. Daarnaast wil ik, namens het bestuur, iedereen bedanken die een bijdrage heeft geleverd aan de e-magazines.

Met vriendelijke groet,

Namens het zestiende bestuur,

Riëlle van der Velde - Voorzitter

