Tijdschrift voor

INTERNET-RECHT

JAARGANG 19 - APRIL 2026 **1**

DEN HOLLANDER

Tijdschrift voor Internetrecht
Uitgeverij Den Hollander BV
Boomkampsweg 1, 7245 WC Laren
tel.: 0570 – 751225
e-mail: info@denhollander.info
www.denhollander.info

E-mail redactiesecretariaat
mr. J.J.H. Vos (jjhvos@pm.me)
mr. C.E. Nugteren (nienke.nugteren@vondst.com)

Abonnement
Zie: https://denhollander.info/

Nieuwe abonnementen
Abonnementen kunnen via onze website worden afgesloten en gaan in op een door u gekozen datum. De looptijd bedraagt 12 maanden.
Wanneer de ingangsdatum niet aansluit op een reeds lopend abonnement bij Den Hollander, wordt het nieuwe abonnement gekoppeld aan de looptijd van het bestaande abonnement. In dat geval wordt het tarief voor de resterende periode van het lopende jaar naar rato berekend, op voorwaarde dat het abonnement ook voor het volgende jaar wordt voortgezet.
Op alle abonnementen zijn onze algemene voorwaarden van toepassing.

Adreswijziging
Adreswijzigingen dienen zo snel mogelijk te worden doorgevoerd in uw account via onze website.

Beëindiging abonnement
Opzegging van abonnementen kan uitsluitend via uw account en dient uiterlijk één maand vóór het einde van het lopende abonnementsjaar te gebeuren.
Bij te late opzegging wordt het abonnement automatisch met één jaar verlengd.

ISSN 1875-7766

Citeerwijze
IR 2026, nr. 1
ISSN: 1875-7766

Tijdschrift voor INTERNETRECHT

JAARGANG 19 - APRIL 2026 - NUMMER 1

Internetrecht: belangrijker dan ooit!

mr. H.A.J. de Jong[1]

Hoe deel je computercapaciteit op afstand om samen, via niet al te betrouwbare communicatielijnen, efficiënt aan onderzoek te werken met verschillende onderzoeksinstituten? Het Amerikaanse Ministerie van Defensie – zorgwekkend genoeg tegenwoordig ook wel aangeduid als het Ministerie van Oorlog – richtte daarvoor een instituut op: DARPA. Dat begon in 1968 met de ontwikkeling van ARPANET. Door de te verzenden gegevens op te delen in kleine pakketjes konden verschillende computers er gelijktijdig gebruik van maken en was het systeem bovendien minder kwetsbaar bij storingen. ARPANET werd gaandeweg verbonden met andere netwerken en zo ontstond het internet zoals we dat vandaag allemaal gebruiken.

Inmiddels is het internet – en zijn talloze daarop aangeboden diensten – zo diep in ons dagelijks leven verankerd dat het een onmisbare factor in ons dagelijks leven is geworden. Het internet speelt sindsdien meer dan eens een prominente rol bij hoopvolle momenten in de recente geschiedenis. Denk aan de Jasmijnrevolutie eind 2010 in Tunesië, waardoor uiteindelijk Ben Ali het veld moest ruimen. De door de staat gecontroleerde media besteedden geen aandacht aan de ontluikende onrust, maar dankzij websites zoals Facebook, Twitter en YouTube verschenen beelden van de protesten razendsnel online. Ook de Egyptische revolutie van 2011 kwam in een stroomversnelling door het grootschalige gebruik van diezelfde sociale media. Hosni Moebarak trad uiteindelijk af. Kwaadaardige regimes zijn zich het 'gevaar' van internet inmiddels maar al te goed bewust: Rusland valt Oekraïense infrastructuur aan met cyberaanvallen en Iran schakelt momenteel – opnieuw – het internet uit om protesten in te dammen.

De schaduwkanten van het internet en de sociale media die daarop worden aangeboden, zijn helaas evenzeer alom bekend. Denk bijvoorbeeld aan Cambridge Analytica en Facebook, die in 2018 grootschalig in het nieuws kwamen vanwege het illegaal manipuleren van gegevens om verkiezingen in de Verenigde Staten en elders te beïnvloeden. Of meer recent: Elon Musk, die via zijn sociale mediaplatform X de publieke opinie wereldwijd probeert te sturen en onder andere heel gericht de verkiezingen in Duitsland trachtte te ondermijnen. Of China, waar via het internet en geavanceerde surveillancesystemen de Oeigoeren worden gevolgd en onderdrukt.

Kunnen we met ons internetrecht het goede van internet en social media behouden en het slechte uitbannen? Dat lijkt mij wat al te ambitieus, maar internetrecht kan wél de broodnodige spelregels bieden om de schadelijke gevolgen te beperken. Zonder goede afspraken over hoe het zou moeten zijn, is er immers geen kader om naartoe te streven. De Digital Services Act dwingt inmiddels grote platforms tot transparantie over algoritmen en contentmoderatie. De Digital Markets Act stelt poortwachters als Google, Meta en Apple aan een onderzoek naar machtsmisbruik bloot. De NIS2-richtlijn verplicht vitale sectoren tot cybersecuritymaatregelen en incidentmelding om het risico op ernstige verstoringen te verkleinen. De AI Act reguleert AI-systemen op basis van risicocategorieën om de kans op grote ongelukken te beperken. De Data Act en Data Governance Act trachten het delen van data te bevorderen voor de goede zaak.

Toch spreken we in ons vakgebied soms over internetrecht alsof het enkel gaat om compliance. Protocolletje hier, policy daar. Terwijl internetrecht in hoge mate bepaalt welke informatie burgers te zien krijgen, wie zeggenschap heeft over bepaalde gegevens, welke digitale knoppen overheden en bedrijven wel of niet mogen indrukken en hoe we ervoor dienen te zorgen dat het internet zo veilig én zo bereikbaar mogelijk blijft. Het gaat dus om het behouden van het goede en het bestrijden van het kwade. Dat is voor ons als internetjuristen veel meer dan procedurewerk of afvinkoefeningen. Daar zouden we ons sterk voor moeten (blijven) maken – en daarbij gerust wat meer ambitie mogen tonen; nu meer dan ooit.

1. Huub de Jong is advocaat bij Turing Advocaten en redacteur van dit tijdschrift.

Opkomen tegen een 'shadowban' via invulling van de maatschappelijke zorgvuldigheidsnorm

N.S.G. de Bruijn en E. Apeldoorn[1]

Dit artikel betreft een verkenning van huidige specifieke wet- en regelgeving op het gebied van *shadowbanning*: een potentieel nieuwe vorm van censuur. De effectiviteit van deze wet- en regelgeving blijkt beperkt omdat deze vooral transparantie- en motiveringsverplichtingen kent en niet effectief wordt gehandhaafd. Deze observatie leidt tot een op *Urgenda* en *Shell/Milieudefensie* geïnspireerde analyse van de mogelijkheid om tegen een *shadowban* op te komen via de maatschappelijke zorgvuldigheidsnorm (artikel 6:162 BW), ingevuld aan de hand van artikel 10 EVRM en soft law zoals UNGP en OESO. De dominante (economische) machtspositie van sociale media platformen en hun functie als infrastructuur van het publieke debat vragen dringend om zo een analyse.

1. INLEIDING

Nederlanders besteden zo een 115 minuten per dag aan sociale media.[2] Voor één op de acht Nederlanders zijn sociale media de belangrijkste nieuwsbron, onder Generatie Z, geboren tussen 1997 en 2012, is dat zelfs drie op de tien.[3] Niet alleen de nieuwsvoorziening, maar ook het publieke debat verschuift hiermee deels naar sociale media: activisme vindt in toenemende mate online plaats.[4] Dit wordt ook wel digitaal activisme genoemd.[5] Demonstraties worden niet alleen online voorbereid (denk aan De Rode Lijn-demonstraties), maar vinden ook in toenemende mate online plaats. Denk hierbij aan hashtag-acties (zoals #BlackLivesMatter, #MeToo en #IkDoeNietMeerMee) en online petities.

De populairste sociale media platformen, Facebook en Instagram, zijn in handen van het techbedrijf Meta.[6] Ook Youtube en X zijn populair. Aanbieders van sociale media platformen, zoals Meta, hebben de mogelijkheid om maatregelen te treffen tegen content van gebruikers die in strijd is met hun gebruikersvoorwaarden, waaronder online vormen van activisme. Eén van deze maatregelen betreft *shadowbanning*, kort gezegd het intransparant (gedeeltelijk) verbergen van berichten.

Onder meer de Digital Services Act ("DSA") biedt enige bescherming tegen *shadowbanning* door transparantie- en motiveringsvereisten op te leggen aan zichtbaarheidsbeperkingen door platformen.[7] De vraag is of het huidige wet- en regelgevingskader voldoende waarborgen biedt tegen het principe van *shadowbanning*, wat mogelijk gezien kan worden als een nieuwe vorm van censuur. In dit artikel bespreken wij censuur in de context van de relatie tussen big tech en gebruikers. In zoverre wijken we dus af van wat doorgaans daaronder wordt verstaan, namelijk toezicht vooraf door overheid of andere instanties op voor publicatie bestemde werken.

Ter beantwoording van die vraag gaat dit artikel eerst in op verschillende vormen van *shadowbanning*. Vervolgens worden de DSA en andere bestaande wet- en regelgeving die bescherming kunnen bieden tegen *shadowbanning* uiteengezet. Hierbij wordt ook ingegaan op procedures waarin werd geoordeeld dat sprake is van *shadowbanning*. Vervolgens wordt verkend of de huidige wet- en regelgeving voldoende bescherming biedt tegen de negatieve gevolgen van *shadowbanning*. We behandelen ten slotte de vraag of invulling van de maatschappelijk zorgvuldigheidsnorm aan onder andere de hand van artikel 10 Europees Verdrag voor de Rechten van de Mens ("EVRM") gebruikers bescherming biedt tegen *shadowbanning*, en hoe dit in het Nederlandse stelsel van wet- en regelgeving zou passen.

2. SHADOWBANNING, CENSUUR EN ONLINE ACTIVISME

In 2022 schreef het Amerikaans-Nederlandse fotomodel Bella Hadid op haar Instagram-pagina dat zij naar aanleiding van pro-Palestina posts werd *geshadowbanned*. In de periode die volgde spraken meerdere personen met een groot online bereik zich uit

1. N.S.G. de Bruijn (Aligamé Law) en E.A.B. Apeldoorn (bureau Brandeis). Dit artikel is mede tot stand gekomen met hulp van Lisa Overbosch en Ole Oerlemans.
2. 'Het Nationale Social Media Onderzoek', Newcom Research, februari 2024.
3. 'Het Nationale Social Media Onderzoek', Newcom Research, februari 2024.
4. E. Kopacheva, 'How the Internet has changed participation: Exploring distinctive preconditions of online activism', *Communication & Society* 2021/34, afl, 2, p. 67-85.
5. Y. Sastramidjaja, 'De kracht van online protesteren', uva.nl, 1 oktober 2025.
6. C. Van Helsdingen, 'Socialmedia-onderzoek 2025: flinke daling X, LinkedIn in de lift & actieve 40-plussers', Frankwatching.com, 25 januari 2025.
7. Artikel 17 Digital Service Act.

over verminderde zichtbaarheid van Instagram-berichten die als pro-Palestina worden aangemerkt.[8] Eind 2023 signaleerde Human Rights Watch systematische censuur van Palestijnse content op Instagram en Facebook, met *shadowbanning* als centraal censuurmechanisme.[9] Vanaf dat moment ontstond er een toename in maatschappelijk bewustzijn over de maatregelen die sociale media platformen treffen tegen online vormen van activisme.

Hoewel censuur van oorsprong verwijst naar voorafgaand toezicht door de overheid of kerk op publicaties, wordt de term in dit artikel ook gebruikt voor bepaalde maatregelen waarmee sociale mediaplatformen content minder zichtbaar maken. Sociale mediaplatformen hebben, gezien hun centrale en onontkoombare rol in het publieke debat, immers een vergelijkbare verantwoordelijkheid als publieke autoriteiten waar het gaat om de vrijheid van meningsuiting. Dit wordt nader toegelicht in paragraaf 4.2. Dit gebruik van de term censuur sluit bovendien aan het gelijknamige gebruik in het rapport van Human Rights Watch, en bij de observatie van de Wetenschappelijke Raad voor het Regeringsbeleid dat contentmoderatie door platforms al gauw raakt aan censuur.[10]

De klassieke definitie van *shadowbanning* is het heimelijk verbergen van berichten van een gebruiker, waarbij bij de gebruiker de indruk wordt gewekt dat berichten nog steeds publiekelijk zichtbaar zijn.[11] Naarmate de marktpositie van sociale media platformen is versterkt is ook de verscheidenheid aan vormen van *shadowbanning* toegenomen.[12] *Shadowbanning* betreft niet alleen de situatie waarin berichten geheel onzichtbaar zijn voor andere gebruikers, maar ook situaties waarin het bereik of de vindbaarheid van berichten wordt verminderd.[13]
Deze vorm van *shadowbanning* wordt in de literatuur ook wel een zichtbaarheidsmaatregel genoemd.[14] Een bekend voorbeeld is *delisting*, waarbij berichten worden uitgesloten van bepaalde platformfunctionaliteiten. Bij *search delisting* worden berichten bijvoorbeeld verwijderd uit de zoekresultaten, waardoor gebruikers deze niet langer via de zoekfunctie kunnen vinden. Bij *demotion* daarentegen blijven berichten wel vindbaar, maar wordt hun rangorde binnen bepaalde functionaliteiten verlaagd. Zo kan een bericht nog steeds via de zoekfunctie worden gevonden, maar verschijnt het bijvoorbeeld pas op de derde pagina van de zoekresultaten in plaats van op de eerste.[15]

Een problematisch kenmerk van *shadowbanning* is de onwetendheid van gebruikers omtrent de tegen hen genomen maatregelen. Variaties in de zichtbaarheid van content zijn immers inherent aan de rol die aanbevelingssystemen spelen bij het sorteren en presenteren van berichten.[16] Waar een activist in de fysieke wereld kan zien wie naar zijn of haar betoog luistert, kan een online activist nietsvermoedend tegen een lege zaal spreken. Het meest ingrijpende gevolg van deze onwetendheid is dat gebruikers feitelijk van elke mogelijkheid tot verweer tegen zulke zichtbaarheidsmaatregelen worden uitgesloten.[17]

Shadowbanning is dus een potentieel nieuwe vorm van censuur, waarin sprake is van een onzichtbare beperking van bereik zonder dat de spreker zich bewust is van de inmenging. Dit kan het publieke debat, dat essentieel is voor het functioneren van de democratische rechtsstaat, ondermijnen.

3. HUIDIGE WET- EN REGELGEVING

Binnen de kaders van de wet- en regelgeving bestaan verschillende aanknopingspunten op basis waarvan *shadowbanning* potentieel onrechtmatig is. In minstens twee juridische procedures in Europa is vastgesteld dat platforms *shadowbanning* toepassen: *Mekic t. Twitter*[18] (Nederland), waarover Menno Weij een dubbele annotatie schreef,[19] en *Vandendriessche/Meta*[20] (België). De juridische gronden die het onderwerp van deze procedures vormden worden hieronder samen behandeld.

3.1. Wanprestatie

In de eerste plaats kan de onrechtmatigheid van *shadowbanning* volgen uit de contractuele verplichtingen van sociale media platformen tegenover hun gebruikers. In *Mekic/Twitter* oordeelt de recht-

8. S. Hermus, F. Rensen, 'Sociale media zetten prominenten stilletjes in schaduw bij uitingen over beladen onderwerpen', *De Volkskrant*, 18 oktober 2023.
9. Human Rights Watch, 'Meta's Broken Promises: Systemic Censorship of Palestine Content of Instagram and Facebook', hrw.org, 21 december 2023.
10. WRR, 'Aandacht voor media. Naar nieuwe waarborgen voor hun democratische functies', wrr.nl, 3 oktober 2024.
11. G. Nicholas, '*Shedding Light on Shadowbanning*', Center for Democracy and Technology, April 2022, p. 10.
12. G. Nicholas, '*Shedding Light on Shadowbanning*', Center for Democracy and Technology, April 2022, p. 10.
13. P. Leerssen, 'An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation', *Computer law & Security review* 2023/48, p. 2.
14. P. Leerssen, 'An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation', *Computer law & Security review* 2023/48, p. 2.
15. P. Leerssen, 'An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation', *Computer law & Security review* 2023/48, p. 3.
16. P. Leerssen, 'An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation', *Computer law & Security review* 2023/48, p. 3.
17. P. Leerssen, 'An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation', *Computer law & Security review* 2023/48, p. 2.
18. Rb. Amsterdam 5 juli 2025, ECLI:NL:RBAMS:2024:3980 (*Mekic/Twitter*).
19. M. Weij, 'De strijd tegen 'shadowbanning': een dubbele annotatie', *IR* 2024-5, p. 197 e.v.
20. Hof van beroep Gent, 3 juni 2023, 2022/AR/508.

bank Amsterdam dat het *shadowbannen* van Mekic wanprestatie in de nakoming van de dienstovereenkomst betreft (artikel 6:74 Burgerlijk Wetboek ("BW")).[21] Door zich in de algemene voorwaarden het recht voor te behouden om gebruikerscontent niet blijvend te hosten of verspreiden, kan Twitter naar eigen goeddunken en zonder enige beperking haar contractuele verplichtingen wijzigen of opschorten. Dit betreft een oneerlijke handelspraktijk.[22]

3.2. DSA

In de tweede plaats kan de onrechtmatigheid van *shadowbanning* volgen uit de DSA. Zeer grote onlineplatformen zijn vanwege hun bereik van belang voor het bevorderen van het publieke debat en de verspreiding bij het publiek van informatie, meningen en ideeën.[23] Tegen die achtergrond beoogt de DSA een veiligere digitale omgeving te creëren waarin de fundamentele rechten van gebruikers worden beschermd, onder andere op sociale media platformen.[24] Zeer grote onlineplatformen hebben daarin een verzwaarde verplichting onder de DSA.[25]
Artikel 17 DSA vormt een verplichting voor platforms om beperkingen die aan gebruikers worden opgelegd te motiveren. In *Mekic/Twitter* oordeelt de rechtbank Amsterdam dat het opleggen van een *shadowban* een beperking van zichtbaarheid is als bedoeld in artikel 17(1)(a) DSA,[26] waarvoor een duidelijke en specifieke motivering moet worden gegeven. Het nalaten hiervan is onrechtmatig.

In artikel 14 DSA kan ook een mogelijke grond voor onrechtmatigheid worden gevonden. Dat artikel bepaalt dat de algemene voorwaarden informatie moeten bevatten over de eventuele beperkingen die platformen aan gebruikers van hun diensten kunnen opleggen.[27] Inhoudsmoderatie zoals *delisting* wordt in dit verband specifiek genoemd.[28] Op grond van artikel 14 lid 4 DSA dient bij de toepassing en handhaving van deze beperkingen een platform zorgvuldig, objectief en evenredig te handelen, met gepaste aandacht voor de fundamentele rechten van de gebruikers.[29] In deze context wordt de vrijheid van meningsuiting expliciet benadrukt.[30] Het is dan ook verdedigbaar dat de vereisten en principes van artikel 10 EVRM toepassing vinden in de uitleg van artikel 14 lid 4 DSA.[31] Deze principes worden uiteengezet onder paragraaf 5.1.

3.3. AVG

In de derde plaats biedt de Algemene Verordening Gegevensbescherming ("AVG") aanknopingspunten waar de onrechtmatigheid van *shadowbanning* uit zou kunnen volgen. Aangezien de AVG Europese wetgeving is, is zowel Nederlandse jurisprudentie als Europese jurisprudentie en jurisprudentie uit andere lidstaten relevant. In *Vandendriessche/Meta* oordeelt het hof van beroep van Gent (België) dat het *shadowbannen* van Vandendriessche gebaseerd is op geautomatiseerde besluitvorming in de zin van artikel 22 AVG. De algemene voorwaarden van Meta bieden in strijd met artikel 22(3) AVG geen mogelijkheid om het besluit aan te vechten. Daarnaast heeft Meta in strijd met artikel 13(2)(f) AVG en 14(2)(g) AVG nagelaten informatie te verstrekken over de logica van de geautomatiseerde besluitvorming, het belang en de verwachte gevolgen van de verwerking voor betrokkenen. Deze AVG-overtredingen kunnen, ieder afzonderlijk, het opleggen van een *shadowban* onrechtmatig maken.[32]

3.4. Effectiviteit huidige wet- en regelgeving

Hoewel de huidige wet- en regelgeving waarborgen kunnen bieden tegen *shadowbanning*, is de vraag of deze waarborgen (voldoende) effectief zijn om de ingrijpende gevolgen van *shadowbanning* te mitigeren. Hierbij is van belang dat het huidig kader bij gebrek aan correcte naleving en effectieve handhaving weinig effectief zal zijn. Handhavende instanties zijn naar eigen zeggen overbelast en kunnen effectieve naleving van deze wettelijke normen niet altijd waarborgen, althans lijken niet geneigd daaraan prioriteit te geven.[33] Zoals eerder aan bod kwam is inherent aan *shadowbanning* dat gebruikers niet op de hoogte zijn van de maatregel. Dit bemoeilijkt handhaving van wettelijke normen door gebruikers die zijn onderworpen aan een *shadowban*.
Daarnaast bevat de bestaande wet- en regelgeving met name transparantie- en motiveringsverplichtingen. Dit zijn formele eisen die worden gesteld aan zichtbaarheidsmaatregelen. Hoewel deze wetgeving gebruikers bij correcte naleving daarvan meer inzicht geeft in toegepaste zichtbaarheidsmaatregelen, biedt dit op zichzelf geen bescherming tegen *shadowbanning* en de mogelijk onrechtmatige gevolgen daarvan.

In dat verband is wet- en regelgeving bestaande uit open (privaatrechtelijke) normen van belang, omdat

21. Rb. Amsterdam 5 juli 2025, ECLI:NL:RBAMS:2024:3980 (*Mekic/Twitter*), r.o. 6-11.
22. Rb. Amsterdam 5 juli 2025, ECLI:NL:RBAMS:2024:3980 (*Mekic/Twitter*), r.o. 9.
23. Overweging 75 DSA.
24. 'De verordening digitale diensten houdt ons online veilig', commission.europa.eu, 22 september 2025.
25. Sectie 3 e.v. DSA.
26. Rb. Amsterdam 5 juli 2025, ECLI:NL:RBAMS:2024:3980 (*Mekic/Twitter*), r.o. 14.
27. Art 14 lid 1 DSA.
28. Artikel 14 lid 1 DSA jo. artikel 3 sub t DSA.
29. Art 14 lid 4 DSA.
30. Overweging 47 van de DSA.
31. J.P. Quintais, N. Appelman, R. Ó Fathaigh, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation', *German Law Journal* 2023/24, afl. 5, p. 898.
32. Hof van beroep Gent, 3 juni 2023, 2022/AR/508, r.o. 1.1.6.4.
33. Beleidsregel Prioritering van handhavingsonderzoeken van 26 mei 2023 (*Strct.* 2023, 15184).

die meer ruimte biedt om de omstandigheden van het geval mee te wegen bij de onrechtmatigheidsbeoordeling. In deze context is nog relevant dat maatregelen die de wetgever al heeft genomen, op zichzelf niet uitputtend zijn.[34]

4. FUNDAMENTELE RECHTEN EN SHADOWBANNING

Het huidige wettelijk kader lijkt niet in alle gevallen een effectief middel tegen *shadowbanning*. Er zijn situaties denkbaar waarin een *shadowban* onrechtmatig is, ondanks dat geen contractuele verplichtingen zijn geschonden en de toepasselijke transparantie- en motiveringsverplichtingen zijn nageleefd. De vraag is of gebruikers, op het moment dat zij weten dat er sprake is van een *shadowban*, via de maatschappelijke zorgvuldigheidsnorm van artikel 6:162 BW met succes kunnen opkomen tegen *shadowbanning*. Die vraag moet wat ons betreft positief worden beantwoord. Dit wordt in het onderstaande toegelicht door eerst in te gaan op de mogelijke horizontale werking van fundamentele rechten, waarna een analyse wordt gemaakt van de (machts)positie van sociale media platformen.

4.1. Horizontale werking fundamentele rechten

Van oudsher betreffen grondrechten afweerrechten tegenover de overheid.[35] Het uitgangspunt is dat het Handvest van de Grondrechten van de Europese Unie ("Handvest") op grond van artikel 51 primair is gericht op EU-instellingen en de lidstaten bij de uitvoering van Unierecht, en dat het EVRM op grond van artikel 1 EVRM verplichtingen oplegt aan staten, niet aan private partijen.
Dit betekent niet dat fundamentele rechten in de verhouding tussen private partijen geheel zonder betekenis zijn. De staat wordt immers geacht te garanderen dat fundamentele rechten worden gewaarborgd, ook in civiele verhoudingen. Fundamentele rechten kunnen dan ook tot op een zekere hoogte kunnen worden ingeroepen door burgers tegen een private onderneming[36] of door burgers onderling.[37]

Via de *indirecte* horizontale werking kunnen grondrechten doorwerken bij de uitleg en invulling van open privaatrechtelijke normen, zoals via de maatschappelijke zorgvuldigheid (art. 6:162 BW). In die benadering worden de waarden die ten grondslag liggen aan de grondrechten meegewogen in de rechterlijke belangenafweging, zonder dat de grondrechtsbepaling als zodanig rechtstreeks wordt toegepast.
Indirecte horizontale doorwerking van fundamentele rechten houdt dus in dat fundamentele rechten niet rechtstreeks tussen private partijen gelden, maar via nationale (privaatrechtelijke) normen in private verhoudingen doorwerken.
Deze indirecte horizontale werking brengt met zich mee dat het handelen van burgers en private ondernemingen geen toetsing behoeft aan artikel 52 lid 3 Handvest noch aan het tweede lid van EVRM-artikelen waarin wordt bepaald dat beperkingen van fundamentele rechten voorzien bij wet en noodzakelijk ter bescherming van een legitiem doel moeten zijn.
De *Urgenda*-uitspraak creëerde een belangrijk precedent voor het civielrechtelijk aanspreken van entiteiten op het nalaten om adequate voorzorgsmaatregelen te nemen tegen maatschappelijke risico's.[38] De Nederlandse Staat werd in deze procedure als privaatrechtelijke rechtspersoon aangesproken. De *Urgenda*-uitspraak bevestigde dat fundamentele rechten kunnen doorwerken in privaatrechtelijke verhoudingen. De Hoge Raad oordeelde specifiek dat artikel 2 en 8 EVRM positieve verplichtingen scheppen voor de staat om burgers te beschermen tegen klimaatverandering.

In het *Shell/Milieudefensie*-arrest werd de *Urgenda*-argumentatie succesvol uitgebreid naar private bedrijven, waarbij Shell werd verplicht om bij te dragen aan de *Paris Climate Agreement*.[39] Het gerechtshof Den Haag vernietigde in 2024 de specifieke reductiedoelstelling van 45%, maar handhaafde de kernoverweging dat bedrijven verantwoordelijkheid kunnen dragen om via indirecte horizontale doorwerking fundamentele rechten te beschermen. Ook werd aangenomen dat sommige fundamentele rechten uit het Handvest in horizontale verhoudingen kunnen worden toegepast.[40] Niet alleen overheden, maar ook bedrijven hebben een positieve verplichting die voortvloeit uit verdragen en beginselen.[41]

4.2. Sociale media platformen als onmisbare infrastructuur van het publieke debat

Grote sociale media platformen vervullen in de huidige digitale infrastructuur een onmisbare functie. Het maatschappelijk debat vindt voornamelijk online plaats, via sociale media platformen die hun gebruikers een ruimte bieden om standpunten uit te wisselen. De platformen zijn dus in belangrijke mate bepalend voor (de toegang tot) het maatschappelijk

34. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*) ro. 7.53.
35. K Jansen, *Waarde, werking en potentie van het EU-Grondrechtenhandvest in de Nederlandse rechtsorde*, Deventer: Wolters Kluwers 2024, par. 4.2.2.
36. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*).
37. HR 9 januari 1987, ECLI:NL:HR:1987:AG5500 (*Edamse bijstandsmoeder*), r.o. 4.4.
38. HR 20 december 2019, ECLI:NL:HR:2019:2006 (*Urgenda*)
39. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*).
40. HvJ EU 6 november 2018, ECLI:EU:C:2018:874 (*Max-Planck/Tetsuji Shimizu*); HvJ EU 9 november 2023, ECLI:EU:C:2023:834 (*Keolis Agen*).
41. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*) r.o. 7.25-7.27.

debat,[42] en worden in de literatuur ook wel aangeduid als "wielders of considerable opinion power".[43] Meer dan driekwart van de jongeren tussen 16 en 24 jaar gebruiken sociale media om op de hoogte te blijven van het laatste nieuws.[44] Men is in een steeds grotere mate afhankelijk van sociale media platformen om tot nieuws en andere informatie te komen die van belang is voor de vrije meningsvorming.[45] De Wetenschappelijke Raad voor het Regeringsbeleid spreekt van een "transformatie van de informatieomgeving" die sociale mediaplatformen een centrale rol geven in de informatieomgeving. [46]

Sociale media platformen vervullen hiermee een onmisbare functie in het publieke debat en zijn voor burgers onontkoombaar. Zo oordeelde het Europees Hof voor de Rechten van de Mens ("EHRM") dat het internet inmiddels een van de belangrijkste middelen is geworden waarmee individuen hun recht op vrijheid van meningsuiting en informatie uitoefenen, aangezien het instrumenten biedt voor deelname aan activiteiten en discussies over politieke kwesties en kwesties van algemeen belang.[47] Dit geldt des te meer voor sociale media platformen waarop journalisten, politici en burgers dagelijks debatteren over actuele gebeurtenissen.

Bij de beoordeling of er sprake is van een inbreuk op de vrijheid van meningsuiting acht het EHRM het verder relevant of er alternatieve plekken zijn waar bepaalde boodschappen kunnen worden uitgedragen.[48] Een beperkt aantal sociale media platformen heeft een groot bereik waarbinnen het publieke debat zich afspeelt. Het groot aantal gebruikers van deze platforms trekt nieuwe gebruikers aan, omdat het publieke debat zich in toenemende mate op deze platforms afspeelt naarmate het aantal gebruikers groeit. Om mee te doen aan dat publieke debat zullen niet-gebruikers zich genoodzaakt voelen om een account aan te maken. Dit fenomeen wordt ook wel netwerkeffecten genoemd.[49]

Dit is een fundamentele verandering ten opzichte van de situatie waarbij de nieuwsvoorziening werd gegenereerd door verschillende kranten, radio- en televisiezenders en andere nieuwsmedia. In die situatie hadden burgers ruime keuze tussen media van verschillende politieke kleuren en invalshoeken, waardoor een krant die een ingezonden brief weigerde geen wezenlijke belemmering vormde voor de toegang tot het publieke debat. Een burger kon immers elders terecht. Die keuzevrijheid ontbreekt grotendeels wanneer een zeer beperkt aantal platforms een groot deel van de informatieomgeving domineert en daarmee de pluriformiteit van de nieuwsvoorziening bepaalt.

Terugkomend op de redenering van het hof in *Shell/Milieudefensie*, heeft het moderatiebeleid van sociale media platformen betrekking op entiteiten met unieke technologische capaciteiten en een vaak zeer dominante (economische) positie op het wereldtoneel. Er zou in lijn met het *Shell/Milieudefensie*-arrest kunnen worden betoogd dat op sociale media platformen een vergelijkbare plicht rust om het publieke debat en hiermee de democratie te beschermen. Zoals fossiele brandstoffen bijdragen aan klimaatverandering, zo vormen sociale media platformen de belangrijkste infrastructuur van het democratisch debat.[50] De quasi-monopolistische positie van sociale media platformen creëert een vergelijkbare machtspositie als die van bedrijven als Shell.

Op basis van het bovenstaande kan worden betoogd dat op sociale media platformen met een dergelijke monopolistische positie, net als op overheden, een grotere verantwoordelijkheid rust om de vrijheid van meningsuiting te waarborgen.
Ondanks dat er nog geen jurisprudentie van het EHRM of het Hof van Justitie van de Europese Unie ("HvJEU") bestaat over het verwijderen van inhoud door platformen, kan wel van platformen worden verlangd dat ze zich houden aan de beginselen uit de rechtspraak van beide rechtscolleges.

5. INVULLING MAATSCHAPPELIJKE ZORGVULDIGHEIDSNORM

Fundamentele rechten kunnen doorwerken in privaatrechtelijke verhoudingen en richting geven aan open normen, zoals aan de maatschappelijke zorgvuldigheidsnorm uit artikel 6:162 BW. Voor de invulling van de maatschappelijke zorgvuldigheidsnorm is het van belang om te kijken naar objectieve aanknopingspunten, zoals wetgeving, algemene rechtsbeginselen, jurisprudentie en deskundigenrapporten.

Cruciaal voor deze invulling is het onderscheid dat het hof Den Haag maakt tussen de terughoudendheid van het EHRM op de toetsing van staatsbeleid enerzijds, en nationale rechterlijke bescherming van fundamentele rechten anderzijds, die minder terug-

42. A.P. Heldt, 'Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum', *Mitchell Hamline Law Review* 2020/46, afl.5, p. 1027.
43. N. Helberger, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power', *Digital Journalism* 2020/8(6).
44. K. Schut, I. Costera Meijer en E. Lauf, 'Jongeren, nieuws en sociale media. Een blik op de toekomst van het nieuws', 2024, p. 8.
45. K. Schut, I. Costera Meijer en E. Lauf, 'Jongeren, nieuws en sociale media. Een blik op de toekomst van het nieuws', 2024, p. 13.
46. WRR, 'Aandacht voor media. Naar nieuwe waarborgen voor hun democratische functies', wrr.nl, 3 oktober 2024.
47. EHRM 18 december 2018, ECLI:CE:ECHR:2012:1218JUD000311110 (*Ahmet Yıldırım v. Turkey)* r.o. 54.
48. EHRM 6 mei 2003, ECLI:CE:ECHR:2003:0506JUD004430698 (*Appleby v. UK*).
49. J. Van Dijk, (2011).'Social media in de netwerkmaatschappij', in: D. Van Zijl (ed.), *Basisboek social media*, Boom Lemma, p. 15-43.
50. A.P. Heldt, 'Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum', *Mitchell Hamline Law Review* 2020/46, afl.5, p. 1027.

houdend hoeft te zijn.[51] Hoewel het EHRM staten bijvoorbeeld een ruime beoordelingsmarge laat bij de keuze van middelen om bijvoorbeeld klimaatverandering tegen te gaan, volgt daaruit *niet* dat de civiele rechter geen concrete rechtsplicht voor een bedrijf zou kunnen aannemen.[52] Het aannemen van die rechtsplicht ontneemt bedrijven immers niet de ruimte om zelf te beoordelen welke middelen er nodig zijn om aan die rechtsplicht te voldoen. Bovendien ziet de terughoudendheid van het EHRM op de toetsing van staatsbeleid, het EHRM schrijft niet voor dat de nationale rechter dezelfde terughoudendheid moet betrachten bij de bescherming van de in het EVRM verankerde fundamentele rechten in verhoudingen van de burger tegenover een onderneming.

In de situatie dat fundamentele rechten doorwerken in open (privaatrechtelijke) normen vindt er een belangenafweging plaats op basis van alle relevante omstandigheden van het geval. Zo een belangenafweging vindt bijvoorbeeld plaats bij de beoordeling van de rechtmatigheid van perspublicaties.[53] Ook in het kader van de beoordeling van de rechtmatigheid van demonstraties die belangen van private ondernemingen raken vindt een belangenafweging plaats.[54] De voor de belangenafweging relevante factoren vinden steeds hun oorsprong in EVRM-bepalingen en -jurisprudentie.

Het hof Den Haag stelde uiteindelijk vast dat de maatschappelijke zorgvuldigheidsnorm, ingevuld aan de hand van fundamentele rechten en soft law-instrumenten als de UNGP en OESO-richtlijnen, bedrijven verplicht hun verantwoordelijkheid te nemen voor fundamentele rechtenschendingen in de uitoefening van hun activiteiten.[55]
Op dezelfde wijze kan de Nederlandse rechter, niettegenstaande de beoordelingsruimte van sociale media platformen, mogelijk vaststellen dat sociale media platformen de maatschappelijke zorgvuldigheidsnorm schenden door *shadowbanning*.

5.1. Fundamentele rechten: artikel 10 EVRM

Hoewel fundamentele rechten niet direct van toepassing zijn op sociale media platformen en burgers hier tegenover sociale media platformen geen direct beroep op kunnen doen, kunnen gebruikers wel een beroep doen op de (indirecte) horizontale werking van fundamentele rechter. Men zou dus kunnen betogen dat gebruikers mogelijk beschermd worden tegen *shadowbanning* via de (indirecte) horizontale doorwerking van artikel 10 EVRM: het recht op vrijheid van meningsuiting.

Deze opvatting wordt onderschreven door de Belgische rechter. In *Vandendriessche/Meta* oordeelde het hof van Gent dat Meta met het opleggen van de *shadowban* niet handelde overeenkomstig het beginsel van de uitvoering te goeder trouw van de overeenkomsten.[56] Het hof van Gent oordeelt in dit verband dat bepalingen uit het EVRM op indirecte wijze kunnen doorwerken in privaatrechtelijke verhoudingen, zoals bij de invulling van open (privaatrechtelijke) normen. Het hof benoemt daarbij expliciet artikel 10 EVRM.[57]

Bij de beoordeling van de rechtmatigheid van *shadowbanning* door invulling van de maatschappelijke zorgvuldigheidsnorm aan de hand van artikel 10 EVRM zijn onder meer de volgende principes van belang.

De uitingsvrijheid is in onze democratische samenleving een belangrijk grondrecht en er moet zeer terughoudend worden omgegaan met een inperking van dit recht.[58] Volgens het EHRM is de toegang tot platformen essentieel voor het uitoefenen van de vrijheid van meningsuiting.[59] De uitingsvrijheid omvat het recht om uitingen te verspreiden en het recht om deze uitingen te kunnen ontvangen.[60] *Shadowbanning* raakt aan beide vrijheden.

Aan zowel politieke uitingen[61] als uitingen over zaken van publiek belang[62] komt een hogere mate van bescherming toe. Het publiek belang omvat onderwerpen die de samenleving zodanig raken dat zij daar legitiem belangstelling voor kan hebben, die publieke aandacht genereren of die burgers direct raken, zoals kwesties hun welzijn of het functioneren van de samenleving beïnvloeden. Dit omvat ook onderwerpen die tot aanzienlijke controverse kunnen leiden, belangrijke maatschappelijke kwesties

51. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*) ro 7.11.
52. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*) ro 7.11.
53. HR 6 januari 1995, ECLI:NL:HR:1995:ZC1602 (*Parool/Van Gasteren*) r.o. 5.8.3.2.
54. Rb. Amsterdam 1 augustus 2024, ECLI:NL:RBAMS:2024:4820 (One-Dyas/Greenpeace).
55. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*) ro 7.26-7.27.
56. Hof van beroep Gent, 3 juni 2023, 2022/AR/508, r.o. 1.1.7.6.6.
57. Hof van beroep Gent, 3 juni 2023, 2022/AR/508, r.o. 1.1.4.2.
58. EHRM 20 februari 2003, ECLI:CE:ECHR:2003:0220JUD002065292 *(Djavit An t. Turkije*), par. 57; EHRM 15 oktober 2015, ECLI:CE:ECHR:2015:1015JUD003755305 (*Kudrevičius c.s. t. Litouwen*), par. 158.
59. EHRM 18 december 2018, ECLI:CE:ECHR:2012:1218JUD000311110 (*Ahmet Yıldırım v. Turkey).*
60. EHRM 26 november 1991, ECLI:CE:ECHR:1991:1126JUD001358588 (*Observer and Guardian v. the United Kingdom*), § 59.
61. EHRM 11 april 2006, ECLI:CE:ECHR:2006:0411JUD00713430 (*Brasilier v. Frankrijk*) § 41.
62. EHRM 8 juni 1999, ECLI:CE:ECHR:1999:0708JUD002668295 (*Sürek v. Turkey*), § 61; EHRM 22 oktober 2007, ECLI:CE:ECHR:2007:1022JUD002127902 (*Lindon, Otchakovsky-Laurens and July v. France*), § 46; EHRM 25 november 1996, ECLI:CE:ECHR:1996:1125JUD001741990 (*Wingrove v. the United Kingdom*), § 58.

omvatten of problemen betreffen waarover het publiek geïnformeerd moet kunnen worden.[63]
Daarbij kan volgens het EHRM worden gedacht aan publicaties over historische gebeurtenissen,[64] milieubescherming en volksgezondheid.[65] Het EHRM benadrukt dat in een democratische samenleving vrij debat moet kunnen plaatsvinden over de oorzaken van feiten van bijzondere ernst die misdrijven tegen de menselijkheid vormen.[66]

Het maakt daarbij niet uit of de uitingen mogelijk beledigen, schokken of verontrusten. De bescherming is immers niet alleen van toepassing op informatie of ideeën die als positief of onschuldig worden ervaren. Dit principe is volgens het EHRM inherent aan het pluralisme en de ruimdenkendheid die een democratische samenleving vormen.[67]
Aan uitingen van *social watchdogs* komt een hoog beschermingsniveau toe.[68] *Social watchdogs* kunnen bijvoorbeeld NGO's zijn, maar ook bloggers en actieve sociale media gebruikers die een actieve rol vervullen in het publieke debat,[69] "*gezien de belangrijke rol die het internet speelt bij het verbeteren van de toegang van het publiek tot nieuws en het vergemakkelijken van de verspreiding van informatie in het algemeen*" (vertaling auteurs).[70] De "publieke waakhond"-functie is dus niet langer exclusief voor traditionele journalistiek gereserveerd.[71] Langs deze lijn kan men eveneens betogen dat online (activistische of politieke) uitingen op zich onder de reikwijdte van de bescherming van artikel 10 EVRM vallen. De internetgebruiker is niet slechts een ontvanger van informatie, maar genereert ook zelf informatie.[72]

Aan uitingen die voor anderen nodeloos grievend zijn en daarmee een inbreuk vormen op hun rechten, en die bovendien niet bijdragen aan enig constructief publiek debat komt juist een beperktere bescherming toe.[73]

Hoewel het beperkingsschema van artikel 10 lid 2 EVRM zoals eerder gezegd niet direct van toepassing is op sociale media platformen, kunnen daaruit wel verschillende omstandigheden worden afgeleid die relevant zijn voor de belangenafweging.[74]
Die omstandigheden kunnen worden gevonden in de legitieme belangen die in artikel 10 lid 2 EVRM worden genoemd, zoals de bescherming van de rechten en vrijheden van anderen. De omstandigheid dat sociale media platformen met een zichtbaarheidsmaatregel handelen in overeenstemming met hun contentbeleid kan relevant zijn, omdat deze richtlijnen een uitwerking zijn van het fundamentele eigendomsrecht van platformen.[75] Zij mogen immers zelfs de regels stellen die op hun platform van toepassing zijn.

Ook kan worden betoogd dat zichtbaarheidsmaatregelen die sociale media platformen nemen ten behoeve van de volksgezondheid een legitieme beperking van de uitingsvrijheid vormen. De rechtbank Amsterdam overwoog in dit verband dat Facebook niet onrechtmatig handelde door haar COVID-19 beleid, dat zij in lijn opstelde met een oproep van de Europese Commissie, toe te passen.[76]
Daarnaast zijn er situaties denkbaar waarin sociale media platformen een *shadowban* toepassen in het belang van nationale veiligheid, de openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten, zoals bij het oproepen tot geweld.

Tot slot is het ook mogelijk dat zichtbaarheidsmaatregelen juist worden genomen om pluriformiteit van het publieke debat te beschermen. Wanneer aanbevelingssystemen extreme content onevenredig veel aandacht geven en de tijdlijn van gebruikers daardoor een vertekend beeld geeft, kunnen zichtbaarheidsmaatregelen de vrijheid van meningsuiting juist ten goede komen. Deze omstandigheid zou ook relevant kunnen zijn in het kader van de belangenafweging.

5.2. Soft law

Het gerechtshof Den Haag overwoog dat uit de *UN Guiding Principles on Business and Human Rights*

63. EHRM 26 juni 2017, ECLI:CE:ECHR:2017:0627JUD000093113 *(Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland)*, § 171.
64. EHRM 14 september 2010, ECLI:CE:ECHR:2010:0914JUD000266807 (*Dink t. Turkije*), § 135.
65. EHRM 7 november 2006, ECLI:CE:ECHR:2006:1107JUD001269703 (*Mamère t. Frankrijk*), § 20; EHRM 8 september 2020, ECLI:CE:ECHR:2020:0908JUD002264908 (*OOO Regnum t. Rusland*), § 68-69.
66. EHRM 31 januari 2006, ECLI:CE:ECHR:2006:0131JUD006401600 (*Giniewski t. Frankrijk*), § 51.
67. EHRM 7 december 1976, ECLI:CE:ECHR:1976:1207JUD000549372 *(Handyside v. the United Kingdom*), § 49; EHRM 26 november 1991, ECLI:CE:ECHR:1991:1126JUD001358588 (*Observer and Guardian v. the United Kingdom)*, § 59.
68. EHRM 17 februari 2015, nr. 6987/07 (*Guseva t. Bulgarije).*
69. EHRM 8 november 2016, nr. 18030/11 (*MHB t. Hongarije*).
70. EHRM 20 maart 2018, ECLI:CE:ECHR:2018:0320JUD004579113 (*Falzon v. Malta*), § 57. EHRM 20 maart 2018, ECLI:CE:ECHR:2018:0320JUD004579113 (*Falzon v. Malta*), § 57.
71. EHRM 8 november 2016, ECLI:CE:ECHR:2016:1108JUD001803011 (*Magyar Helsinki Bizottság v. Hungary*); M. Oosterveld, M. Oostveen, 'Van 'public watchdog' naar 'public watchblog': het EHRM en journalistieke weblogs'. *Mediaforum 2013, nr. 6.*
72. T.M. Harrison, B. Barthel, 'Wielding new media in Web 2.0: exploring the history of engagement with the collaborative construction of media products',*New Media & Society* 2009, p. 159-160.
73. EHRM 20 september 1994, ECLI:CE:ECHR:1994:0920JUD001347087 (*Otto-preminger-instituut v. Oostenrijk*) § 49.
74. Rb. Amsterdam 13 oktober 2020, ECLI:NL:RBAMS:2020:4966, r.o. 4.23.
75. Rb. Amsterdam 13 oktober 2020, ECLI:NL:RBAMS:2020:4966, r.o. 4.23.
76. Rb. Amsterdam 13 oktober 2020, ECLI:NL:RBAMS:2020:4966, r.o. 4.23, 4.24.

("UNGP")[77] en OESO-richtlijnen[78] volgt dat bedrijven hun verantwoordelijkheid moeten nemen voor (dreigende) fundamentele rechtenschendingen waarmee zij in de uitoefening van hun activiteiten worden geconfronteerd.[79] Door het *Shell/Milieudefensie*-arrest wordt het normatieve gehalte van '*soft law*' zichtbaar, wat leidt tot een nieuwe vorm van niet-bindende (private) regelgeving waaraan de rechter doorslaggevende betekenis kan toekennen.[80]

Uit onder meer de UNGP volgt dat de plicht van bedrijven om fundamentele rechten te respecteren een mondiale gedragsnorm is die voor alle ondernemingen geldt, ongeacht waar zij opereren. Ondernemingen kunnen zich daarbij niet beperken tot het volgen van ontwikkelingen of maatregelen die door staten worden getroffen.[81] In de UNGP is ook vastgelegd dat bedrijven zich moeten inspannen om negatieve gevolgen voor fundamentele rechten die rechtstreeks samenhangen met hun activiteiten, producten of diensten, via hun zakelijke relaties te voorkomen of te beperken, ook wanneer zij daar niet zelf direct aan hebben bijgedragen.[82] Sociale media platformen zoals Meta hebben de UNGP onderschreven en erkennen daarmee deze verantwoordelijkheid.

Verder oordeelde de Hoge Raad dat verwacht mag worden dat bedrijven zich houden aan de door henzelf opgestelde voorschriften, denk aan de contractuele verplichtingen van techbedrijven tegenover hun gebruikers. Niet naleving kan een toerekenbare tekortkoming en onrechtmatige daad opleveren.[83]

5.3. Beoordeling

Bij de beoordeling of het opleggen van een shadowban door een platform een onrechtmatige daad oplevert in de zin van artikel 6:162 BW, wordt aangesloten bij de maatschappelijke zorgvuldigheidsnorm. Deze norm wordt ingevuld aan de hand van objectieve aanknopingspunten zoals wetgeving, fundamentele rechten (met name artikel 10 EVRM), jurisprudentie en internationale soft law-instrumenten (zoals de UNGP en OESO-richtlijnen).

De kernvraag is of het platform heeft gehandeld in strijd met hetgeen in het maatschappelijk verkeer betaamt, waarbij de bijzondere positie van platforms als poortwachters van het publieke debat zwaar weegt. Bij de invulling van de zorgvuldigheidsnorm komt het erop aan welk handelen van een persoon of onderneming mag worden gevergd, met name wanneer dat handelen niet is voorgeschreven in specifieke regelgeving. De vraag is dus: wat mag van sociale media platformen worden verwacht?
Sociale media platformen zoals Meta en X genieten vrijheid in hoe zij modereren, maar deze beoordelingsruimte ontslaat hen volgens ons niet van de fundamentele plicht om uitingsvrijheid te respecteren.

Van sociale media platformen mag worden verwacht dat zij de vrijheid van meningsuiting respecteren, conform hun eigen gebruiksvoorwaarden handelen en zich houden aan de beginselen die zij zelf onderschrijven in internationale richtlijnen zoals de UNGP. Deze verwachting vindt haar grondslag in de maatschappelijke (machts)positie die deze platformen innemen als poortwachters van het publieke debat.
Platformen genieten weliswaar beoordelingsruimte in hun moderatiebeleid, maar deze vrijheid is niet onbegrensd. Van hen mag worden verlangd dat zij moderatiepraktijken transparant maken, willekeur vermijden en voorzien in effectieve rechtsmiddelen wanneer gebruikers worden beperkt in hun mogelijkheden om uitingen te verspreiden, ook als deze beledigen, schokken of verontrusten.

Het enkele feit dat specifieke wettelijke verplichtingen gelden, zoals de transparantievereisten van artikel 17 DSA, ontslaat platformen niet van deze bredere zorgvuldigheidsverplichtingen. Het gerechtshof overwoog immers eerder dat door de wetgever genomen maatregelen op zichzelf niet uitputtend zijn.[84] Hetzelfde geldt voor de huidige wet- en regelgeving omtrent *shadowbanning*.

De maatschappelijke zorgvuldigheid, ingevuld aan de hand van 10 EVRM en soft law als de UNGP en de OESO-richtlijnen, vergt van sociale media platformen dat zij in dit opzicht hun verantwoordelijkheid nemen. *Shadowbanning* schendt de zorgvuldigheidsnorm, omdat het de kern van artikel 10 EVRM aantast: het censureert onzichtbaar juist die politieke uitingen die volgens het EHRM de hoogste bescherming genieten, meestal zonder kennisgeving, motivering of beroepsmogelijkheid.
Platformen bezitten bovendien de technische en financiële capaciteit om transparante moderatie te bieden, waardoor *shadowbanning* noch technisch noch financieel noodzakelijk is.

Shadowbanning kan dus onrechtmatig zijn wanneer het platform zonder transparantie, motivering of effectieve rechtsmiddelen uitingen beperkt, vooral als

77. '*Guiding principles on business and human rights; Implementing the United Nations "Protect, Respect and Remedy" Framework*', United Nations Human Rights, Office of the High Commissioner, 2011.
78. *OESO-richtlijnen voor multinationale ondernemingen inzake maatschappelijk verantwoord ondernemen*, OECD, OECD Publishing, Parijs, 2024.
79. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (Milieudefensie/Shell) ro. 7.21.
80. B.A. Kuiper-Slendebroek, 'Soft law, hard consequences? Over niet-bindende instrumenten en aansprakelijkheid', *AV&S* 2023/19, afl. 4, p. 110.
81. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*), ro 4.3.
82. '*Guiding principles on business and human rights; Implementing the United Nations "Protect, Respect and Remedy" Framework*', United Nations Human Rights, Office of the High Commissioner, 2011, hs. II.
83. HR 2 maart 2001, ECLI:NL:HR:2001:AB0377 (*Trombose I*) r.o. 3.3.3.
84. Hof Den Haag 12 november 2024, ECLI:NL:GHDHA:2024:2099 (*Milieudefensie/Shell*) ro. 7.53.

het gaat om politieke of maatschappelijk relevante uitingen. De toerekenbaarheid volgt uit het niet naleven van contractuele, wettelijke of zelfopgelegde normen. Schade doet zich vervolgens voor doordat gebruikers worden uitgesloten van het publieke debat zonder melding of mogelijkheid tot verweer, wat de vrijheid van meningsuiting aantast. Er is sprake van causaal verband, nu de *shadowban* direct leidt tot beperking van bereik en zichtbaarheid. Tot slot is de relativiteit gegeven, omdat de maatschappelijke zorgvuldigheidsnorm mede strekt tot bescherming van uitingsvrijheid en het publieke debat.

Hierbij moet de kanttekening worden geplaatst dat (ook) de onrechtmatige daad geen effectieve remedie kan vormen tegen shadowbanning als de gebruiker niet op de hoogte is (gebracht) van de opgelegde *shadowban*.

6. CONCLUSIE

Shadowbanning ondermijnt het publieke debat doordat het gebruikers – zonder dat zij zich hier van bewust zijn - beperkt in hun mogelijkheden om uitingen te verspreiden, zonder kennisgeving, motivering of beroepsmogelijkheid. *Shadowbanning* schendt artikel 10 EVRM op twee niveaus tegelijk. Enerzijds belemmert het de spreker in zijn recht om informatie en ideeën te verspreiden. Anderzijds ontneemt het het publiek de mogelijkheid om die informatie te ontvangen. Deze schending is des te ernstiger omdat het onzichtbaar geschiedt: noch de spreker noch het publiek weet dat censuur plaatsvindt.

Hoewel de DSA en AVG transparantie- en motiveringsverplichtingen bevatten, zijn deze bij gebrekkige naleving en handhaving weinig effectief. Inherent aan *shadowbanning* is immers dat gebruikers niet op de hoogte zijn van de opgelegde maatregel, wat effectieve handhaving door betrokkenen bemoeilijkt. Bovendien betreffen deze verplichtingen formele eisen, die geen inhoudelijke toets bieden met betrekking tot de rechtmatigheid van zichtbaarheidsbeperkingen zelf.

De maatschappelijke zorgvuldigheidsnorm van artikel 6:162 BW, ingevuld aan de hand van artikel 10 EVRM en soft law-instrumenten als de UNGP, biedt een juridisch kader om deze lacune te adresseren. In navolging van het *Shell/Milieudefensie*-arrest kunnen fundamentele rechten via indirecte horizontale doorwerking richting geven aan open privaatrechtelijke normen. Sociale media platformen vervullen als infrastructuur van het publieke debat een quasi-publieke functie en hebben door hun dominante marktpositie, beperkte alternatieven voor gebruikers, en het onderschrijven van internationale fundamentele rechtenrichtlijnen een vergelijkbare verantwoordelijkheid als de staat voor de bescherming van artikel 10 EVRM.

Van platformen mag worden verwacht dat zij transparant modereren, willekeur vermijden en effectieve rechtsmiddelen bieden. Het enkele bestaan van specifieke wettelijke verplichtingen ontslaat hen niet van deze bredere zorgvuldigheidsverplichtingen; maatregelen die de wetgever heeft genomen zijn immers op zichzelf niet uitputtend. *Shadowbanning* van (politieke en activistische) uitingen kan daarom een schending van artikel 6:162 BW opleveren wanneer platforms daarmee hun verantwoordelijkheid voor de bescherming van de vrijheid van meningsuiting niet nakomen, ongeacht naleving van formele transparantievereisten. Hierbij geldt wel dat onrechtmatige daad pas een effectief rechtsmiddel kan vormen indien de gebruiker op de hoogte is van de *shadowban,* hetgeen niet steeds het geval zal zijn.

Digital en AI Omnibus: simplificatie is nog geen deregulering

mr. F.P. Sickinghe[1]

Dit artikel bevat een overzicht van de voorstellen van de Europese Commissie inzake de Digital Omnibus Package en de belangrijkste discussiepunten.

Op 19 november 2025 presenteerde de Europese Commissie de zogenaamde *Digital Omnibus Package, te weten:* een voorstel voor een Digitale Omnibus inzake data, privacy en cybersecurity,[2] en een voorstel inzake kunstmatige intelligentie: de AI Omnibus. Het betreft een pakket van maatregelen ter vereenvoudiging en stroomlijnen van het digitale regelgevingskader voor toegang tot data, privacy, cyberbeveiliging en kunstmatige intelligentie.

In de mededeling 'Een eenvoudiger en sneller Europa'[3] presenteerde de Commissie haar aanpak tot aanpassing van het regelgevingskader van de Unie. De Commissie wil het EU-acquis vereenvoudigen, verduidelijken en verbeteren. De naleving voor bedrijven moet eenvoudiger en goedkoper worden, als een belangrijke maatregel ter ondersteuning van het concurrentievermogen van de EU. Deze visie weerspiegelt het bredere plan dat Commissievoorzitter Von der Leyen heeft uiteengezet in haar politieke richtlijnen voor de periode 2024-2029.[4] Zoals ook benoemd in de rapporten van Draghi en Letta heeft de opeenstapeling van regels een negatief effect op het concurrentievermogen. Snelle en zichtbare verbeteringen zijn nodig voor burgers en bedrijven, door een meer kosteneffectieve en innovatievriendelijke implementatie van de regels – met behoud van hoge normen en de eerder vastgestelde doelstellingen, aldus – verkort weergegeven - de Commissie in het toelichtend memorandum bij de Digitale Omnibus.

De voorstellen moeten worden beschouwd als het standpunt van de Commissie aan het begin van een levendig debat en intense onderhandelingen in de Raad van Ministers en het Europees Parlement.

De Digitale Omnibus aan maatregelen omvat – benoemd in kerndomeinen - voorstellen voor:

A. Data/Privacy: Wijzigingen in de Algemene Verordening Gegevensbescherming (AVG)[5], wijzigingen in de Dataverordening[6], met inbegrip van de consolidatie van de Digital Governance Act[7], de Open Data Richtlijn[8] en de verordening betreffende het vrije verkeer van niet-persoonsgebonden gegevens[9] in de Dataverordening;
B. Cybersecurity: Het instellen van één centraal meldpunt voor alle incidenten in het kader van de AVG, de Richtlijn Netwerk- en Informatiebeveiliging 2 (NIS2)[10], de Richtlijn Digitale Operationele Veerkracht (DORA)[11] en de Richtlijn Veerkracht Kritieke Entiteiten (CER)[12];

– Intrekking van het Platform to Business (P2B) verordening[13];
– Wijziging van de regels voor "cookie-toestemming";
– Wijziging van de definitie van persoonsgegevens en bijzondere categorieën gegevens; en
– Het toestaan van de verwerking van persoonsgegevens voor het trainen van AI-modellen op basis van een gerechtvaardigd belang.

Op dezelfde datum publiceerde de Commissie een aanbeveling over niet-bindende modelcontractvoorwaarden voor toegang tot en gebruik van gegevens en niet-bindende standaardcontractbepalingen voor cloudcomputingcontracten in het kader van de Da-

1. Feyo Sickinghe is principal regulatory counsel bij Bird & Bird in Den Haag en Brussel. Dit artikel is tot stand gekomen met bijdragen van Francine Cunningham, Berend van der Eijk, Nora Santalu en Tobias Bräutigam van Bird & Bird. De tekst van dit artikel is afgesloten op 20 maart 2026.
2. https://digital-strategy.ec.europa.eu/nl/library/digital-omnibus-regulation-proposal
3. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, Een eenvoudiger en sneller Europa: Mededeling over implementatie en vereenvoudiging, COM(2025)47 final, 11 februari 2025: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex
4. Von der Leyen, U. (2024) *Europe's Choice: Political Guidelines for the Next European Commission 2024-2029*: https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf
5. Verordening (EU) 2016/679
6. Verordening (EU) 2023/2854
7. Verordening (EU) 2022/868
8. Richtlijn (EU) 2019/1024
9. Verordening (EU) 2018/1807
10. Richtlijn 2025/2555
11. Verordening (EU) 2022/2554
12. Richtlijn (EU) 2022/2557
13. Verordening (EU) 2019/1150. Deze verordening is grotendeels vervangen door Verordening (EU) 2022/1925 (de Digital Markets Act (DMA) en Verordening (EU) 2022/2065 (de Digital Services Act (DSA). De relevante wijzigingen worden in dit artikel niet verder besproken

taverordening.[14] De Commissie zal tevens richtlijnen publiceren over redelijke vergoedingen om te verduidelijken welke bedragen aan gegevensontvangers in rekening mogen worden gebracht voor het verplicht delen van gegevens op grond van artikel 5 van de Dataverordening. Verder heeft de Commissie aangekondigd dat zij een juridische helpdesk voor de Dataverordening wil opzetten om bedrijven te helpen met concrete vragen over de toepassing van de nieuwe regels.

De AI Omnibus is gericht op het wijzigen van aspecten van de EU-wetgeving inzake kunstmatige intelligentie.[15] Gezien het belang van de Digitale Omnibus en de AI Omnibus zijn meerdere commissies van het Europees Parlement betrokken bij het opstellen van rapporten. De voorstellen worden hieronder op hoofdlijnen besproken.

1. Dataverordening - Belangrijkste voorgestelde wijzigingen

De wijzigingen zijn erop gericht de administratieve lasten te verlichten, de wetgeving te verduidelijken en de concurrentiepositie van Europa te versterken. Volgens het ontwerp gaat het hierbij om het aanpakken van de volgende onderling samenhangende uitdagingen:

- Bescherming van bedrijfsgeheimen tegen het risico van lekken naar derde landen in het kader van de verplichte bepalingen inzake het delen van IoT-gegevens.
- Het huidige gefragmenteerde en complexe kader voor de samenwerking tussen bedrijven en overheden is deels verouderd en te breed, wat leidt tot juridische onzekerheid.
- De regels inzake essentiële vereisten voor slimme contracten in overeenkomsten voor het delen van gegevens zijn in de praktijk onduidelijk gebleken.
- De bepalingen die het mogelijk maken over te stappen tussen cloud- en gegevensverwerkingsdiensten blijven cruciaal voor het openstellen van de datamarkt, maar zijn niet geschikt voor bestaande contracten voor op maat gemaakte gegevensverwerkingsdiensten en vormen een te zware last, niet alleen voor kleine en middelgrote ondernemingen, maar ook voor grote ondernemingen.
- Het 'wettelijk kader voor gegevensbescherming' is de afgelopen jaren uitgebreid met meerdere regelgevende instrumenten. Dit heeft geleid tot juridische complexiteit, waaronder overlappingen, niet op elkaar afgestemde definities en vragen over de wisselwerking tussen de Data Governance Act en de Dataverordening, de Verordening inzake het vrije verkeer van niet-persoonlijke gegevens[16] en de Open Data Richtlijn.[17]
- De Commissie ziet noodzaak tot vereenvoudiging van de regelgeving en het samenbrengen van regels inzake het hergebruik van gegevens die in handen zijn van overheidsinstanties.

De Commissie stelt voor deze kwesties als volgt aan te pakken:

- *Bescherming van bedrijfsgeheimen (§ 3 en 5)* - Het voorstel introduceert aanvullende waarborgen voor bedrijven die zich zorgen maken dat de huidige Dataverordening onvoldoende bescherming biedt om te voorkomen dat vertrouwelijke informatie in verkeerde handen terechtkomt. Datahouders kunnen weigeren informatie aan gebruikers te verstrekken wanneer er een aanzienlijk risico bestaat dat bedrijfsgeheimen onrechtmatig worden verkregen, gebruikt of bekendgemaakt aan entiteiten in derde landen, met name die landen die opereren onder rechtsstelsels die een zwakkere bescherming bieden dan de EU. Deze wijziging beantwoordt aan de zorgen van talrijke bedrijven over het gebruik van waardevolle informatie en waar de wettelijke waarborgen tekortschieten. De weigering moet gebaseerd zijn op een beoordeling per geval van alle objectieve factoren.

- *Beperking van mogelijkheden voor gegevensuitwisseling tussen bedrijven en overheden (§ 5 t/m 19)* - Het voorstel beperkt de omstandigheden waaronder overheidsinstanties gegevens van bedrijven kunnen eisen aanzienlijk. De trigger verschuift van breed gedefinieerde "uitzonderlijke behoeften" naar specifiek gedefinieerde "openbare noodsituaties". Een nieuw ontwerp van artikel 15a van de Dataverordening zou de enige toegangspoort worden voor dergelijke verzoeken, die alleen van toepassing is wanneer gegevens daadwerkelijk noodzakelijk zijn om te kunnen reageren op een noodsituatie of de gevolgen daarvan te beperken of te herstellen. Dit brengt de broodnodige precisie in wat voorheen een ongemakkelijk vage verplichting was. Cruciaal is dat micro-ondernemingen en kleine bedrijven het recht krijgen compensatie te eisen wanneer zij tijdens noodsituaties verplicht zijn gegevens te verstrekken – waarbij wordt erkend dat de nalevingskosten hoog kunnen zijn, met name voor kleinere spelers. Grotere gegevenshouders zouden in deze noodsituaties kosteloos gegevens moeten verstrekken.

- *Verduidelijking van slimme contracten (§ 26)* - De Commissie schrapt artikel 36 van de Dataverordening waarin essentiële vereisten voor slimme contracten in data-uitwisselingsregelingen zijn vastgelegd. Hiermee beoogt de Commissie juridische onzekerheden op te lossen en innovatie te stimuleren op het terrein van data-uitwisselingsovereenkomsten, waardoor bedrijven meer ruimte krijgen om oplossingen te ontwikkelen die werken voor hun specifieke omstandigheden.

14. https://digital-strategy.ec.europa.eu/en/library/draft-recommendation-non-binding-model-contractual-terms-data-access-and-use-and-non-binding
15. digital-strategy.ec.europa.eu/nl/library/digital-omnibus-ai-regulation-proposal
16. Verordening (EU) 2018/1807
17. Verordening (EU) 2019/1024

– *Regime voor cloud-switching aangepast (§ 20-22)* - Er komt een soepeler regime voor op maat gemaakte dataverwerkingsdiensten (dat wil zeggen diensten die niet standaard zijn en zonder voorafgaande aanpassing niet zouden functioneren), maar alleen als deze worden geleverd onder contracten gesloten vóór of op 12 september 2025. Evenzo krijgen MKB-bedrijven en kleine bedrijven die andere diensten dan infrastructuur-as-a-service (IaaS diensten) leveren onder contracten die vóór of op 12 september 2025 zijn gesloten, vrijstellingen van bepaalde vereisten. De wijzigingen beogen de lasten voor aanbieders van maatwerkdiensten en kleinere bedrijven te verlichten, terwijl tegelijkertijd gewerkt wordt aan het elimineren van *vendor lock-ins*. Ze weerspiegelen ook het standpunt van de Commissie over boetes voor vroegtijdige beëindiging, een onderwerp dat de afgelopen zes maanden veelvuldig is besproken.

– *Opzeggen van cloudcontracten* - De Dataverordening voorziet in de eis dat ieder cloudcontract, ook contracten voor bepaalde tijd, tussentijds kunnen worden opgezegd met een opzegtermijn van 2 maanden. Voor andere dataverwerkingsdiensten dan IaaS diensten mogen aanbieders bepalingen over evenredige boetes voor vroegtijdige beëindiging opnemen in een contract met een vaste looptijd. Het voorstel gaat niet in op de redenen waarom IaaS diensten zijn uitgesloten.

– *Vrijwillige certificering en versterking van vertrouwen (§ 23 t/m 25)* - Het verplichte regime voor databemiddelingsdiensten, voortvloeiend uit de Data Governance Act, wordt omgevormd tot een vrijwillig, vertrouwensversterkend kader. Dit stelt neutrale marktpartijen in staat zich te onderscheiden en tegelijkertijd de regelgevingslast te verminderen. De Commissie gaat een openbaar EU-register bijhouden met erkende aanbieders van databemiddelingsdiensten en erkende organisaties voor data-altruïsme. Dit moet zorgen voor transparantie en bedrijven helpen betrouwbare partners te vinden in het ecosysteem voor gegevensdeling.

– *Drie rechtsinstrumenten worden samengevoegd (§ 27)* - De Commissie stelt verder voor drie afzonderlijke rechtsinstrumenten samen te voegen in de Dataverordening: De consolidatie van de Verordening inzake het vrije verkeer van niet-persoonlijke gegevens, Data Governance Act en de Open Data-richtlijn heeft tot doel een uniform reglement op te stellen voor het hergebruik van gegevens die in handen zijn van overheidsinstanties. Hiermee worden de overlappende en soms tegenstrijdige bepalingen die zowel bedrijven als overheidsinstanties in verwarring brengen geëlimineerd. Verouderde eisen worden afgeschaft en vervangen door een samenhangend geheel van regels.

2. AI Verordening, AVG en cyber - Belangrijkste voorgestelde wijzigingen

– *Verlenging van termijnen (§ 30)* - Het voorstel omvat wijzigingen in de termijnen voor systemen met een hoog risico. De regels voor systemen met een hoog risico in Bijlage III zijn momenteel van toepassing vanaf 2 augustus 2026. Het voorstel verlengt deze termijn op basis van het moment waarop de Commissie vaststelt dat de noodzakelijke ondersteuningsmaatregelen voor naleving beschikbaar zijn. Zodra de Commissie dit vaststelt, hebben entiteiten 6 maanden de tijd om aan de regels te voldoen. Ongeacht de vaststelling door de Commissie zullen de regels uiterlijk op 2 december 2027 van toepassing zijn. De regels met betrekking tot systemen met een hoog risico in Bijlage I gaan gelden vanaf 2 augustus 2027, maar het voorstel geeft dergelijke systemen ook een verlenging van één jaar vanaf de datum waarop de beschikbaarheid van ondersteuningsmaatregelen voor naleving is bevestigd. Deze maatregelen zullen uiterlijk op 2 augustus 2028 van toepassing zijn als de voorstellen worden aanvaard. Risicovolle systemen die vóór 2 augustus 2026 op de markt zijn gebracht, hoeven niet te voldoen aan de verplichtingen van de AI- Verordening, tenzij het systeem een significante wijziging ondergaat. Risicovolle systemen benoemd in bijlage III die vóór 2 december 2027 op de markt zijn gebracht, en risicovolle systemen benoemd in bijlage I die vóór 2 augustus 2028 op de markt zijn gebracht, zijn vrijgesteld van de AI-verordening, tenzij er een significante wijziging aan die systemen wordt aangebracht (of tenzij eerdere termijnen van toepassing zijn op de handhaving ervan, zoals hierboven vermeld).

– *Verplichtingen voor aanbieders van door AI gegenereerde content met machineleesbare watermerken (§29)* - Het voorstel voorziet in een overgangsperiode voor de verplichtingen tot het aanbrengen van machineleesbare watermerken voor generatieve AI-systemen onder artikel 50(2) tot 2 februari 2027, mits het AI-systeem vóór 2 augustus 2026 op de markt wordt gebracht. Dit zou echter betekenen dat AI-systemen die na 2 augustus 2026 op de markt worden gebracht, onmiddellijk aan de watermerkregels moeten voldoen.

– *Afschaffing van de registratieplicht voor systemen benoemd in bijlage III die niet als hoog risico worden beschouwd (§ 5,6 en 30)* – De AI-verordening voorziet momenteel in een uitzonderingsmechanisme voor systemen van bijlage III die als hoog risico worden beschouwd, indien zij aan bepaalde voorwaarden voldoen, zoals het gebruik voor beperkte procedurele taken, mits zij geen profilering van personen inhouden. Wanneer bedrijven van mening zijn dat hun systeem niet als hoog risico moet worden beschouwd, zijn zij momenteel verplicht deze systemen in de EU-database te registreren. Het voorstel beoogt deze registratieplicht af te schaffen, terwijl de documentatieplicht behou-

den blijft. Dit betekent dat bedrijven hun beslissingen nog steeds moeten documenteren en deze gegevens moeten bewaren voor eventueel toezicht door de regelgevende instanties.

– *AI-geletterdheid (§ 3)* - De huidige AI-verordening legt aan bedrijven een algemene verplichting te zorgen voor AI-geletterdheid van gebruikers van AI-systemen die onder de wet vallen. Deze verplichting is ingegaan op 2 februari 2025. De Commissie stelt voor deze verplichting voor aanbieders en gebruikers af te schaffen en over te dragen aan de Commissie en de lidstaten.

– *Gewijzigde definitie van persoonsgegevens* – Aan artikel 4 AVG wordt een lid inzake relatieve identificeerbaarheid toegevoegd waarin is opgenomen dat informatie niet als persoonsgegevens voor een bepaalde entiteit wordt beschouwd wanneer er geen middelen bestaan die redelijkerwijs kunnen worden gebruikt om de natuurlijke persoon op wie de informatie betrekking heeft te identificeren. Een dergelijke entiteit valt derhalve in beginsel niet onder het toepassingsgebied van die Verordening. Dit voorstel roept weerstand op bij privacy-autoriteiten die vrezen dat de fundamentele rechten van personen worden aangetast. De voorgestelde wijzigingen gaan veel verder dan een gerichte aanpassing van de AVG, een 'technische wijziging' of een loutere codificatie van de jurisprudentie van het Hof van Justitie van de EU.[18]

– *Bijzondere categorieën persoonsgegevens* – Een nieuw artikel 9, tweede lid, van de AVG voorziet in twee extra uitzonderingen op de verwerking van bijzondere categorieën persoonsgegevens: Ten eerste een uitzondering op het algemene verbod op de verwerking van biometrische gegevens, wanneer dit noodzakelijk is voor de bevestiging van de identiteit van de betrokkene en wanneer de gegevens en de middelen voor een dergelijke verificatie volledig onder de controle van die betrokkene vallen. Ten tweede een uitzondering voor de verwerking van bijzondere categorieën persoonsgegevens voor de ontwikkeling en werking van een AI-systeem of een AI-model, onder bepaalde voorwaarden, waaronder passende organisatorische en technische maatregelen om het verzamelen van bijzondere categorieën persoonsgegevens te voorkomen en dergelijke gegevens te verwijderen. Dit voorstel heeft geleid tot een brede discussie over de wenselijkheid ervan.

– *Toestemming voor de verwerking van bijzondere categorieën persoonsgegevens om AI-systemen te ontdoen van bias (§ 4)* - Het voorstel bevat een uitzondering voor de verwerking van bijzondere categorieën persoonsgegevens wanneer dergelijke verwerking niet kan worden vermeden ondanks de genomen maatregelen. Deze uitzondering is relevant wanneer de verwerking van bijzondere categorieën persoonsgegevens niet noodzakelijk is voor de werking van het AI-systeem. Indien de verwerking van bijzondere categorieën persoonsgegevens wel noodzakelijk is, moet een beroep worden gedaan op de uitzondering op grond van artikel 9, lid 2, van de AVG. Een van die uitzonderingen is het verwijderen van bias uit AI-systemen met een hoog risico, wat momenteel een vereiste is onder de AI Verordening. Het voorstel tot wijziging is deze uitzondering voor het verwijderen van vooringenomenheid ook uit te breiden naar andere soorten AI-systemen (d.w.z. systemen die geen hoog risico vormen). Deze systemen zullen onderworpen worden aan strikte verplichtingen, waaronder het waarborgen van de beveiligings- en privacymaatregelen, het niet overdragen van of het toestaan van toegang tot bijzondere categorieën persoonsgegevens door derden, en het verwijderen van de bijzondere categorieën persoonsgegevens zodra vooringenomenheid is vastgesteld en gecorrigeerd of de bewaartermijn is verlopen (afhankelijk van wat zich het eerst voordoet). Deze voorstellen zijn juridisch controversieel en zullen nog stevige onderhandelingen vergen.

– *Cookies* – Artikel 5(3) van de e-Privacyrichtlijn[19] is thans van toepassing op het plaatsen van cookies om informatie te verkrijgen uit de eindapparatuur van een gebruiker, terwijl de daaropvolgende verwerking van persoonsgegevens onderworpen is aan de AVG. Voorgesteld wordt de verwerking van persoonsgegevens op en van eindapparatuur uitsluitend te regelen in de AVG, waarbij ook de vereiste toestemming voor toegang tot de eindapparatuur van een natuurlijke persoon bij het verzamelen van persoonsgegevens wordt opgenomen. De voorgestelde wijzigingen voorzien tevens in bepaalde doeleinden waarvoor geen toestemming vereist is en waarvoor de daaropvolgende verwerking rechtmatig is, met name wanneer deze een laag risico vormen voor de rechten en vrijheden van de betrokkenen of wanneer de plaatsing van dergelijke technologieën noodzakelijk is voor de levering van een door de betrokkene gevraagde dienst.

– Er komt één centraal toegangspunt voor het melden van incidenten op basis van de NIS2-richtlijn, de eIDAS-verordening[20], de DORA-richtlijn, de CER-richtlijn[21] en de AVG. De rapportageverplichtingen in de e-Privacyrichtlijn worden ingetrokken. Er wordt één centraal meldpunt belegd bij het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) voor alle incidenten in het kader van de AVG en cybersecurity regelgeving, onder het motto: *report once, share many*.

18. Gezamenlijk rapport van de EDPB en de EDPS van 10 februari 2026: www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf
19. Richtlijn (EU) 2002/58/EC
20. Verordening (EU) 910/2014
21. Richtlijn (EU) 2022/2557

Overige wijzigingen
Andere voorgestelde wijzigingen betreffen onder meer:
– het stimuleren van een breder gebruik van AI-sandboxes en praktijktesten (§3a, 5,13 en 60);
– het uitbreiden van de vereenvoudigingen van regelgeving die zijn toegekend aan kleine en middelgrote ondernemingen naar kleine en middelgrote bedrijven (§ 9, 22, 27)
– het centraliseren van het toezicht op een groot aantal AI-systemen die zijn gebouwd op algemene AI-modellen of zijn ingebed in zeer grote online platforms (VLOP's) en zeer grote zoekmachines (VLOSE's) bij het AI-Bureau; en het verstrekken van richtlijnen (waarvan sommige oorspronkelijk bedoeld waren als uitvoeringswetgeving). Met name enkele bevoegdheden van de Commissie om uitvoeringsbesluiten uit te vaardigen op grond van de AI-verordening, zoals die met betrekking tot postmarktmonitoring (§ 25)

Kortom, het betreft omvangrijke maatregelen met een hoog ambitiegehalte, waarbij het zeer de vraag is of en in welke vorm de voorstellen de eindstreep zullen halen.

3. Gevolgen voor de markt

AVG-cybersecurity regelgeving
Binnen 18 maanden na de inwerkingtreding van de Digitale Omnibus (en uiterlijk binnen 24 maanden) moet ENISA de werking van het centrale meldpunt voor elke toegevoegde EU-rechtsinstrument testen en invoeren. De invoering van één centraal meldpunt kan op veel steun rekenen van de markt. Dit zou een aanzienlijke vereenvoudiging van het systeem voor het afhandelen van het melden van incidenten inhouden. Daar staat tegenover dat de werklast verschuift naar het centrale meldpunt en het doorleiden van de meldingen naar de juiste toezichthoudende instanties. Lidstaten maken zich zorgen over de centralisatie van macht bij een meldpunt aangezien dat de verantwoordelijkheden van de lidstaten zou aantasten. Daarnaast zijn er zorgen over de beveiliging van het meldpunt. Een centraal meldpunt kan immers makkelijk zelf het mikpunt worden van cyberaanvallen.

Dataverordening
De wijzigingen in de Dataverordening vormen een duidelijke eerste stap richting pragmatisme en proportionaliteit. Door drie afzonderlijke juridische instrumenten samen te voegen tot één kader, wordt een deel van de verwarring en overlapping weggenomen die het navigeren door de Europese gegevensregelgeving tot nu toe lastig heeft gemaakt. Voor EU-bedrijven die actief zijn op wereldwijde markten biedt de versterkte bescherming van bedrijfsgeheimen een welkome geruststelling. Wie zich zorgen maakt over het delen van gevoelige informatie met gebruikers in rechtsgebieden met zwakke waarborgen, heeft een duidelijke juridische basis dit te weigeren – mits het risico overtuigend kan worden aangetoond. Veel uitdagingen die voortvloeien uit het bredere EU-digitale acquis blijven echter onopgelost, zoals de onduidelijkheden over de definities, welke data vallen onder de afzonderlijke hoofdstukken van de Dataverordening en de reikwijdte van de overstapregeling voor clouddiensten.

In het voorstel worden IaaS diensten uitgesloten van de mogelijkheid bepalingen over evenredige boetes voor vroegtijdige beëindiging op te nemen in een contract met een vaste looptijd. Voor deze merkwaardige uitzondering ontbreekt een motivering. Aanbieders van IaaS diensten lopen immers vergelijkbare commerciële risico's als aanbieders van ander as-a-service diensten als een klant voortijdig vertrekt. Naar verluidt heeft ook de Commissie dit ingezien en wordt een wijziging voorbereid zodat ook aanbieders van IaaS diensten een vergoeding te verlangen voor vroegtijdige beëindiging van een contact. Dit is een terechte keuze.

De uitbreiding van de regels voor bescherming van bedrijfsgeheimen bij het delen van data is beperkt tot risico's ten opzichte van entiteiten in derde landen. Het bedrijfsleven zal willen inzetten op uitbreiding met entiteiten in algemene zin. De beperking van mogelijkheden voor gegevensuitwisseling tussen bedrijven en overheden tot naar specifiek gedefinieerde "openbare noodsituaties" zal zeker worden verwelkomd. Dit geeft rechtszekerheid, nog los van de vraag hoe vaak overheden in de praktijk van de mogelijkheden gebruik zullen maken. Het verkrijgen van data en het vaststellen van de voorwaarden blijft een tijdrovend proces, terwijl in noodsituaties doorgaans de tijd hiervoor ontbreekt.

AI-verordening
De wijzigingen in de AI-verordening leiden vooral tot onzekerheid in de markt over het moment van inwerkingtreding van verplichtingen en in welke mate persoonsgegevens kunnen worden gebruikt voor het trainen van AI-modellen en -systemen. De huidige AI-verordening bepaalt dat de regels voor AI-systemen met een hoog risico op 2 augustus 2026 van kracht worden.

Voorgesteld wordt de artikelen inzake hoog-risico AI-systemen in de AI-verordening uit te stellen tot eind 2027. De EU-instellingen staan onder druk vóór 2 augustus 2026 tot een definitief akkoord te komen over de AI-Omnibus. Dit is namelijk de oorspronkelijke datum voor de volledige toepassing van de "hoog risico" AI-regels onder de AI-verordening. Als de AI-Omnibus niet vóór deze datum wordt aangenomen, kunnen de oorspronkelijke hoogrisicoregels alsnog van kracht worden, voordat de ondersteunende infrastructuur voor naleving gereed is. Dit kan leiden tot onvolledige richtlijnen voor naleving en juridische onzekerheid voor bedrijven. Zelfs als door het Europees Parlement een spoedprocedure wordt toegepast waarbij de fase van commissiebehandelingen wordt overgeslagen, is nauwelijks

denkbaar dat voor 2 augustus 2026 de verdere onderhandelingen met de Raad en de Commissie kunnen worden afgerond. Per die datum zullen de hoogrisicoregels in werking treden en staat Europa voor de keuze ze later alsnog te wijzigen. Dat is bepaald geen fraaie vorm van regelgeving die tot grote onzekerheden bij bedrijven leidt. Het is dan ook terecht dat door het presidentschap van Cyprus en leidende parlementsleden vaste data van inwerkingtreding zijn voorgesteld.[22]

Een *hot topic* is het vervaardigen van pornografisch beeldmateriaal met behulp van AI. Bekende vrouwen zijn vaak het doelwit, waaronder beroemdheden, modellen, journalisten, politici en activisten. Door het Europees Parlement wordt bepleit dat AI-pornografie tools worden opgenomen in de lijst van verboden toepassingen in de AI-verordening.

4. Hoe nu verder

De Europese Commissie heeft de voorstellen in december 2025 naar het Europees Parlement gestuurd. De Commissie Industrie, Onderzoek en Energie (ITRE) en de Commissie Burgerlijke Vrijheden, Justitie en Binnenlandse Zaken (LIBE) spelen een leidende rol, samen met de Commissie Interne Markt en Consumentenbescherming (IMCO) en de Commissie Juridische Zaken (JURI). De AI-Omnibus wordt behandeld door de LIBE- en IMCO-commissies. Europarlementariërs Arba Kokalari (EPP) en Michael McNamara (Renew) zijn aangesteld als rapporteurs. De Digitale Omnibus wordt onder handen genomen door de LIBE en ITRE-commissies met als rapporteurs Aura Salla (EPP, voormalig Meta lobbyist) en Marina Kaljurand (S&P). De leden van deze commissies zijn begonnen met het bespreken van de voorstellen en het indienen van amendementen, met als doel de definitieve rapporten uiterlijk in het tweede kwartaal van 2026 vast te stellen. Parallel zijn vertegenwoordigers van de 27 EU-lidstaten in de zogenaamde Antici-groep besprekingen gestart om het gezamenlijke standpunt voor de AI-Omnibus voor te bereiden, bekend als de *general approach*, die naar verwachting in het tweede kwartaal van 2026 zal worden gepresenteerd. Het presidentschap van Cyprus streeft ernaar de *general approach* van de lidstaten eind maart of begin april gereed te hebben. Dat zal niet eenvoudig zijn. Duitsland vindt de voorstellen van de Commissie niet ver genoeg gaan en is van mening dat de Europese AI regels verder moeten worden vereenvoudigd. Veertien landen, waaronder Nederland, zijn nogal kritisch over de Digitale Omnibus voorstellen. Zij vinden dat privacy aangelegenheden exclusief in de AVG moeten worden geregeld. Veel landen zijn voorstander van een betere bescherming van bedrijfsgeheimen. De landen zijn verdeeld over het voorstel om het delen van bepaalde gegevens tussen bedrijven en overheden te beperken tot noodsituaties.

Nadat de verantwoordelijke commissies van het Europees Parlement hun eindrapporten hebben aangenomen, moeten deze in een plenaire vergadering door alle Europarlementariërs worden goedgekeurd. Daarna kunnen de gesprekken met leden van het Europees Parlement en de Commissie van start gaan. Het doel is vóór augustus een definitief akkoord te bereiken over de AI-Omnibus. Daarover werd in maart 2026 nog stevig onderhandeld, onder meer oer het toevoegen van een verbod op het vervaardigen van pornografisch getint materiaal met behulp van AI. Desalniettemin zijn alle inspanningen erop gericht om de AI-Omnibus op 1 augustus 2026 in werking te laten treden. De verwachting is dat het Europess parlement voor de Digitale Omnibus eerst in 2027 een definitief standpunt gereed zal hebben. Men lijkt hiermee minder haast te willen maken.

De Commissie heeft ook de Digital Fitness Check gelanceerd, een consultatie die bedoeld is de wisselwerking tussen de verschillende regels, hun cumulatieve impact op bedrijven en de mate waarin ze het concurrentievermogen, de waarden en de grondrechten van de EU ondersteunen, te analyseren. De consultatie liep tot 11 maart 2026 en is ook de start van de discussie over hervormingen van andere digitale wetten, zoals de Digital Services Act en de Digital Markets Act.

Tot slot: De Commissie zal naar verwachting eind mei een voorstel voor een Cloud and AI Development Act (CADA) bekend maken, samen met een voorstel voor een tweede Chips Act, een Open Source Strategy en het investeringsprogramma EUR-3C, als onderdeel van een Tech Sovereignty Package. Verder kwam de Commissie op 21 januari 2026 ook met een voorstel voor ingrijpende herziening van de Cybersecurity Act, dat een separaat overzichtsartikel waard is. Kortom, niet minder, maar vooral meer regelgeving.

Voor bedrijven wordt 2026 een jaar met meer dan gebruikelijke regelgevende onzekerheden. Mijn advies: volg de geldende regelgeving, en begin met het in kaart brengen van de mogelijke impact voor de wijzigingsvoorstellen zodat daarop op de bedrijfsvoering kan worden geanticipeerd. Houd uiteraard ook de nieuwe regelgevende voorstellen van de Commissie in de gaten.

22. 2 december 2027 met betrekking tot AI-systemen die als hoog risico zijn geclassificeerd overeenkomstig artikel 6(2) en bijlage III, en (ii) op 2 augustus 2028 met betrekking tot AI-systemen die als hoog risico zijn geclassificeerd overeenkomstig artikel 6(1) en bijlage I

Aansprakelijkheid voor ontbrekende back-up na servercrash

Annotatie bij Gerechtshof Amsterdam 3 februari 2026, ECLI:NL:GHAMS:2026:275 (Hallo/Blok)

mr. M. Weij[1]

1. INLEIDING

Dit kort geding draait om de vraag of leverancier Hallo aansprakelijk is jegens opdrachtgever Blok wegens het ontbreken van een back-up na een servercrash. Heel concreet is het probleem dat een nieuw geplaatste server niet in het back-up proces is meegenomen.

In eerste aanleg[2] oordeelt de voorzieningenrechter dat Hallo (i) toerekenbaar tekort is geschoten in de kern van haar verplichting, en (ii) géén beroep toekomt op het exoneratiebeding uit de Nederland ICT Voorwaarden (tegenwoordig NL Digital Voorwaarden). De voorzieningenrechter wijst een bedrag van ruim EUR 368.000 toe als voorschot op schadevergoeding.

In dit hoger beroep wijst het hof die vordering alsnog af.[3] Het hof (i) benadrukt de maatstaf voor toewijzing van een geldvordering in kort geding, (ii) acht de contractuele back-upverplichting ten aanzien van de nieuwe server voorshands 'onvoldoende aannemelijk' en (iii) oordeelt bovendien dat bewuste roekeloosheid of bijzondere bijkomende omstandigheden niet aannemelijk zijn. Daarbij weegt mee dat de schade van Blok onder de toepasselijke voorwaarden in beginsel is uitgesloten.

De zaak in eerste aanleg heeft destijds de nodige media-aandacht gekregen. Zo kopte Computable bijvoorbeeld "*Ontbrekende backup dreigt voor Hallo uit te lopen op miljoenenstrop*".[4] Ook Dutch IT Channel besteedde destijds aandacht aan de zaak.[5]

In juridische kring is het kort geding evenmin onopgemerkt gebleven. ICTRecht benoemt de zaak in haar jurisprudentieblog[6], Turing Advocaten bespreekt de zaak in haar jaaroverzicht 2024[7] en in het Advocatenblad komt de zaak voorbij in de Kroniek IT-recht 2024[8]. Polo van der Putt en Nienke Nugteren[9] besteden er ook aandacht aan in hun (lezenswaardige!) artikel "exoneraties en kernverplichtingen" in Computerrecht[10]. Ten slotte benoem ook ik deze uitspraak nog kort, namelijk in mijn annotatie "De aansprakelijkheid voor een ransomware aanval" als gepubliceerd in dit tijdschrift.[11]

Ik bespreek het arrest van het hof hierna voornamelijk vanuit de verschillen met het vonnis in eerste aanleg.

2. FEITEN

Essentie

In een paar zinnen is de essentie van dit geschil dat er medio 2022 een serverupgrade is doorgevoerd bij Blok in verband met een upgrade van een - voor Blok belangrijke - ERP applicatie. Daarbij heeft Hallo een nieuwe server geleverd en is de migratie zelf door de leverancier (ECI) van de ERP applicatie uitgevoerd.

In 2024 vindt er vervolgens een crash met meerdere servers plaats, waarbij óók die nieuwe server is gecrasht. Als vervolgens de back-up wordt geplaatst,

1. Menno Weij is advocaat tech & privacy law bij The Data Lawyers en redactielid van dit tijdschrift. De auteur dankt ChatGPT (versie 5.2, in de "*thinking*" modus) voor zijn hulp bij het analyseren van het arrest als ook het vonnis in eerste aanleg.
2. Rechtbank Noord-Holland 4 december 2024, ECLI:NL:RBNHO:2024:12523.
3. In hoger beroep is Hallo trouwens van advocaat gewisseld.
4. https://www.computable.nl/2024/12/09/ontbrekende-backup-dreigt-voor-hallo-uit-te-lopen-op-miljoenenstrop/
5. https://www.dutchitchannel.nl/news/580414/rechter-blok-enterprise-vastgoed-bv-krijgt-schadevergoeding-van-hallo
6. https://www.ictrecht.nl/blog/it-jurisprudentieblog-januari-2025
7. https://turing.testduck.nl/wp-content/uploads/Jaaroverzicht-IT.pdf
8. https://magazine.advocatenblad.nl/2025-03/kroniek-it-recht-2024/
9. Beiden ook verbonden aan dit mooie tijdschrift, Polo als hoofdredacteur en Nienke als redactiesecretaris.
10. P.G. van der Putt & C.E. Nugteren, 'exoneraties en kernverplichtingen', Computerrecht 2025/127.
11. Annotatie bij Rechtbank Noord-Nederland 21 september 2022, ECLI:NL:RBNNE:2022:5577, Tijdschrift voor Internetrecht nr.1, maart 2025, blz. 39 – 42. Zie onder het kopje "Tot slot".

blijkt dat er sinds juli 2022 geen back-ups meer zijn gemaakt van die nieuwe server. Daaropvolgend stelt Blok Hallo aansprakelijk.

Verschil in vastgestelde feiten

Het hof vermeldt expliciet dat het bij de vaststelling van de feiten rekening houdt met grieven die zich richten tegen een aantal door de voorzieningenrechter in eerste aanleg opgesomde feiten. Het is daarom interessant die verschillen in kaart te brengen.

Een eerste wezenlijk verschil is met name de precisering van de back-upproblematiek. In eerste aanleg luidt het feit dat sinds juli 2022 geen back-up van de nieuwe server is gemaakt.[12] Het hof formuleert dit specifieker als: er is geen *cloud* back-up van de nieuwe server gemaakt.[13]

Ook voegt het hof feiten toe die in eerste aanleg ontbreken. Het hof vermeldt een afspraak tussen partijen uit januari 2018 over cloud back-updiensten (ingaande per 1 februari 2018), inclusief de beschreven werkwijze:

> "De werkwijze is aldus dat van de server eerst een lokale back-up wordt gemaakt, die daarna wordt overgezet naar een externe opslag in een datacenter, zodat bij calamiteiten altijd een externe back-up beschikbaar is (hierna: cloud back-up). "[14]

Ten slotte benoemt het hof dat de leverancier van de ERP applicatie (ECI) bij de migratie in 2022 een *lokale* back-up heeft gemaakt.[15] Het is mij niet duidelijk uit het arrest of dit om een eenmalige kopie gaat en het is mij ook niet duidelijk of ECI sowieso die lokale back-ups maakte.

Overige relevante feiten in beide instanties

De contractuele relatie tussen partijen is als volgt. Op 19 december 2017 hebben Blok en de rechtsvoorganger van Hallo (Support Groep B.V.) een overeenkomst van opdracht gesloten voor beheer van de ICT-infrastructuur van Blok.

De gecontracteerde ICT-diensten hebben betrekking op Remote Management, een Servicedesk op afstand, Applicatiebeheer, Systeembeheer op locatie, Licentie Management en Operationeel Management. Op de overeenkomst zijn de NL ICT-voorwaarden van toepassing.

Artikel 23.1 van de NL ICT-voorwaarden luidt als volgt:

> "Indien de dienstverlening aan klant op grond van de overeenkomst het maken van back-ups van gegevens van klant omvat, zal leverancier met inachtneming van de schriftelijk overeengekomen periodes, en bij gebreke daarvan eens per week, een volledige back-up maken van de bij hem in bezit zijnde gegevens van klant. Leverancier zal de back-up bewaren gedurende de overeengekomen termijn, en bij gebreke van afspraken daaromtrent, gedurende de bij leverancier gebruikelijke termijn. Leverancier zal de back-up zorgvuldig als een goed huisvader bewaren."

Het exoneratiebeding in de NL ICT-voorwaarden luidt als volgt:

> 16.1.
>
> "De totale aansprakelijkheid van leverancier wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of op welke rechtsgrond dan ook (…) is beperkt tot vergoeding van directe schade tot maximaal het bedrag van de voor die overeenkomst bedongen prijs (excl. BTW). Indien de overeenkomst hoofdzakelijk een duurovereenkomst is met een looptijd van meer dan één jaar, wordt de voor die overeenkomst bedongen prijs gesteld op het totaal van de vergoedingen (excl. BTW) bedongen voor één jaar."
>
> (…)
>
> 16.3
>
> "De aansprakelijkheid van leverancier voor indirecte schade, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade als gevolg van aanspraken van afnemers van klant, schade verband houdende met het gebruik van door klant aan leverancier voorgeschreven zaken, materialen of programmatuur van derden en schade verband houdende met de inschakeling van door klant aan leverancier voor geschreven toeleveranciers, is uitgesloten. Eveneens is uitgesloten de aansprakelijkheid van leverancier verband houdende met verminking, vernietiging of verlies van gegevens of documenten."
>
> (…)
>
> 16.5
>
> "De in artikel 16.1 tot en met 16.4 bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van de bedrijfsleiding van leverancier."

Blok heeft Hallo op 7 oktober 2024 in gebreke gesteld. In haar reactie heeft Hallo een dag later onder meer het volgende gemeld:

12. Zie rechtsoverweging 2.9 van het vonnis.
13. Zie rechtsoverweging 3.5 van het arrest.
14. Idem als hiervoor: zie rechtsoverweging 3.5.
15. Zie rechtsoverweging 3.7 van het arrest.

> "De IT Support Groep neemt het standpunt in te hebben voldaan aan de contractuele verplichtingen tussen IT support groep en Blok. De IT Support Groep legt elke vorm van pro- en reactief beheer vast en voert ook dagelijks controles uit of back-ups volledig hebben gedraaid. Door een fout is de desbetreffende server niet in de automatisering rondom back-up meegenomen, waardoor de server ook niet naar voren is gekomen bij steekproeven die periodiek worden uitgevoerd." [16]

3. JURIDISCH KADER

De voorzieningenrechter en het hof leggen het juridisch kader verschillend aan. Daarbij moeten in deze zaak drie vragen uit elkaar worden gehouden: (i) onder welke maatstaf in kort geding een voorschot op schadevergoeding kan worden toegewezen, (ii) of uit de overeenkomst volgde dat Hallo ook voor de nieuwe server cloud back-ups moest verzorgen, en (iii) onder welke omstandigheden het beroep op de exoneratie strandt. In de hier gekozen opzet bespreek ik meer in het bijzonder de inhoud en kwalificatie van de contractuele verplichtingen, alsmede de vraag of Hallo een beroep op de contractuele exoneratie toekomt.

Het vonnis in eerste aanleg over de verplichtingen van Hallo

De voorzieningenrechter overweegt nadrukkelijk dat het maken van back-ups een kernverplichting betreft van Hallo:

> "De kern van de opdracht bestond uit het zorgdragen voor een goed werkend ICT-systeem, waarbij het snel kunnen herstellen van dit systeem na een eventuele calamiteit cruciaal is. Het maken van back-ups is daarom een kernverplichting onder de overeenkomst." [17]

Ook vermeldt het vonnis dat tussen partijen níet in geschil is dat Hallo in dat kader de taak had om dagelijks back-ups te maken. De voorzieningenrechter hangt dit vervolgens op aan het hierboven geciteerde artikel 23 van de ICT-voorwaarden over back-ups:

> "Daarin is voorgeschreven dat de leverancier een volledige back-up zal maken en die back-up zorgvuldig zal bewaren."

Volgens de voorzieningenrechter is het daarom "evident dat er voortdurend een recente, herplaatsbare back-up van (de gegevens vanuit) dit systeem moest zijn." De voorzieningenrechter wijdt de afwezigheid ervan aan een menselijke fout: "anders dan door een menselijke fout is dit niet te verklaren", en verwijst hierbij naar voornoemd citaat waarin Hallo over een 'fout' spreekt.

Ook overweegt de voorzieningenrechter dat Hallo in reguliere rapportages steeds expliciet heeft aangegeven dat er extra aandacht was besteed aan de nieuwe server (waarop het ERP-systeem draaide). Hiermee heeft Hallo bij Blok de indruk gewekt dat "alles goed geregeld was, waardoor er voor Blok geen reden was nadere maatregelen te treffen." [18]

Het hof in beroep over de verplichtingen van Hallo

Het hof kijkt anders naar het geschil. Partijen twisten over de vraag of Hallo op grond van de overeenkomst gehouden was cloud back-ups te maken van de nieuwe server. Uit de overeenkomst volgt die verplichting volgens het hof niet zonder meer: "dat in het Dienstenoverzicht onder Remote management het begrip "dagelijkse back-up controle' is opgenomen, kan die conclusie niet dragen." [19]

Voorts acht het hof van belang dat de overeenkomst alleen betrekking had op de infrastructuur-laag en dat voor andere softwareproducten, zoals de ERP-applicatie, nadere afspraken nodig waren.

Ook overweegt het hof dat de back-up verplichting niet uit artikel 23 van de NL ICT-voorwaarden volgt: "daarin is slechts beschreven wat geldt als het maken van back-ups is overeengekomen." [20]

Wel staat volgens het hof vast dat ten aanzien van - aanvankelijk - tien servers opdracht is gegeven aan Hallo om cloud back-ups te maken. Maar niet is gesteld of gebleken dat Blok expliciet opdracht heeft gegeven aan Hallo om ook van de nieuwe server back-ups te maken. Blok stelt dat Hallo dit uit eigen beweging had moeten doen. Hallo stelt daartegen dat zij ervan uitging dat de ERP-leverancier ECI de back-ups voor haar rekening nam. Het hof verwijst hier simpelweg naar de bodemrechter:

> "Of Hallo NL uit hoofde van de overeenkomst gehouden was om de nieuwe server eigener beweging toe te voegen, dan wel Blok erop te wijzen dat deze daartoe een opdracht diende te verlenen volgt niet zonder meer uit de tekst van de overeenkomst en is een kwestie van uitleg. Daarvoor is nadere bewijsvoering noodzakelijk, waarvoor dit kort geding zich niet leent."[21]

Ten slotte neemt het hof nog de volgende omstandigheden mee in zijn overwegingen: (i) uit de verzonden facturen volgt niet dat voor de nieuwe server is gefactureerd, en (ii) uit de periodieke rapportages volgt slechts dat de back-up en restore functies zijn gecontroleerd.[22]

16. Zie rechtsoverweging 2.10 van het vonnis en 3.12 van het arrest.
17. Zie rechtsoverweging 4.5.
18. Zie rechtsoverweging 4.15.
19. Zie rechtsoverweging 6.4.
20. Zie rechtsoverweging 6.4.
21. Zie rechtsoverweging 6.4.
22. Zie rechtsoverweging 6.5.

De voorzieningenrechter over het beroep op de exoneratie
De voorzieningenrechter neemt de volgende omstandigheden mee in het voorlopig oordeel dat Hallo zich níet op de exoneratie kan beroepen:

- het maken van back-ups een van de kernverplichtingen van de tussen partijen gesloten overeenkomst.
- Het is essentieel dat een recente, herplaatsbare back-up aanwezig is.
- Hallo is ermee bekend dat het ERP-systeem cruciaal is voor het functioneren van Blok.
- Hallo heeft ten onrechte geen (herplaatsbare) recente back-up van de data op de cruciale server gemaakt.
- Ook het controlesysteem van Hallo functioneerde niet. Hallo heeft dit zelf beaamd door aan te geven dat de nieuwe server door een fout niet in het back-up proces is meegenomen.

In dit licht bezien kan Hallo zich volgens de voorzieningenrechter niet beroepen op haar algemene voorwaarden, waarin haar aansprakelijkheid wordt beperkt tot "een bedrag dat niet in verhouding staat tot de ontstane schade." [23] Verder weegt mee dat (i) partijen hebben verklaard dat bij de totstandkoming van de overeenkomst niet over de ICT-voorwaarden onderhandeld kon worden, en dat het terzijde schuiven van het exoneratiebeding niet leidt tot onoverkomelijke financiële problemen voor Hallo.

Het hof over het beroep op de exoneratie
Het hof stelt als uitgangspunt voorop dat partijen gebonden zijn aan de tussen hen gesloten overeenkomst en Hallo dus in beginsel een beroep toekomt op de exoneratie, mits sprake is van een toerekenbare tekortkoming. De uitsluitingen in het exoneratiebeding, te weten opzet of bewuste roekeloosheid van de bedrijfsleiding van leverancier, zijn volgens het hof in overeenstemming met de vaste jurisprudentie.

Aan de hand van de feiten, zoals weergegeven in het arrest van het hof, ziet het hof voorshands allereerst geen toerekenbare tekortkoming. Maar ook als daarvan wel zou moeten worden uitgegaan, volgt daaruit naar het voorlopig oordeel van het hof nog niet dat sprake is van bewuste roekeloosheid van (de bedrijfsleiding van) Hallo: "er zijn geen aanwijzingen dat het niet opnemen van de nieuwe server berust op bewust handelen van (de bedrijfsleiding van) Hallo." Voorts overweegt het hof dat Hallo adequaat heeft toegelicht waarom een en ander niet is opgemerkt: "om de eenvoudige reden dat deze server niet in het systeem van Hallo voorkwam."

Dat brengt het hof tot de volgende tussenconclusie:

> "Mede in dat licht is niet, althans niet voldoende gemotiveerd gesteld dat de bedrijfsleiding van Hallo bewust maatregelen heeft achterwege gelaten ter voorkoming van aanzienlijke schade. Dat Hallo Blok bewust in de waan zou hebben gelaten dat er wel back-ups werden gemaakt is, zoals hiervoor reeds overwogen, evenmin gebleken. Van roekeloos handelen is dan ook geen sprake. "[24]

Onder verwijzing naar het arrest Saladin/HBU[25] stelt het hof ten slotte dat Blok geen bijzondere bijkomende omstandigheden heeft gesteld die maken dat een beroep op de exoneratie naar maatstaven van redelijkheid en billijkheid onaanvaardbaar is. Daarbij neemt het hof in aanmerking dat de overeenkomst is gesloten tussen twee professionele partijen. De keuze van Blok om zich niet te laten adviseren door een jurist is geen bijzondere omstandigheid, aldus het hof. Ook neemt het hof als factor van belang mee dat partijen het erover eens zijn dat de NL ICT-voorwaarden in de branche gebruikelijk zijn.

4. OVERDENKINGEN ANNOTATOR

Het hof volgt – terecht – een strakke lijn. Het gaat immers om een voorschot op schadevergoeding in kort geding. Dan moeten de grondslag van de vordering en de omvang van de schade voldoende aannemelijk zijn, terwijl ook het restitutierisico een rol speelt. In deze zaak komt daar nog bij dat pas ná beantwoording van de contractuele uitlegvraag over de verplichting zelf, de exoneratie-problematiek echt in beeld komt.

Het gegeven dat het om een kernverplichting gaat – waarop de voorzieningenrechter zwaar leunt – weegt het hof minder zwaar. Nugteren en Van der Putt verwijzen in dit verband naar de uitspraak van de Hoge Raad inzake het Bakker Bart-arrest[26], waarin is bepaald dat het enkele schenden van een kernverplichting onvoldoende is om het exoneratiebeding opzij te zetten. In de woorden van Nugteren en Van der Putt:

> "In die zaak ging het om de huur van een bakkerij van Bakker Bart door een franchisenemer. Het pand bleek dusdanig veel asbest te bevatten dat het gesloten moest worden. Franchisenemer maakte aanspraak op vergoeding van bedrijfsschade, maar dat was contractueel uitgesloten. De Hoge Raad overwoog dat de omstandigheid dat een exoneratiebeding wordt ingeroepen voor de kern van de prestatie (het beschikbaar stellen van het pand), op zichzelf onvoldoende is om te oordelen dat een beroep op het exoneratiebeding naar maatstaven van redelijkheid en billijkheid onaanvaardbaar is"."

De motivering van het hof roept op het punt van de nieuwe server wel enige spanning op. Enerzijds laat het hof de uitlegvraag nadrukkelijk aan de bodem-

23. Zie rechtsoverweging 4.15.
24. Zie rechtsoverweging 6.8.
25. Hoge Raad 19 mei 1967, ECLI:NL:HR:1967:AC4745.
26. Hoge Raad 29 januari 2021, ECLI:NL:HR:2021:153.

rechter, omdat daarvoor nadere bewijsvoering nodig is. Anderzijds formuleert het hof tamelijk beslist dat er geen aanwijzingen zijn voor bewuste roekeloosheid bij het niet opnemen van de nieuwe server in het back-upproces. De overweging "om de eenvoudige reden dat deze server niet in het systeem van Hallo voorkwam" vind ik daarom te kort door de bocht. Immers vast staat dat Hallo zelf spreekt van een 'fout', terwijl juist in geschil is of Hallo verantwoordelijk was voor het opnemen van de nieuwe server in het back-up regime.

Voor wat betreft de externe correctie langs de lijn van Saladin/HBU, moest ik nog denken aan de uitspraak van de rechtbank Rotterdam in de zaak tussen NKB Forwarding en Greencat.[27] De rechtbank acht het beroep op een exoneratie naar maatstaven van redelijkheid en billijkheid onaanvaardbaar voor zover het de uitsluiting van aansprakelijkheid betreft. De rechtbank neemt hierbij de volgende punten mee, die ook in het geschil tussen Blok en Hallo spelen: (i) het gaat om een overeenkomst tussen twee professionele partijen, een deskundige leverancier en een niet-deskundige klant, (ii) er staat vast dat er aanzienlijke schade is, (iii) over de exoneratie is niet onderhandeld, en (iv) de exoneratie leidt praktisch tot een bijna volledige uitsluiting, waardoor er onvoldoende prikkel overblijft voor de leverancier om verplichtingen zorgvuldig na te komen. Tegelijk weegt de rechtbank mee dat leveranciers bij een relatief lage vergoeding niet onbeperkt risico kunnen dragen en dat aansprakelijkheidsbeperking (en risicoverzekering door de opdrachtgever) in de branche gebruikelijk en verdedigbaar is.

Met dit vonnis in het achterhoofd had het hof mijns inziens kunnen verkennen of een gedeeltelijke buitenwerkingstelling van de exoneratie denkbaar was, en aldus de optie kunnen onderzoeken om de uitgesloten "indirecte" schade onder de cap van de wél gedekte "directe" schade te laten vallen, zoals opgenomen in 16.1 van de tussen partijen geldende NL ICT-voorwaarden. Anders gezegd, het hof had het proportioneel derogeren tot een aansprakelijkheidsbeperking voor gevolgschade, kunnen verkennen. In zijn annotatie bij voornoemde Greencat uitspraak destijds, schrijft Tycho de Graaf dat dergelijk proportioneel derogeren van exoneraties in de literatuur al langer bepleit werd:

> "Al in 1994 verzuchtte Vranken dat het exoneratiebeding één van de laatste bolwerken is waarop de alles-of-niets benadering nog steeds opgeld doet en bepleitte dat die benadering zou worden verlaten. Verheij stond voor dat exoneraties, door analoge toepassing van art. 3:42 BW, werden geconverteerd in gevallen waarin conversie mogelijk was en de gelaedeerde zich op art. 6:248 lid 2 BW beriep. En Tjong Tjin Tai werkte uit waarom en hoe proportioneel aan exoneraties kon worden gederogeerd door toepassing van de beperkende werking van de redelijkheid en billijkheid."[28]

Tot slot nog kort een woord over de eind 2025 ingevoerde NLdigital voorwaarden. De regeling over back-ups is daarin primair geconcentreerd in artikel 27. Wat opvalt is dat het herstelregime verder is beperkt: de leverancier hoeft in beginsel slechts, voor zover mogelijk, de laatst beschikbare back-up terug te plaatsen. Vergeleken met de NL ICT voorwaarden die in deze casus van toepassing zijn, hebben de NLdigital Voorwaarden 2025 op het punt van back-ups een duidelijk meer afbakenend en aansprakelijkheidsbeperkend karakter. Tegelijk keert de oude, expliciete data-exoneratie uit artikel 16.3 niet meer als zelfstandige algemene uitsluiting in het aansprakelijkheidsartikel terug.

27. Rechtbank Rotterdam 10 februari 2016, ECLI:NL:RBROT:2016:1016.
28. mr. dr. T.J. de Graaf "Aansprakelijkheidsuitsluiting voor gevolgschade wordt met behulp van art. 6:248 lid 2 BW proportioneel gederogeerd tot een aansprakelijkheidsbeperking voor gevolgschade tot de factuurwaarde, mede op grond van de stelling dat software leveranciers standaard bedingen dat hun aansprakelijkheid voor gevolgschade tot de factuurwaarde wordt beperkt, al dan niet met factor 2 of 3.", Computerrecht 2016/88.

Jurisprudentie

mr. F. Schemkes en M.V. Avanesian LL.M, BSc, CIPP/e

NOVEMBER 2025

Rechtbank Zeeland-West-Brabant, 4 november 2025, ECLI:NL:RBZWB:2025:7551

Incidentenrapport, belangenafweging, inzagerecht

Verzoeker heeft deelgenomen aan een opleidingstraject waarbij hij tijdens een parachutesprong op 14 mei 2025 ernstig gewond is geraakt. In juni 2025 verzoekt hij de Koninklijke Nederlandse Vereniging voor Luchtvaart (KNVvL) om inzage in, dan wel verstrekking van, het incidentenrapport. Verzoeker stelt het rapport nodig te hebben om zich een beeld te vormen van het ongeval, waaraan hij zelf geen herinnering meer heeft. De KNVvL wijst het verzoek af en stelt dat de gegevens uit het incidentenrapport geen persoonsgegevens zijn en dat vertrouwelijkheid van incidentmeldingen essentieel is voor een veilige meldcultuur binnen de luchtvaart.

De rechtbank wijst het verzoek gedeeltelijk toe. Voor zover het verzoek ziet op directe persoonsgegevens van verzoeker, zoals vermeld op het voorblad van het incidentenrapport (naam, geslacht, gewicht en adres- en contactgegevens), heeft verzoeker recht op inzage op grond van artikel 15 AVG. Voor het overige wijst de rechtbank het verzoek af. Op grond van artikel 23 AVG in samenhang met artikel 41 lid 1 onder c UAVG kan het inzagerecht worden beperkt ter bescherming van gewichtige algemene belangen.

Na een belangenafweging oordeelt de rechtbank dat het belang van de KNVvL bij vertrouwelijke incidentmeldingen, die uitsluitend worden gebruikt ter bevordering van de luchtvaartveiligheid, zwaarder weegt dan het belang van [verzoeker] bij inzage in het volledige rapport, ook indien die inzage wordt verlangd in het kader van een mogelijke aansprakelijkheidsstelling. Er volgt geen proceskostenveroordeling.

Rechtbank Noord-Nederland, 6 november 2024, ECLI:NL:RBNNE:2024:4317

Digitale werkomgeving, zorgplicht, Multi-factor authentication

A is een ICT-dienstverlener die zich richt op het MKB en voor haar klanten digitale werkomgevingen beheert binnen Microsoft Azure. Omdat A zelf geen directe contractuele relatie met Microsoft kan aangaan, koopt zij de benodigde clouddiensten in via haar distributeur. Binnen deze constructie richt A voor haar eindklanten zogeheten tenants in, waarin de Azure-diensten worden afgenomen en beheerd.

Na een hack in de digitale omgeving van een eindklant van A werden binnen korte tijd grote aantallen Azure-servers aangemaakt. Dit leidde tot een factuur van Microsoft van ruim € 860.000, welke via de distributeur aan A werd doorbelast. A heeft de distributeur hiervoor primair aansprakelijk gesteld. Zij stelt dat de distributeur haar zorgplicht heeft geschonden door haar onvoldoende te waarschuwen voor het belang van het activeren van Multi-Factor Authenticatie (MFA) en door ten onrechte geen monitoring uit te voeren om afwijkend gebruik te signaleren.

Subsidiair heeft A haar verzekeraar aangesproken tot vergoeding van de schade, stellende dat sprake is van een verzekerd risico. Daarnaast heeft A haar assurantietussenpersoon aansprakelijk gesteld wegens vermeend onjuist advies en schending van de zorgplicht bij het afsluiten van de verzekering.

De rechtbank oordeelt dat de distributeur niet aansprakelijk is voor de schade als gevolg van de hack. Daarbij stelt de rechtbank vast dat de reseller (A) binnen de Microsoft-cloudomgeving de tenant aanmaakt en beheert ten behoeve van de eindgebruiker. De reseller is verantwoordelijk voor de inrichting van de tenant en voor instellingen met betrekking tot gebruikersbeheer, toegangsrechten en beveiliging. De toegang tot en het beheer van de tenant verlopen rechtstreeks via de Azure-omgeving, zonder tussenkomst van de distributeur. De rechtbank acht voldoende onderbouwd dat de distributeur. technisch niet in staat is tot het beheren of monitoren van de tenants van eindgebruikers. De rechtbank overweegt bovendien dat een eventuele Tier 1-status van de distributeur niet door A gebruikt kan worden om zichzelf te ontslaan van haar eigen verantwoordelijkheden jegens eindgebruikers. Uit de communicatie en openbare uitingen van A volgt dat zij zelf het IT-beheer en de beveiliging van de accounts van haar eindklanten op zich neemt, waaronder het treffen van adequate beveiligingsmaatregelen zoals MFA.

Ten aanzien van de vordering tegen verzekeraar oordeelt de rechtbank dat de schade niet onder de dekking van de afgesloten verzekering valt. De polis vereist een aanspraak door een derde, waarvan in dit geval geen sprake is. De schade betreft een eigen kostenpost van A en kwalificeert niet als een gedekte gebeurtenis. Ook de vordering tegen de assurantietussenpersoon wordt afgewezen, nu A onvoldoende heeft onderbouwd dat sprake is geweest van onjuist

advies of een schending van de zorgplicht.
Alle vorderingen van A in conventie worden afgewezen. In reconventie wordt vastgesteld dat A het door de distributeur in rekening gebrachte bedrag van ruim € 860.000 dient te voldoen. A wordt veroordeeld in de proceskosten, welke aan haar zijde worden begroot op ruim € 38.000.

Parket bij de Hoge Raad, 7 november 2025, IT 5013, ECLI:NL:PHR:2025:1212

Clouddiensten, Wanprestatie, Schadebegroting
Deze zaak betreft een geschil tussen ICT-dienstverlener Acknowledge en cloudprovider Interconnect over het gebruik en de facturering van werkgeheugen (RAM) binnen een cloudomgeving. Acknowledge nam clouddiensten af tegen een vaste prijs. In geschil is of die vaste prijs slechts betrekking had op 2.229 GB aan actief ("powered on") werkgeheugen, aangevuld met gereserveerd ("powered off") geheugen en uitwijkcapaciteit, en of Interconnect extra kosten mocht rekenen wegens overschrijding daarvan.
Het hof oordeelde dat de vaste prijs zag op 2.229 GB actief werkgeheugen, 1.494 GB gereserveerd geheugen en 3.723 GB uitwijkcapaciteit. Acknowledge heeft, doordat technische begrenzingen ontbraken, structureel meer RAM actief gebruikt dan was overeengekomen, zonder de contractueel voorgeschreven uitbreidingsprocedure te volgen en zonder daarvoor te betalen. Dit kwalificeerde het hof als wanprestatie en het veroordeelde Acknowledge tot betaling van € 494.462,39, vermeerderd met buitengerechtelijke kosten en contractuele rente van 1,5% per maand.
In cassatie klaagt Acknowledge onder meer over de uitleg van de overeenkomst, de schadebegroting, eigen schuld van Interconnect (art. 6:101 BW) en schending van de zorg- en informatieplicht (art. 7:401 en 7:403 BW). De procureur-generaal acht deze klachten ongegrond. Hij volgt het oordeel van het hof dat het uitbreiden van werkgeheugen actieve handelingen vereiste binnen de organisatie van Acknowledge en dat de wetenschap daarvan aan haar kan worden toegerekend, zodat geen sprake is van een zorgplichtschending door Interconnect.
Wel acht de procureur-generaal de klacht over de rente gegrond. Het hof is niet ingegaan op het verweer dat de contractuele rente van 1,5% per maand buitensporig is en dat toewijzing daarvan naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn. De procureur-generaal adviseert daarom het arrest uitsluitend te vernietigen voor zover het de renteveroordeling betreft en dit voor het overige in stand te laten.

Rechtbank Rotterdam, 10 november 2025, ECLI:NL:RBROT:2025:15253

Overeenkomst van Opdracht; Intellectueel eigendom, website ontwikkeling
Tussen De Veiligheidsgroup en eiser is een overeenkomst van opdracht tot stand gekomen voor de ontwikkeling van een website en digitale leeromgeving, tegen een vergoeding van € 37.390. De opdracht eindigde vóór voltooiing; eiser had de werkzaamheden niet afgerond en De Veiligheidsgroup had nog niet betaald. In de procedure vordert De Veiligheidsgroup overdracht van het technisch fundament van de website, terwijl eiser betaling van het volledige bedrag verlangt.
De voorzieningenrechter constateert dat partijen wel afspraken hadden gemaakt over intellectuele eigendomsrechten, maar dat eiser tijdens de zitting verklaarde daarop geen aanspraak (meer) te maken. De beoordeling vindt daarom geheel plaats binnen het kader van het opdrachtrecht.
Op grond van art. 7:411 lid 1 BW heeft eiser, nu de overeenkomst vóór volbrenging is geëindigd en betaling afhankelijk was van oplevering, slechts recht op een redelijk deel van het loon. Partijen zijn het erover eens dat in elk geval 21% van de opdracht is uitgevoerd. De rechter stelt het voorlopig verschuldigde loon daarom vast op € 7.851,90.
Eiser wordt veroordeeld tot overdracht van het technisch fundament van de website en de bijbehorende accountgegevens; De Veiligheidsgroup moet het voorlopig vastgestelde bedrag betalen. De overige vorderingen worden afgewezen en de proceskosten gecompenseerd.

Rechtbank Noord-Holland, 10 november 2025, ECLI:NL:RBNHO:2025:13692

Persoonsgegevens, Wet Politiegegevens, Wjsg
IptiQ, verzekeraar van de overleden verzekerde, verzocht op grond van art. 196 Rv om afgifte van door de politie opgemaakte processen-verbaal naar aanleiding van diens overlijden bij een treinongeluk. De toedracht was onduidelijk, terwijl de polis een uitsluitingsclausule bevat voor (pogingen tot) zelfdoding binnen twee jaar na ingangsdatum. De nabestaanden wilden geen inzageverzoek bij de politie indienen. IptiQ stelde dat de politie de enige bron was om objectief duidelijkheid te verkrijgen over de omstandigheden van het overlijden.
De rechtbank wijst het verzoek af. De gevraagde stukken zijn politiegegevens in de zin van de Wet politiegegevens (Wpg). Voor deze gegevens geldt een strikte geheimhoudingsplicht (art. 7 Wpg) en een gesloten verstrekkingenregime: inzage of afgifte aan derden is alleen mogelijk in de specifiek in de Wpg of het Besluit politiegegevens genoemde gevallen. Verzekeraars vallen daar niet onder. Dat de uitkomst voor IptiQ onwelgevallig is, vormt geen grond om van dit stelsel af te wijken.
Het beroep van IptiQ op de Wet justitiële en strafvorderlijke gegevens (Wjsg) faalt eveneens, omdat het hier niet om strafvorderlijke gegevens gaat. De Wjsg schept bovendien slechts een bevoegdheid, geen verplichting tot verstrekking. Het verzoek tot voorlopige bewijsverrichting wordt afgewezen. IptiQ wordt veroordeeld in de proceskosten.

Hof van Justitie van de Europese Unie, 13 november 2025, ECLI:EU:C:2025:871

Artikel 13 e-Privacyrichtlijn, AVG, gratis accounts

In deze prejudiciële procedure werd het Hof gevraagd te verduidelijken hoe artikel 13 van de e-privacyrichtlijn (Richtlijn 2002/58/EG) moet worden uitgelegd in de context van een online uitgever van een tijdschrift dat een breed publiek informeert over dagelijkse wetswijzigingen.

Inteligo Media biedt gebruikers de mogelijkheid een gratis account aan te maken, waarmee zij gratis toegang krijgen tot enkele artikelen, een dagelijkse nieuwsbrief ontvangen met samenvattingen van wetswijzigingen en links naar de artikelen, en tegen betaling toegang kunnen krijgen tot aanvullende en verdiepende content.

Het Hof oordeelt dat het verkrijgen van het e-mailadres in dit kader plaatsvindt "in het kader van de verkoop van een product of dienst" zoals bedoeld in artikel 13 lid 2 van de richtlijn. Zelfs het gratis account vormt een dienst van economische waarde, mede omdat het toegang geeft tot premium content. De verzending van de dagelijkse nieuwsbrief kwalificeert volgens het Hof als het gebruik van e-mail "voor direct marketing van gelijkaardige producten of diensten".

Verder heeft het Hof verduidelijkt dat wanneer een verwerkingsverantwoordelijke handelt op grond van artikel 13 lid 2, de voorwaarden van artikel 6 lid 1 AVG voor rechtmatige verwerking niet van toepassing zijn, omdat artikel 95 AVG voorziet dat de e-privacyrichtlijn in deze context als lex specialis geldt.De derde prejudiciële vraag, over de verhouding tussen het begrip "direct marketing" en "commerciële communicatie" uit de e-commerce richtlijn, werd niet-ontvankelijk verklaard, en de overige vragen behoeven geen beantwoording.

Kortom bevestigt het Hof dat het gebruik van e-mailadressen die via gratis accounts zijn verkregen voor nieuwsbrieven met inhoud die vergelijkbaar is met betaalde content, valt onder de uitzonderingen van art. 13 lid 2 e-privacyrichtlijn, en dat dit gebruik rechtsgeldig is zonder aparte grondslag onder de AVG.

Rechtbank Noord-Nederland 13 november 2025, ECLI:NL:RBNNE:2025:4621

Computervredebreuk, cryptomining, schadevergoeding

Verdachte, voormalig technisch manager bij een windmolenpark, is vervolgd ter zake van het zonder toestemming aansluiten van drie cryptominingcomputers en twee zogenoemde Helium nodes op het bedrijfsnetwerk van zijn werkgever, Nordex. De apparatuur werd aangesloten op routers en servers van Nordex en maakte daarbij gebruik van door de werkgever beschikbaar gestelde elektriciteit en netwerkvoorzieningen.

Aan verdachte zijn drie feiten ten laste gelegd: (1) diefstal van elektriciteit, (2) het opzettelijk en wederrechtelijk toevoegen van gegevens aan een geautomatiseerd werk in de zin van artikel 350a Sr, en (3) computervredebreuk. Ten aanzien van het tweede feit oordeelt de rechtbank dat niet wettig en overtuigend bewezen kan worden dat verdachte zich daaraan schuldig heeft gemaakt. Het enkele verzenden van gegevens via het netwerk in het kader van cryptomining is onvoldoende om te kwalificeren als het "toevoegen van gegevens" aan een geautomatiseerd werk. De rechtbank overweegt daarbij dat de bij mining gegenereerde en verzonden data niet individueel zijn te herleiden of concreet te benoemen, zodat niet kan worden vastgesteld dat sprake is van een strafbaar toevoegen van gegevens als bedoeld in artikel 350a Sr. Verdachte wordt van dit feit vrijgesproken.

De rechtbank acht wel wettig en overtuigend bewezen dat verdachte zich schuldig heeft gemaakt aan diefstal van elektriciteit en aan computervredebreuk. Door zonder toestemming apparatuur aan te sluiten op het netwerk van Nordex heeft verdachte zich wederrechtelijk toegang verschaft tot een geautomatiseerd werk en gebruikgemaakt van elektriciteit die hem niet toebehoorde. Daarbij heeft de rechtbank vastgesteld dat verdachte handelde in strijd met de belangen van zijn werkgever.

Bij de strafoplegging weegt de rechtbank mee dat verdachte de strafbare feiten heeft gepleegd in de uitoefening van zijn functie en daarbij misbruik heeft gemaakt van het in hem gestelde vertrouwen als technisch manager. De rechtbank rekent het verdachte zwaar aan dat hij zich niet heeft bekommerd om het risico op verstoring van de werking van de windturbines. Daarnaast houdt de rechtbank rekening met de persoonlijke omstandigheden van verdachte, waaronder het ontbreken van een strafblad, zijn volledige medewerking aan het onderzoek en de overschrijding van de redelijke termijn. Tevens wordt betrokken dat Nordex kort vóór de ontdekking van de cryptominingapparatuur te maken had gehad met een cyberaanval, waardoor de impact van de feiten werd vergroot.

De rechtbank legt aan verdachte een taakstraf op van 120 uur. Daarnaast wordt verdachte veroordeeld tot betaling van een schadevergoeding aan Nordex, te vermeerderen met wettelijke rente en kosten.

Hof Arnhem-Leeuwarden, 17 november 2025, ECLI:NL:GHARL:2025:7218

AVG, handelsregister KvK, Inzagerecht

Graydon NL, Creditsafe NL en Graydon Holding (appellant) komen in hoger beroep op tegen een beschikking van de rechtbank Midden-Nederland, waarin zij waren gelast om een volledige lijst te verstrekken van alle ontvangers aan wie persoonsgegevens van geïntimeerde waren doorgegeven. verwerkt persoonsgegevens als bedrijfsinformatiespecialist en is in dat verband verwerkingsverantwoordelijke. Geïntimeerde had een inzageverzoek gedaan op grond van art. 15 AVG.

Het hof stelt voorop dat art. 15 AVG de betrokkene

recht geeft op informatie over ontvangers van persoonsgegevens, maar dat dit recht kan worden beperkt op grond van art. 23 AVG, zoals uitgewerkt in art. 41 UAVG. Appellant beroept zich op art. 41 lid 1 onder i UAVG: bescherming van de rechten en vrijheden van anderen, waaronder haar bedrijfsdebiet.
Het hof volgt dit beroep. De persoonsgegevens van geïntimeerde zijn afkomstig uit het handelsregister en dus openbaar. De Kamer van Koophandel informeert niet over wie het handelsregister raadpleegt. Een bestuurder krijgt dus ook niet te weten wie zijn gegevens rechtstreeks bij de KvK heeft ingezien. Volgens het hof bestaat daarom geen relevant verschil met de situatie waarin appellant niet onthult welke van haar afnemers kennis heeft genomen van dezelfde gegevens. Verstrekking van de volledige ontvangerslijst zou bovendien het bedrijfsdebiet van appellant schaden.
Het hoger beroep slaagt. De beschikking wordt vernietigd voor zover het inzageverzoek was toegewezen; dat deel van het verzoek van geïntimeerde wordt alsnog afgewezen.

Gerecht van Aruba, 19 november 2025, ECLI:NL:OGEAA:2025:347

Ontwikkelen applicatie, ontbinding, opzegging
Tourism Corporation Bonaire (TCB) heeft Dot1 Technologies opdracht gegeven tot de ontwikkeling van een mobiele applicatie. Dot1 stelt dat de app in de loop van 2021 gereed was voor opname in de appstores van Apple en Google, maar dat daadwerkelijke publicatie uitbleef omdat TCB de daarvoor vereiste registraties niet tijdig heeft verzorgd. TCB betwist dat zij de app tijdig heeft ontvangen of dat zij voldoende is geïnformeerd over de voortgang en de gereedheid van de applicatie.
Binnen TCB vonden in deze periode interne personele wisselingen plaats en werd een beleidswijziging doorgevoerd, waaronder een rebranding en de ontwikkeling van een nieuwe website. Hierdoor raakte het app-project gedurende enige tijd op de achtergrond. Eind 2022 werd het contact tussen partijen hervat. In deze fase ontstonden communicatieproblemen en wantrouwen, mede doordat Dot1 informatie aan TCB verzond via een voor TCB onbekend e-mailadres. TCB heeft daarop bij brief de overeenkomst buitengerechtelijk ontbonden.
Het Gerecht oordeelt dat Dot1 voldoende aannemelijk heeft gemaakt dat zij substantiële werkzaamheden heeft verricht en dat de applicatie zich in een vergevorderd stadium van ontwikkeling bevond. Daarbij betrekt het Gerecht mede zijn eigen waarnemingen ter zitting over de functionaliteit en vormgeving van de app. Wel wordt vastgesteld dat Dot1 is tekortgeschoten doordat zij, ondanks verzoeken van TCB, de app na oktober 2022 niet tijdig heeft getoond. Deze tekortkoming wordt echter niet aangemerkt als zodanig ernstig dat zij de buitengerechtelijke ontbinding van de overeenkomst rechtvaardigt. De ontbinding mist daarom rechtsgevolg.
Nu vaststaat dat TCB niet met Dot1 wenst voort te gaan en dat de overeenkomst haar praktische betekenis heeft verloren, mede omdat TCB inmiddels beschikt over een goed functionerende website, kwalificeert het Gerecht de brief van TCB van 26 februari 2023 als een opzegging door de opdrachtgever in de zin van artikel 7:408 BW. Door deze opzegging is de overeenkomst geëindigd.
Op grond van artikel 7:411 BW heeft Dot1 in dat geval recht op een naar redelijkheid vast te stellen deel van het loon voor de tot aan de opzegging verrichte werkzaamheden. Het Gerecht oordeelt dat Dot1 geen aanspraak kan maken op het volledig overeengekomen loon, gelet op haar verzuim om de app tijdig aan TCB te tonen. Dot1 wordt opgedragen een gespecificeerde opgave te doen van de bestede tijd en de door haar bespaarde kosten. TCB krijgt vervolgens de gelegenheid daarop te reageren. De vaststelling van het redelijke loon en iedere verdere beslissing worden aangehouden.

Rechtbank Noord-Nederland, 19 november 2025, ECLI:NL:RBNNE:2025:4814

Erfrecht, Dwaling, AI
In een geschil tussen erfgenamen over de verdeling van een nalatenschap vordert eiser vernietiging van de toedeling van een werkplaats aan haar broer (gedaagde). Eiseres stelt dat de werkplaats tegen een te lage waarde is ingebracht, waardoor zij is benadeeld. Primair doet zij een beroep op dwaling, subsidiair op het bestaan van een (gedeeltelijke) gift.
De rechtbank wijst de vorderingen grotendeels af. Dwaling ex art. 6:228 BW is bij verdelingen uitgesloten (art. 6:199 BW). Een beroep op art. 3:196 BW slaagt evenmin: Eiseres heeft niet gedwaald over de waarde van het goed zelf, maar over haar vermeende invloed op de waardering. De verwijzingen naar jurisprudentie waarop zij zich beroept blijken bovendien onjuist. de rechtbank vermoedt dat deze via ChatGPT of een vergelijkbare zoekmachine in de processtukken zijn beland. Ook de stelling dat sprake zou zijn van een gift vindt geen steun in de feiten.
Wel wijst de rechtbank een door gedaagde erkend bedrag van € 30.000 toe, vermeerderd met wettelijke rente vanaf 5 december 2024. De proceskosten worden gecompenseerd vanwege de familierelatie.

Rechtbank Noord-Holland, 20 november 2025 ECLI:NL:RBNHO:2025:13490

Persoonlijke levenssfeer, cameragebruik, AVG
Partijen zijn buren. Gedaagde heeft meerdere camera's aan zijn woning geplaatst, welke onder andere het perceel van eisers registreren. Eisers stellen dat hiermee een ongerechtvaardigde inbreuk wordt gemaakt op hun persoonlijke levenssfeer. In kort geding vorderen zij dat gedaagde de camera's verwijdert, althans zodanig vastzet of verplaatst dat daarmee hun eigendommen niet langer (kunnen) worden gefilmd.
Gedaagde voert verweer en stelt dat de plaatsing van de camera's gerechtvaardigd is vanwege ernstig en structureel overlastgevend gedrag van eisers. Sinds

een conflict met de aannemer van gedaagde in april 2025 zouden eisers zich schuldig hebben gemaakt aan herhaaldelijke vervuiling, besmeuring, bekladding, bekogeling en uiteindelijk zelfs vernieling van eigendommen van gedaagde. Ter bescherming van zijn eigendommen en ter bewijsverzameling heeft hij camera's geplaatst. In reconventie vordert gedaagde dat aan eisers een drietal verboden wordt opgelegd ter voorkoming van verdere overlast. Daarnaast vordert hij vergoeding van zowel materiële als immateriële schade.
De voorzieningenrechter wijst de vordering van eisers tot verwijdering, verplaatsing of het vastzetten van de camera's af. Daarbij overweegt de voorzieningenrechter dat de vastgestelde gedragingen van eisers, waaronder het meermalen bevuilen, besmeuren, bekogelen en vernielen van eigendommen van gedaagde, dermate ernstig zijn dat deze het plaatsen van camera's ter beveiliging rechtvaardigen. Bij de beoordeling van het gebruik van de camera's wordt dit beveiligingsdoel als uitgangspunt genomen.
De vorderingen van gedaagde in reconventie worden toegewezen. De voorzieningenrechter legt de gevraagde verboden aan eisers op en veroordeelt hen tot betaling van materiële en immateriële schadevergoeding aan gedaagde. De toegewezen schadevergoedingen worden wel gematigd ten opzichte van de gevorderde bedragen.

Rechtbank Rotterdam 21 november 2025, ECLI:NL:RBROT:2025:13631

Ontvankelijkheid, AVG, Identificatie
In deze procedure vordert eiser een verklaring voor recht dat Jingdong in strijd handelt met de artikelen 12 en 15 AVG, alsmede volledige inzage in zijn persoonsgegevens, op straffe van een dwangsom. De vorderingen zijn gebaseerd op het standpunt dat Jingdong niet (volledig) heeft voldaan aan haar informatie- en inzageverplichtingen als verwerkingsverantwoordelijke.
Jingdong heeft voorafgaand aan een inhoudelijke behandeling een incident opgeworpen, waarin zij stelt dat eiser niet-ontvankelijk is in zijn vorderingen. Volgens Jingdong is niet vast komen te staan dat [eiser] een bestaande natuurlijke persoon is, terwijl uitsluitend een natuurlijke persoon zich op de rechten uit de AVG kan beroepen. Jingdong suggereert dat mogelijk de gemachtigde van eiser de feitelijke procespartij is, hetgeen, indien juist, aan ontvankelijkheid in de weg zou staan.
De kantonrechter overweegt dat op basis van de overgelegde processtukken niet kan worden vastgesteld of eiser daadwerkelijk bestaat als natuurlijke persoon. Daarmee raakt het incident aan een fundamentele processuele voorvraag, te weten de identiteit en het bestaan van de eiser als rechtssubject. De kantonrechter acht het, mede uit praktische overwegingen, aangewezen om dit punt eerst mondeling met partijen te bespreken, alvorens tot een inhoudelijke beoordeling van de AVG-vorderingen over te gaan. Daartoe wordt een zitting bepaald die uitsluitend ziet op de vraag of eiser een bestaande natuurlijke persoon is. De kantonrechter merkt expliciet op dat eiser daarbij in ieder geval een legitimatiebewijs zal moeten tonen.
De behandeling van de zaak blijft beperkt tot deze ontvankelijkheidsvraag; inhoudelijke beoordeling van de gestelde schendingen van de AVG blijft vooralsnog achterwege. Voor de zitting wordt een behandeltijd van maximaal dertig minuten gereserveerd. Iedere verdere beslissing wordt aangehouden.

DECEMBER 2025

Rechtbank Den Haag, 1 december 2025, ECLI:NL:RBDHA:2025:23627

Kort geding, kansspelen, reputatieschade
Verzoekster biedt kansspelen aan in Nederland onder de naam 'Unibet'. De Kansspelautoriteit heeft vastgesteld dat verzoekster in de periode 14 juli 2022 tot en met 1 juli 2024 ten aanzien van 10 spelers haar zorgplicht heeft geschonden en daarmee de Wet op de kansspelen heeft overtreden. De kansspelautoriteit een boete opgelegd van 4 miljoen euro. Verzoekster heeft hiertegen bezwaar gemaakt. De boete is omstreeks 1 oktober 2025 geopenbaard. Verzoekster is het hier niet mee eens en verzoekt om de openbaarmaking van de boete te schorsen tot het moment dat op haar bezwaar is beslist.
De rechter wijst dit verzoek af. Zij weegt de belangen af, waarbij de belangen van verweerder – het openbaren van het besluit op grond van haar wettelijke toezichthoudende taak – en het belang van verzoekster om deze niet openbaar te maken. Verzoekster heeft geen zwaarwegende redenen heeft aangedragen die opwegen tegen het algemene belang dat is gediend met de openbaarmaking. Zij heeft slechts in algemene termen verwezen naar mogelijke reputatieschade die zij zou lijden door de mogelijke toename van schadeclaims. Het belang van openbaarmaking van verweerder weegt zwaarder dan het belang van verzoekster om geen nadelen te ondervinden door de openbaarmaking.

Rechtbank MiddenNederland, 3 december 2025, ECLI:NL:RBMNE:2025:6664

Kort geding, websiteontwikkeling, vervangende schadevergoeding
Kort geding. Een van de eisers heeft een overeenkomst voor het bouwen van een webshopsite gesloten met gedaagde, eind 2023. Volgens eisers wordt de website in december 2024 prematuur live gezet, functioneert deze sindsdien gebrekkig en blijft herstel daarvan telkens uit. Op 20 oktober 2025 volgt een ingebrekestelling van eisers, waarna eisers de overeenkomst omzetten in een recht op vervangende schadevergoeding. Zij wensen een derde in te schakelen om de website af te bouwen en verlangen toegang tot de technische infrastructuur, alsmede een voorschot op de te vorderen schadevergoeding.

Gedaagde bestrijdt de tekortkomingen, betwist wie haar contractspartner is en beroept zich op haar intellectuele eigendomsrechten.
De rechter stelt vast dat eisers een spoedeisend belang hebben: de webshop draait al een jaar onvoldoende, omzet blijft achter en de bedrijfsvoering is afhankelijk van een goed functionerende website. De bodemrechter zal waarschijnlijk de tekortkomingen aannemen door bewijs dat is overlegd door eisers. Het beroep op verzoeksters intellectuele eigendomsrechten slaagt niet. De vorderingen zien niet op overdracht daarvan, maar enkel tot toegang door een derde om overeengekomen functionaliteiten af te bouwen. De vordering tot medewerking aan toegang tot de website, servers, databases, repositories en applicaties wordt toegewezen. De vordering tot een voorschot op vervangende schadevergoeding wordt gedeeltelijk toegewezen. De vordering tot medewerking aan overdracht van hosting en domeinnamen wordt volledig toegewezen.

Rechtbank Noord-Nederland, 9 december 2025, ECLI:NL:RBNNE:2025:4982

Refundfraude Amazon, computervredebreuk, oplichting
De verdachte wordt o.a.vervolgd voor grootschalige refundfraude via Amazon en het hacken van PostNL-terminals. Uit onderzoek blijkt dat verdachte ruim 500 retourlabels heeft gescand met behulp van een gekloonde PostNL-terminal. Hierdoor leek het alsof producten werden teruggestuurd aan Amazon, terwijl verdachte in werkelijkheid niets, lege verpakkingen of waardeloze goederen retourneerde. Amazon keert bij iedere scan automatisch het aankoopbedrag terug, waardoor verdachte goederen behoudt zonder daarvoor te betalen. Gedurende bijna twee jaar bestelt verdachte op deze wijze honderden producten en verkoopt een deel door. De rechtbank acht dit patroon van handelen een gewoonte. Daarnaast wordt de verdachte veroordeeld voor computervredebreuk, doordat hij hackte in het PostNL-systeem om zo de PostNL-terminal te klonen. Ook wordt hij veroordeeld voor oplichting en het voorhanden hebben van professioneel vuurwerk en soften harddrugs. Vrijspraak m.b.t. valsheid in geschrifte van urendeclaraties. De rechtbank veroordeelt verdachte tot een gevangenisstraf van 18 maanden, waarvan 8 maanden voorwaardelijk met een proeftijd van drie jaren. De vorderingen van Amazon en PostNL m.b.t. de door hen geleden worden hoofdelijk toegewezen.

Gerechtshof ArnhemLeeuwarden, 11 december 2025, ECLI:NL:GHARL:2025:7962

Doxing, smaadschrift, schadevergoeding
Hoger beroep. Vonnis in eerste aanleg waarin verdachte deels is veroordeeld voor doxing en smaadschrift en het OM deels nietontvankelijk is verklaard. Verdachte heeft op Facebook onder openbare berichten persoonsgegevens van de benadeelde partij gedeeld (naam, initialen en woonplaats) en haar beschuldigd van mishandeling van haar kleinzoon.
Het hof oordeelt dat het OM ontvankelijk is in de vervolging, omdat – hoewel er geen formele klacht is ingediend - op basis van het dossier o.a. blijkt dat de benadeelde partij uitdrukkelijk aangifte doet, vervolging wenst, schadevergoeding vordert en betrokken blijft bij de procedure. Daarmee is binnen de wettelijke termijn de wens tot vervolging voldoende vast komen te staan en is het OM ontvankelijk. Het hof oordeelt daarnaast dat er verdachte schuldig is aan doxing en smaad: verdachte heeft op Facebook persoonsgegevens van de benadeelde partij heeft verspreid. Het hof acht bewezen dat verdachte besefte dat haar uitlatingen ernstige overlast, reputatieschade en professionele hinder voor de benadeelde partij zouden veroorzaken. Daarmee is zowel het oogmerk voor doxing als de wettelijke vereisten voor smaadschrift vervuld. Het hof acht de feiten ernstig: verdachte maakt doelbewust misbruik van de laagdrempeligheid van sociale media en publiceert beschuldigingen in een context die reacties uitlokt. De impact op het slachtoffer is groot: zij werkt in de kinderopvang en krijgt te maken met bedreigingen, stress en aanzienlijke reputatieschade. Oplegging van een taakstraf van 120 uur, waarvan 40 uur voorwaardelijk met een proeftijd van drie jaar. Oplegging bijzondere voorwaarde van het zich onthouden van het doen van uitlatingen over de benadeelde partij. Daarnaast wordt de immateriële schadevergoeding van € 2.500 volledig toegewezen.

Rechtbank Den Haag, 16 december 2025, ECLI:NL:RBDHA:2025:24070

Kort geding, onrechtmatige uitlating, art. 8 EVRM
Het COA vordert in kort geding dat gedaagde (een voormalig asielzoeker die in 2022–2023 in een COA-locatie verbleef) honderden berichten over COA-medewerkers verwijdert en verwijderd houdt, en dat hij zich in de toekomst onthoudt van soortgelijke uitingen. Gedaagde plaatst sinds 2023 berichten op meerdere socialemediaaccounts (met name Instagram) waarin hij individuele COA-medewerkers bij naam en met foto afbeeldt, hen beschuldigt van onder meer racisme, discriminatie, moord en het veroorzaken van zelfdoding, en hen uitmaakt voor nazi's of ernstige ziektes toewenst. Deze berichten betreffen medewerkers zonder publieke functie. De rechter wijst de vordering van het COA toe. Zij weegt de belangen van de gedaagde (de vrijheid van meningsuiting, art. 10 EVRM) en de werknemers van het COA (recht op privéleven art. 8 EVRM) af. De rechter stelt voorop dat werknemers die geen publieke functie vervullen extra bescherming toekomt. Hun handelingen zijn onderdeel van het uitvoeren van COA-beleid en vormen geen aanleiding om hen persoonlijk in de openbaarheid te trekken. Daarnaast kan gedaagde misstanden binnen de opvang aankaarten zonder het publiceren van persoonsgegevens van individuele uitvoerende medewerkers. De vordering tot het verwijderen van deze berichten wordt afge-

wezen, nu vaststaat dat de berichten door gedaagde zijn verwijderd. De vordering tot het "verwijderd houden" wordt toegewezen: niet duidelijk is of de berichten permanent verwijderd zijn of slechts onzichtbaar door het deactiveren van accounts. Er bestaat, mede gezien het eerdere gedrag en mogelijke mentale problematiek van gedaagde, reëel risico op recidive.

Rechtbank Noord-Nederland, 16 december 2025, ECLI:NL:RBNNE:2025:5182

Belangenafweging, naamswijziging, TBS

Verzoeker wil voornaam en achternaam wijzigen omdat hij als gevolg van zijn ontsnapping uit een tbs-kliniek veelvuldig in het nieuws is geweest. Hij is op het internet makkelijk vindbaar, waardoor het maken van een nieuwe start bemoeilijkt wordt.

De Staatssecretaris heeft besloten de achternaamswijziging wel mogelijk te maken. Echter, de rechtbank wijst dit verzoek af: het algemeen belang weegt zwaarder dan het recht op privacy van de verzoeker in dit geval, vanwege de bescherming van de samenleving, de geloofwaardigheid van het rechtssysteem, vrijheid van informatie en de gelijke behandeling. Dit, mede omdat verzoeker is veroordeeld voor een aantal zedenmisdrijven en de publicatie van zijn gegevens een gevolg is van zijn eigen keuze om tijdens zijn verlof te ontsnappen. De rechtbank is o.a. tot deze slotsom gekomen, omdat er een zwaarwegend individueel belang moet bestaan om een verdachte of veroordeelde een nieuwe identiteit te geven. Dat belang ontbreekt hier. Het verzoek wordt afgewezen.

Rechtbank Gelderland, 23 december 2025, ECLI:NL:RBGEL:2025:11614

Kort geding, onrechtmatige uitlatingen, social media

Kort geding. De Stichting Driegasthuizengroep ('Stichting') vordert een verbod op de door gedaagde geplaatste openbare uitlatingen op sociale media over haar zorglocatie, personeel en bestuurders. Gedaagde plaatst op diverse social media platforms herhaaldelijk berichten, foto's en video's waarin hij deze personen beschuldigt van mishandeling, verwaarlozing, intimidatie en corrupte zorgpraktijken. Daarbij noemt hij hun namen, toont hun gezichten en roept anderen op om adressen te achterhalen in ruil voor geld. Ook volgt hij een medewerker van de zorglocatie van werk naar huis.

Gedaagde verschijnt niet in de zaak waardoor er in verstek wordt geoordeeld. De voorzieningenrechter weegt de belangen tussen enerzijds het recht op bescherming van eer en goede naam (art. 8 EVRM) van de betrokken personen en anderzijds de vrijheid van meningsuiting (art. 10 EVRM) van gedaagde af. De uitlatingen van gedaagde gaan aanzienlijk verder dan het uiten van kritiek op zorgverlening: het gaat om ernstige beschuldigingen, beledigingen, bedreigingen en opruiende teksten zonder feitelijke basis. De berichten zijn agressief van toon, intimiderend en roepen aan tot confrontatie, het achterhalen van privéadressen en het opstellen van een zwarte lijst. Het belang van de Stichting bij bescherming van haar medewerkers, bestuurders, cliënten en reputatie weegt zwaarder dan de vrijheid van meningsuiting van gedaagde. De rechter wijst de vorderingen grotendeels toe: gedaagde moet binnen 24 uur alle onrechtmatige uitlatingen van zijn eigen sociale media verwijderen en verwijderd houden en krijgt een benaderverbod op straffe van een dwangsom. Het verzoek om lijfsdwang wordt deels toegewezen.

Wet- en regelgeving

mr. S. Zamani

NL

Wet modernisering elektronisch bestuurlijk verkeer

Op 1 januari 2026 is de Wet modernisering elektronisch bestuurlijk verkeer in werking getreden. Deze wet wijzigt bepalingen in de Algemene wet bestuursrecht (hierna: Awb) over elektronisch bestuurlijk verkeer en geeft burgers en bedrijven het recht om langs elektronische weg berichten aan een bestuursorgaan te zenden, op een door het bestuursorgaan bepaalde wijze. Met deze wet krijgen burgers en bedrijven meer mogelijkheden om via digitale kanalen met de overheid in contact te treden, waarbij de keuze tussen het volgen van de elektronische of de papieren weg blijft bestaan. Het verplichte gebruik van de elektronische weg kan wel in andere wetten dan de Awb worden voorgeschreven.

Bron:
https://zoek.officielebekendmakingen.nl/stb-2023-183.html

Wetsvoorstel Uitvoeringswet verordening cyberweerbaarheid

Op 22 december 2025 is het wetsvoorstel Uitvoeringswet verordening cyberweerbaarheid gepubliceerd. Het wetsvoorstel strekt tot uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (hierna: de Verordening cyberweerbaarheid, Cyber Resilience Act of CRA). De CRA voorziet in een gefaseerde inwerkingtreding. De voorgestelde artikelen of onderdelen daarvan treden, conform de CRA, op verschillende momenten in werking. Zo treden de artikelen die betrekking hebben op de aanmelding van conformiteitsbeoordelingsinstanties op een eerder tijdstip in werking.

Bron:
https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails\&qry=wetsvoorstel

EU

Voorstel Wet inzake digitale netwerken (Digital Networks Act)

Op 21 januari 2026 heeft de Europese Commissie een voorstel ingediend om de EU-regels inzake connectiviteitsnetwerken te moderniseren, te vereenvoudigen en te harmoniseren. Het voorstel heeft mede tot doel de veiligheid en veerkracht van digitale netwerken te versterken. Daarnaast strekt het voorstel ertoe de thans geldende regels te actualiseren om investeringen in snelle, veilige en toekomstgerichte connectiviteit – zoals geavanceerde glasvezel- en mobiele netwerken – te stimuleren en daarmee de Europese concurrentiekracht te versterken. Voor aanbieders wordt het eenvoudiger om diensten in meerdere lidstaten aan te bieden en worden de administratieve en rapporteringsverplichtingen verminderd.

Bron:
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX

Voorstel Cybersecurity Verordening 2 (Cybersecurity Act 2)

Op 20 januari 2026 heeft de Europese Commissie het voorstel voor de Cybersecurity Verordening 2 (Verordening (EU) 2026/0011) ingediend. Het voorstel beoogt onder meer de rol van ENISA bij de ondersteuning van de implementatie van NIS2 te versterken, het Europees Cybersecurity Certificeringskader te hervormen en een geharmoniseerd kader voor ICT-toeleveringsketens in te voeren. Daarnaast worden aanpassingen van de NIS2-richtlijn voorgesteld, gericht op vereenvoudiging en afstemming met het voorstel voor de Cybersecurity Verordening 2. Een belangrijk onderdeel van het voorstel betreft de invoering van verplichte cybersecuritycertificering voor cybersecurityproducten en -diensten binnen de EU. Bedrijven die onder meer securitysoftware, netwerkapparatuur of clouddiensten aanbieden, zullen moeten aantonen dat hun producten voldoen aan Europese beveiligingsnormen. Daarnaast worden de meldingsverplichtingen voor cyberincidenten aangescherpt, onder meer door kortere rapportagetermijnen. Het voorstel voorziet voorts in de oprichting van een Europees Cybersecurity Incident Response Fund, dat is bedoeld om financiële onder-

steuning te bieden aan lidstaten bij grootschalige cyberaanvallen. Daarnaast worden verplichte cybersecurityaudits ingevoerd voor kritieke sectoren zoals energie, transport, gezondheidszorg en financiële dienstverlening. De Cybersecurity Verordening 2 voorziet in een gefaseerde inwerkingtreding. De basiseisen treden naar verwachting in 2026 in werking, waarna organisaties een overgangsperiode van 18 tot 24 maanden krijgen. Voor exploitanten van kritieke infrastructuur geldt een kortere overgangsperiode. Lidstaten moeten de wetgeving omzetten in nationale regelgeving.

Bron:
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX

Voorstel wijziging NIS2-Richtlijn

Op 20 januari 2026 heeft de Europese Commissie een voorstel tot wijziging van de NIS2-richtlijn (Richtlijn (EU) 2022/2555) ingediend om de EU-regels inzake cyberbeveiliging te vereenvoudigen en af te stemmen met het voorstel voor de Cybersecurity Verordening 2. Het voorstel bevat maatregelen om de naleving van EU-cyberbeveiligingsregels en risicobeheervereisten voor bedrijven die in de EU actief zijn te vereenvoudigen. De voorgestelde wijzigingen van de NIS2-richtlijn zijn erop gericht de rechtszekerheid te vergroten, onder meer door vereenvoudiging van bevoegdheidsregels, stroomlijning van de gegevensverzameling over ransomware-aanvallen en het faciliteren van het toezicht op grensoverschrijdende entiteiten, met een versterkte coördinerende rol voor ENISA.

Bron:
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX

Signaleringen

mr. H.A.J. de Jong en A. Podvorica

EC deelt eerste boete uit aan X van 120 mln voor niet naleven DSA

De Europese Commissie heeft op 5 december 2025 de eerste boete opgelegd wegens het overtreden van de Digital Services Act (DSA). X (voorheen Twitter) heeft een boete gekregen van €120 miljoen voor het overtreden van de transparantieverplichtingen uit artikel 25, lid 1 van de DSA. De Commissie heeft geoordeeld dat het gebruik van 'blauwe vinkjes' waarmee op X geverifieerde accounts worden aangeduid, misleidend is. Het blauwe vinkje zegt weinig over een echte verificatie, omdat het voor iedereen beschikbaar is tegen een betaling. Hierdoor wordt het volgens de Commissie lastig voor gebruikers van X om de authenticiteit van accounts te beoordelen. X moet binnen 60 dagen laten zien welke maatregelen het bedrijf voornemens is te nemen om een einde te maken aan de inbreuk. Daarnaast heeft de Commissie ook geoordeeld dat X de regels rond de openheid over reclame niet na heeft geleefd en er vaak essentiële informatie mist in het register. Hiervoor heeft X 90 dagen de tijd gekregen om doeltreffende maatregelen te nemen.

Bron:
https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934

ACM bevoegd om toezicht te houden op Data Act

Sinds 21 november 2025 is de Autoriteit Consument & Markt (ACM) bevoegd toezicht te houden op de Europese Data Act. De ACM ziet in samenwerking met andere Europese toezichthouders erop toe dat bedrijven tegenover consumenten en andere bedrijven transparant moeten zijn over de gegevens die worden verzameld. Ook moet transparant zijn op welke wijze toegang tot die gegevens wordt verleend. De ACM zal zich richten op cloudaanbieders en leveranciers van slimme apparaten met een hoofdkantoor in Nederland. Eerder dit jaar heeft de ACM een conceptleidraad over de Data Act gepubliceerd, om bedrijven te ondersteunen bij het naleven van de verplichtingen. Daarnaast zal de ACM zich ook focussen op het geven van voorlichtingen. De ACM heeft als doel met de voorlichtingen bedrijven op weg te helpen en ontwikkelingen van de sector te stimuleren. Op de website van de ACM is een meldpunt beschikbaar voor wie vermoedt dat een bedrijf zich niet houdt aan de Data Act.

Bron:
https://www.acm.nl/nl/publicaties/acm-vanaf-nu-bevoegd-om-toezicht-te-houden-op-de-data-act

ACM werkt mee aan DMA-onderzoeken naar clouddiensten

De Autoriteit Consument & Markt (ACM) werkt samen met de Europese Commissie aan drie onderzoeken die de Commissie onlangs gestart is naar clouddiensten onder de Digital Markets Act (DMA). Een van de onderzoeken richt zich op het wegnemen van belemmeringen bij het overstappen naar andere spelers. Dit zorgt ervoor dat Europese bedrijven makkelijker kunnen toetreden tot de cloudmarkten. Doelstellingen van de DMA zijn onder andere het beschermen van ondernemers en consumenten, meer keuze geven aan consumenten en ondernemers in de digitale wereld en meer groeikansen voor bedrijven op de digitale markt. Op de naleving van de DMA biedt de wetgeving de Europese Commissie de mogelijkheid om een gezamenlijk onderzoeksteam op te zetten met een of meer nationale autoriteiten. De ACM is nu voor het eerst gaan samenwerken met de Europese Commissie in de onderzoeken naar de clouddiensten.

Bron:
https://www.acm.nl/nl/publicaties/acm-werkt-samen-met-europese-commissie-aan-onderzoek-naar-clouddiensten

CvdM: afspraken over de toegankelijkheid van e-boeken

De European Accessibility Act (EAA) verplicht sinds 28 juni 2025 dat e-boekdiensten voor iedereen toegankelijk moeten zijn, ook voor mensen met een beperking. Het Commissariaat voor de Media (CvdM) ziet toe op de naleving van de EAA op het gebied van e-boeken. De afgelopen maanden heeft het CvdM overleg gevoerd met verschillende partijen, zoals brancheverenigingen, om duidelijk te krijgen welke e-boeken toegankelijk moeten zijn en welke manier dit kan worden gerealiseerd. De betrokken partijen hebben gezamenlijk e-boeken ingedeeld in drie categorieën. Afhankelijk van de categorie waarin een boek valt, is vastgesteld hoe toegankelijk het moet worden gemaakt. Daarnaast zijn er ook afspraken gemaakt over oudere, verkrijgbare e-boeken, waarvoor een overgangsperiode geldt tot uiterlijk 1 mei 2027 (de zogeheten 'blacklist').

Bron:
https://www.cvdm.nl/voor-uitgevers/toegankelijkheidseisen-voor-e-boeken/toegankelijkheid-van-e-boeken-afspraken-en-richtlijnen/

EC: samenvatting en reacties op de herziening van de DMA

Op 8 januari 2025 heeft de Europese Commissie een samenvatting en de individuele reacties op de consultatie over de lopende herziening van de Digital Markets Act (DMA) gepubliceerd. De voorlopige herziening trok meer dan 450 reacties van een breed scala aan belanghebbenden. Over het algemeen zijn de reacties ten aanzien van de doelstellingen van de DMA ondersteunend en wordt aangegeven dat de verordening al voordelen heeft opgeleverd. Tegelijkertijd wordt in de reacties gevraagd om versterking van de datatoegang en interoperabiliteit en ziet de Commissie ook reacties over de reikwijdte van de DMA binnenkomen. Zo wordt bijvoorbeeld gevraagd naar een uitbreiding richting AI en clouddiensten. De commissie zal de input meenemen in een reviewrapport. Het reviewrapport zal 3 mei 2026 aan het Europees Parlement, het Europees Economisch en Sociaal Comité en de Raad worden gepresenteerd.

Bron:
https://digital-markets-act.ec.europa.eu/commission-publishes-summary-and-responses-consultation-ongoing-review-digital-markets-act-2026-01-08_en

EDPB doet aanbevelingen om privacy bij online shoppen te waarborgen

Het European Data Protection Board (EDPB) heeft tijdens de laatste vergadering aanbevelingen aangenomen over het verplicht stellen van gebruikersaccounts bij webshops. Meer specifiek heeft de EDPB aanbevelingen aangenomen om te verduidelijken wanneer e-commercewebsites gebruikers mogen verplichten een account aan te maken. Het aanmaken van een account kan leiden tot het verzamelen en verwerken van persoonsgegevens. Zo moet volgens het EDPB bijvoorbeeld beschikbaar zijn voor gebruikers, om aankopen te doen via een website zonder een account aan te maken via een 'gastmodus'. Het EDPB wil hiermee gebruiksvriendelijke en privacyvriendelijke praktijken in de e-commercesector stimuleren. De aanbevelingen liggen open voor feedback van de belanghebbenden. Daarnaast heeft het EDPB gediscussieerd over het voorstel voor de digitale omnibuswet en is een nieuwe vicevoorzitter benoemd.

Bron:
https://www.edpb.europa.eu/news/news/2025/edpb-gives-recommendations-make-online-shopping-more-respectful-users-privacy_en

Nieuw comité: CDNET

Vanaf 1 januari 2026 zal de nieuwe Steering Committee for New and Emerging Digital Technologies (CDNET) opereren binnen Europa. Onder het takenpakket van de CDNET vallen onder andere de intergouvernementele werkzaamheden van de Raad van Europa op het gebied van nieuwe en opkomende technologieën coördineren en uitvoeren. Daarnaast zal CDNET innovatie in deze werkzaamheden ondersteunen en het Comité van Ministers voorzien van juridische en beleidsmatige expertise op het gebied van opkomende technologieën. CDNET beheert bovendien de Framework Convention on Artificial Intelligence and Human Rights and Democracy and the Rule of Law en zal op dit juridische terrein het werk overnemen van the Committee on Artificial Intelligence (CAI).

Bron:
https://www.coe.int/en/web/artificial-intelligence/-/new-committee-established-cdnet-1

AI-tool Grok, mogelijke schending van DSA

De mediatoezichthouder in Frankrijk heeft een melding ontvangen over de AI-chatbot Grok. Volgens Franse autoriteiten genereert Grok illegale content, waaronder deepfakes. De autoriteiten stellen hiermee dat de AI-chatbot, ontwikkeld door xAI voor X, de Digital Services Act schendt door het genereren van illegale content. Er zijn naar schatting duizenden seksuele deepfakes zonder toestemming gegenereerd en daarna gepubliceerd op X. Honderden vrouwen en tieners hebben gemeld dat Grok de op sociale media gedeelde foto's heeft gebruikt om zogenoemde 'uitgeklede' beelden te genereren. Ook in het Verenigd Koninkrijk heeft de nationale toezichthouder Ofcom een onderzoek naar Grok gestart naar aanleiding van de seksuele beelden. X heeft al maatregelen genomen zoals het verwijderen van de aanstootgevende afbeeldingen. Volgens xAI kunnen sinds kort alleen betalende gebruikers nog afbeeldingen genereren.

Bron:
https://www.nu.nl/economie/6382329/brits-onderzoek-naar-x-en-grok-vanwege-zeer-verontrustende-seksuele-beelden.html?referrer=https%3A%2F%2Fwww.google.com%2F en https://www.politico.eu/article/france-lawmaker-investigate-deepfakes-women-stripped-naked-grok-x/

Consultatie Kaderwet toetsing algoritmen

De consultatie voor de nieuwe initiatiefwet, Kaderwet toetsing algoritmen, is op 11 november 2025 geopend en heeft als einddatum 18 januari 2025. Het wetsvoorstel heeft tot doel bescherming te bieden aan personen die mogelijk gedupeerd worden door discriminerende algoritmen. In deze wet wordt specifiek verplichte wetenschappelijke toets op algorit-

men die gebruikt worden voor risicoprofilering binnen overheidsorganisaties geregeld. Het gaat hierbij vooral om risicoprofileringsalgoritmen die binnen bestuursorganen worden gebruikt om besluiten te nemen of om besluiten voor te bereiden. Daarnaast zal er een algoritmeregister komen waar informatie over de algoritmen en de bijbehorende toetsen moeten worden gepubliceerd.

Bron:
https://www.internetconsultatie.nl/wettoetsingalgoritmen/b1

Tijdschrift voor Kapitaalmarktenrecht

Het Tijdschrift voor Kapitaalmarktenrecht (KMR) bevat voor de rechtspraktijk relevante artikelen, annotaties en korte opiniërende columns.

KMR richt zich als eerste Nederlandse tijdschrift uitsluitend op kapitaalmarktenrecht:
(i) publiekrechtelijke regulering van kapitaalmarkten (financieel toezichtrecht); en
(ii) civielrechtelijke onderwerpen met betrekking tot kapitaalmarkten

NIEUW!

Voor wie

- Bedrijfsjuristen (met name bij beursgenoteerde ondernemingen)
- Wetgevingsjuristen
- Advocatuur
- Financiële instellingen waaronder:
  - *Banken*
  - *Beleggingsondernemingen*
  - *Handelsplatformen*
  - *Beleggingsanalisten*
  - *Credit Rating Agencies*
  - *ESG Rating Providers*
  - *Benchmark Administrators*
  - *Proxy Advisers*
  - *Clearinginstellingen & CCP's*
  - *Custodians*
- Toezichthouders
- (Register-) Accountants
- Universiteiten

Inhoud

Het focusgebied van KMR valt uiteen in de volgende hoofd- en subcategorieën:

- Algemeen
  - *Kapitaalmarktunie*
  - *Economische ratio & doelstellingen toezichtregels*
  - *Regelgeving- en toezichtstructuur*
  - *Transactietypen (zoals aandelen-emissies, obligatie-emissies, beursgang, securitisations)*
  - *Financiële instrumenten*
  - *Duurzaamheid (ESG)*
  - *Digitalisering*
- Openbaarmaking informatie
  - *Prospectus*
  - *Periodieke publicatieverplichtingen*
  - *Openbaarmaking voorwetenschap*
  - *Melding zeggenschap*
- Handel & afwikkeling
  - *Handelsplatformen*
  - *Handelsregels (inclusief transparantieregels en handelsverplichtingen)*
  - *Short Selling*
  - *Algoritmische handel & HFT*
  - *Clearing & Settlement*
- Markmisbruik
  - Handel met voorwetenschap
  - Marktmanipulatie
- Tussenpersonen & gatekeepers
  - *Beleggingsondernemingen*
  - *Beleggingsanalisten*
  - *Credit Rating Agencies*
  - *ESG Rating Providers*
  - *Benchmark Administrators*
  - *Proxy Advisers*
  - *Clearinginstellingen & CCP's*
  - *Custodians*
- Civielrechtelijke aspecten
  - *Contractuele en vennootschappelijke aspecten financiële instrumenten*
  - *Administratie & bewaring effecten*
  - *Giraal effectenverkeer*
  - *Aansprakelijkheidsvraagstukken*
  - *Civielrechtelijke gevolgen overtreding toezichtrecht*

Meer informatie: https://denhollander.info/kapitaalmarktenrecht

DEN HOLLANDER

info@denhollander.info • www.denhollander.info