Tijdschrift voor

INTERNET-RECHT

JAARGANG 17 - MAART 2024 **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

Redactiesecretarissen
mr. K. Konings (NORD Advocaten)
mr. B. de Vos (ICTRecht)

E-mail redactiesecretariaat
mr. K. Konings: koen@nord.legal
mr. B. de Vos: b.devos@ictrecht.nl

Hoofdredacteur
mr. P.G. van der Putt (Vondst Advocaten)

Redactie
mr. B.D.P. van der Eijk (Bird & Bird)
mr. I.S. Feenstra (McKinsey & Company)
mr. H.A.J. de Jong (Turing Advocaten)
mr. C.C.M. Kroeks - De Raaij (Nestor Notabilis Iuris B.V.)
dr. mr. T. van der Linden (Hogeschool Utrecht)
mr. dr. E.D.C. Neppelenbroek (Rijksuniversiteit Groningen)
Marc Peeters (Tele2 AB)
mr. dr. E.P.M. Thole (Van Doorne N.V.)
mr. R.J.J. Westerdijk (Kennedy Van der Laan)
mr. M. Weij (The Data Lawyers)
G.J. Zwenne (Pels Rijcken Drooglever Fortuijn/eLaw@Leiden)

Vaste medewerkers
M.V. Avanesian LL.B, BSc (The Tech Lawyer)
mr. ir. A.P. Engelfriet (ICTRecht en beheerder van www.iusmentis.com)
mr. N. Hermans-Falot (ABN AMRO)
dr. C. Jeloschek (Kennedy Van der Laan)
mr. V.I. Laan (The Data Lawyers)
mr. F. Schemkes (BDO)
mr. drs. E.F. Vaal (The Data Lawyers)
mr. J.J.H. Vos (Autoriteit Persoonsgegevens)

Abonnement
Zie: https://denhollander.info/

Nieuwe abonnementen
Abonnementen kunnen via de website worden afgesloten Abonnementen kunnen worden gestart per 1 januari van een kalenderjaar. Valt de aanvraag van een abonnement niet samen met het begin van een kalenderjaar, dan wordt op aanvraag het tarief voor het lopende jaar naar rato berekend indien het abonnement ook in het jaar daaropvolgend wordt afgenomen. Op al onze abonnementen zijn de Algemene voorwaarden van toepassiing

Adreswijziging
Bij adreswijziging wordt u verzocht deze zo spoedig mogelijk en bij voorkeur schriftelijk door te geven aan de uitgeverij onder de vermelding van: adreswijziging Tijdschrift voor Internetrecht.

Beëindiging abonnement
Abonnementen kunnen alleen schriftelijk, tot 1 december van het lopende abonnementsjaar, worden opgezegd. Bij niet-tijdige opzegging wordt het abonnement automatisch voor een kalenderjaar verlengd.

ISSN 1875-7766

Citeerwijze
IR 2024, nr. 1
ISSN: 1875-7766

Tijdschrift voor INTERNETRECHT

JAARGANG 17 - MAART 2024 - NUMMER 1

Online oprichten van BV's eindelijk mogelijk

mr. P.G. van der Putt[1]

Het is eindelijk zo ver: BV's kunnen geheel online worden opgericht. De wetwijziging die dit mogelijk maakt, is 1 januari 2024 van kracht geworden.[2] Laachir en Rensen schreven in ons tijdschrift al eerder over deze wet.[3]

Het heeft wel even geduurd. Het is iets meer dan 24 jaar geleden dat de richtlijn elektronische handtekeningen in Europa werd aangenomen, waarin de eerste basis voor online notariële verrichtingen werd neergelegd.[4] De praktijk heeft daar niet op gewacht. Vlottere aanbieders boden al sinds jaar en dag de mogelijkheid om "online" een BV op te richten.[5] Maar helemaal digitaal was dat proces niet. De akte moest nog altijd op papier worden ondertekend door de oprichter(s) en de notaris.

Als gevolg van COVID-19 werd er tijdelijk voorzien in versoepeling van het (oude) regime. De Tijdelijke wet COVID-19 voorzag in de mogelijkheid om een akte te passeren met gebruikmaking van tweezijdige audiovisuele communicatiemiddelen.[6] De enige voorwaarde die werd gesteld aan een audiovisueel communicatiemiddel was dat de notaris in staat moest zijn om de identiteit van partijen vast te stellen, en dat partijen via dat communicatiemiddel direct met de notaris konden communiceren. Zoom of Teams was in beginsel voldoende. De oprichter kon dan online zijn paspoort tonen. Op 1 september 2023 is deze soepele regeling vervallen. Dat is aan de ene kant jammer, want volgens mij kon de praktijk er prima mee uit de voeten. Aan de andere kant was het natuurlijk geen solide systeem. Over fraude of misbruik heb ik overigens niets verontrustends gehoord.

Gebruiksgemak is zeer bepalend voor het succes van digitale middelen. In Nederland zijn wij al aardig gewend aan elektronisch verkeer. Vele formele handelingen, zoals belastingaangiftes en contact met de rechtbank kunnen relatief eenvoudig digitaal worden verricht. Toen ik afgelopen jaar aan internationale collega's de werking van DigiD liet zien, was er verbazing alom. Er werd met bewondering gekeken naar het gebruiksgemak en de -mogelijkheden.

Op dit moment staat er een wijziging van de zogenaamde eIDAS-verordening op stapel, die naar verwachting dit jaar zal worden aangenomen.[7] Die wijziging regelt dat alle Europese burgers gratis de mogelijkheid moeten krijgen om een geharmoniseerd Europees digitaal identiteitsmiddel aan te schaffen, gebaseerd op Europese technische eisen. Zeg maar een Europees DigiD.[8] Ik verwacht dat hiermee een grote stap zal worden gezet naar de verdere digitalisering van Europa.

Maar digitalisering zet oude gewoontes niet zomaar opzij. De eerst BVs zijn inmiddels online opgericht.[9] KNBkanaal, het YouTubekanaal dat wordt beheerd door de Koninklijke Notariële Beroepsorganisatie, bevat een aandoenlijk filmpje van de totstandkoming van de eerste digitale oprichtingsakte.[10] We zien de oprichter van de BV en de notaris samen, fysiek bij elkaar, aan tafel zitten, met ieder hun eigen laptop. De oprichter identificeert zichzelf met behulp van zijn telefoon en laptop. Ook zijn instemming brengt hij tot uiting met zijn devices. De notaris lacht hem vriendelijk toe en schudt hem de hand. Niet bepaald "online".

---

1. Polo van der Putt is hoofdredacteur van dit tijdschrift.
2. https://zoek.officielebekendmakingen.nl/stb-2023-277.html.
3. K. Laachir / G. Rensen, *Digitale oprichting besloten vennootschap*, Tijdschrift voor Internetrecht 2022, nr. 4.
4. https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A31999L0093.
5. Zie voor voorbeelden van huidige aanbieders onder andere https://www.ligo.nl/bv-oprichten en https://www.firm24.com/.
6. Zie artikel 26 van de Tijdelijke wet COVID-19 Justitie en Veiligheid, https://wetten.overheid.nl/BWBR0043413/2020-12-17/#Paragraaf5_Artikel26.
7. Zie voor de eIDAS-verordening https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX en voor de voorgestelde wijziging https://www.eerstekamer.nl/eu/europeesvoorstel/com_2021_281_voorstel_voor_een/document/f=/vlkbdpxcwyh6.pdf.
8. Zie ook mr. A. van Zuijlen, mr. H.A. de Voogt CIPP/E en dr. Mr. M. van der Linden, *Self Sovereign Identity*, Tijdschrift voor Internetrecht 2022, nr. 5.
9. https://www.knb.nl/nieuwsberichten/eerste-digitale-akten-gepasseerd.
10. https://www.youtube.com/watch?v=W1mY0tUNXuA.

MiCA: Eén Europese markt, maar 27 keuringsstations?

drs. H.A. Koning[1]

De invoering van de Markets in Crypto Assets Regulation (MiCA) die eind 2024 compleet is, zal voor de cryptomarkt binnen de EU als geheel duidelijkheid scheppen. Wat zijn nu naast dat er één Europese interne markt wordt gecreëerd voor aanbieders van cryptoactiva de gevolgen van MiCA? Dit artikel beschrijft de aanleiding voor MiCA, wat deze verordening beoogt, en kijkt naar de gevolgen die de invoering meebrengt voor de aanbieders van cryptoactiva. Voor een nieuw fenomeen als cryptoactiva is dat niet altijd zo eenduidig als men zou willen, en dat kan ook niet anders. Onder MiCA kan elke nationale toezichthouder toestemming verlenen aan aanbieders van crypto-activiteiten en waarmee toetreding tot de gehele EU-markt wordt verkregen. Dat zal (onbedoeld) kunnen leiden tot 'concurrentie' tussen de onderlinge toezichthouders in de EU, waarbij sommige landen binnen de EU blockchain technologie en cryptoactiva als een economische kans en groeimodel zullen zien en wellicht toetreding tot de markt beter faciliteren dan andere lidstaten. Eén Europese markt, maar mogelijk met 27 verschillende keuringsstations?

1. Introductie

What's law got to do with IT? Onder deze titel werd vorig jaar een artikel gepubliceerd over de onsamenhangendheid ten aanzien van de regulering van technologie. Daarbij werd een analyse gemaakt van wetgeving en internet, waaruit bleek dat terwijl de wetgeving wel meer grip op het internet kreeg, deze zelfde wetgeving steeds incoherenter is geworden wanneer deze wordt toegepast op opkomende innovatieve technologieën.[2] Het zou best eens zo kunnen zijn dat deze incoherentie momenteel ook op blockchain van toepassing is. Met de intrede van de Markets in Crypto Assets Regulation (MiCA) lijkt daaraan een einde te komen. Innovatie, te zien als ontwikkeling en introductie van nieuwe technologieën, is soms te vergelijken met een kat-en-muisspel tussen enerzijds de aanbieders van technologie en anderzijds de wetgever en toezichthouder. Wetgever en toezichthouder hebben een verantwoordelijkheid naar zowel de consument als de markt. De verantwoordelijkheid naar de consument richt zich dan met name op bescherming, zoals het stellen van standaarden en zekerheden op geleverde producten en diensten. De verantwoordelijkheid naar de markt richt zich op het toezien op een eerlijke en pluriforme markt waarbij voor de aanbiedende partijen het speelveld zo gelijk mogelijk wordt gemaakt en gehouden. Dit kat-en-muisspel is soms ook een haatliefde verhouding waar nut en noodzaak wel van ingezien worden, maar wat ook vaak als rompslomp en tegenhouden of erger nog als tegenwerken, wordt gezien. Zie hier het dilemma: te vroeg ingrijpen belemmert innovatie, te laat ingrijpen laat de ontwikkeling van technologie ongebreideld doorgaan. Daarmee zou men kunnen zeggen dat in zekere zin regulering meer een timings-issue is dan een noodzakelijkheids-issue.

Dat dit niet alleen theoretisch is maar zich ook daadwerkelijk in de praktijk laat zien is het beste met een voorbeeld te illustreren. Een voorbeeld waarbij regulering te laat was betreft AI of kunstmatige intelligentie. AI heeft zich tot de afgelopen jaren vrij kunnen ontwikkelen en werd meer als leuk, spannend en als een natuurlijke ontwikkeling in computertechnologie gezien dan dat er kritisch naar toepassingen, consequenties of governance werd gekeken. Een bepaalde naïviteit kan wel aan gebruikers, aanbieders en toezichthouders worden toegedicht. Een eerste grote wake-up call was het Cambridge Analytica (CA) schandaal.[3] Aanvankelijk lag daarbij de focus met name op privacy en het onrechtmatig verzamelen en gebruiken van data van Facebookgebruikers. De app van CA verzamelde en gebruikte data van maar liefst 87 miljoen Facebook profielen. De door CA gebruikte AI gaf naar nu is gebleken een doorslaggevend voordeel aan de politieke campagne van Ted Cruz en Donald Trump in 2016. De door Aleksandr Kogan ontwikkelde app en zijn algoritme bouwde voort op een eerder door Facebook ontwikkelde personality quiz app uit 2013.[4] Dat CA deze data verwerkte is pas in 2015 bij Facebook bekend geworden, waarop Kogan gevraagd is deze data te ver-

1. Hans A. Koning is buiten promovendus aan het Amsterdam Law & Technology Institute, Vrije Universiteit Amsterdam, en onderzoekt blockchain governance.
2. Cooper, Z., & Lodder, A. R. (Accepted/In press). What's Law Got To Do With IT: an analysis of techno-regulatory incoherence. In O. Kanevskaia, P. Palka, & B. Brozek (Eds.), *Research handbook on Law & Technology* Edward Elgar.
3. Confessore, Nicholas (April 4,2018). "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far". The New York Times. ISSN0362-4331. https://web.archive.org/web/20201011222703/https
4. Smith, Allan.There's an open secret about Cambridge Analytica in the political world: It doesn't have the 'secret sauce' it claims. Business Insider. March 2018. https://web.archive.org/web/20200731112500/https

wijderen.[5] Dit is niet door Kogan gedaan zoals later door Facebook CEO Zuckerberg aan het Congress is gemeld.[6] Overigens is het niet nieuw om via gebruikers content AI te ontwikkelen en te verbeteren: ook Facebook zelf doet hier volop aan mee.[7]

De keerzijde – regulering schaadt innovatie – kent ook voorbeelden. Deze zijn veelvuldig onderzocht door onder andere Thatchenkery en Katila.[8] Hier wordt met name gekeken vanuit het perspectief van het mededingingsrecht. Vroegtijdige regulering kan ongewenste neveneffecten hebben. Dit manifesteert zich bijvoorbeeld door het belemmeren van de grotere technologie bedrijven om overnames te mogen doen. De dan niet overgenomen partij is nog zelfstandig maar dikwijls te klein en armlastig (en mist dus de schaalgrootte) om de technologie wel succesvol te vermarkten. En dus bestaat de kans dat de innovatie daarmee uiteindelijk verloren gaat. Thatchenkery en Katila refereren hier aan de Microsoft v Department of Justice zaak, waarbij Microsoft ervan werd beticht concurrent Netscape uit de markt te drukken.[9] Aghion, Bergeaud en Van Reenen verwijzen onder andere naar Frankrijk waar innovatieve startups vaak onder de 50 werknemers blijven omdat ze anders ineens aan allerlei aanvullende voorwaarden moeten voldoen die tijd en geld wegnemen bij de innovatie zelf.[10] Het tijdstip van regulering is daarmee complex en genuanceerd te noemen.

Dit brengt ons bij het onderwerp van dit artikel, namelijk de Europese regulering van toepassingen van blockchain technologieën waaronder dus ook cryptoactiva en cryptocurrencies. Aanvankelijk heeft de EU jarenlang een afwachtende houding aangenomen. De lidstaten afzonderlijk ontwikkelden hun eigen en vaak verschillende regimes, soms met grote verschillen tussen lidstaten tot gevolg. Aangezien dit in strijd is met het harmonisatie principe, waarbij de EU streeft naar één interne markt, is de stap naar EU regelgeving logisch. Hierbij worden de standaarden binnen de Europese markt als geheel gelijkgetrokken om daarmee een vrijer verkeer te bewerkstelligen en bescherming aan inwoners te bieden zoals beschreven in de doelstellingen van Europese Unie.[11] Een onderzoek van Eest Firma noemt Estland, Tsjechië, Litouwen en Polen als meest crypto vriendelijk in Europa.[12] Slovenië steekt daar nog net weer wat verder bovenuit omdat met name daar het gebruik onder de bevolking met 18 procent het hoogste is volgens een WEF studie.[13] Als de meer negatieve en onvriendelijke tegenhanger worden de Scandinavische landen gezien.[14] De invoering van Markets in Crypto Assets Regulation (hierna MiCA) als EU brede regelgeving zal voor sommige lidstaten een verandering in de afwachtende positie betekenen, en ook in die lidstaten duidelijkheid (moeten) scheppen.[15]

Cryptocurrencies zijn na de introductie van Bitcoin in 2009 wel een blijvende factor gebleken. Hoewel de adoptie nog steeds laag is, de totale liquiditeit van alle cryptocurrencies nog marginaal is ten opzichte van de totale liquiditeit in de financiële wereld, en een aanzienlijk deel van de bevolking het nog steeds als een grote luchtbel ziet, heeft zich intussen een grote verandering voltrokken die aangeeft dat cryptocurrencies wel degelijk serieus moeten worden genomen.[16] Na een kleine twee jaar op Europees niveau besproken te zijn geweest heeft MiCA op 20 april 2023 de goedkeuring van het Europees Parlement gekregen.[17] Op 16 mei 2023 is de verordening vervolgens door de Raad aangenomen.[18] MiCA is op

5. Salinas, Sara (March 21, 2018). "Zuckerberg on Cambridge Analytica: 'We have a responsibility to protect your data, and if we can't then we don't deserve to serve you'".
6. Mark Zuckerberg's Written Testimony to the House of Representatives" (PDF). June 2018. .Retrieved April 14, 2018. https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf
7. Krikhaar, december 2023. Meta heft zijn AI-beeldgenerator getraind met miljard Facebook en Instagram posts. https://nl.hardware.info/nieuws/87861/meta-heeft-zijn-ai-beeldgenerator-getraind-met-miljard-facebook--en-instagram-posts
8. Thatchenkery, S., & Katila, R. (2023). Innovation and profitability following antitrust intervention against a dominant platform: The wild, wild west? Strategic Management Journal, 44(4), 943–976. https://doi.org/10.1002/smj.3470. en Melissa De Witte, Stanford University News, September 2023 https://news.stanford.edu/2023/09/27/antitrust-regulation-can-backfire/ .
9. United States of America v. Microsoft Corporation, 253 F.3d 34 (D.C. Cir. 2001) https://law.justia.com/cases/federal/district-courts/FSupp2/97/59/2339529/
10. Aghion P.,Bergeaud, A., Reenen, J. van, The Impact of Regulation on Innovation, , National Bureau of Economic Research, January 2021, http://www.nber.org/papers/w28381
11. https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_nl .
12. Sidorowich, A, May 2023, Merkelon, Regulatory blog, "Best Jurisdiction for Cryptocurrency Exchange: EU Crypto Regulation". https://www.merkeleon.com/blog/best-jurisdiction-for-cryptocurrency-exchange-eu-crypto-regulation/
13. World Economic Forum, March 2023, Gilbert Fontana, "Charted: Crypto popularity across the EU". https://www.weforum.org/agenda/2023/03/charted-crypto-popularity-across-the-eu/.
14. Attlee, October 2022, Cointelegraph, "The state of crypto in Northern Europe: hostile Scandinavia and vibrant Baltics" https://cointelegraph.com/news/the-state-of-crypto-in-northern-europe-hostile-scandinavia-and-vibrant-baltics
15. Verordening (EU) 2023/1114 van het Europees Parlement en de Raad van 31 mei 2023 betreffende cryptoactivamarkten en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937, eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX
16. Visual Capitalist, December 2022, "All the world's money". https://www.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization-2022/. En ML Manoylov, The Block, January 2024. https://www.theblock.co/post/273769/global-crypto-owners-increased-34-to-580-million-by-end-of-2023-crypto-com-says-in-report.
17. ESMA, Advice Initial Coin Offerings and Crypto Assets, 2019. Europese Commissie, FinTech-actieplan, COM(2018) 109 final. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf
18. Europese Raad, mei 2023, persmededeling, "Digitaal geld: Raad neemt nieuwe regels aan over markten in cryptoactiva". https://www.consilium.europa.eu/nl/press/pre

grond van artikel 149 op 30 juni 2023 in werking getreden en wordt gefaseerd van toepassing en zal op 30 december 2024 in haar geheel gelden zoals in de Memorie van Toelichting bij de (concept) Nederlandse uitvoeringswet wordt beschreven.[19]

2. Cryptoactiva

Cryptocurrencies worden vaak omschreven met de populaire verzamelterm digital assets. MiCA hanteert de verzamelterm cryptoactiva, of crypto assets in de oorspronkelijke Engelse tekst. Een belangrijke constatering is dan ook dat wordt gesproken over assets (activa in Nederlands), en niet over currencies. Currencies, oftewel valuta's, zijn het domein van overheden en mogen niet door een derde partij worden vervaardigd, uitgegeven of beheerd, terwijl dat niet geldt voor cryptoactiva. De bevoegdheid voor eurobiljetten ligt bij de Europese Centrale Bank (ECB) en de nationale centrale banken.[20]

Valuta zijn het domein van overheden omdat zij een paar belangrijke functies in het economisch verkeer vervullen. Zonder die functies zou de economie zo goed als tot stilstand komen. De eerste functie is het zogenaamde medium of exchange (ruilmiddel). Hierbij wordt valuta – geld – bijvoorbeeld gebruikt ter betaling van diensten en producten. Daarnaast is een belangrijke functie de "store of value", waarvoor waardevastheid belangrijk is. Verder heeft valuta een functie als "measure of value" waarmee we standaardisering aanbrengen zoals dat ook in natuurkunde is gedaan met bijvoorbeeld de meter en de gram. De drie genoemde functies worden niet, deels of nog niet toegekend aan of vervuld door cryptoactiva. Hoewel fanatieke cryptoaanhangers dat zullen bestrijden, doen de prijsfluctuaties in bitcoin bijvoorbeeld afbreuk aan de store of value functie. Doordat de uitgevende overheid de waarde van de valuta garandeert, heeft die valuatie daarmee per definitie een store of value functie binnen haar eigen landsgrenzen. Buiten de landsgrenzen van die valuta heeft een garantie overigens minder betekenis op de waardering van een valuta.

MiCA richt zich op drie type cryptoactiva, te weten de asset-referenced tokens (ART), de electronic money tokens (EMT) en de utility tokens. Daarmee beperkt MiCA zich tot slechts een deel van de huidige cryptomarkt. Wat buiten beschouwing wordt gelaten, zijn de meeste non-fungible tokens (NFTs), de Central Bank Digital Currencies (CDBC) en Decentralized Finance (DeFi).[21] Dat laatste, het buiten beschouwing laten van DeFi, is opvallend, omdat binnen DeFi financiële instrumenten zoals lenen en sparen worden aangeboden, en het dus per definitie financiële dienstverlening betreft. Dat in MiCA gekozen wordt voor de term cryptoactiva (een digitale en via blockchain overdraagbare vertegenwoordiging van waarde) in plaats van de in de cryptomarkt vaak gebruikte term digital assets (alles wat digitaal is en mogelijkerwijs waarde vertegenwoordigt, waaronder ook foto's en pdf's) is in mijn optiek een goede keuze, omdat dit duidelijkheid en afbakening geeft.

3. Waarom MiCA

De eerste contouren van wat we nu MiCA noemen, begonnen zich in 2017 af te tekenen. Dit hangt waarschijnlijk niet toevalligerwijs samen met de bull-run van bitcoin en de grote populariteit van fondsenwerving voor blockchain projecten via cryptovaluta zoals de Initial Coin Offerings. En uiteraard de plannen van Facebook om een stablecoin uit te geven.[22] Ten gevolge van een toenemende kapitalisatie van cryptocurrencies, de grote fluctuaties in prijs, en een toenemend aantal scams heeft de toenmalige EU-commissaris Valdis Dombrovskis op de gevaren gewezen en de noodzaak tot bescherming van consumenten benadrukt.[23] Hij doelde hier onder andere op het speculatieve karakter, het blootstellen aan risico's voor investeerders, en het gemak waarmee blockchain projecten ongecontroleerd grote investeringen kunnen binnenhalen. Hierop hebben de Europese Bankautoriteit (EBA) en de Europese Autoriteit voor effecten en markten (ESMA) in 2019 een advies opgesteld.[24] In dat advies werd gesteld dat de bestaande EU-wetgeving mogelijkerwijs in theorie wel van toepassing is op cryptoactiva, maar dat wil niet zeggen dat het in de praktijk ook (goed) mogelijk is deze wetgeving op de cryptoactiva toe te passen. Dit wordt verder in paragraaf 4 toegelicht.

Verder wordt er in het advies stil gestaan bij Distributed Ledger Technology (DLT). Een distributed ledger is een database die wordt beheerd door meerdere gebruikers, die verdeeld zijn over meerdere knooppunten (nodes). Het is een verzamelterm voor tech-

ss-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/

19. Uitvoeringswet verordening cryptoactiva, EU 2023/114, Memorie van Toelichting. https://www.internetconsultatie.nl/verordeningmica/document/11562.
20. ECB website, veelgestelde vragen over contant geld, https://www.ecb.europa.eu/euro/cash_strategy/html/cash-faq.nl.html#.
21. European Parliament, Think Tank, briefing September 2023. Markets in crypto-assets (MiCA). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022. Legal Nodes, July 2023. The EU Markets in crypto-assets (MiCA) Regulation explained. https://legalnodes.com/article/mica-regulation-explained
22. Jeff Kauflin, Forbes Magazine, 29 oktober 2018. FinTec & Crypto. "Where did the money go? Inside the big crtpto ICOs of 2017." https://www.forbes.com/sites/jeffkauflin/2018/10/29/where-did-the-money-go-inside-the-big-crypto-icos-of-2017/ en Pontem blog, september 2021, "The full history of Facebook backed Diem". https://pontem.network/posts/the-full-history-of-facebook-backed-diem-when-will-diem-be-launched
23. European Commission website, February 2018. "Remarks by Vice-President Dombrovskis at the Roundtable on Cryptocurrencies. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_1242
24. ESMA, Advice Initial Coin Offerings and Crypto Assets, 2019. Europese Commissie, FinTech-actieplan, COM(2018) 109 final. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

nologieën die het opslaan en distribueren van data tussen meerdere gebruikers faciliteren. Blockchain is een specifieke toepassing van DLT, en daarmee een subset van DLT. In het advies wordt gesteld dat de bestaande EU-wetgeving remmend kan werken op de ontwikkeling van DLT. Dit zit in het feit dat harmonisatie tussen nationale wetgevingen ontbreekt en daardoor het bestaande reguleringskader onvoldoende is. Maar belangrijker is nog dat de EBA en ESMA stellen dat - met uitzondering van de EU-wetgeving op het gebied van bestrijding van witwaspraktijken en terrorismefinanciering – sommige cryptoactiva buiten het toepassingsgebied van de EU-wetgeving inzake financiële diensten vallen.[25] Hierdoor zijn serviceproviders niet of minder gebonden aan bepalingen zoals die erop gericht zijn de consument te beschermen.

In de toelichting bij het MiCA voorstel wordt benadrukt dat de EU "vastbesloten [is] een kader te scheppen om de mogelijkheden van cryptovermogensbestanddelen ten volle te kunnen benutten".[26] Dit sluit ook aan bij de nadrukkelijke wens van de EU een ruimere digitale agenda voor te staan.[27] MiCA legt de focus op cryptoactiva die buiten de bestaande wetgeving vallen. Hierdoor komen er garanties tegen stablecoins die de mogelijke stabiliteit van het financiële stelsel kunnen ondermijnen, en een verdere controle op het monetaire beleid. MiCA heeft de volgende vier algemene doelstellingen:[28]

1. Bieden van rechtszekerheid;
2. Ondersteunen van innovatie en bevorderen eerlijke concurrentie;
3. Bieden van marktintegriteit waardoor bescherming van consument en beleggersbelangen worden gerealiseerd;
4. Garanderen van financiële stabiliteit.

4. Waarom maatregelen op Europees niveau

In de toelichting op het voorstel van MiCA worden twee redenen aangegeven waarom maatregelen op Europees niveau moeten worden geïntroduceerd.[29]

1. Er bestaat onvoldoende zekerheid of en hoe bestaande EU-regels van toepassing zijn. In de toelichting wordt gesteld dat als een cryptoactivum volgens MiFID II als financieel instrument kan worden gezien het niet duidelijk is of de bestaande regels op dat cryptoactivum en bijbehorende dienstverlening van toepassing zijn. Deze ambiguïteit is ontstaan omdat in het regelgevend kader pre-MiCA geen rekening is gehouden met DLT of cryptoactiva. Daardoor werden nationale autoriteiten met uitdagingen geconfronteerd over hoe MiFID II kon worden uitgelegd en toegepast, met als gevolg uiteenlopende interpretaties en toepassingen van MiFID II op een wereldomvattend fenomeen als cryptoactiva en DLT. Mogelijk gevolg hiervan is een compartimentering van de Europese markt.[30] Dat is niet alleen als onwenselijk te bestempelen, maar ook als onhoudbaar. Verder druist het in tegen de Digitale Agenda, en heeft waarschijnlijk ook een rem op DLT innovatie in Europa gezet.[31]

2. Er zijn geen regels over cryptoactiva op EU-niveau en er bestaan uiteenlopende nationale regels. Dit betekent dat als een cryptoactivum niet onder de EU-wetgeving valt er daardoor ook geen regels beschikbaar zijn waar de consument bescherming aan kan ontlenen. Deze omissie heeft er wellicht toe geleid dat lidstaten zelf regelingen introduceerden. De wijze waarop is echter significant verschillend in die lidstaten in die zin dat de scope van wat een cryptoactivum is, de verplichtingen die gesteld worden aan serviceproviders, markt integriteitsmaatregelen en het optionele versus verplichte karakter variëren.

Een belangrijke constatering is ook de verwijzing in MiCA naar MiFID II (Markets in Financial Instruments Directive 2014).[32] Deze richtlijn biedt een geharmoniseerd regelgevend kader om de belegger beter te beschermen, de integriteit van financiële markten te borgen, transparantie te bevorderen en de Europese beurshandel en beleggersmarkt te harmoniseren. Hierdoor wordt een omgeving gecreëerd die meerdere aanbieders aanmoedigt, de investeerder beschermt en het speelveld meer gelijk maakt. In de toelichting van MiCA wordt gesteld dat als een cryptoactivum volgens MiFID II als financieel instrument kan worden gezien het niet duidelijk is of de bestaande regels van MiFID II op die cryptoactiva en bijbehorende dienstverlening van toepassing zijn. Met andere woorden de term financieel instrument in MiFID II schept onduidelijkheid, en zou daardoor ruimte laten voor cryptoactiva zich daar aan te onttrekken. In artikel 4(1)(44) MiFID II wordt in de definitie van overdraagbare aandelen en effecten de term betaalinstrumenten uitgezonderd. Terecht dat Van der Linden en Shirazi constateren dat cryptocurrencies – die worden gezien als instrumenten of betaalinstrumenten – wellicht of waarschijnlijk bui-

25. Europese Raad, "Bestrijding van witwassen van geld en terrorismefinanciering". https://www.consilium.europa.eu/nl/policies/fight-against-terrorism/fight-against-terrorist-financing/
26. Toelichting MiCA.
27. Website Europese Unie, "Shaping Europe's Digital Future." https://digital-strategy.ec.europa.eu/nl
28. Website AFM, Markets in Crypto-Assets Regulation (MiCAR). https://www.afm.nl/nl-nl/sector/themas/digitalisering/micar
29. Toelichting bij MiCA. .
30. Toelichting bij MiCA, ". pagina 2, 1e alinea. https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX,
31. Toelichting bij MiCA.
32. Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU, laatste geconsolideerde versie beschikbaar op Geconsolideerde TEKST: 32014L0065 — NL — 23.03.2023 (europa.eu).

ten het toezicht vallen en dus ongereguleerd zijn.[33] Deze onduidelijkheid neemt MiCA weg met de term cryptoactiva.[34] Dit was ook al eerder door de Autoriteit Financiële Markten (AFM) gesignaleerd.[35]

Ook staat de toelichting stil bij de mogelijke toegevoegde waarde die MiCA kan genereren als zij eenmaal van toepassing is.[36] In de eerste plaats zal een EU-breed optreden meer voordelen opleveren dan wanneer er alleen op een nationaal niveau wordt geacteerd. Verder biedt het vanwege de paraplu EU-regelgeving ook een goede pilot omgeving voor Distributed Ledger Technology (DLT) toepassingen, waaronder uitgifte van, handel in en afwikkeling van financiële instrumenten. Dit bevordert het vinden van een ingang voor cryptoactiva in de financiële markten, terwijl financiële stabiliteit en beleggersbescherming gegarandeerd zijn. Daarnaast is het ook belangrijk voor cryptoactiva die nu nog niet benoemd en erkend worden en lidstaten die nog geen nationale regelgeving hebben ontwikkeld. Dat die lidstaten zonder nationale regelgeving nu MiCA volgen draagt bij een verdere harmonisatie van het speelveld. Hierdoor kan de interne markt zich verder ontwikkelen. Ten slotte is er ook een schaalvoordeel, namelijk middels harmonisering van operationele vereisten voor serviceproviders, wat zich naar verwachting ook zal vertalen in voordelen op het gebied van consumenten- en beleggersbescherming en financiële stabiliteit.

5. MiCA in hoofdlijnen

MiCA maakt deel uit van het Digital Finance-pakket.[37] Dit is een pakket van maatregelen die in het leven is geroepen om enerzijds meer ruimte te geven aan digitale financiële diensten met name op het gebied van innovatie en concurrentie, terwijl anderzijds wordt getracht de risico's te beperken. In de toelichting bij MiCA wordt hierover het volgende gezegd: "Het Digital Finance-pakket omvat een nieuwe Digital Finance-strategie voor de financiële sector in de EU die ervoor moet zorgen dat de EU de digitale revolutie omarmt en het voortouw neemt met innovatieve Europese bedrijven in koppositie, zodat Europese consumenten en bedrijven de voordelen van digitale financiële diensten kunnen plukken."[38]

In grote lijnen beoogt MiCA een breed kader voor de EU te bieden waarin de uitgave van cryptoactiva en de toelating van serviceproviders tot de markt wordt gereguleerd:

- Er wordt een vergunningenstelsel voor cryptoasset serviceproviders geïntroduceerd;
- De verplichtingen voor deze serviceproviders vanuit de toezichthouder worden verduidelijkt;
- Het vertrouwen in de cryptoactiva markten wordt versterkt door de introductie van maatregelen gericht op het voorkomen van marktmanipulatie en;
- Vanwege het sanctiebeleid worden de rol en bevoegdheden van verantwoordelijke autoriteiten automatisch verder verduidelijkt.

Daarnaast worden nog een tweetal fenomenen specifiek genoemd, namelijk Distributed Ledger Technology en stablecoins. Het bevat een voorstel voor een pilot om marktinfrastructuur op basis van DLT mogelijk te maken.[39] Hierdoor wordt een proeftuin geschapen die als veilige omgeving kan dienen om inzichten te verkrijgen hoe met DLT omgegaan moet worden. Een stablecoin is een cryptoactivum waarbij de waarde van dit cryptoactivum verondersteld wordt gekoppeld te zijn aan bijvoorbeeld de US-dollar of euro. Hiermee vervult het activum een van de functies van geld, namelijk refereren aan een bestaande en bekende waarde. Vanwege die koppeling is het dan ook logisch dat juist toezichthouders zich op deze specifieke cryptoactiva richten. Ten aanzien van stablecoins stelt de toelichting dat het gebruik van stablecoins beperkt is en vooralsnog geen bedreiging vormt voor de financiële stabiliteit.[40] Dit kan veranderen als er een "global stablecoin" komt en als deze een bedreiging voor de financiële stabiliteit dreigt te worden.[41]

MiCA gaat zich specifiek richten op het viertal hierboven genoemde doelstellingen. Het beginsel van technologische neutraliteit moet er niet alleen voor zorgen dat regelgeving niet als hinderpaal gezien kan worden, maar dat er tegelijkertijd ook geen voordeel wordt gegeven aan een technologie. Vervolgens moeten de zogenaamde Initial Coin Offerings (ICO's) en Securities Token Offerings (STO's) als financieringsbronnen beschikbaar worden gemaakt voor ondernemingen. Verder moeten de risico's op fraude en illegale praktijken beperkt worden op de cryptoactivamarkten. Tenslotte moet de Europese consument toegang krijgen tot nieuwe beleggingsmogelijkheden en nieuwe vormen van betaalinstrumenten die met name grensoverschrijdend opereren.[42]

De crypto asset service providers (CASPs), in het Nederlands aanbieders van cryptoactivadiensten, zijn

33. Van der Linden, T., Shirazi, T. Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?. Financ Innov 9, 22 (2023). https://rdcu.be/dtLfL .
34. Peráček T (2021) A few remarks on the (im)perfection of the term securities: a theoretical study. Jurid Trib Trib Jurid11(2):135–149. https://doi.org/10.24818/TBJ/2021/11/2.01
35. Website AFM, Consumenten, Crypto's, "Crypto's grotendeels buiten toezicht AFM". https://www.afm.nl/nl-nl/consumenten/themas/crypto/buiten-toezicht-afm
36. Zie punt 1.5.2 van het Financieel Memorandum MiCA.
37. finance.ec.europa.eu/publications/digital-finance-package_en
38. Toelichting bij MiCA.
39. Zie het Financieel Memorandum MiCA, Kader, 1.4.3. en Kader 1.5.2.
40. FSB Chair's letter to G20 Finance Ministers and Central Bank Governors, March 2018. https://www.fsb.org/2018/03/fsb-chairs-letter-to-g20-finance-ministers-and-central-bank-governors/
41. G7 Working Group on Stablecoins, Report on 'Investigating the impact of global stablecoins', 2019.
42. Zie het Financieel Memorandum MiCA, Kader 1.4.2.

de belangrijkste normadressaten van MiCA.[43] Met CASPs worden de handelsplatformen voor crypto bedoeld, waaronder portfolio management, advies en de daadwerkelijke cryptohandel. Het Nederlandse Bitvavo bijvoorbeeld is dus een CASP in MiCA terminologie. In Annex 4 van MiCA worden de financiële voorwaarden voor CASPs toegelicht.[44] Hieronder vallen kapitaalvereisten, governance structuur, interne controles en service specifieke voorwaarden.

6. Beoogd resultaat MiCA zoals omschreven in Financieel memorandum

Om het beoogde resultaat te kunnen beoordelen, is het ook goed om nog even stil te staan bij de uitdagingen die MiCA poogt te adresseren (zie ook paragraaf 3).

1. Consumentenbescherming en opruimen van hinderpalen voor innovatie: Cryptoactiva worden gezien als een van de belangrijkste toepassingen van blockchaintechnologie in de financiële sector. Daarom moeten de kansen en uitdagingen die van cryptoactiva uitgaan goed onderzocht worden. Zowel de EBA als de ESMA hebben betoogd dat er ambiguïteit bestaat ten aanzien van het enerzijds wel erkennen dat enkele cryptoactiva mogelijk binnen de EU-wetgeving vallen, maar dat die wetgeving anderzijds voor de meeste cryptoactiva niet van toepassing is. Bovendien is de daadwerkelijke toepassing van regelgeving dikwijls problematisch. Dit kan remmend werken op innovatie. De hierdoor ontstane situatie, een soort vacuüm, is ongewenst en moet geadresseerd worden.
2. Compartimentering: Sommige lidstaten hebben reeds specifieke maatregelen ingevoerd, andere zijn bezig deze aan te passen, nog weer anderen overwegen dit. Dat kan leiden tot een divers en verdeeld scala aan regelgeving die soms onderling tegenstrijdig kan zijn. Daardoor is er een verdeeld en ongelijk speelveld.
3. Financiële stabiliteit: De (potentiële) populariteit van en het soms buiten het huidige regelgevingskader opereren van stablecoins is een ongewenste situatie die de financiële stabiliteit kan ondermijnen.

Ten aanzien van het resultaat van MiCA is er een aantal verwachtingen. Met de komst van MiCA wordt verwacht dat er een volledig geharmoniseerd raamwerk voor cryptoactiva wordt gerealiseerd, waarmee ook de cryptoactiva die nu buiten de bestaande EU wetgeving vallen worden afgedekt. Daardoor wordt er ook ruimte geboden aan tests met DLT en het gebruik van cryptoactiva als financieel instrument. De opgenomen bepaling voor een pilot op basis van DLT infrastructuur zal bijdragen aan een verbeterd experimenteel klimaat, en wellicht leiden tot een secundaire markt voor financiële instrumenten.[45] Hierbij is het verkrijgen van schaalgrootte erg belangrijk om zo concurrerend te kunnen worden. Een belangrijk bijkomend voordeel is dat er in een testomgeving kan worden beoordeeld of MiCA voldoende houvast en bescherming biedt, of dat deze aangepast moet worden, zeg maar een sandbox EU style.[46]

Aan de belangrijkste aanbieders van cryptoactiva diensten worden voorwaarden opgelegd op het gebied van governance en operationele vereisten. Hierbij valt te denken aan uitgifte van cryptoactiva, bewaarportemonnees (custodial wallets), en omwisselfaciliteiten (exchanges).[47] Dit zal niet alleen bijdragen aan een hoger niveau van consumenten- en beleggersbescherming en marktintegriteit, maar ook aan bestrijding van fraude en diefstal. Door bijzondere voorwaarden op te leggen aan e-money tokens wordt getracht de financiële stabiliteit en het monetaire beleid te blijven garanderen.[48] Concluderend kan gesteld worden dat door deze harmonisering nationale regelgeving als het ware wordt geneutraliseerd waardoor het gevaar op compartimentering gemitigeerd wordt.

Alle argumentatie in ogenschouw genomen, en het uitgangspunt van de Digital Agenda respecterend, heeft de voorzitter van de Europese Commissie Ursula von der Leyen benadrukt dat het essentieel is een gedeelde en gezamenlijke benadering van cryptoactiva te hebben teneinde een balans te vinden tussen kansen benutten enerzijds en risico's erkennen en voorkomen anderzijds.[49] Hiermee wordt het in de inleiding genoemde dilemma van te vroeg of te laat ingrijpen absoluut onderkend.

7. Verwachte consequenties MiCA

Wat betreft de invoering van MiCA verwacht ik dat het landschap, hoewel MiCA een breed pakket aan maatregelen bevat, niet al te dramatisch zal veranderen. De effecten van MiCA zijn grofweg in de volgende vier componenten merkbaar: het scheppen van duidelijkheid, DLT test omgeving, e-money en passporting.

In de eerste plaats wordt er een enorme bijdrage geleverd aan duidelijkheid: waar sta je als aanbieder, en hoe wordt er tegen de onderliggende technologie aangekeken. Die duidelijkheid is een goede ontwikkeling en een enorme winst voor een ieder die zich in

43. Art. 52 en verder MiCA.
44. Annex IV https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL
45. Financieel Memorandum MiCA Kader, 1.4.3. en Kader 1.5.2..
46. Toelichting bij MiCA. ,
47. Art. 59-66 MiCA.
48. Art. 43-52 MiCA.
49. Verslag met aanbevelingen aan de Commissie over opkomende risico's in verband met crypto valuta — uitdagingen in zake regelgevingen toezicht op het gebied van financiële diensten, instellingen en markten, 2020/2034(INL), September 2020. https://www.europarl.europa.eu/doceo/document/A-9-2020-0161_NL.html

dit speelveld begeeft. Dit leidt dan ook tot opheffing van de eerder genoemde compartimentering waarbij alle EU lidstaten onder een zelfde regime van wet- en regelgeving passen. Er wordt ook voor cryptoactiva één interne markt gecreëerd.

Een tweede aspect is de DLT test omgeving die er moet komen.[50] Dit doet sterk denken aan de regulatory laboratories of sandboxes van de Verenigde Arabische Emiraten VAE).[51] Daarbij worden bedrijven uitgenodigd om te experimenteren en te innoveren onder supervisie en met ondersteuning van bijvoorbeeld de toezichthouder of de centrale bank. Deze sandbox is zeer succesvol gebleken en heeft VAE zeker prominent neergezet als ondersteunend ten aanzien van financieel innovatieve ontwikkelingen. Op dit moment heeft de VAE een grote aantrekkingskracht op de crypto-industrie vanwege het vestigingsklimaat, en daar heeft de sandbox omgeving zeker aan bijgedragen. De hier voorgestelde "speeltuin/sandbox EU style" is (te) laat, maar toch ook zeker een enorm positieve ontwikkeling. Deze sandbox heeft hier overigens niet alleen ten doel om de blockchain technologie en DLT te testen, maar ook om de financiële en regulerings- infrastructuur binnen de EU te testen. Zeker ook op het gebied van governance moeten toepassingen van blockchain technologie nog een ontwikkeling doormaken, en dat zou zich uitstekend in zo'n sandbox omgeving laten testen en toetsen.

De opmerking over de VAE en de sandbox, is goed op de EU toe te passen. Welke lidstaten zullen deze sandboxes – en dus ook de vestiging van bedrijven in blockchain technologie – graag binnen hun grenzen hebben? Dan lijkt het zeer voor de hand te liggen dat de op dit moment al crypto-vriendelijke landen hierbij de hoogste ogen gaan gooien. Ik verwacht dat Estland niet alleen haar positie behoudt maar zelfs uitbreidt. Uit een in 2023 gepubliceerd onderzoek van Vsquare-kwam naar voren dat Estland in 2021 maar liefst 55% van alle virtuele currency service providers geregistreerd had.[52] Daarmee is Estland een crypto powerhouse te noemen. Kan MiCA hiermee onbedoeld een concurrentiemiddel worden onder de EU lidstaten? Met andere woorden: gaan afzonderlijke EU lidstaten proberen het meest aantrekkelijkste vestigingsklimaat te bieden? Zeker voor een land als Estland zal de economie voor een groot deel afhankelijk zijn van deze bedrijven en zou een gunstig vestigingsklimaat en een vriendelijker bevoegde autoriteit (Competent Authority) onderdeel van haar businessmodel kunnen zijn. Dit is overigens niet nieuw. Malta bijvoorbeeld heeft een gunstig investeringsklimaat voor buitenlanders waarbij investeringen vanaf 600.000 euro vaak vergezeld gaan van een Maltees – dus EU – paspoort.[53] Een ander aspect is ook de in MiCA gestelde tijdlijn van 60 dagen (artikel 18, lid 2 MiCA) tussen indienen aanvraag en voorlopige beslissing. Zeker een lidstaat die al veel crypto bedrijven binnen haar grenzen heeft, heeft daar waarschijnlijk een goed geolied proces voor, en kan dan waarschijnlijk (met gemak) aan dit criterium voldoen.

Bijzondere aandacht moet gegeven worden aan de zogenaamde e-money tokens. MiCA heeft de mogelijkheid bijzondere voorwaarden te stellen aan e-money tokens.[54] Deze mogelijkheid bestaat om de financiële stabiliteit en het monetaire beleid te kunnen blijven garanderen. Hoewel ik zie dat dit een belangrijk aspect is, kun je je hierbij twee dingen afvragen. In de eerste plaats lijkt het hier een beetje op twee benen te hinken. Eerst wordt gesteld dat cryptoactiva geen valuta zijn.[55] Als dat dan zo is, waarom zou je je er dan druk om maken en wel nadrukkelijk de mogelijkheid open willen houden daar voorwaarden aan op te kunnen leggen? Misschien is de EU toch niet helemaal gerust op de rol die cryptoactiva mogelijkerwijs kunnen gaan spelen en zich dus buiten de invloedsfeer van de EU kan voltrekken. Daarnaast kan men zich afvragen wie er daadwerkelijk bevoegd is om voorwaarden aan e-money tokens te stellen. Het lijkt voor de hand te liggen dat binnen Europa de ECB daar een nadrukkelijke rol in gaat spelen. Maar in mijn ogen misschien nog belangrijker is dat dit ook tot protectionisme kan leiden en de EU zich daardoor een monopolie positie bemachtigt op e-money. En een monopolie op e-money is natuurlijk belangrijk als er een digitale euro gaat of moet komen. Op haar website omschrijft de Europese Commissie in de FAQ van de financiële sectie de noodzaak van de digitale euro als "Stablecoins and other crypto-assets that are not denominated in euro, if widely used for payments, could also undermine the stability of our monetary system."[56] Daar staat de deur wijd open voor het nemen van maatregelen die het speelveld enorm kunnen beïnvloeden, en is wellicht ingegeven door de dreiging die van Facebook's mogelijke introductie van de Diem coin uitging.[57] Binnen het gedecentraliseerde ecosysteem zijn uitgangspunten als transparantie, gelijkwaardigheid en open toegang en deelname niet alleen heilig, maar ook noodzakelijk voor vertrouwen. Daar kan een digitale euro zich niet aan onttrekken. Dat afbakenen en beschermen van een mo-

50. zoals vermeld in het financieel memorandum onder punt 1.4.3. "Verwacht resultaat".
51. Website Central Bank of the UAE, Sandbox Initiatives. https://www.centralbank.ae/en/our-operations/fintech-digital-transformation/sandbox-initiatives/
52. Laine, Kund, Aljas and others. VSquare, October 2023. Investigative Report. "Tales from the Crypto". https://vsquare.org/tales-from-the-crypto-money-laundering-fraud-sanctions-estonia-lithuania-russia/#
53. Website Malta Immigration. www.maltaimmigration.com/
54. Art. 43-52 MiCA. 5
55. Website DNB, november 2022. "We zien crypto's niet als geld". https://www.dnb.nl/algemeen-nieuws/nieuwsbericht-2022/we-zien-crypto-s-niet-als-geld/
56. Website European Commission, Business, Economy, Euro. "FAQ on the digital euro". https://finance.ec.europa.eu/digital-finance/digital-euro/frequently-asked-questions-digital-euro-and-legal-tender-cash_en
57. Pontem blog, september 2021, "The full history of Facebook backed Diem". https://pontem.network/posts/the-full-history-of-facebook-backed-diem-when-will-diem-be-launched

gelijk monopolie is wellicht vergezocht en mogelijk achterdochtig, maar ik zou hierbij graag het bekende trustless trust principe van blockchain van toepassing willen zien. Dit kan het gemakkelijkst omschreven worden als "don't trust but verify", wellicht het beste vertaald als eerst zien dan geloven.

Eén bijzonder in het oog springend aspect van MiCA wil ik nog afzonderlijk benoemen, namelijk passporting. Hiermee wordt bedoeld dat als een aanbieder van cryptoactiva in de EU wil opereren, deze aanbieder in één van de lidstaten gevestigd en geregistreerd moet zijn en aldaar de toestemming moet aanvragen om zo een vergunning te verkrijgen. Wanneer deze toestemming is verleend, kan automatisch toestemming verleend worden - en daarmee toegang verkregen wordt - tot alle andere EU lidstaten. Artikel 62 MiCA regelt de aanvraag, en artikel 65 MiCA regelt de EU brede toestemming, de zogenaamde cross border provision. Met deze regeling is er voor gekozen om de goedkeuring en uitgifte van vergunningen niet centraal op EU niveau te beleggen, maar dit aan de lidstaten zelf over te laten. Om uiteindelijk toestemming te krijgen om binnen de gehele EU te kunnen opereren moet de aanbieder aan een aantal voorwaarden voldoen. Ten eerste moet er een legale entiteit gevestigd zijn in een van de EU lidstaten, en vervolgens moet die entiteit toestemming hebben gekregen van de zogenaamde Competent Authority van de lidstaat waar ze gevestigd is. In Nederland is er voor gekozen het toezicht op MiCA te beleggen bij DNB en bij de AFM.[58] Hierbij ziet DNB toe op stablecoins en dergelijke, en de AFM op CASPs.

Een door mij in 2018 geschreven artikel in CryptoSlate signaleerde ik dit fenomeen al in de wereldwijde cryptomarkt.[59] Hierbij werden met name wat de door mij "Island Jurisdictions" zijn genoemd (zoals Singapore, Britse Maagdeneilanden en Gibraltar) als crypto-vriendelijk omschreven In mijn artikel heb ik drie zogenaamde regulatory clusters beschreven, namelijk vriendelijk, neutraal en negatief. Deze zelfde indeling zal zich waarschijnlijk binnen de EU gaan aftekenen, waarbij de eerder genoemde crypto-vriendelijke landen eerder gekozen worden als land van vestiging. Nederland, hoewel een land met enorm veel positieve voorwaarden om als vestigingsklimaat gekozen te worden heeft door de opstelling van DNB veel minder kans om blockchain technologie tot een succesvolle sector in Nederland te maken.[60] Recente uitspraken staven dat.[61] Dat vind ik een gemiste kans, maar wellicht leidt uiteindelijk pragmatisme tot een andere aanpak.

8. De reacties vanuit de cryptomarkt

De reacties in de cryptomarkt op het MiCA-voorstel lijken over het algemeen positief te zijn, met name ten aanzien van het bereiken van één interne markt, transparantie en bescherming voor de consument.[62] De kritische noot gaat met name over de veelheid aan regels en voorwaarden die worden opgelegd, en aan de papiermolen die moet worden opgetuigd. Bij sommigen bestaat de vrees dan ook dat ondanks de goede bedoelingen van MiCA om innovatie te stimuleren, dit een tegengesteld effect kan hebben, zoals Thatchenkery en Katila al vaststelden.[63] Ook de noodzakelijke financiële slagkracht om aan MiCA te voldoen, of beter gezegd het gebrek daaraan bij startups, kan een belemmering zijn om zich op de cryptomarkt te begeven. Hoewel ik dit betwijfel, is er een incidentele en niet met bron of argumentatie vergezeld gaande vrees dat er een mogelijke ongelijkheid zou ontstaan. Dit zou dan komen omdat als cryptoactiva buiten de EU wordt aangeboden MiCA niet daarop van toepassing is, waardoor de aanbieders die het aangaat zich niet aan die regels hoeven te houden zodat er daarmee ongelijkheid ontstaat ten opzichte van de spelers binnen de Europese markt.

Een tweede punt van zorg wat ik zie, is de impact op decentralisatie. Decentralisatie is een diep gekoesterd goed binnen de blockchain gemeenschap, dus alles wat belemmerend of dreigend zou kunnen zijn voor dit kernprincipe ligt onder het vergrootglas. Ik heb wat dat betreft enige zorg over de positie van de decentralized autonomous organizations (DAO's). Decentralisatie manifesteert zich vaak middels een DAO en daarmee zijn DAO's redelijk ongrijpbaar gebleken. De positie van de DAO is door de Dutch Blockchain Coalition eerder beschreven in een whitepaper.[64] Met de introductie van de term "certain

58. Website AFM, Digitalisering, Markets in crypto-assets regulation (MiCAR) https://www.afm.nl/nl-nl/sector/themas/digitalisering/micar
59. Koning, H.A. January 2018, Cryptoslate. "Are regulators dividing in order to conquer". https://cryptoslate.com/regulators-dividing-conquer/ (VPN op VS zetten).
60. Website DNB, november 2022. "We zien crypto's niet als geld ". https://www.dnb.nl/algemeen-nieuws/nieuwsbericht-2022/we-zien-crypto-s-niet-als-geld/
61. De Rechtspraak, oktober 2023. "Uitspraken over het in rekening brengen van toezichtkosten bij cryptodienstverleners. https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Rotterdam/Nieuws/Paginas/Uitspraken-over-het-in-rekening-brengen-van-toezichtkosten-bij-cryptodienstverleners.aspx en Crypto update BNR, oktober 2023. https://www.bnr.nl/podcast/cryptocast/10527237/crypto-update-toezichthouder-dnb-opnieuw-teruggefloten-door-rechter.
62. Timmermans, M, mei 2023, Alles over Crypto, "MiCA uitgelegd". https://allesovercrypto.nl/blog/mica-uitgelegd-eerste-europese-cryptowetgeving#Conclusie
63. Thatchenkery, S., & Katila, R. (2023). Innovation and profitability following antitrust intervention against a dominant platform: The wild, wild west? *Strategic Management Journal*, 44(4), 943–976. https://doi.org/10.1002/smj.3470. en De Witte, Stanford University News, September 2023 https://news.stanford.edu/2023/09/27/antitrust-regulation-can-backfire/ .en The Impact of Regulation on Innovation, Aghion, Bergeaud, Van Reenen, National Bureau of Economic Research, January 2021, http://www.nber.org/papers/w28381
64. Pomp, M., Wermers, C., Sanders, S., Tervoort, A. ,Gideons, B. mei 2023, Dutch Blockchain Coalition. "Dutch corporate law aspects of Decentralised Autonomous Organisations". https://dutchblockchaincoalition.org/assets/images/default/Whitepaper-DBC-Corporate-law-aspects-DAO.pdf

other undertakings"[65] worden DAOs en DeFi-aanbieders nu toch ineens benoemd als potentieel binnen de scope van MiCA vallend.[66] Als - en dat is voor nu speculatief maar zeker niet ondenkbaar – er aanvullende eisen aan deze "certain other undertakings" worden gesteld, zou dat grote gevolgen kunnen hebben. Te denken valt aan eisen dat een DAO een rechtspersoon is of heeft, of dat er KYC-procedures doorlopen moeten worden voor DAO's. Ter verduidelijking, decentrale blockchains zijn permisionless. Dat betekent dat de blockchain open source code gebruikt, er geen centrale autoriteit is en iedereen vrij toegang heeft. Dit houdt ook in dat elke CASP handelen in bijvoorbeeld bitcoin zonder meer op haar platform kan aanbieden. Sterker nog, het is onmogelijk om toestemming aan bitcoin te vragen omdat niemand eigenaar of beslisser is. Door redenerend zou dit een doodsteek voor DeFi-projecten kunnen zijn. Die vervullen een belangrijke rol in de cryptomarkt door het verlenen van liquiditeit. Nogmaals, dit is speculatief, en wellicht ook getriggerd door zo'n vage term als certain other undertakings (niet zijnde natuurlijke personen of rechtspersonen).

9. Conclusie

De belangrijkste toegevoegde waarde van MiCA moet wel het geven van duidelijkheid aan de cryptomarkt zijn, en het creëren van één interne Europe markt. Dat is absoluut iets waar behoefte aan was. Ik omschrijf de wereldwijde cryptomarkt vaak als vol met regulatoire onzekerheid en onduidelijkheid. Die verdwijnt nu grotendeels in Europa en dat is een groot winstpunt. Ironisch genoeg wordt er gelijk wel weer nieuwe onduidelijkheid geïntroduceerd ten aanzien van e-money, en met name ook met de term "certain other undertakings" waardoor DAOs en DeFi zo maar ineens in de vuurlinie terecht kunnen komen. De ambitie voor de DLT sandbox is ook een positieve ontwikkeling, en zal zeker ook worden aangegrepen door de financiële en logistieke sector, R&D om maar een paar te noemen. De cross border provisioning of zogenaamde passporting is een belangrijke facilitator om tot één interne markt te komen. Maar dat zou ook wel eens een tweesnijdend zwaard kunnen blijken te zijn waarbij de crypto-vriendelijke landen de toetredingscriteria voor bijvoorbeeld CASPs soepeler interpreteren. Hierdoor zou het zo kunnen zijn dat de ene lidstaat gemakkelijker een vergunning afgeeft dan de andere lidstaat. Binance, een van 's werelds grootste CASPs heeft na in 2022 tegen een bestuurlijke boete te zijn aangelopen op 17 juli 2023 op gezag van de DNB moeten stoppen met het aanbieden van diensten in Nederland.[67] Op dit moment heeft Binance al een registratie onder andere in Frankrijk, Italië, Spanje en de crypto-vriendelijke Baltische staten Estland en Litouwen.[68] Ik voorspel dat Binance via een van die registraties wellicht volgend jaar alweer actief wordt in Nederland, en gok daarbij op Vilnius of Tallinn als vestigingsplaats? Wetende dat MiCA ingevoerd wordt kun je je afvragen of DNB zichzelf niet in verlegenheid heeft gebracht en beter hangende die invoering als alternatief voor een tijdelijke schorsing had kunnen kiezen. Het "nu kan het nog signaal" wat DNB heeft willen afgeven is echter duidelijk: we zien crypto's niet als geld.[69]

Tenslotte nog een opmerking over decentralisatie. Door de goedkeuring en verlening van toestemming bij een individuele lidstaat te beleggen heeft de EU voor een vorm van decentralisatie gekozen. Zou het zo kunnen zijn dat nu juist decentralisatie - een aan blockchain ten grondslag liggende gedachtengoed - ertoe kan leiden dat er meer ruimte kan worden gegeven aan blockchainprojecten op de EU-markt? Of, is er met de introductie van de term "certain other undertakings" nu een wapen gevonden om juist dat bijna heilige gedachtengoed van de blockchain – decentralisatie - een halt toe te kunnen roepen?

Wat MiCA ook gaat brengen, dat wellicht decentralisatie een rem en/of een versneller kan zijn is absoluut ironisch te noemen. Hoe een en ander ook uitpakt, de voorlopige conclusie van deze "jury" is: And the 12 points go to..... Estonia!

65. Art. 2 MiCA over het toepassingsgebied: naast natuurlijke en rechtspersonen is de verordening ook van toepassing op "bepaalde andere ondernemingen".
66. Rolo, A.G., The European Law Blog, May 2023. "Out of scope, out of mind, and don't say decentralization". https://europeanlawblog.eu/2023/05/23/out-of-scope-out-of-mind-and-dont-say-decentralisation-brief-remarks-on-the-new-mica-regulation/
67. Website DNB, 18 juli 2022. "Boete voor Binance Holdings Ltd. vanwege het zonder de wettelijk vereiste registratie aanbieden van cryptodiensten." https://www.dnb.nl/nieuws-voor-de-sector/handhavingsmaatregel-2022/boete-voor-binance-holdings-ltd-vanwege-het-zonder-de-wettelijk-vereiste-registratie-aanbieden-van-cryptodiensten/ en website Banken.nl (platform NL bankensector), 21 juni 2023, "Binance vertrekt uit Nederland". https://www.banken.nl/nieuws/24601/binance-vertrekt-uit-nederland
68. Website Binance, "Licenses, Registrations and other Legal Matters." https://www.binance.com/en/legal/licenses
69. Website DNB, november 2022. "We zien crypto's niet als geld". https://www.dnb.nl/algemeen-nieuws/nieuwsbericht-2022/we-zien-crypto-s-niet-als-geld/

Bits en sloten vanuit een cybersecurityperspe

Begrijpen en voorkomen van ransomware-aanvallen met LockBit als voorbeeld van gijzelsoftware van de hoogste orde

mr. dr. E. Moyakine[1]

LockBit is één van de meest geavanceerde vormen van ransomware die tot nu toe wereldwijd een groot aantal slachtoffers heeft gemaakt. Het is noodzakelijk dat organisaties zich daarvan bewust zijn en zich tijdig wapenen tegen deze en andere soortgelijke malware die door cybercriminelen op een geraffineerde en agressieve wijze worden ingezet. In dit stuk wordt LockBit als voorbeeld genomen en wordt stilgestaan niet alleen bij de werking daarvan maar ook bij mogelijke gevolgen van de infectie daarmee. Daarnaast wordt in het kort uitgelegd welke maatregelen genomen kunnen worden door zowel organisaties als natuurlijke personen om zich tegen de aanvallen met gijzelsoftware zoals LockBit te beschermen.

1. Inleiding

U hebt het ongetwijfeld ook al vernomen dat een aantal grote organisaties in zowel het binnen- als het buitenland recentelijk door LockBit werd getroffen. Te denken valt aan de Amerikaanse vliegtuigbouwer "Boeing"[2], het Britse postbedrijf "Royal Mail"[3], de Duitse bank "Deutsche Bank"[4], de Koninklijke Nederlandse Voetbalbond (KNVB)[5] en de Brabantse zorginstelling "Joris Zorg"[6]. Onder slachtoffers van LockBit vindt men natuurlijk niet alleen grote bedrijven. Regelmatig worden ook kleine en middelgrote ondernemingen het mikpunt van cybercriminelen. Het is opmerkelijk dat het vaak organisaties van de NAVO-landen en hun bondgenoten zijn die met LockBit worden besmet en ongeveer 50% van alle hacks ermee wereldwijd vindt volgens sommige inschattingen plaats tegen Amerikaanse bedrijven.[7] Eind februari 2024 is bekend geworden dat de LockBit-servers in een gezamenlijke operatie van de opsporingsdiensten van verschillende landen, waaronder de VS, het VK, Frankrijk, Duitsland en Nederland, in beslag waren genomen.[8] Met de "Operation Cronos" was de verspreiding van deze ransomware aanzienlijk verstoord maar deze interventie heeft slechts geleid tot een tijdelijke onderbreking van de criminele activiteiten van de LockBit-groep die haar verwoestende digitale aanvallen weer heeft voortgezet.[9]

Menig IT-recht jurist heeft over LockBit gehoord. Uit de interacties tussen de auteur van dit artikel en zijn directe en indirecte collega's en studenten is gebleken dat er nog weinig bewustzijn is onder juristen over de manier waarop aanvallen met deze ransomware worden uitgevoerd en welke (juridische) consequenties daaraan zijn verbonden. Onwetendheid over cyberdreigingen vormt op zichzelf een kwetsbaarheid die vroeg of laat uitgebuit zal worden. Bent u al bekend met de dreiging van het uiterst gevaarlijke gijzelvirus LockBit? Er heersen nog enkele vragen daarover en het verdient aanbeveling om ze nader te verduidelijken. Wat is LockBit? Hoe werkt het? Door wie wordt het gebruikt? Wat zijn de gevolgen van de infectie met LockBit en andere soorten ransomware? Hoe kan men weer toegang tot zijn bestanden krijgen als computers worden geïnfecteerd? Wat kan men zelf doen om geen slachtoffer van gijzelsoftware zoals LockBit te worden? Het stuk dat voor u ligt, heeft als doel het verhelderen van deze vragen en het vergroten van het bewustzijn van het publiek van dit tijdschrift over ransomware, LockBit en (juridische) gevolgen van aanvallen ermee.

1. Evgeni Moyakine, universitair docent IT-recht aan de Rijksuniversiteit Groningen, geassocieerd lid van de STeP-onderzoeksgroep van dezelfde universiteit en research fellow bij het Information Society Law Center van de Universiteit van Milaan.
2. 'Boeing assessing Lockbit hacking gang threat of sensitive data leak', reuters.com, 28 oktober 2023.
3. 'Royal Mail hit by Russia-linked ransomware attack', bbc.com, 12 januari 2023.
4. '60GB Deutsche Bank data allegedly for sale on dark web', cybernews.com, 15 maart 2023.
5. 'Cybercriminelen eisen meer dan miljoen euro van KNVB na ransomware-aanval', rtlnieuws.nl, 19 april 2023.
6. 'Cyberaanval bij zorginstelling: gegevens van cliënten gedeeld', nos.nl, 20 april 2023.
7. 'Dark Web Profile: LockBit 3.0 Ransomware', socradar.io, 27 april 2023.
8. 'Law enforcement disrupt world's biggest ransomware operation', europol.europa.eu, 20 februari 2024; 'Servers neergehaald van 's werelds grootste ransomware groepering', politie.nl, 20 februari 2024.
9. 'Feds hack LockBit, LockBit springs back. Now what? The busted ransomware gang leader returns with a promise of vengeance', techcrunch.com, 26 februari 2024.

2. LockBit als RaaS

Volgens experts is LockBit in feite de meest effectieve *RaaS* van het moment die de marktleidende positie heeft weten te bereiken.[10] De afkorting "RaaS" staat voor "Ransomware-as-a-Service". Ransomware (ook wel *cryptoware* of *cryptolocker* genoemd) is een vorm van *malware* (*malicious software*) oftewel kwaadaardige software. Deze computervirussen worden ontwikkeld en ingezet om computersystemen te infecteren en te gijzelen. Ze versleutelen bestanden en vervolgens wordt een betaling (vaak in cryptovaluta) gevraagd voor het ontgrendelen van die bestanden. RaaS houdt in principe in dat software-ontwikkelaars afkomstig uit de duistere hoeken van cyberspace zich als legitieme bedrijven gedragen en hun gijzelsoftware als dienst aanbieden en aan klanten leveren. Het infecteren van computers met ransomware is nu een businessmodel geworden. Deze praktijken zijn niet alleen verwarrend maar ook ethisch verwerpelijk en strafbaar. In Nederland kunnen ze worden gekwalificeerd als gegevensmanipulatie (art. 350a Wetboek van Strafrecht) en afpersing (art. 317 Wetboek van Strafrecht).

3. Ontwikkelaars en klanten

Wie ten slachtoffer aan LockBit kan vallen, is helder. Dat kan in principe iedereen overkomen maar wie houdt zich bezig met het ontwikkelen en verspreiden van deze ransomware-variant? LockBit wordt sinds 2019 vermoedelijk door een groep Russische hackers aangeboden op het dark web. Dat verborgen segment van het internet is niet via traditionele browsers toegankelijk maar is benaderbaar met behulp van de speciale Tor-browser. Het LockBit-team claimt vanuit Nederland actief te zijn en benadrukt in zijn blogpost: "We are located in the Netherlands, completely apolitical and only interested in money".[11] De gijzelsoftware wordt constant verbeterd en er zijn inmiddels de versie 3.0 en de meest recente iteratie "LockBit Green" die zich op de aanbieders van clouddiensten richt, in omloop.[12] De LockBit-ontwikkelaars noemen het zelf een "affiliate-programma" waarbij hun "klanten" (de *affiliates*) een licentie op de inzet van deze ransomware kunnen afnemen. De *affiliates* zijn doorgaans kwaadwillende personen of groeperingen die met behulp van LockBit relatief gemakkelijk maar illegaal extra inkomsten willen vergaren en die dus – hoe paradoxaal het ook klinkt – nauwkeurig de "algemene voorwaarden" moeten lezen die op het dark web-portaal van de LockBit-bende staan. Of de schimmige klanten op deze voorwaarden terug kunnen vallen in geval van een meningsverschil met de ontwikkelaars en wat ze daaraan hebben, valt natuurlijk te bezien.

4. De werking van LockBit

Om de gijzelsoftware van LockBit te kunnen uitrollen moet eerst toegang tot computers worden verkregen. Het heet *initial access* en affiliates mogen zelf weten hoe ze het bewerkstelligen; daar bestaan weer verschillende technieken, tools en diensten van andere cybercriminelen voor. Te denken valt aan *phishing* waarbij vervalste e-mails worden verstuurd die van betrouwbare afzenders afkomstig lijken te zijn, *drive-by*-aanvallen die via gehackte websites worden uitgevoerd en het misbuiken van kwetsbaarheden in het *Remote Desktop Protocol* (RDP). Momenteel zijn het voornamelijk op Windows draaiende computers die door LockBit worden aangevallen, maar de macOS-versie is nu al in ontwikkeling.[13] Zodra de toegang is geregeld, worden de binnengedrongen systemen besmet met de ransomware die ze afspeurt naar bepaalde bestandsextensies zoals *.pdf en *.doc(x). Zulke bestanden zijn vaak van onschatbare waarde voor niet alleen bedrijven en andere organisaties maar ook natuurlijke personen. Een fictief voorbeeld zou de Rijksuniversiteit Groningen kunnen zijn: zowel docenten als studenten bewaren hun CV's, wetenschappelijke artikelen en scripties digitaal en zulke documenten bevatten in de meeste gevallen persoonsgegevens. LockBit ontzegt vervolgens de getroffen gebruikers toegang tot deze bestanden (soms samen met systeembestanden) door ze te versleutelen met behulp van geavanceerde encryptietechnieken. Voor het ontsleutelen van de gegijzelde data wordt vervolgens losgeld (de "ransom") gevraagd. Als iemands computer wordt geïnfecteerd, dan verschijnt het volgende bericht op het scherm:

> *"~~~LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~*
>
> *»»> Your data is stolen and encrypted.*
>
> *If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe."*[14]

Na het betalen van het losgeld ontvangt het slachtoffer een *decryptor* waarmee de versleutelde bestanden kunnen worden hersteld, en hopelijk verdwijnt de aanvaller in stilte.

10. 'Understanding Ransomware Threat Actors: LockBit', cisa.gov, 14 juni 2023; ZEROFOX, *LockBit Targeting: Ransomware & Digital Extorsion* (Rapport), 2023, zerofox.com; 'LockBit 3.0, de marktleider in ransomware', techzine.nl, 21 april 2023.
11. 'LockBit, de gevaarlijkste gijzelsoftwarebende, staat 24 uur per dag paraat voor chantage', nrc.nl, 19 juli 2023; 'Explainer: What is Lockbit? The digital extortion gang on a cybercrime spree', reuters.com, 11 november 2023.
12. Australian Cyber Security Centre, *ACSC Ransomware Profile – Lockbit 3.0*, 15 juni 2023, cyber.gov.au.
13. 'Onderzoekers vinden versie van LockBit-ransomware voor macOS', security.nl, 17 april 2023.
14. '#StopRansomware: LockBit 3.0', cisa.gov, 16 maart 2023.

5. Money matters

LockBit en de door deze ransomware gebruikte encryptietechnieken zijn dermate geavanceerd en effectief en de druk om losgeld over te maken is zo groot dat de KNVB zich ertoe gedwongen voelde om cybercriminelen te betalen voor het ontsleutelen van een omvangrijke hoeveelheid (persoons)gegevens. Het is trouwens niet strafbaar om over te gaan tot losgeldbetaling en voor de getroffen organisaties is het vooral een kostenafweging op basis waarvan ze handelen: het zelfstandig herstellen van versleutelde computers komt dikwijls neer op hogere kosten en brengt onder andere omzetverlies en imagoschade met zich mee. In 2023 heeft 18% van de door ransomware geïnfecteerde Nederlandse organisaties ervoor gekozen om de hackers voor een decryptietool te betalen terwijl dit percentage wereldwijd 46% bedraagt.[15] De gegevens van de KNVB waren in april 2023 buitgemaakt, zoals bekendgemaakt door de bond vijf maanden later.[16] De voorzitter van de Autoriteit Persoonsgegevens (AP), Aleid Wolfsen, was bepaald niet gecharmeerd van het feit dat het geëiste losgeld was betaald, en beweerde dat hiermee een "verwerpelijk verdienmodel" in stand wordt gehouden.[17] Het valt wel op dat de LockBit-groep zich gedraagt als een professionele commerciële organisatie die zich aan de gemaakte afspraken houdt. Slachtoffers krijgen namelijk altijd toegang tot hun data nadat ze hebben betaald. Het spreekt in principe voor zich aangezien de LockBit-bende de naam hoog heeft te houden en wil overkomen als een betrouwbare RaaS-aanbieder met wie men "zaken kan doen". Het team achter LockBit streeft ernaar om een imago van betrouwbaarheid en geloofwaardigheid uit te stralen en het lijkt erop dat het zich aan bepaalde ethische regels houdt. Eind 2022 verontschuldigde de groep zich voor de aanval op een Canadees kinderziekenhuis, verstrekte een gratis decryptor en beëindigde de samenwerking met de affiliate die in strijd met haar ethische beleid had gehandeld.[18] De hackers zijn echter verre van consequent in het naleven van dat beleid wat blijkt uit andere aanvallen met deze ransomware zoals die van eind 2023 op het Saint Anthony Hospital, een Amerikaans kinderziekenhuis, waarbij een betaling van $800.000 werd geëist.[19] Na het betalen van het losgeld krijgt het slachtoffer van LockBit weer toegang tot zijn versleutelde data maar heeft geen enkele garantie dat die gegevens alsnog niet openbaar zullen worden gemaakt of dat er na de eerste betaling geen ander bedrag zal worden geëist (wat *double extorsion* oftewel "dubbele afpersing" wordt genoemd). Of met cybercriminelen moet worden onderhandeld, is een andere cruciale en interessante vraag waar mr. M. Weij op in is gegaan in zijn verhelderende opinie die in juni 2023 in dit tijdschrift is gepubliceerd.[20]

LockBit-aanvallers eisen niet zelden vrij hoge bedragen afhankelijk van de omzet van de door hen geïnfecteerde bedrijven. Het valt met hen trouwens wel te onderhandelen. Zo kan een royale korting van soms wel 90% worden bedongen. Als *LockBitSupp* ("Supp" van "Support") die als leider van het LockBit-team wordt beschouwd, echter in de chat van het portaal tevoorschijn komt en aan deze onderhandelingen deelneemt, dan zal daar geen sprake van zijn. Het schijnt namelijk niet mogelijk te zijn om bij hem het bedrag van het gevraagde losgeld te verlagen.[21] Het is trouwens nog steeds niet bekend wie deze persoon is maar degene die erin slaagt om zijn identiteit te ontrafelen, zal worden beloond met $1 miljoen in cryptovaluta door LockBitSupp zelf.[22] Daarnaast is er ook een *bug bounty*-programma van LockBit waarbij hackers, onderzoekers en anderen voor het ontdekken van fouten in de gijzelsoftware een beloning ter hoogte van minimaal $1.000 en maximaal $1.000.000 kunnen ontvangen. Ook al denkt men soms dat onzichtbare cybercriminelen miljoenen aan losgeld van bedrijven en andere organisaties afhandig maken, is dat niet helemaal waar. Het komt wel voor – zoals in het geval van de KNVB die naar verluidt ruim €1.000.000 moest betalen – maar bedragen van tussen de €50.000 en €100.000 zijn volgens experts meer de norm.[23] 80% van dat oneerlijk verdiende geld gaat naar de affiliates en de ontwikkelaars van LockBit ontvangen 20%.[24]

6. Gevaren en gevolgen

Als hackers een organisatie met LockBit of soortgelijke malware binnendringen, zullen niet alleen bedrijfsgegevens maar ook andere soorten informatie zoals persoonsgegevens ontoegankelijk worden gemaakt en worden ontvreemd. Informatiesystemen zijn dan vaak uit de lucht en de materiële schade kan enorm hoog oplopen. De getroffen gegevens zijn dan namelijk niet meer beschikbaar en kunnen door criminelen worden misbruikt, verwijderd of openbaar gemaakt. Zo werden de computersystemen van de gemeente Hof van Twente in 2020 platgelegd in een

15. Nationaal Cyber Security Centrum, *Jaarbeeld Ransomware 2023* (Project Melissa), ncsc.nl, 22 februari 2024.
16. 'Informatie cyberinbraak KNVB', knvb.nl, 12 september 2023.
17. 'Voorzitter waakhond: KNVB houdt verwerpelijk verdienmodel cybercriminelen in stand', ad.nl, 12 september 2023.
18. 'LockBit ransomware gang apologizes for SickKids hospital attack and offers free decryptor', engadget.com, 2 januari 2023; 'Update on SickKids response to cybersecurity incident', sickkids.ca, 22 december 2022.
19. 'Lockbit slaat toe bij kinderziekenhuis VS', security.nl, 3 februari 2024; 'Cybersecurity incident', sahchicago.org, 2 februari 2024.
20. M. Weij, 'Opinie: Over cyberaanvallen en principes', *Tijdschrift voor Internetrecht 2023/3.*
21. 'Lockbit is marktleider in de ransomware', bnr.nl, 12 september 2023 (podcast).
22. 'Understanding Ransomware Threat Actors: LockBit', cisa.gov, 14 juni 2023.
23. 'What Is LockBit Ransomware?', blackberry.com; 'Lockbit is marktleider in de ransomware', bnr.nl, 12 september 2023 (podcast).
24. 'LockBit, de gevaarlijkste gijzelsoftwarebende, staat 24 uur per dag paraat voor chantage', nrc.nl, 19 juli 2023.

ransomware-aanval.[25] De informatie op die IT-systemen en de back-ups werden door de hackers versleuteld en een groot aantal virtuele servers werd door hen verwijderd.[26] De kosten van het herstel bedroegen meer dan €4.000.000.[27] Na de gijzelsoftwarehack van het ROC Mondriaan in Den Haag uit 2021 hadden zowel studenten als medewerkers geen toegang meer tot hun bestanden en applicaties.[28] Omdat de onderwijsinstelling geen losgeld had betaald, zetten de cybercriminelen vervolgens de door hen gestolen gegevens, waaronder digitale kopieën van geldige identiteitsbewijzen, online.[29] De kosten voor het aanvragen van nieuwe identiteitsbewijzen werden door het ROC vergoed.[30] Het is tevens niet uitgesloten dat dergelijke aanvallen met ransomware kunnen leiden tot een psychische impact op slachtoffers in de vorm van onder andere het gevoel van onveiligheid, angst en stress. Naast de materiële schade kan dus ook immateriële schade optreden.

In geval van een infectie met LockBit is het niet uit te sluiten dat zowel bedrijfsprocessen als personen gevaar zullen lopen: denkt u aan klanten en personeel. Bij de aanval op de KNVB waren dat niet alleen NAW-gegevens van bepaalde spelers maar ook hun salarisgegevens, handtekeningen en identiteitsbewijzen en handtekeningen van ouders en verzorgers van sommige minderjarige spelers. Los van de vraag of deze persoonlijke informatie vóór de hack conform de Algemene Verordening Gegevensbescherming (AVG) was verzameld en bewaard, is de situatie zonder meer zorgwekkend. Dergelijke ransomware-aanvallen kunnen namelijk resulteren de openbaarheid van data van klanten en anderen, phishing, identiteitsfraude, verlies van intellectuele eigendom, aansprakelijkheid van de gehackte organisaties voor de opgetreden schade en vanzelfsprekend hoge kosten die moeten worden gemaakt.

Organisaties hebben al verplichtingen op het gebied van cybersecurity en dienen hun systemen en netwerken te beschermen tegen cybercriminelen en hun schadelijke software. Zo moeten verwerkingsverantwoordelijken en verwerkers op grond van art. 32 AVG passende technische en organisatorische maatregelen nemen om persoonsgegevens die door hen worden verwerkt, te beveiligen. Als deze gegevens toch door LockBit ontoegankelijk worden gemaakt en worden gestolen, dan verplicht art. 33 de verwerkingsverantwoordelijke ertoe om dergelijke datalekken te melden aan de AP als het waarschijnlijk is dat ze een risico voor de rechten en vrijheden van natuurlijke personen inhouden.[31] Als er echter sprake is van een hoog risico, dient ook een mededeling te worden gedaan aan de betrokkenen wiens persoonlijke informatie is buitgemaakt. Is een onderneming slachtoffer van ransomware geworden, dan is het bovendien aan te raden om aangifte bij de politie te doen. In de praktijk doet maar een klein deel van de met ransomware aangevallen bedrijven het daadwerkelijk: in 2022 heeft 13% van deze bedrijven aangifte gedaan, wat vrij zorgwekkend is.[32] Bovendien zijn er in art. 7 t/m 15 van de Wet beveiliging netwerk- en informatiesystemen (Wbni) de zorg- en meldplichten vastgelegd die op de aanbieders van essentiële diensten en digitaledienstverleners rusten. Daarin wordt vereist dat zij hun netwerk- en informatiesystemen beveiligen en mogelijke incidenten bij de overheid melden. Deze wet wordt momenteel gewijzigd in verband met de implementatie van de nieuwe *Network and Information systems Security 2*-richtlijn (de NIS2-richtlijn). Zowel essentiële als belangrijke organisaties uit verschillende sectoren, zoals bankwezen, energie en nu ook overheid, zullen onder de werking ervan vallen en zullen worden onderworpen aan beveiligings- en rapportageverplichtingen. Wilt u weten hoe een bepaalde organisatie moet worden gekwalificeerd, gebruikt u dan de handige NIS2-zelf-evaluatietool die recentelijk door de Rijksinspectie Digitale Infrastructuur (RDI) is ontwikkeld.[33]

Hieronder wordt in het kort een aantal maatregelen beschreven dat het overwegen waard is. Het nalaten om een adequaat beveiligingsniveau te garanderen kan namelijk aanzienlijke administratieve geldboeten tot gevolg hebben. In geval van een ransomware-aanval waarbij persoonsgegevens worden versleuteld en een verwerkingsverantwoordelijke of een verwerker niet conform art. 32 AVG heeft gehandeld, is de AP bevoegd om een boete tot €10.000.000 – of tot 2% van de totale wereldwijde jaaromzet als dat bedrag hoger is – op te leggen.[34] Net zoals andere Europese toezichthoudende autoriteiten dient de AP zich daarbij naast haar eigen beleidsregels[35] te houden aan de richtsnoeren die door de Groep gegevensbescherming artikel 29 en de European Data Protection Board (EDPB of het Comité) zijn uitgevaardigd.[36] Overtredingen uit categorie II waaronder een mogelijke schending van art. 32 AVG valt,

25. De Winter Information Solutions, *Te goed van vertrouwen? Duidingsrapportage ransomware-aanval Hof van Twente* (Rapport), 8 maart 2021, hofvantwente.nl.
26. 'Hof van Twente getroffen door cyberaanval, veel persoonlijke informatie van inwoners weg', rtvoost.nl, 3 december 2020.
27. 'Schade na hack Hof van Twente loopt op tot 4,2 miljoen euro, gemeente wil bedrag verhalen', rtvoost.nl, 22 september 2022.
28. 'ROC Mondriaan in Den Haag gehackt: 'Medewerkers staan werkloos bij de vestigingen', nos.nl, 23 augustus 2021.
29. 'Vragen en antwoorden hack ROC Mondriaan', rocmondriaan.nl, 16 december 2021.
30. 'ROC Mondriaan: 'Onze aanvallers specialiseren zich in onderwijs- en zorginstellingen', surf.nl.
31. 'Zo meldt u een datalek', autoriteitpersoonsgegevens.nl.
32. 'Schaam je niet langer, gehackt worden is niet jouw schuld', rijksoverheid.nl, 31 oktober 2023.
33. 'Zelf-evaluatie NIS2 gelanceerd', rdi.nl, 18 oktober 2023.
34. Zie art. 32, art. 83 lid 2 onder d en art. 83 lid 4 onder a AVG.
35. Beleidsregels van de Autoriteit Persoonsgegevens van 6 juni 2023 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (*Stcrt.* 2023, 34541).
36. Groep gegevensbescherming artikel 29, *Richtsnoeren voor de toepassing en vaststelling van administratieve geldboeten in de zin van Verordening (EU) 2016/679*, WP253, goedgekeurd op 3 oktober 2017; EDPB, *Richtsnoeren 04/2022 voor de berekening van administratieve geldboeten krachtens de AVG*, vastgesteld op 24 mei 2023.

zijn conform artikel 3 van de beleidsregels van de Nederlandse toezichthouder gekoppeld aan de boetebandbreedte tussen de €120.000 en €500.000 met de basisboete van €310.000. Wat aanbieders van essentiële diensten en digitaledienstverleners betreft, kunnen bestuurlijke boeten door bevoegde autoriteiten worden uitgedeeld die ten hoogste €5.000.000 bedragen als deze organisaties zich niet aan de in artikel 7 Wbni neergelegde verplichting inzake risicobeheer hebben gehouden.[37] De maximumbedragen van administratieve geldboeten die in de NIS2-richtlijn worden genoemd, zijn trouwens hoger en zijn ten minste €10.000.000 voor essentiële entiteiten en ten minste €7.000.000 voor belangrijke entiteiten.[38]

Bovendien moet worden opgemerkt dat het bij een aanval met gijzelsoftware mogelijk is dat het niet aanleggen van een adequate IT-beveiliging door een IT-leverancier civiele aansprakelijkheid jegens klanten met zich mee zal brengen, wat blijkt uit de uitspraak van de rechtbank Amsterdam.[39] De gemeente Hof van Twente hield trouwens het door haar ingehuurde IT-bedrijf "Switch IT Solutions" uit Enschede verantwoordelijk voor de ransomwarehack uit 2020 en wilde de daardoor ontstane schade verhalen op deze ICT-beheerder, maar is er uiteindelijk toch niet in geslaagd. In mei 2023 wees de rechter haar vordering af omdat er geen sprake was van onrechtmatig handelen door het IT-bedrijf.[40] De rechter heeft niet kunnen vaststellen dat het zijn contractuele verplichtingen niet was nagekomen of onzorgvuldig jegens de gemeente had gehandeld.[41] Het bedrijf heeft zich als "een redelijk handelend vakbekwaam ICT-beheerder" gedragen en de hack is deels te wijten aan twee onzorgvuldigheden van de gemeente zelf: een medewerker had namelijk niet alleen een zwak wachtwoord ("Welkom2020") ingesteld op de gemeentelijke *domain admin account* maar had ook een regel in de *firewall* aangepast waardoor de FTP-server van de gemeente via het internet benaderbaar werd.[42] Beide wijzigingen waren niet gemeld aan het IT-bedrijf.

7. Maatregelen

Het blijkt dus weer dat de menselijke factor een onverminderd groot risico voor digitale veiligheid is en blijft, in het bijzonder als het gaat om de inzet van ransomware. De kans is erg klein dat een afzonderlijk individu zal worden afgeperst door een affiliate van LockBit, hetgeen niet betekent dat een (werk)computer van een medewerker niet kan worden gegijzeld. Iemand die dus voor een (winstgevend) bedrijf werkt of werkzaam is bij een overheidsinstelling/-organisatie zoals de gemeente Hof van Twente of een universiteit zoals de Universiteit van Maastricht die in 2019 slachtoffer van de verwoestende ransomware-aanval werd[43], moet vooral aan zijn eigen cyberhygiëne denken en ervoor zorgen dat cybercriminelen geen kans krijgen om IT-systemen van zijn werkgever te infecteren. De dreiging en de impact van ransomware nemen namelijk met de jaren alleen maar toe waardoor organisaties gedwongen worden om continu hun cyberverdedigingsstrategieën te actualiseren en aan te scherpen.

De relevante bepalingen van de Europese en Nederlandse wetgeving waarnaar hierboven is verwezen, zijn vrij technologieneutraal geformuleerd zodat ze niet snel worden achterhaald door snelle technologische ontwikkelingen. Hoe netwerk- en informatiesystemen precies beveiligd dienen te worden, is afhankelijk van elke concrete situatie en factoren zoals de huidige stand van de techniek en de uitvoeringskosten. Het verhogen van de *awareness* rondom IT-beveiliging binnen organisaties, het volgen van trainingen, het organiseren van oefeningen en het opstellen van *best practices* zorgen voor meer kennis en bewustzijn bij medewerkers en zijn vanzelfsprekend, maar wat zijn meer specifieke maatregelen tegen ransomware die men kan treffen? Het Nederlandse Nationaal Cyber Security Centrum (NCSC) adviseert organisaties om:

a. beveiligingsmaatregelen tegen phishing te nemen (bijv. het gebruik van spamfilters en phishingtests);
b. voldoende aandacht aan *vulnerability management*, *patch management* en netwerksegmentering te besteden (bijv. het tijdig uitvoeren van updates en het monitoren van netwerken);
c. de mogelijkheden van het uitvoeren van code te beperken (bijv. het gebruik van applicatiewhitelisting en het uitschakelen van macro's in Microsoft Office);
d. het filteren van webbrowserverkeer mogelijk te maken (bijv. het blokkeren van malafide websites);
e. het gebruik van externe gegevensdragers te beperken (bijv. het blokkeren van USB-opslag).[44]

In het gezamenlijke advies van het Federal Bureau of Investigation, het Cybersecurity and Infrastructure Security Agency en het Multi-State Information Sharing & Analysis Center met betrekking tot LockBit 3.0 wordt een aantal aanvullende concrete maatregelen genoemd dat kan worden genomen.[45] Zo wordt aangeraden om binnen organisaties phishingbestendige meervoudige authenticatie voor alle IT-diensten en -toepassingen te verplichten en netwerken te segmenteren. Daarnaast is het aan te bevelen

37. Zie art. 7, art. 24 en art. 29 lid 1 onder a en lid 2 onder b Wbni.
38. Zie art. 21, 31 lid 1, 32 leden 1 en 4 onder i, 33 leden 1 en 4 onder h en art. 34 leden 1, 4 en 5 NIS2-richtlijn.
39. Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124.
40. Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731.
41. Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731, r.o. 4.5.
42. Rb. Overijssel 10 mei 2023, ECLI:NL:RBOVE:2023:1731, r.o. 4.2.9, 4.4.1 en 4.4.2.
43. Inspectie van het Onderwijs, *Cyberaanval Universiteit Maastricht*, mei 2020, rijksoverheid.nl.
44. Nationaal Cyber Security Centrum, *Factsheet Ransomware*, juni 2020, ncsc.nl.
45. '#StopRansomware: LockBit 3.0', cisa.gov, 16 maart 2023.

om een passend wachtwoordbeleid te voeren waarbij wachtwoorden in een gehashte vorm worden opgeslagen en niet mogen worden hergebruikt.

Zelf kunnen medewerkers van elke organisatie natuurlijk ook het een en ander doen om ransomware te weren. Richt een bedrijf zich dus tot u voor advies met betrekking tot een overzicht van door zijn personeel te treffen maatregelen, dan kunt u medewerkers van dat bedrijf het volgende adviseren:

> *"Houdt u goed uw mailbox in de gaten en opent u nooit bijlagen van e-mails van verdachte afzenders of met een verdachte inhoud. Hetzelfde geldt voor andere spamberichten die u bijv. op uw telefoon ontvangt. Klikt u nooit op links op onbekende websites die u niet vertrouwt en op links in spamberichten, downloadt u bestanden zoals programma's alleen van bekende betrouwbare websites, blijft u van onbekende USB-sticks en andere gegevensdragers af en zorgt u ervoor dat uw besturingssysteem en applicaties die u gebruikt, up-to-date zijn."*

8. Conclusie

Wat men ook zou kunnen doen om te voorkomen dat LockBit zich op bedrijfscomputers nestelt, zijn het wijzigen van de toetsenbordinstellingen in Windows en het toevoegen van talen zoals Russisch of Arabisch (Syrië). De versie 3.0 van deze ransomware infecteert namelijk geen computers met bepaalde taalinstellingen die *by design* niet worden aangevallen.[46] Hoelang deze "halve maatregel" nog effectief blijft, is echter maar zeer de vraag. Mocht een organisatie door LockBit 3.0 toch zijn getroffen, dan is het de moeite waard om de website van het project "No More Ransom" te bezoeken. Het is een initiatief van het Team High-Tech Crime van de Nederlandse politie, het European Cybercrime Centre van Europol, Kaspersky en McAfee dat in het leven is geroepen om de activiteiten van ransomwaregroeperingen te ontwrichten. Op die website is namelijk een decryptor te vinden die door de Japanse politie, de FBI en Europol is ontwikkeld en gratis kan worden gedownload om de versleutelde bestanden te herstellen.[47]

Het lijkt erop dat de LockBit-groep inmiddels slachtoffer van haar eigen succes is geworden en heeft het de afgelopen jaren niet makkelijk gehad bij het behouden van haar markleiderspositie. Gelukkig maar, zou ik eraan willen toevoegen. De aanvallen met deze ransomware hebben wereldwijd veel aandacht van rechtshandhavingsinstanties getrokken en er wordt nu al hard strafrechtelijk opgetreden tegen de LockBit-criminelen in onder andere de VS en Canada.[48] De grootschalige "Operation Cronos" heeft geresulteerd in een kortstondige verstoring van de illegale praktijken van de groep en voor een deuk in haar imago gezorgd maar is nog niet afgelopen. Er werd – vermoedelijk door de hackers zelf – beweerd dat hun back-up servers niet waren opgerold en onderzoekers bevestigden het feit dat een groot deel van hun digitale infrastructuur na de operatie nog online was.[49] De herstelwerkzaamheden waren meteen in volle gang en het hackerscollectief was niet van plan om op te geven en te stoppen; inmiddels is de kwaadaardige infrastructuur weer *up and running*.[50] In zijn op het dark web gepubliceerde bericht drijft de bendeleider de spot met de Amerikaanse FBI, legt uit dat hij door zijn eigen enorme succes erg lui is geworden en schrijft blij te zijn voor deze *wake-up call.* "Het enige wat mij motiveert om te werken zijn sterke concurrenten en de FBI... Ik houd van mijn werk, het brengt me vreugde in het leven, geld en luxe brengen niet dezelfde vreugde als mijn werk. Daarom ben ik bereid mijn leven te riskeren voor mijn werk. Zo helder, rijk en gevaarlijk zou het leven naar mijn mening moeten zijn."

Als de leden van het LockBit-team inderdaad in Rusland zijn gevestigd, is het onwaarschijnlijk dat ze ooit strafrechtelijk zullen worden vervolgd. Dat land levert zijn staatsburgers niet uit aan andere landen omdat art. 61 lid 1 van de Russische grondwet het verbiedt en is in feite "een veilige haven"[51] voor de hackers die vanuit zijn grondgebied cyberaanvallen tegen westerse doelwitten lanceren en malware verspreiden. De verwachting is dat LockBit verder in dezelfde of andere vorm zal worden ontwikkeld en als LockBit 4.0 of onder een andere naam zal worden ingezet in Nederland en over de hele wereld. Om die reden is het van fundamenteel belang dat organisaties voldoende gewapend zijn tegen deze ransomware of zijn verwanten en een actieve houding aannemen op het gebied van IT-beveiliging. Een gebrekkige cybersecurity brengt een scala aan gevaren met zich mee en vormt een open deur voor cybercriminelen die voortdurend op zoek zijn naar nieuwe manieren om toe te slaan: investeert u dus vooral in een robuust slot. [52]

46. '#StopRansomware: LockBit 3.0', cisa.gov, 16 maart 2023.
47. 'Ontsleuteltools', nomoreransom.org.
48. 'Russian and Canadian National Charged for Participation in Lockbit Global Ransomware Campaign', justice.gov, 10 november 2022; 'Russian National Charged with Ransomware Attacks Against Critical Infrastructure', justice.gov, 16 mei 2023.
49. 'Beruchte hackersbende Lockbit geraakt door internationale politieoperatie', nos.nl, 20 februari 2024; 'LockBit ransomware group taken down in multinational operation', arstechnica.com, 20 februari 2024.
50. 'LockBit keert terug met bijgewerkte encryptors en nieuwe servers', techzine.nl, 29 februari 2024; 'Ransomware Operation LockBit Reestablishes Dark Web Leak Site: LockBit Leader Vows to Continue Hacking', govinfosecurity.com, 24 februari 2024.
51. 'United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group', home.treasury.gov, 20 februari 2024.
52. 'LockBit ransomware returns, restores servers after police disruption', bleepingcomputer.com, 25 februari 2024. (het volledige bericht is te raadplegen op: https://www.bleepstatic.com/images/news/u/1100723/2024/LockBit_Revival_Message.jpg

Datalek HAN

Annotatie bij Rechtbank Gelderland 4 oktober 2023, ECLI:NL:RBGEL:2023:5435

mr. dr. T.F. Walree[1]

1. Feiten

Met behulp van 'SQL-injection' kon een hacker misbruik maken van een kwetsbaarheid in een verouderd webformulier van de Hogeschool van Arnhem en Nijmegen (HAN). Door die kwetsbaarheid kreeg de hacker toegang tot honderdduizenden persoonsgegevens van (oud)studenten. Daarbij zaten ook persoonsgegevens van eiser, waaronder adresgegevens en medische gegevens. Onduidelijk is wat de hacker met de gegevens van eiser heeft gedaan. Op grond van art. 82 AVG vordert eiser van de HAN een vergoeding van zijn immateriële schade van 1000 euro voor de diefstal van zijn persoonsgegevens die heeft kunnen plaatsvinden door de gebrekkige beveiliging. De rechtbank oordeelt uiteindelijk dat de student recht heeft op een vergoeding van 300 euro. Ook de vordering van eiser voor een verklaring voor recht dat de HAN zijn beveiligingsplicht niet heeft nageleefd, wordt toegewezen.

2. Datalek is niet altijd een inbreuk op de AVG

De eerste vraag die de rechtbank Gelderland moet beantwoorden is of de HAN door de kwetsbaarheid in strijd handelde met de AVG. Uit het vonnis blijkt dat de aanvaller de gegevens kon buitmaken door middel van SQL-injection. Met deze bekende en veelvoorkomende techniek voert een hacker in een tekstveld van het webformulier een stukje code in om een database te manipuleren. Op die manier geeft een database (bij een slecht beveiligde website) meer informatie terug dan de bedoeling is. Informatie kan op deze wijze uit de database naar de aanvaller worden gelekt of 'gedumpt'. Dat leidt tot een 'inbreuk in verband met persoonsgegevens' (art. 4 onder 12 AVG), of ook wel in lekentaal: een 'datalek'.

De rechtbank overweegt terecht en goed gemotiveerd dat een datalek niet automatisch betekent dat in strijd met de AVG is gehandeld. Voor beoordeling van de onrechtmatigheid van het datalek is uitsluitend van belang of het beveiligingsniveau 'passend' was ten tijde van de hack (zie ook art. 32 AVG). Uit het woordje 'passend' volgt dat verwerkingsverantwoordelijken – in dit geval de HAN - niet alle maatregelen hoeven te nemen die er maar mogelijk waren [r.o. 4.4].[2] Een waterdichte beveiliging is dus niet vereist. Ook bij passende maatregelen kunnen datalekken optreden, waardoor een datalek niet noodzakelijkerwijs duidt op een inbreuk op de AVG. Voor de meeste AVG-deskundigen is dit niets nieuws onder de zon, maar het is fijn dat het hardnekkige misverstand dat 'datalekken onrechtmatig zijn' de kop wordt ingedrukt.[3]

Ook uit een recent arrest van het Hof van Justitie blijkt dat de 'ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens' aan derden op zich niet volstaat om aan te nemen dat de door de verwerkingsverantwoordelijke getroffen technische en organisatorische maatregelen niet 'passend' zijn.[4] Een dergelijke uitleg of een dergelijk vermoeden zou er anders op neerkomen dat datalekken waarbij de vertrouwelijkheid van persoonsgegevens wordt aangetast altijd onrechtmatig zijn. Het criterium van 'passende maatregelen' zou in dat geval worden ondergraven. Bovendien zou dat onweerlegbaar vermoeden ervoor zorgen dat de verwerkingsverantwoordelijke de mogelijkheid (die hem op grond van art. 5 lid 2 en art. 24 AVG toekomt) wordt ontnomen aan te tonen dat hij wél degelijk in overeenstemming met de AVG heeft gehandeld.[5]

---

1. Tim Walree is universitair docent burgerlijk recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit en Of counsel bij Freshfields Bruckhaus Deringer.
2. Dat maatregelen slechts passend hoeven te zijn, en niet in absolute zin hoeven te beschermen tegen schendingen van vertrouwelijkheid, beschikbaarheid of integriteit, is logisch gelet op de *risk-based approach* die verweven is in de AVG. Het zou ook onzinnig zijn als de bakker om de hoek dezelfde beveiligingsmaatregelen zou moeten nemen als Ahold of ASML. De beveiliging moet worden afgestemd op de risico's voor de betrokkenen maar dus ook op de financiële mogelijkheden van de verwerkingsverantwoordelijke en de stand van de techniek. Zie over art. 32 AVG ook J.A. Hofman, *De beveiliging van persoonsgegevens. Over de juridische invulling van art. 5 lid 1 onder f en 32 AVG* (diss. Nijmegen), Deventer: Wolters Kluwer 2022.
3. Het gaat immers niet altijd goed, zie Rb. Noord-Nederland 15 januari 2021, ECLI:NL:RBNNE:2021:106 (*Datalek Gemeente Oldambt*), *JA* 2021/44, m.nt. T.F. Walree, zie mijn noot onder punt 2.
4. HvJ EU 14 december 2023, C 340/21, ECLI:EU:C:2023:986 (*VB/Natsionalna agentsia za prihodite*), punt 29-39.
5. HvJ EU 14 december 2023, C 340/21, ECLI:EU:C:2023:986 (*VB/Natsionalna agentsia za prihodite*), punt 32.

3. De invloed van de AVG op de stelplicht en verdeling van bewijslast

De HAN had gelet op art. 32 AVG passende beveiligingsmaatregelen moeten treffen. Eiser stelt gemotiveerd dat daar geen sprake van is, omdat de HAN de persoonsgegevens niet gepseudonimiseerd of versleuteld had opgeslagen, gebruikmaakte van een verouderd webformulier, en bestand had moeten zijn tegen een SQL-injection. De rechtbank Gelderland merkt op dat de HAN alleen algemene maatregelen heeft benoemd, maar niet 'concreet/inzichtelijk' heeft gemaakt welke specifieke maatregelen zij had genomen ten aanzien van het webformulier of de achterliggende server. Daardoor heeft de HAN volgens de rechtbank niet duidelijk gemaakt 'wat dan wél passend was en of de hogeschool daaraan voldeed.' De rechtbank oordeelt daarmee dat de door eiser gestelde inbreuk op art. 32 AVG door de hogeschool onvoldoende is betwist. De inbreuk komt daarmee vast te staan (r.o. 4.4).

In deze zaak motiveerde eiser uitvoerig waarom het beschermingsniveau van de HAN niet passend was. Om die gestelde inbreuk te betwisten, was het aan de HAN om aan te tonen dat haar beschermingsniveau wél passend was. In deze zaak doet eiser geen beroep op art. 5 lid 2 AVG (de verantwoordingsplicht van de verwerkingsverantwoordelijke). Die regel dicteert dat de verwerkingsverantwoordelijke moet kunnen aantonen dat hij de regels van de AVG naleeft. Ik durf de stelling wel aan dat ook als eiser de schending van art. 32 AVG door de HAN niet zo uitvoerig had gesteld, het in dat geval óók aan de HAN zou zijn geweest om als verwerkingsverantwoordelijke aan te tonen dat zij conform art. 32 AVG had gehandeld. In beginsel is de regel 'wie moet stellen, die moet bewijzen' (art. 150 Rv).[6] Die regel komt er in de praktijk bijna altijd op neer dat eiser bewijs moet leveren van een normschending. Van die verdeling van de bewijslast kan volgens art. 150 Rv echter worden afgeweken als een bijzondere regel dat vergt. Artikel 5 lid 2 AVG is zo'n bijzondere regel.[7] Deze omkering van de bewijslast wordt bevestigd door een recent arrest (14 december 2023) van het Hof van Justitie (*VB/Natsionalna agentsia za prihodite*). Volgens het Hof van Justitie volgt uit de tekst van de relevante bepalingen (art. 5 lid 2, 24 en 32 AVG) 'ondubbelzinnig' dat het in het kader van een vordering op grond van art. 82 AVG aan de verwerkingsverantwoordelijke is om te bewijzen dat hij passende maatregelen heeft genomen.[8] Met andere woorden, bij een schadeclaim draagt de verwerkingsverantwoordelijke de bewijslast voor het feit dat de beveiligingsmaatregelen passend zijn.[9] Die overweging wordt door het Hof van Justitie nog eens herhaald in het arrest *BL/MediaMarktSaturn* (25 januari 2024).[10] Dit leidt er in de praktijk dus toe dat de betrokkene de inbreuk op art. 32 AVG wel (gemotiveerd) zal moeten stellen, maar op grond van art. 5 lid 2 AVG niet de bewijslast draagt voor het feit dat de verwerkingsverantwoordelijke *geen* passende beveiligingsmaatregelen heeft genomen.

In dat laatste arrest oordeelt het Hof van Justitie ook dat de persoon die op grond van art. 82 AVG schadevergoeding vordert, moet 'bewijzen' dat er sprake is van een schending van de bepalingen van de AVG.[11] Ik denk echter niet dat dat afbreuk doet aan de omkering van de bewijslast ten aanzien van art. 32 AVG. Het Hof overweegt dat – dat een betrokkene een schending moet bewijzen - immers in algemene zin.[12] Dit terwijl het Hof eerder in datzelfde arrest - maar ook in *VB/Natsionalna agentsia za prihodite* - specifiek ten aanzien van schadeclaims wegens schendingen van art. 32 AVG oordeelde dat de bewijslast bij de verwerkingsverantwoordelijke ligt voor het feit dat de door hem genomen beveiligingsmaatregelen passend zijn. Dat pleit daarom voor de gedachte dat een omkering van de bewijslast bij AVG-schendingen in het algemeen niet direct voor de hand ligt, maar in het specifieke geval van art. 32 AVG dus wel (mits de betrokkene die schending gemotiveerd stelt).

In mijn optiek is de bewijslastomkering ten aanzien van art. 32 AVG gerechtvaardigd vanwege de informatie-asymmetrie tussen de verwerkingsverantwoordelijke en de betrokkene.[13] De betrokkene heeft immers vaak niet of nauwelijks inzicht in de wijze waarop de verwerkingsverantwoordelijke beveiligingsmaatregelen heeft genomen. Het aantonen door de verwerkingsverantwoordelijke dat de beveiligingsmaatregelen passend zijn, strekt echter niet zover dat hij aan de betrokkene alle (vertrouwelijke) informatie over zijn beveiligingsmethoden moet geven. Dit kan namelijk allerlei beveiligingsrisico's in het leven roepen, en kan daarom dus ook in strijd zijn met art. 32 AVG.[14] De verwerkingsverantwoordelijke kan daarom gewichtige redenen hebben om niet alle informatie met de betrokkene te delen. Het niet verschaffen van die informatie kan er wel toe leiden dat de verwerkingsverantwoordelijke wegens bewijsproblemen de procedure verliest. De verwerkingsverantwoordelijke doet er in dergelijke gevallen dus verstandig aan om de rechter mede te de-

6. H.J. Snijders, H.B. Krans, C.J.M. Klaassen & G.J. Meijer, *Nederlands burgerlijk procesrecht*, Deventer: Wolters Kluwer 2022, p. 279.
7. Zie ook Rb. Amsterdam 15 maart 2023, ECLI:NL:RBAMS:2023:1407 (*DPS/Facebook*), r.o 11.14-11.20.
8. HvJ EU 14 december 2023, C 340/21, ECLI:EU:C:2023:986 (*VB/Natsionalna agentsia za prihodite*), punt 52. Zie ook Rb. Amsterdam 15 maart 2023, ECLI:NL:RBAMS:2023:1407 (*DPS/Facebook*), r.o 11.14-11.20.
9. HvJ EU 14 december 2023, C 340/21, ECLI:EU:C:2023:986 (*VB/Natsionalna agentsia za prihodite*), punt 57.
10. HvJ EU 25 januari 2024, C-687/21, ECLI:EU:C:2024:72 (*BL/MediaMarktSaturn*), punt 43.
11. HvJ EU 25 januari 2024, C-687/21, ECLI:EU:C:2024:72 (*BL/MediaMarktSaturn*), punt 61.
12. Daarnaast is die overweging van het Hof terloops. Zie ook de formulering van de wat sturende prejudiciële vraag van de verwijzende rechter: HvJ EU 25 januari 2024, C-687/21, ECLI:EU:C:2024:72 (*BL/MediaMarktSaturn*), punt 56.
13. T.F. Walree, *Schadevergoeding bij de onrechtmatige verwerking van persoonsgegevens* (diss. Nijmegen), Deventer: Wolters Kluwer 2021, p. 149.
14. Vergelijk overweging 63 AVG.

len dat vanwege 'gewichtige redenen' uitsluitend de rechter kennis zal mogen nemen van de vertrouwelijke informatie (art. 22 lid 2 Rv). Ook kan de verwerkingsverantwoordelijke de rechter verzoeken om een 'gedeeltelijke behandeling met gesloten deuren' (art. 27 Rv).

4. Het recht op schadevergoeding

In deze zaak vordert eiser een schadevergoeding op grond van art. 82 AVG. Het arrest *Österreichische Post* van het Hof van Justitie (4 mei 2023) gaat over de uitleg van art. 82 AVG.[15] De rechtbank Gelderland verwijst daarom naar dit arrest en benoemt de belangrijkste overwegingen. De rechtbank zegt onder meer: "Niet elke inbreuk op de AVG resulteert in een recht op schadevergoeding." [r.o. 4.5] Ik neem aan dat zij daarmee bedoelt: 'de enkele inbreuk als zodanig leidt niet direct tot een recht op schadevergoeding'.[16] Uit het arrest volgt immers dat er een recht op schadevergoeding bestaat als er is voldaan aan drie cumulatieve voorwaarden: (1) geleden schade; (2) het bestaan van een inbreuk en (3) causaal verband tussen die schade en de inbreuk.[17] Het Hof van Justitie maakt daarbij geen onderscheid tussen verschillende typen inbreuken. Er is daarom geen enkele reden om aan te nemen dat sommige inbreuken - mits zij leiden tot vergoedbare schade - zouden zijn uitgesloten voor een recht op schadevergoeding.

Het Hof van Justitie bevestigt in *Österreichische Post* dat schade in de zin van art. 82 AVG een autonoom en uniform begrip is.[18] Lindenbergh en Samsom merken terecht op bij hun analyse van *Österreichische Post* dat de Uniewetgever en het Hof van Justitie dus leidend zijn voor de invulling van het begrip 'immateriële schade' van art. 82 AVG.[19] Desondanks wordt er in dit vonnis en óók in andere Nederlandse uitspraken (waarin het gaat om claims op grond van art. 82 AVG) aansluiting gezocht bij het nationale schadevergoedingsrecht.[20] De verklaring daarvoor is dat de Uniewetgever en het Hof van Justitie nog geen concrete invulling hadden gegeven aan het begrip 'immateriële schade' bij AVG-schendingen.

Na het wijzen van dit vonnis heeft het Hof van Justitie echter wel invulling gegeven aan het schadebegrip. Zo heeft het Hof recent in *VB/Natsionalna agentsia za prihodite* en *VX & AT/Gemeinde Ummendorf* erkend dat het 'verlies van controle over persoonsgegevens' en de 'gegronde vrees voor misbruik' immateriële schade in de zin van art. 82 AVG kunnen veroorzaken.[21] Dat oordeel komt niet als verrassing, omdat het Hof van Justitie in *Österreichische Post* al aangaf dat er geen schadedrempel bestaat.[22] Het Hof van Justitie geeft in alle drie deze arresten wél te kennen dat die ruime uitleg van schade niet wegneemt dat de betrokkene die wordt getroffen door een inbreuk op de AVG met negatieve gevolgen voor hem, moet bewijzen dat die gevolgen immateriële schade in de zin van art. 82 AVG opleveren.[23] Of daar sprake van is, is ter beoordeling van de nationale rechter. Het EBI-arrest geeft vooralsnog de spelregels voor het aantonen van immateriële schade. Dat zien we ook terug in dit vonnis [r.o. 4.5], aangezien de rechtbank Gelderland onmiddellijk na de verwijzing naar *Österreichische Post* art. 6:106 BW en de bijbehorende formule uit het EBI-arrest toepast.

Die EBI-formule geeft aan dat voor de toekenning van smartengeld eiser in principe met concrete gegevens moet aantonen dat hij, gelet op de aard en de ernst van de normschending en van de gevolgen daarvan voor hem, in zijn persoon is aangetast.[24] En inderdaad, in lijn met de hoofdregel van de EBI-formule moest de oud-student in deze zaak in beginsel aantonen dat hij nadelige gevolgen ondervond als gevolg van het datalek, en dat die gevolgen volstonden voor de toekenning van schadevergoeding. Ten aanzien van de 'algemene persoonsgegevens' overweegt de rechtbank dat het datalek niet bij eiser tot vergoedbare schade heeft geleid. Louter ergernis komt volgens de rechtbank niet voor vergoeding in aanmerking [r.o. 4.6]. Het is de vraag of dat in algemene zin nog zo te zeggen is na de recente arresten van het Hof van Justitie: er is immers geen schadedrempel. Aan de andere kant valt daar tegenin te brengen dat ergernis en frustratie niet op het spectrum van 'schade' thuishoren.

In deze zaak zijn niet alleen algemene persoonsgegevens gelekt, maar ook bijzondere persoonsgegevens, in dit geval medische gegevens van eiser. Volgens de rechtbank kan er bij bijzondere persoonsgegevens "eerder worden aangenomen dat sprake is van schade, omdat het bij uitstek gegevens zijn waarvan niet gewenst is dat ze "op straat" komen te liggen. De nadelige gevolgen daarvan liggen voor de hand."[r.o. 4.7][25] De rechtbank Gelderland past hier-

15. HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, C-300/21 (*Österreichische Post*).
16. Met andere woorden: er is naast een normschending ook schade nodig voor de toekenning van schadevergoeding.
17. Zie HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, C-300/21 (*Österreichische Post*), punt 32-33.
18. HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, C-300/21 (*Österreichische Post*), punt 30.
19. S.D. Lindenbergh & M.C. Samsom, 'Smartengeld wegens AVG-inbreuken na 'Österreichische Post', *NJB* 2023/1621, afl. 23., p. 1898.
20. Zie bijvoorbeeld: Rb. Noord-Nederland 15 januari 2020, ECLI:NL:RBNNE:2020:247 (*X/NDC Mediagroep*); Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 (*X/UWV*); Rb. Zeeland-West-Brabant 21 september 2022, ECLI:NL:RBZWB:2022:5457 (*Bravis ziekenhuis).*
21. HvJ EU 14 december 2023, C 340/21, ECLI:EU:C:2023:986 (*VB/Natsionalna agentsia za prihodite*), punt 82-83; HvJ EU 14 december 2023, ECLI:EU:C:2023:988, C-456/22 (*VX & AT/Gemeinde Ummendorf*), punt 22.
22. HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, C-300/21 (*Österreichische Post*), punt 51.
23. HvJ EU 4 mei 2023, ECLI:EU:C:2023:370, C-300/21 (*Österreichische Post*), punt 50; HvJ EU 14 december 2023, C 340/21, ECLI:EU:C:2023:986 (*VB/Natsionalna agentsia za prihodite*), punt 84; HvJ EU 14 december 2023, ECLI:EU:C:2023:988, C-456/22 (*VX & AT/Gemeinde Ummendorf*), punt 22-23.
24. HR 15 maart 2019, ECLI:NL:HR:2019:376 (*EBI*), r.o. 4.2.1.
25. Het blijft gissen wat de rechtbank bedoelt met de constatering dat het datalek niet tot 'concrete negatieve gevol-

bij de uitzonderingsregel van het EBI-arrest toe. Die regel komt er op neer dat de aard en ernst van de normschending kunnen meebrengen dat de nadelige gevolgen voor de benadeelde zó voor de hand liggen, dat een persoonsaantasting kan worden aangenomen.[26] Dat betekent in de praktijk dat bij ernstige normschendingen nadelige gevolgen door de rechter worden verondersteld of in ieder geval sneller worden aangenomen. Dat zorgt voor een verlichting van de bewijslast van de betrokkene. De rechtbank Gelderland past die uitzonderingsregel toe omdat in deze zaak medische gegevens zijn gelekt. Volgens de rechtbank maakt het niet uit dat onduidelijk is wat de hacker uiteindelijk met de gegevens heeft gedaan: dat hij toegang had tot deze specifieke gegevens is al voldoende voor het aannemen van schade.[27]

Het toepassen van de uitzonderingsregel bij AVG-inbreuken waarbij bijzondere persoonsgegevens zijn betrokken, hebben we eerder gezien.[28] Die tweedeling is te rechtvaardigen, omdat voor dergelijke gegevens in de AVG een bijzonder regime geldt. De Uniewetgever vond dat type gegevens kennelijk meer het beschermen waard. Ook de rechtbank Gelderland merkt op dat bijzondere persoonsgegevens 'naar hun aard een hoger beschermingsniveau' verlangen [r.o. 4.3]. De veronderstelling van schade bij de onrechtmatige verwerking van bijzondere persoonsgegevens zorgt voor een verlichting van de bewijsnood voor de betrokkene. Toch is die tweedeling niet helemaal gelukkig. Algemene persoonsgegevens - zoals NAW-gegevens - kunnen in sommige contexten net zo goed risico's in het leven roepen voor de betrokkene (denk bijvoorbeeld aan het huisbezoek aan Kaag nadat haar adresgegevens online waren verspreid of aan een verzekeraar die geheime adresgegevens van een vrouw en haar kinderen verstrekte aan een dreigende ex-echtgenoot).[29] Bovendien vervaagt het grensgebied tussen algemene en bijzondere persoonsgegevens.[30]

Het is de vraag of de trend - het toepassen van de EBI-uitzonderingregel bij de onrechtmatige verwerking van bijzondere persoonsgegevens - zich zal voortzetten. Het antwoord op deze vraag zal van groot belang zijn voor WAMCA-procedures waarin het gaat om AVG-schendingen. Belangenorganisaties zullen graag stellen dat bij de AVG-inbreuken waartegen zij in actie komen *bijzondere* persoonsgegevens zijn betrokken. Dat geeft hen immers een bewijsvoordeel. Bovendien zorgt de toepassing van die uitzonderingsregel ervoor dat de groep van betrokkenen aanspraak kan maken op een vergoeding voor dezelfde soort immateriële schade. Ook dat geeft een voordeel aan belangenorganisaties: een rechter zal daardoor in de voorfase van een WAMCA-procedure niet snel beslissen dat er een 'niet voldoende bundelbare claim' is (waardoor de collectieve vordering niet-ontvankelijk is).[31]

De HAN wijst er op dat de uitzonderingsregel niet is bedoeld voor het onderhavige geval, omdat die alleen is bedoeld voor uitzonderlijk ernstige situaties (zoals *Oudejaarsrellen* en *Wrongful life*).[32] De rechtbank maakt met dat argument korte metten: "Elk geval zal echter apart moeten worden beoordeeld. Het zal van de geschonden norm en de daardoor beschermde belangen afhangen of sprake is van een schending die naar zijn aard of vanwege de ernst daarvan zodanig is dat een noemenswaardige aantasting in de persoon kan worden aangenomen. Als uitgangspunt moet in dit geval gelden dat de AVG bepaalt dat het begrip schade ruim moet worden uitgelegd, op een wijze die recht doet aan de doelstellingen van de verordening. Het belang waar [eiser] in is getroffen is een belang dat in de voorschriften van de AVG juist beoogd wordt te beschermen." Dit komt neer op een verordenings- of AVG-conforme interpretatie van de EBI-formule.[33] Die verordeningsconforme interpretatie is verplicht op grond van Europese rechtspraak. Daaruit volgt dat de nationale rechter de plicht heeft om de volle werking van het Unierecht te verzekeren en de daarin aan particulieren toegekende rechten te beschermen.[34] Dat brengt ook met zich dat de rechter het nationale recht conform de doelstellingen van het relevante Unierecht dient uit te leggen.[35]

gen' heeft geleid [r.o. 4.8]. De rechtbank vindt immers de emoties en gevoelens van eiser voor de hand liggen, bovendien heeft eiser die nadelige gevolgen toegelicht. Het lijkt erop dat de rechtbank daarmee wil zeggen dat eiser geen materiële/vermogensrechtelijke gevolgen heeft ondervonden. Zie ook de noot bij dit vonnis van A.C. Hendriks, *JBP* 2023/163, onder 7.

26. HR 15 maart 2019, ECLI:NL:HR:2019:376 (EBI), r.o. 4.2.1.
27. Zie ook GvA EU 15 januari 2019, T-881/16, ECLI:EU:T:2019:5 (*HJ/EMA*), punt 57. Vergelijk EHRM 17 juli 2008, nr. 20511/03, ECLI:CE:ECHR:2008:0717JUD002051103 (*I./Finland*).
28. ABRvS 1 april 2020, ECLI:NL:RVS:2020:898 (*Pieter Baan Centrum*); Rechtbank Zeeland-West-Brabant 21 september 2022, ECLI:NL:RBZWB:2022:5457, *JA* 2023/24, m.nt. T.F. Walree; Rb. Noord-Nederland 12 januari 2021, ECLI:NL:RNNNE:2021:106, *JA* 2021/44, m.nt. T.F. Walree (*Datalek gemeente Oldambt*).
29. Rb. Utrecht 12 augustus 2009, ECLI:NL:RBUTR:2009:BJ5273 (*X/Agis*), r.o. 4.12.
30. Zie HvJ EU 1 augustus 2022, C-184/20, ECLI:EU:C:2022:601 (*OT/VTEK*), punt 128.
31. Vergelijk Rechtbank Amsterdam 25 oktober 2023, ECLI:NL:RBAMS:2023:6694, *Computerrecht* 2024, afl. 2, m.nt. J. Doerga (*TikTok*), r.o. 2.44.3-2.44.4.
32. HR 9 juli 2004, ECLI:NL:HR:2004:AO7721, *NJ* 2005/391 (*Oudejaarsrellen*); HR 18 maart 2005, ECLI:NL:HR:2005:AR5213, *NJ* 2006/606 (*Wrongful life*). Zie ook Walree 2021, p. 128.
33. Zie Rb. Noord-Nederland 15 januari 2020, ECLI:NL:RBNNE:2020:247 (*X/NDC Mediagroep*), r.o. 4.107; Rb. Amsterdam 2 september 2019, ECLI:NL:RBAMS:2019:6490 (*X/UWV*), r.o. 18 (3e alinea). Zie ook Walree 2021, p. 138.
34. Zie bijvoorbeeld HvJ EG 20 september 2001, C-453/99, ECLI:EU:C:2001:465 (*Courage/Crehan*), punt 25; HvJ EG 13 juli 2006, gevoegde zaken C-295/04-C-298/04, ECLI:EU:C:2006:461 (*Manfredi*), punt 89.
35. Zie bijvoorbeeld HvJ EG 26 september 2000, C-262/97, ECLI:EU:C:2000:492 (*Engelbrecht*), punt 39; HvJ EG 7 januari 2004, C-60/02, ECLI:EU:C:2004:10 (*Rolex e.a.*), punt 59.

Jurisprudentie

mr. F. Schemkes en M.V. Avanesian LL.B, BSc

NOVEMBER 2023

Rechtbank Midden-Nederland, 1 november 2023, ECLI:NL:RBMNE:2023:5728
Privacyrecht, verplichting tot gegevenslevering, indirect identificeerbare persoonsgegevens

Eisers vorderen om de NZa te verbieden gegevens te verwerken totdat het eindvonnis is gewezen. Er dient te worden gekeken of eisers voldoende aannemelijk hebben gemaakt dat de verplichting tot gegevenslevering en de verwerking daarvan duidelijk in strijd is met hoger recht en daardoor gestaakt moet worden.
De rechtbank oordeelt dat er in casu sprake is van indirect identificerende persoonsgegevens en gaat over tot een oordeel of artikel 4.2 lid 4 van de Regeling een ongerechtvaardigde inbreuk maakt op het medisch beroepsgeheim. Voort oordeelt de rechtbank dat het doelbindingzbeginsel niet wordt geschonden, omdat de gegevens alleen worden gebruikt voor het ijken van het algoritme zorgvraagtypering en van de verdeling van zorgvraagtyperingen. Tot slot toetst de rechter aan het noodzakelijkheidsbeginsel. De uitvraag van de gegevens door de NZa is naar het oordeel echter gerechtvaardigd. Daarnaast acht de rechtbank de werkwijze proportioneel, omdat de NZa stelt dat de gegevensuitvraag en verwerking nodig is voor de zorgvraagtypering, waarbij minder zware maatregelen niet volstaan.
De rechtbank concludeert dat eisers onvoldoende aannemelijk hebben gemaakt dat de verwerking door de NZa onrechtmatig is. De verwerking is namelijk noodzakelijk om te voldoen aan een wettelijke verplichting die op de Nza rust.

Rechtbank Amsterdam, 2 november 2023, ECLI:NL:RBAMS:2023:6923
Deepfake, cyberonderzoek, privacybelang

Aangeefster heeft aangifte gedaan tegen verdachte, nadat bekend was geworden dat van haar een zogenoemde deelfake pornovideo op het internet staat. Vervolgens hebben cyberonderzoekers op verzoek van aangeefster achterhaald wat het IP-adres van verdachte is. Verdachte heeft bij de politie bekend dat hij de plaatser van de video is. Er dient te worden onderzocht of het openbaar maken van een zogeheten deepfake pornovideo onder het bereik van artikel 139h Sr valt.
Op basis van de grammaticale interpretatie kan naar het oordeel van de rechtbank een deepfake pornovideo onder het begrip afbeelding van seksuele aard vallen. Hoewel er teleologisch niet kan worden gesteld dat er expliciet is gebroken over digitaal of anderszins gemanipuleerde beelden, oordeelt de rechtbank dat ook nieuwe en toekomstige normenvan wraakporno en daaraan aanverwante vormen van openbaarmaking hieronder vallen. In dit geval beoogt de rechter middels artikel 139h Sr ook het privacybelang van de aangeefster te beschermen, aangezien dit beeldmateriaal tegen haar zin in vervaardigd is. De rechtbank komt met een bewezenverklaring van het ten laste gelegde feit aan de verdachte en veroordeelt de verdachte tot een geheel voorwaardelijke taakstraf van 180 uren.

Gerechtshof Arnhem-Leeuwarden, 7 november 2023, ECLI:NL:GHARL:2023:9394
Persoonsgegevens, verwijderingsverzoek, AVG

In deze zaak heeft de Rabobank de persoonsgegevens van een klant opgenomen in het interne verwijzingsregister, het incidentenregister en het extern verwijzingsregister. Voorts heeft de Rabobank de bankrelatie met de klant opgezegd. De klant heeft in het kort geding verwijdering van zijn gegevens uit de registers en herstel van de bankrelatie gevorderd, die door de vorderingen is toegewezen. Met dit hoger beroep wil de Rabobank dat de toegewezen vorderingen van de klant alsnog worden afgewezen.
Allereerst heeft de rechter getoetst of de Rabobank de gegevens volgens de AVG mocht registreren. Aangezien de Rabobank een gerechtvaardigd belang heeft en de betrokkene hierover heeft geïnformeerd, heeft de rechtbank geoordeeld dat er geen bezwaren zijn om deze gegevens te registreren. Dit betekent daarmee ook dat registratie in de registers niet verboden is.
Daarna oordeelt de rechter over de vraag of de registratie van persoonsgegevens momenteel ook nog noodzakelijk is. Hierbij dient er gekeken te worden of de klant genoeg belang heeft bij het verwijderen van haar persoonsgegevens. De klant heeft de stelling van Rabobank dat zijn belangen op dit moment minder zwaar wegen dan het belang van de financiële sector om te worden gewaarschuwd voor de gedragingen van de klant onvoldoende concreet onderbouwd. Door de klant is namelijk niet aangevoerd of en op welke wijze hij nu zou worden belemmerd door een registratie in een van de registers. Het hof is daarom van oordeel dat door Rabobank voldoende is onderbouw dat er prevalerende dwingende gronden bestaan voor de registraties. Op de mondeling behandeling is door beide partijen toegelicht dat de relatie is verstoord en dat er geen belang is bij de instandhouding van de relatie. Het beroep van de Rabobank slaagt.

Gerechtshof Amsterdam, 10 november 2023, ECLI:NL:RBAMS:2023:7874
Voorzieningenrechter, openbaarmaking videobeelden, privacybelang

Noordkaap TV producties produceert het tv programma 'Undercover in Nederland'. Eiser was eigenaar van een autorijschool, gespecialiseerd voor mensen met rijangst en autisme. Tussen de eiser en oud-leerlingen zijn ontuchtige handelingen geweest, waarvan proces-verbaal is opgemaakt. Eiser is hiervoor veroordeeld geweest en heeft hiervoor beroep ingesteld. Eiser mocht na de initiële veroordeling geen lessen meer geven. Uit het tv programma bleek echter dat de eiser toch les geeft, waarvan bewijs middels verborgen camerabeelden is verkregen. Noordkaap wil deze beelden openbaar maken, maar eiser verzet zich hiertegen.
De vordering van eiser wordt afgewezen. Ondanks dat de veroordeling van eiser nog niet onherroepelijk is, betekent dit niet dat er geen misstanden mogen worden gepubliceerd. Daarnaast is het gebruik van verborgen camera's in dit geval gerechtvaardigd, omdat het gaat om een ernstige overtreding van eiser en deze misstanden niet op een andere wijze aan de kaak konden worden gesteld. Het belang bij uitingsvrijheid weegt zwaarder dan het privacybelang van eiser.
Eiser (appellant) is hierna met meerdere grieven in hoger beroep gekomen tegen dit vonnis en vordert een verbod voor een toekomstige uitzending van het programma 'Undercover in Nederland'. Het Hof gaat echter wederom niet mee in vorderingen van appellant. Noordkaap heeft met het onherkenbaar maken van gezichten, het niet noemen van namen en woonplaatsen ervoor gezorgd dat de herkenbaarheid van appellant wordt weggenomen. Appellant wordt ook verwezen in de kosten van het geding in hoger beroep.

Rechtbank Midden-Nederland, 15 november 2023, ECLI:NL:RBMNE:2023:6299
Crypto, fraude, schadevergoeding

Coinbase is een platform voor de handel in cryptomunten, waar je een account voor moet aanmaken voor gebruik. Bij het aanmaken van een account, moet je de gebruikersvoorwaarden van Coinbase accepteren. Eiser is het slachtoffer geworden van fraude in zijn zoektocht tot begeleiding bij het investeren in bitcoins. Tijdens deze zoektocht, heeft hij zijn contactgegevens achterlaten op een website. Hierna werd hij door een adviseur gebeld, die de eiser een account heeft laten aanmaken op Coinbase. Op advies van zijn adviseur heeft hij ook bitcoins gekocht. De adviseur bleek echter niet oprecht en heeft de bitcoins overgemaakt op externe wallets. Eiser heeft later telefonisch en per e-mail contact gehad met andere personen, die hem ertoe hebben bewogen grote geldbedragen over te maken. Eiser heeft aangifte gedaan, maar de oplichters zijn niet achterhaald. In deze procedure vordert eiser een verklaring voor recht dat de overeenkomst tussen eiser en Coinbase buitengerechtelijk is vernietigd, dan wel dat Coinbase onrechtmatig heeft gehandeld jegens eiser. De vordering strekt tot terugbetaling van de geleden schade.
Eiser stelt daarbij dat Coinbase zich schuldig heeft gemaakt aan meerdere misleidende handelspraktijken. Zo zou zij op haar website de indruk hebben gewekt dat zij haar diensten legaal aanbood, terwijl zij niet aan de vereisten van de Wwft-registratie bij de DNB voldeed. De rechter ziet het causale verband tussen de vermeende onrechtmatige handelspraktijken van Coinbase en de totstandkoming van de overeenkomst. Rechtbank oordeelt dat eiser zich onvoldoende kritisch heeft opgesteld en wijst de vorderingen af.

Rechtbank Amsterdam, 15 november 2023, ECLI:NL:RBAMS:2023:7233
Aandeelhoudersovereenkomst, fraude, schadevergoeding

Eiser is houder van een vennootschap en is een samenwerking aangegaan met Bi4 om een SaaS bedrijf op te richten. In de aandeelhoudersovereenkomst is bedongen dat bij het eindigen van de overeenkomst tussen partijen de door eiser gehouden aandelen automatisch worden aangeboden en dat de vennootschapdit accepteert. Nadat de overeenkomst is opgezegd, is een geschil ontstaan betreft de prijs waarvoor de aandelen zijn overgedragen. De nominale waarde bedraagt 20 euro maar eiser voert aan dat de inbreng mede bestaat uit een verleende korting per maand op zijn loon.
Eiser vordert een verklaring voor recht dat er tussen eiser en het bedrijf een koopovereenkomst tot stand is gekomen. Hieraan legt zij de totstandkoming van de koopovereenkomst ten grondslag. De vennootschap voert verweer en concludeert tot afwijzing van de vordering van eiser. In reconventie voert de vennootschap om eiser te veroordelen tot medewerking aan de overdracht van de aandelen voor de koopprijs van 20 euro. Partijen zijn het erover eens dat de genoemde koopprijs 20 euro bedraagt, maar verschillen van mening of hier nog een bedrag bij komt. De rechtbank zal de bepaling in de overeenkomst moeten uitleggen door middel van toepassing van de Haviltex-maatstaf.
De rechtbank is van oordeel dat partijen redelijkerwijs mochten verwachten dat de bedoelde koopprijs alleen bestond uit het bedrag dat eiser stortte ten tijde van de oprichting. Eiser mocht er niet van uitgaan dat de korting hier ook onder zou vallen. Ook tijdens de vergaderingen voorafgaand aan de oprichting van de vennootschap blijkt niet dat de eiser de korting terug zou moeten krijgen wanneer de samenwerking eindigt. De rechter acht de uitleg van eiser gezien bovengenoemde redenen niet logisch en verwerpt het gevorderde.

Hof van Justitie van Europa, 16 november 2023, ECLI:EU:C:2023:874
Prejudiciële beslissing, verwerking persoonsgegevens, toezichthoudende autoriteit

BA, een Belgische burger, heeft de Nationale Veiligheidsoverheid verzocht om een veiligheidsattest af te geven voor beroepsdoeleinden. De Nationale Veiligheidsoverheid heeft dit echter geweigerd omdat BA heeft deelgenomen aan 10 betogingen. Hierna heeft BA het Controleorgaan verzocht de verantwoordelijken voor de betrokken verwerking van persoonsgegevens te identificeren. Het Controleorgaan heeft BA enkel laten weten dat de nodige verificaties verricht waren. BA is hiertegen in hoger be-

roep gegaan bij de rechter in eerste aanleg, die zich onbevoegd heeft verklaard. Het Hof van Brussel, dat door de betrokkene en de mensenrechtenorganisatie Ligue des droits humains is aangezocht, vraagt het Hof of lidstaten verplicht zijn om te voorzien in de mogelijkheid dat een betrokkene een besluit van de toezichthoudende autoriteit kan betwisten.
Het Hof benadrukt dat de lidstaten een natuurlijke persoon of rechtspersoon in staat moeten stellen om tegen een juridisch bindend besluit van een toezichthoudende autoriteit op te komen en zijn rechten kan verdedigen. Zodoende moet worden bepaald of de bevoegde toezichthoudende autoriteit een besluit dat onder deze definitie valt vaststelt wanneer zij de betrokkene informeert over het resultaat van de controles voor een veiligheidsattest. Een persoon die door deze autoriteit geïnformeerd wordt, met het recht hebben om een doeltreffende voorziening in rechte te stellen tegen het besluit van die autoriteit om het controleproces te beëindigen. Tegen een dergelijk besluit moet dus beroep kunnen worden ingesteld, stelt het Hof in deze prejudiciële beslissing.

Hof van Justitie van Europa, 16 november 2023, ECLI:NL:RBAMS:2023:7466
Social media , verwerking persoonsgegevens,

Gedaagde heeft in de zomer van 2023 berichten op LinkedIn geplaatst en e-mails gestuurd naar zakelijke contacten van eisers, waarin een van de eisers werd beschuldigd van onder meer fraude, diefstal, inbraak en huisvredebreuk. Zo zouden eisers onder andere hebben gesjoemeld met het persoonsgebonden budget van de moeder van gedaagde en zaken hebben ontvreemd uit haar huis. Eisers geven ter zitting aan dat deze beschuldigingen volstrekt onjuist zijn en eisen dat het gedaagde wordt verboden om contact op te nemen met zakelijke relaties van eisers en om zich in welke vorm dan ook negatief uit te laten over eisers. Daarnaast eisen ze dat alle reeds geplaatste berichten op LinkedIn worden verwijderd.
Gedaagde heeft nagelaten om aannemelijk te maken dat de geplaatste informatie juist is. Daarnaast waren er andere mogelijke manier om eisers aan te spreken, zonder over te gaan tot het plaatsen van beschuldigende berichten op het internet en het e-mailen van relaties. De plaatsing van de berichten tast de reputatie van de eisers aan en vormt een hinderlijke inbreuk op het privé-leven van eisers. De hiervoor genoemde vorderingen worden toegewezen.

Rechtbank Limburg, 27 november 2023, ECLI:NL:RBLIM:2023:6922
Voorzieningenrechter, audiofragmenten, artikel 6 EVRM

Gedaagden zijn de ouders van een minderjarige die een zware vorm van autisme heeft. Het Robertshuis is een zorgcentrum en biedt dagbehandeling voor onder meer kinderen met een autismestoornis. Gedaagden hebben tijdens een dagbehandeling bij het Robertshuis audiofragmenten laten opnemen vanuit de rugzak van de minderjarige. Het Robertshuis vordert gedaagden te bevelen om het Robertshuis een kopie te verstrekken van alle audiofragmenten. Gedaagden voeren hiertegen verweer. Het Robertshuis heeft volgens de voorzieningenrechter spoedeisend en rechtmatig belang bij haar vordering om beschikking te krijgen tot de audiofragmenten. Gedaagden willen de audiofragmenten laten afspelen aan getuigen. Het Robertshuis wil de audiofragmenten ook horen. Zij bevinden zich in een nadeligere rechtspositie als zij de audiofragmenten niet horen.
De weigering tot afgifte van de audiofragmenten is in strijdt met artikel 6 EVRM volgens het Robertshuis. Voor de waarheidsvinding vindt de voorzieningenrechter het belangrijk dat de getuigen, bestaande uit (ex-)werknemers, antwoorden geven op vragen op basis van wat zij hebben waargenomen. Hiermee wordt voorkomen dat er antwoord wordt gegeven op de vragen op basis van de audiofragmenten. Gedaagden zijn bereid een kopie van de audiofragmenten over te dragen aan het Robertshuis na het getuigenverhoor, zodat dit verhoor onafhankelijk zal verlopen. Hierdoor zal het verhoor eerlijk verlopen en zal het Robertshuis zich niet in een nadeligere positie bevinden. Er is volgens de voorzieningenrechter dus geen schending op een eerlijk proces. De vordering wordt om die reden afgewezen.

Rechtbank Midden Nederland, 27 november 2023, ECLI:NL:RBMNE:2023:6293
Voorzieningenrechter, privacyrecht, verbod verspreiding materiaal

Eiseres, een publiekelijk bekend persoon, en gedaagde hebben in 2018 en 2019 een relatie gehad. Tijdens de relatie met gedaagde heeft eiseres meerdere filmpjes gemaakt waarop te zien is dat zij seksuele handelingen bij zichzelf verricht. Deze filmpjes heeft zij aan gedaagde verstuurd. De relatie is inmiddels verbroken, waardoor eiseres vreest dat gedaagde dit materiaal zal verspreiden. Eiseres vordert in conventie onder andere inzage/afschrift van beslagen bescheiden die verband houden met pornografisch materiaal, gedaagde te verbieden om pornografisch of anderszins belastende materialen waarop of waarin eiseres te zien of te horen is aan derden te verspreiden en gedaagde te verbieden om met betrekking tot eiseres contact op te nemen met roddelpers of juice kanalen. Eiseres heeft een spoedeisend belang.
Om de eerste eis te verwezenlijken moet er worden voldaan aan drie eisen: eiseres moet een rechtmatig belang hebben bij inzage of afschrift; het moet gaan om bepaalde bescheiden en er moet een bepaalde rechtsbetrekking zijn. Eiseres heeft voldoende aannemelijk gemaakt dat gedaagde onrechtmatig tegenover eiseres heeft gehandeld door het pornografisch materiaal zonder haar toestemming in zijn bezit te hebben, en te verspreiden. Het verspreiden van pornografisch materiaal is onrechtmatig en maakt inbreuk op het recht op privacy van eiseres. De dreiging van verspreiding is reëel, nu op 17 augustus 2023 er vanaf een onbekend telefoonnummer een filmpje van eiseres naar haar huidige partner gestuurd. Het is niet vastgesteld dat gedaagde het filmpje heeft verstuurd, maar het karakter van het kort geding, waar ordemaatregelen worden opgelegd, rechtvaardigen dat aan gedaagde een verbod wordt opgelegd om pornografisch materiaal of waarin eiseres te zien of te horen is aan derden te verspreiden. De vordering tot verbod van verspreiding wordt toegewezen.

Eiseres heeft tevens een rechtmatig belang bij inzage en afschrift van de video- en audiobestanden en afbeeldingen. De vorderingen van eiseres uit onrechtmatige daad ziet volgens de rechter alleen rechtmatig op bescheiden die verband houden met het pornografische materiaal. De voorzieningenrechter heeft acht het bestaan van de rechtsbetrekking waarop de vordering ziet voldoende aannemelijk is en wijst deze vordering toe. Een van de vorderingen van eiser ziet op een verbod voor gedaagde om contact op te nemen met de roddelpers en 'juice' kanalen.
De voorzieningenrechter is het met gedaagde eens dat het verbod om verdere informatie te delen met deze partijen veel te algemeen is geformuleerd. Het staat gedaagde tot op zekere hoogte vrij om informatie met de roddelpers en/of juice kanalen te delen, mits hij geen onrechtmatige inbreuk maakt op de persoonlijke levenssfeer van eiseres. Die nuance mist in het gevraagde gebod. De voorzieningenrechter ziet niet in wel belang eiseres, bovenop het verspreidingsverbod, heeft bij dit verbod. Deze vordering zal worden afgewezen.

Rechtbank Rotterdam, 29 november 2023, ECLI:NL:RBROT:2023:10986
Nationale frequentieplan, frequentieruimte 5G-netwerken, telecomproviders

In deze zaak beoordeelt de rechtbank de beroepen van een aantal telecomproviders en lokale gebruiker tegen de besluiten van de Minister van Economische zaken en Klimaat (hierna: EZK) en Inmarsat Solution B.V. tot wijziging van het Nationaal frequentieplan (NFP). Het EZK heeft plannen om de 3,5 GHz-band aan te passen om de implementatie van snellere 5G-netwerken mogelijk te maken. EZK overweegt een gedeeltelijke vrijmaking van de band tussen 3400 en 3800 MHz voor 5G, ondanks het feit dat eiseressen op dit moment van deze frequenties gebruikmaken. Het EZK streeft ernaar om de onderste en bovenste 50 MHz te reserveren voor lokale gebruikers, terwijl de resterende 300 MHz beschikbaar wordt gesteld voor telecomproviders.
Lokale gebruikers uiten echter ontevredenheid over de beperkte ruimte onder- en bovenaan de frequentieband. Voorts betogen telecomproviders dat lokale gebruikers een te groot deel van de frequentieruimte krijgen. Hun voorkeur gaat uit naar het volledig beschikbaar stellen van de 3,5 GHz-frequentieruimte voor 5G. In deze zaak dient er gekeken te worden of het EZK met haar besluit een doelmatig gebruik van frequentieruimte nastreeft.
De rechtbank kan niet zelf vaststellen of er sprake is van een doelmatig gebruik van frequentieruimte. Het EZK heeft namelijk een ruime beoordelings- en beleidsruimte. Deze ruimte mag niet in strijd zijn met het evenredigheidsbeginsel. De rechtbank is van oordeel dat het EZK zorgvuldig te werk is gegaan bij de voorbereiding van het besluit, waarbij het de nodige adviezen van experts heeft geraadpleegd. Daarbij heeft de Minister volgens de rechtbank haar keuzes en afwegingen voldoende gemotiveerd. De rechtbank oordeelt dat de beroepen van de telecomproviders niet-ontvankelijk zijn, omdat zij niet zijn opgekomen tegen het vorige besluit. Voorts oordeelt de rechtbank dat de beroepen van alle eiseressen tegen besluit 2 ongegrond zijn.

Rechtbank Gelderland, 30 november 2023, ECLI:NL:RBGEL:2023:6486
Voorzieningenrechter, privacyrecht, journalistieke vrijheid

Het CBR is een bestuursorgaan die de rijvaardigheid van personen bevordert. Gedaagden zijn beide autorijschoolhouders. Bij op tegenspraak gewezen vonnis van de voorzieningenrechter van 10 maart 2023 is het aan gedaagden verboden examenritten te volgen of te spotten op een wijze die het normale verkeer frustreert. Sinds september 2023 houden gedaagden zich weer regelmatig op bij het CBR. Gedaagden hebben vervolgens op hun website de namen van medewerkers van het CBR geplaatst. Bij de brief van 9 oktober 2023 is gevraagd de namen van de websites te halen. Gedaagden hebben hier geen gehoor aan gegeven. Het CBR vordert onder andere dat de voorzieningenrechter gedaagden gebiedt om van de websites elke vorm van persoonsgegevens van medewerkers of oud-medewerkers te verwijderen.
Gedaagden voeren verweer en concluderen tot afwijzingen van de vorderingen van CBR. Gedaagden hebben betwist dat zij geen invloed hebben over de content van de websites. Bij de mondelinge behandeling heeft gedaagde erkend dat hij de geplaatste artikelen over het CBR heeft aangeleverd. Voorts wordt er bij de artikelen van de websites naar gedaagden verwezen en geciteerd. Dit verweer houdt dus geen stand.
Voorts stellen gedaagden dat zij als journalist persoonsgegevens van CBR-medewerkers op de website hebben geplaatst om misstanden van het CBR aan de kaak te stellen. Hierbij dient een belangenafweging gemaakt te worden tussen enerzijds het recht op privacy van de medewerkers en anderzijds het algemeen belang om misstanden aan de kaak te stellen. De persoonsgegevens van desbetreffende werknemers van het CBR die op de website zijn geplaatst zijn van personen die hoge functies binnen het CBR vervullen. Journalisten dienen het recht op privacy van personen te respecteren en dat recht mag niet verder worden aangetast dan noodzakelijk is. Zo kon de journalist de persoonsgegevens van de medewerkers achterwege laten, waardoor de misstanden alsnog aan de kaak werden gesteld. Om die reden weegt het recht op eerbiediging van hun persoonlijke levenssfeer zwaarder dan het aan het licht brengen van misstanden.
De voorzieningenrechter gebiedt gedaagden om binnen 24 uur na betekening van dit vonnis de persoonsgegevens van de medewerker te verwijderen. Voorts verbiedt de voorzieningenrechter de gedaagden om rondom het CBR of omgeving van hun woonplaats op te houden.

DECEMBER 2023

Centrale Raad van Beroep, 5 december 2023, ECLI:NL:CRVB:2023:2349
Bijstand, sociaal zekerheidsrecht, internetbankieren

Appellanten hebben bijstand aangevraagd. Het dagelijks bestuur heeft deze buiten behandeling gesteld, omdat niet alle gevraagde informatie is ontvangen. Dit betreft ook bankafschriften van twee Bulgaarse bankrekeningen van appellanten. Appellanten hebben aange-

voerd dat zij niet de beschikking konden krijgen, omdat zij hiervoor fysiek af dienden te reizen naar Bulgarije.
De Raad wijst deze beroepsgrond af en laat de buiten behandelingstelling in stand. Appellanten hebben geen controleerbare bewijsstukken overgelegd waaruit blijkt dat het niet mogelijk is om de benodigde (bank)gegevens in te leveren, zoals een bewijsstuk waaruit blijkt dat zij contact hebben opgenomen met de Bulgaarse bank over de mogelijkheid tot internetbankieren. Dit hadden zij wel kunnen doen, omdat het college erop heeft gewezen dat uit de website van de United Bulgarian Bank blijkt dat internetbankieren wel tot de mogelijkheden behoort.

Hof van Justitie van de Europese Unie, 5 december 2023, gevoegde zaken C-683/21 ECLI:EU:C:2023:949 en C-807/21 - ECLI:EU:C:2023:950
Prejudiciële vragen, AVG, boete

Antwoord op prejudiciële vragen. In deze twee zaken zijn de voorwaarden voor het opleggen van een administratieve boete verduidelijkt en de gezamenlijke verwerkingsverantwoordelijkheid door het Hof van Justitie van de Europese Unie. Het betreft een Litouwse zaak waarin het Nationaal Centrum voor Volksgezondheid een privébedrijf een mobile applicatie heeft laten ontwikkelen en daarvoor een boete heeft ontvangen, vanwege het onrechtmatig registreren en monitoren van gegevens van personen met Covid-19. De Duitse zaak betreft een boete voor het overschrijden van de bewaartermijn van gegevens van huurders.
Het Hof stelt dat de AVG stelt dat er geen boete opgelegd wordt, tenzij er sprake is van een opzettelijke inbreuk of nalatig gedrag. De verwerkingsverantwoordelijke kan worden bestraft wanneer deze niet onkundig kon zijn van het inbreukmakende karakter van zijn gedrag, ongeacht of hij zich ervan bewust was de bepalingen van de AVG te schenden. Ook wordt de boete opgelegd aan de rechtspersoon, het is niet relevant of de gedraging is gepleegd door de managementlaag. Een boete wordt opgelegd aan de verwerkingsverantwoordelijke voor een gedraging van de verwerker, voor zover de verantwoordelijke daar verantwoordelijk voor gehouden kan worden. Indien de ontvanger onderdeel is van een groep bedrijven, wordt berekening van de boete gebaseerd op de omzet van de gehele groep.
Met betrekking tot gezamenlijke verwerkingsverantwoordelijkheid stelt het Hof dat gezamenlijke controle al aanwezig is op het moment dat twee entiteiten het doel en middelen bepalen. Voor gezamenlijke verantwoordelijkheid is het niet vereist dat er een formele overeenkomst is, een gezamenlijke beslissing is voldoende om dat te bewerkstelligen.

Rechtbank Gelderland, 7 december 2023, ECLI:NL:RBGEL:2023:6640
PGP, klacht, Autoriteit Persoonsgegevens

Eiseres verkocht via haar ondernemingen Pretty Good Privacy telefoons (PGP-telefoons). Deze telefoons zijn ook betrokken geweest bij de Ennetcom onderzoeken. Eiseres twijfelt aan de rechtmatigheid van deze onderzoeken. Als gevolg van deze onderzoeken heeft eiseres een klacht ingediend bij de AP met het verzoek handhavend op te treden. De AP heeft dit afgewezen: zij heeft globaal (bureau)onderzoek gedaan en geconcludeerd dat een overtreding door een derde partij niet aannemelijk is.
Eiseres spant een procedure aan bij de rechtbank. Deze wijst de vorderingen af. De rechtbank is, ongeacht de vraag er of vanuit moet worden gegaan dat het een nieuwe technologie betreft – van oordeel dat de Autoriteit Persoonsgegevens kon concluderen dat er geen DPIA uitgevoerd hoefde te voeren. De Autoriteit Persoonsgegevens heeft hierbij terecht in aanmerking genomen dat verwerkingen op grond van de Wpg en de Wjsg altijd worden uitgevoerd in het kader van een opsporings- of onderzoekstaak en dat dergelijke verwerkingen, vanwege het doel en de mogelijke gevolgen van de uitkomst hiervan voor de betrokkenen, per definitie een 'gevoelige' component hebben.
Een dergelijke verwerking betekent niet automatisch dat sprake is van een hoog risico op basis waarvan een DPIA is vereist.

Hof van Justitie, 7 december, HvJ EU zaken C-634/21 en C-26/22 & C-64/22
Prejudiciële vragen, automatische besluitvorming, krediet

Antwoord op prejudiciële vragen inzake het kredietinformatiebureau SCHUFA. SCHUFA verzamelt hoeveelheden persoonlijke gegevens om op basis daarvan de kredietwaardigheid van een persoon vast te stellen. De score wordt door banken en bedrijven gebruikt voor beoordelingen voor bijv. leningen en telefoonabonnementen.
Gegevens van personen worden zowel in het nationale insolventieregister bewaard en door de SCHUFA apart, waarbij SCHUFA een langere termijn hanteert. De vragen zien er o.a. op of nationale rechters beslissingen van toezichthouders in het geheel kunnen herbeoordelen en of de praktijken van het SCHUFA vallen onder "automatische besluitvorming" in de zin van de AVG
Het Hof oordeelt o.a. dat scoring door de SCHUFA valt onder de automatische individuele beslissing van de AVG. De nationale rechter moet beoordelen of dit een geoorloofde uitzondering betreft. Het langer bewaren door de SCHUFA van de kredietgegevens is in strijd met de AVG, mede omdat er het risico is van een negatieve beoordeling van de betrokkene. Betrokkene heeft na het verstrijken van de bewaartermijn in het nationale register recht op verwijdering uit de databases van de SCHUFA. De nationale rechter moet de rechtmatigheid van de parallelle opslag door de SCHUFA beoordelen. Ten slotte dient de nationale rechter volledig de beslissing van de toezichthouder te kunnen reviewen.

Rechtbank Zeeland-West-Brabant, 8 december 2023, ECLI:NL:RBZWB:2023:8581
Strafrecht, opruiing, Social Media.

Dit betreft het onderzoek Coldenhove. Dit onderzoek richt zich op een aantal verdachten die veelvuldig berichten op X (Twitter) en YouTube plaatsen met beschuldigingen jegens anderen van misbruik van (eigen) kinderen en deelname aan een Haags pedofielennetwerk. Dit is gebaseerd op het 'Verhaal van Lisa', de verklaringen van een van de dochters van een van de medever-

dachten. Naast de berichten op internet zijn de slachtoffers ook thuis bedreigd. De rechtbank veroordeelt de verdachte tot een gevangenisstraf van 66 dagen, waarvan 60 voorwaardelijk met een proeftijd van twee jaar. Daarnaast legt zij een contactverbod op met drie slachtoffers en de verdachte mag geen uitspraken over hen doen in het openbaar, waaronder op het internet.
Zie ook:
ECLI:NL:RBZWB:2023:8597
ECLI:NL:RBZWB:2023:8593

Rechtbank Rotterdam, 12 december 2023, ECLI:NL:RBROT:2023:11678
Boete ACM, misleidende informatie, websites

Eiseres ondersteunt bedrijven bij het vinden van nieuwe klanten via internet (leadgeneratie). De ACM heeft geconstateerd dat misleidende en onjuiste informatie is opgenomen op websites waarop diensten van slotenmakers worden aangeboden en die aan eiseres te relateren zijn. Ook wordt bepaalde verplichte informatie niet verstrekt, volgens de ACM. Zij heeft een boete opgelegd. Eiseres heeft bezwaar ingediend hiertegen, maar te laat. De ACM heeft beoordeeld het bezwaar niet-ontvankelijk is verklaard. Eiseres tekent hiertegen beroep aan bij de rechtbank om zich enkel te richten op het persbericht.
De rechtbank oordeelt dat de e-mailberichten die eiseres – hoewel zij niet thuis is in dergelijke procedures - niet aan te merken zijn als beroep. ACM heeft eiseres terecht niet-ontvankelijk verklaard en de ACM hoefde niet meer informatie geven over de resterende overtredingen. Wel had zij haar in de gelegenheid moeten stellen om een zienswijze in te dienen. De rechtbank verklaart het beroep ongegrond.

Rechtbank Noord-Holland, 13 december 2023, ECLI:NL:RBNHO:2023:12695
Fraude, online beleggen, crypto

De zaak draait om online beleggingsfraude (ook wel: boilerroomfraude). Gedaagden bieden zowel E-Moneydiensten als cryptovalutadiensten aan. Eiseres heeft gebruik gemaakt van deze diensten. Via deze diensten is geld overgemaakt naar externe 'wallets' van een derde partij om zo o.a. bitcoins te kunnen kopen. Eiseres is hierbij opgelicht door deze derde partij en eist o.a. een schadevergoeding van gedaagden. De DNB heeft in januari 2023 een boete opgelegd.
Waar gedaagden betwisten dat er sprake is van fraude, stelt de rechtbank vast dat dit het geval is. Daarnaast stelt eiseres dat vanwege het feit dat een DNB-registratie ontbreekt, er sprake is van oneerlijke handelspraktijken. De rechtbank wijst dit af, na uitvoerige overwegingen, omdat de overeenkomst niet het gevolg is van een oneerlijke handelspraktijk. Ook is er geen sprake van een onrechtmatige daad, nu het causaal verband ontbreekt en er geen schending van de zorgplicht is.
De rechtbank wijst de vorderingen af.

Rechtbank Noord-Nederland, 19 december 2023, ECLI:NL:RBNNE:2023:5192
Vrijheid van meningsuiting, uitlatingen, boek

Eiseres is een stichting die een belangrijke schakel is in het bepalen van (jeugd-)hulp voor kwetsbare mensen en gezinnen. Gedaagde is de ouder van een minderjarige wiens jeugdproblematiek via de stichting is verlopen. Gedaagde heeft verschillende e-mailberichten aan een medewerker die betrokken was bij de hulpverlening verzonden met verschillende beschuldigingen. Daarnaast heeft de gedaagde een boek geschreven over haar traject met verschillende beschuldigingen jegens de hulpverlener. De stichting vordert o.a. dat gedaagde geen contact opneemt met de medewerker en het boek uit de handel te halen (evenals de promotie te staken). De rechter wijst de vorderingen toe, nu deze geen steun vinden in de feiten.

Raad van State, 20 december 2023, ECLI:NL:RVS:2023:4752
Herleidbaarheid, persoonsgegevens, Wob-verzoek

Achmea wil middels verschillende Wob-verzoeken MV- en V-log-bestanden ontvangen die informatie geven over verkeerslichtinstallatie. Als deze bestanden in een daarvoor bestemd programma worden ingelezen, verschijnt er een beeld met verschillende kleuren, die zijn gekoppeld aan een nummer. Op deze manier wordt aan de hand van verkeersstromen bepaald op welk moment en hoe lang verkeerslichten groen of rood licht krijgen. Ook kan bij ongelukken worden nagegaan wat de status van de verkeerslichten was. Achmea wil deze ontvangen om te achterhalen of een van de betrokken partijen bij een verkeersongeval door rood licht is gereden.
Het college heeft besloten deze niet vrij te geven, omdat de openbaarmaking niet opweegt tegen het belang van de opsporing en vervolging van strafbare feiten en tegen de eerbiediging van de persoonlijke levenssfeer. Door het combineren van de gegevens (o.a. door software op internet) kan de identiteit van weggebruikers worden achterhaald. Achmea gaat tegen dit besluit in hoger beroep.
De Afdeling oordeelt dat, in combinatie met andere gegevens, de gegevens zijn te herleiden tot een persoon en dus wel persoonsgegevens zijn. De Afdeling acht aannemelijk dat Achmea zorgvuldig met de gegevens om zal gaan, maar het is niet uitgesloten dat anderen de gegevens op onzorgvuldige wijze zullen gebruiken en daarmee de persoonlijke levenssfeer niet eerbiedigen. Als de wetgever meent dat verzekeraars voor het oplossen van een verzekeringsgeschil dit soort gegevens in moeten kunnen zien, moet hij daarvoor een wettelijke basis bieden. De Afdeling honoreert het hoger beroep en zal het beroep van Achmea tegen het besluit van het college ongegrond verklaren.

Rechtbank Midden-Nederland, 20 december 2023, ECLI:NL:RBMNE:2023:6933
Strafrecht, oplichting platform

Verdachten (zie hieronder voor gerelateerde zaken) hebben via Marktplaats en soortgelijke verkoopplatformen doelbewust (veelal oudere) slachtoffers benaderd. Zij wilden – en hebben – zich via verschillende oplichtingstactieken toegang verschaft tot hun internetbankieren en geld overgeschreven naar de eigen bankrekening. Deze omvatten de 1 cent-methode en het afstaan van verificatiecodes.

Verdachten wisten slachtoffers tussen de 350 en bijna 10.000 Euro per keer afhandig te maken, waarbij dit een groot aantal aangevers en benadeelden omvatte (minimaal 18 personen).
Mede gelet op zijn rol in het geheel is verdachte veroordeeld tot een gevangenisstraf van 12 maanden.
Zie ook:
ECLI:NL:RBMNE:2023:6878
ECLI:NL:RBMNE:2023:6890

Rechtbank Amsterdam, 21 december 2023, ECLI:NL:RBAMS:2023:8234
Strafrecht, social media, afpersing

Verlening van verlof tot tenuitvoerlegging in Nederland van gevangenisstraf in Canada. Veroordeelde is in Canada veroordeeld tot een gevangenisstraf van dertien jaar, omdat hij tussen 2009 en 2012 een toentertijd twaalfjarig slachtoffer heeft afgeperst op verschillende social mediaplatforms en haar verleidde tot het uitvoeren van pornografische webcamshots voor hem.
De rechtbank heeft de Canadese straf omgezet naar Nederlandse maatstaven en een gevangenisstraf van zes jaar opgelegd.
De rechtbank heeft daarbij naar aanleiding van een verweer van de raadslieden onder meer geoordeeld dat artikel 63 van het Wetboek van Strafrecht niet van toepassing is in deze procedure nu zij niet komt tot een "schuldigverklaring aan een misdrijf of overtreding" in de zin van die bepaling, maar tot een omzetting van de Canadese straf naar een Nederlandse straf.

Gerechtshof Den Haag, 27 december 2023, ECLI:NL:GHDHA:2023:2638
Social Media, bedreiging, strafrecht

Verdachte heeft in de Coronaperiode een tweet geplaatst waarin hij dreigt om twee politici te vermoorden en vervolgens te begraven. In eerste aanleg is verdachte daarvoor veroordeeld. Dit is het hoger beroep. Het gerechtshof neemt in overweging dat deze tweet is geplaatst in de Coronaperiode, hij meer dan 17.000 volgers had op Twitter (nu X), de tweet een half uur voor de persconferentie is verzonden en de tweet gezien de inhoud niet anders kan zijn gericht dan op de dood van de twee politici. Dat het bericht na 20 minuten is verwijderd maakt dat niet anders.
Het gerechtshof komt tot een bewezenverklaring, legt deels voorwaardelijke gevangenisstraf op en een dadelijk uitvoerbare vrijheidsbeperkende maatregel ex artikel 38v Sr.

Wet- en regelgeving

mr. J.J.H. Vos

NL

Wetsvoorstel Wet digitale algemene vergadering privaatrechtelijke rechtspersonen

Op 11 januari 2024 is het wetsvoorstel tot wijziging van Boek 2 en 5 BW en enige andere wetten in met het oog op het aanpassen van de regels inzake de digitale algemene vergadering van rechtspersonen en de regels voor digitale oproeping voor de algemene vergadering gepubliceerd. Het doel van dit wetsvoorstel is om het gebruik van elektronische communicatiemiddelen bij algemene vergaderingen van privaatrechtelijke rechtspersonen te faciliteren en te normeren. Dit doel wordt bereikt aan de hand van drie maatregelen. Allereerst voorziet het wetsvoorstel in een aantal wijzigingen om de volledige digitale algemene vergadering te faciliteren voor NV's, BV's, verenigingen (van eigenaars), coöperaties en onderlinge waarborgmaatschappijen. Deze wijziging zal dan bestaan naast de al bestaande mogelijkheid van een gedeeltelijk digitale algemene vergadering. Ten tweede stelt het voorstel nadere voorwaarden aan het gebruik van elektronische communicatiemiddelen bij de algemene vergadering, zodat een digitale vergadering zoveel mogelijk een afspiegeling vormt van een fysieke vergadering en dat deelnemers ook langs digitale weg daarin volwaardig kunnen participeren. Ten derde worden de regels voor oproeping voor de algemene vergadering aangepast, zodat oproeping langs elektronische weg vereenvoudigd wordt.

Bron:
https://www.eerstekamer.nl/wetsvoorstel/36489_wet_digitale_algemene

Wetsvoorstel Implementatiewet digitale operationele weerbaarheid

Op 14 december 2023 is het wetsvoorstel tot wijziging van de Wet op het financieel toezicht (Wft) ter implementatie van Richtlijn (EU) 2022/2556 betreffende een kader voor digitale operationele weerbaarheid van de financiële sector gepubliceerd. Het wetsvoorstel voorziet in noodzakelijke wijzigingen in de Wft voor de implementatie van Richtlijn 2022/2556. Die richtlijn vormt samen met Verordening (EU) 2022/2554 betreffende digitale operationele weerbaarheid voor de financiële sector een gezamenlijk kader ter verbetering van de digitale operationele weerbaarheid voor de financiële sector. De wijzigingen die worden doorgevoerd in de Wft zijn erop gericht dat duidelijk is dat voor de ondernemingen waar reeds ICT-eisen voor bestonden, zich nu aan de in de verordening gestelde eisen moeten houden, waarin één uniform kader is vastgesteld. Voor enkele richtlijnen zijn ook wijzigingen op besluitniveau nodig. De richtlijn dient op 17 januari 2025 te zijn geïmplementeerd.

Bron:
https://www.eerstekamer.nl/wetsvoorstel/36482_implementatiewet_digitale

Signaleringen

mr. P.G. van der Putt

Apple doet toezeggingen aan EU: gratis NFC toegang voor derden

De Europese Commissie onderzocht de dominante positie van Apple in de markt voor mobiele portemonnees. Met name de beperkte toegang voor derden tot de NFC-technologie van Apple was een doorn in het oog. Apple heeft toezeggingen gedaan om concurrentieproblemen aan te pakken, waaronder gratis toegang voor derden tot NFC's. Ook extra functies, een geschillenbeslechtingsmechanismes en eerlijke criteria maken deel uit van de voorgestelde maatregelen. De toezeggingen zouden tien jaar gelden en worden gecontroleerd door een toezichthouder. Belanghebbenden worden door de Commissie uitgenodigd om hun mening te geven.
https://ec.europa.eu/commission/presscorner/detail/en/ip_24_282

Creditcardbedrijf ICS krijgt boete na ontbrekende risicoanalyse

De Autoriteit Persoonsgegevens (AP) heeft International Card Services B.V. (ICS) een boete opgelegd van 150.000 euro. ICS had nagelaten om een data protection impact assessment (DPIA) uit te voeren. ICS begon in 2019 met het digitaal identificeren van zo een 1,5 miljoen klanten in Nederland. In dat kader was het ICS toegestaan om gegevens van haar klanten op te vragen. Echter is een DPIA verplicht bij dit soort verwerkingen die een hoog privacyrisico opleveren. Op basis van de uitkomsten van een DPIA kunnen van te voren maatregelen worden genomen om de privacy te beschermen.
https://www.autoriteitpersoonsgegevens.nl/actueel/boete-voor-creditcardbedrijf-ics-na-ontbrekende-risicoanalyse

Europese Commissie vervolgt platform op grond van de DSA

De Europese Commissie start een formele inbreukprocedure tegen X, op basis van de Digital Services Act (DSA). Het onderzoek richt zich op de naleving van verplichtingen die voortvloeien uit de DSA en specifiek van toepassing zijn op zeer grote online platformen. X moet sinds augustus 2023 als zeer groot online platform voldoen aan de DSA verplichtingen. Er wordt onder andere beken of X voldoende doet om illegale inhoud tegen te gaan en manipulatie van informatie te bestrijden op het platform. Daarnaast wordt er beoordeeld of X voldoende transparant is en ook het ontwerp van de gebruikersinterfaces met betrekking tot de blauwe vinkjes wordt onderzocht op mogelijke misleiding. Als inbreuk wordt bewezen kan de Commissie handhavingsmaatregelen nemen. Dit markeert de eerste formele DSA-handhaving. Hoe lang dit onderzoek gaat duren is nog onzeker.
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709

The New York Times klaagt OpenAI aan voor auteursrechtinbreuk

The New York Times heeft OpenAI en Microsoft aangeklaagd wegens vermeende auteursrechtinbreuk. De krant is van mening dat miljoenen artikelen zonder toestemming van The New York Times zijn gebruikt om geautomatiseerde chatbots te trainen. Er wordt gesteld dat de gedaagden verantwoordelijk moeten worden gehouden voor de schade in verband met het onrechtmatig kopiëren en gebruiken van de werken van The New York Times. Bovendien wordt er geëist dat OpenAI en Microsoft alle chatbotmodellen en trainingsgegevens vernietigen waarin auteursrechtelijk beschermd werk van The New York Times is gebruikt. In april vorig jaar heeft The New York Times zowel OpenAI als Microsoft benaderd voor een mogelijke schikking. Deze gesprekken hebben niet tot een oplossing geleid.
https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

De Eerste Kamer krijgt vaste commissie Digitalisering

Op 16 januari 2024 heeft de Eerste Kamer gestemd over de instelling van een vaste commissie Digitalisering. Deze beslissing volgde op een brief van de leden Veldhoen, Panman, Prins, Belhirch en Perin-Gopie. Het voorstel werd ingediend naar aanleiding van een onderzoek dat was uitgevoerd door een werkgroep en het Rathenau Instituut. Het onderzoek richtte zich op het versterken van de kennis van Eerste Kamerleden met betrekking tot digitalisering, met als specifiek doel meer inzicht te krijgen in algoritmische besluitvorming bij de overheid. De oprichting van de commissie is bedoeld om de kennis over digitalisering te vergroten, met een bijzondere focus op begrip en omgang met algoritmes. Het voorstel is met instemming van de senaat aangenomen. Hierdoor krijgt de Eerste Kamer, net als de Tweede Kamer, nu ook een aparte commissie Digitalisering.

https://www.eerstekamer.nl/verslag/20240116/verslag

HelloFresh moet voortaan duidelijke communiceren over inhoud en voorwaarden abonnement

De Autoriteit Consument & Markt (ACM) heeft HelloFresh aangesproken op het duidelijker communiceren over de inhoud en voorwaarden van abonnementen naar consumenten toe. De ACM had klachten ontvangen van consumenten die onbedoeld een abonnement hadden afgesloten bij HelloFresh. Bovendien waren veel consumenten ontevreden over de afhandeling van klachten door HelloFresh. De ACM heeft HelloFresh hierop aangesproken en het bedrijf heeft haar procedures aangepast en informeert nu duidelijker over de abonnementsvoorwaarden bij het bestelproces. Daarnaast heeft het bedrijf veranderingen doorgevoerd in de omgang met klachten over niet ontvangen maaltijdboxen en ontbrekende producten. Consumenten krijgen nu hun geld terug als een product niet geleverd is, vervangen of hersteld kan worden in plaats van dat het alleen een tegoed krijgt. De ACM blijft HelloFresh volgen om te kijken of het bedrijf de afgesproken aanpassingen daadwerkelijk uitvoert.
https://www.acm.nl/nl/publicaties/hellofresh-informeert-voortaan-duidelijker-over-inhoud-en-voorwaarden-abonnement

Keuze tussen gratis of betaalde accounts op Meta zijn misleidend en agressief

Europese consumentenorganisaties, waaronder de Consumentenbond, hebben een klacht ingediend bij de Consumer Protection Cooperation met betrekking tot Meta. Meta dwingt gebruikers van Facebook en Instagram een keuze te maken tussen een betaalde of een gratis variant. Bij de betaalde optie worden persoonlijke advertenties uitgeschakeld, terwijl bij de gratis variant gebruikers akkoord gaan met gegevensverwerking. Dit zorgt voor onder andere misleiding, omdat de zogenaamde gratis opties in feite afbetaald wordt door het verstrekken van persoonsgegevens. Deze vorm van gegevensverwerking is ook een vorm van betaling. Bovendien worden de gegevens van degene die wel betalen voor de app alsnog gebruikt. Sandra Molenaar, directeur Consumentenbond, vindt een dergelijk aanbod aan gebruikers van Meta agressief en oneerlijk. Consumenten voelen zich gedwongen om een keuze te maken die ze eigenlijk niet willen maken. Bovendien is er niet echt een alternatieve app omdat Facebook en Instagram ontzettend dominant zijn. Hierdoor hebben consumenten geen keuze en zorgt dit voor een oneerlijke keuze.
https://www.consumentenbond.nl/nieuws/2023/metas-keuze-voor-gratis-of-betaalde-variant-misleidend-en-agressief

Generative AI in Nederland: visie, uitdagingen en actieplan van het Kabinet

Het Nederlandse kabinet heeft als een van de eerste EU-lidstaten een visie op generatieve AI gepresenteerd. Generatieve AI is een specifieke vorm van kunstmatige intelligentie. Het helpt mensen bij het genereren van onder andere tekst, computercode, beeld en audio. Volgens het kabinet biedt generative AI kansen en mogelijkheden en het zal grote impact hebben op economie en maatschappij. Tegelijkertijd zitten er ook risico's aan, waaronder de mogelijke aantasting van informatieverstrekking en de impact op de democratie. Het kabinet formuleert vier centrale uitgangspunten voor generatieve AI: veilige ontwikkeling, rechtvaardige toepassing, dienstbaarheid aan menselijk welzijn en autonomie en bijdrage aan duurzaamheid en welvaart. Om deze visie in actie om te zetten, introduceert het kabinet zes actielijnen. Deze omvatten samenwerking met belanghebbenden, nauwgezet volgen van AI-ontwikkelingen, ontwikkelen van wet- en regelgeving, vergroten van kennis en vaardigheden, experimenteren met generatieve AI door de overheid en sterk toezicht op AI met handhaving indien nodig. Hiermee hoopt het kabinet Nederland voorop te laten lopen in de onvermijdelijke veranderingen die generatieve AI in onze samenleving teweeg zal brengen.
https://www.rijksoverheid.nl/actueel/nieuws/2024/01/18/kabinet-presenteert-visie-op-generatieve-ai

Amerikaanse staat Montana mag TikTok voorlopig niet verbieden

De Amerikaanse staat Montana mag van de federale rechter TikTok voorlopig niet verbieden. Het gaat tegen de vrijheid van meningsuiting van gebruikers in om de app te verbieden. De staat wilde de app te verbieden om te voorkomen dat gevoelige data van Amerikanen in handen vallen van China. Het moederbedrijf van TikTok is ByeteDance, een Chinees bedrijf. TikTok ontkent dat data van gebruikers in handen van de Chinese overheid kan komen.
https://storage.courtlistener.com/recap/gov.uscourts.mtd.73544/gov.uscourts.mtd.73544.115.0_1.pdf

Nederland staakt tijdelijk de omstreden sleepnetmethode

De Nederlandse overheid staakt tijdelijk het gebruik van de omstreden sleepnetmethode waarmee sociaaleconomische zwakkere wijken worden onderzocht. De methode, bekend als de LSI-methode, heeft tot doel de leefbaarheid in buurten te verbeteren door risicosignalen te delen en 'verwonderadressen' te identificeren voor mogelijke controles. Volgens Follow the Money zijn er geen nieuwe projecten gestart in 2023, en lopende trajecten zijn afgerond of vroegtijdig beëindigd. Het ministerie van Sociale Zaken en Werkgelegenheid wacht op de resultaten van een DPIA voordat nieuwe projecten worden gestart. Een dergelijke analyse is verplicht als de overheid persoonsgegevens van burgers verwerkt en er grote privacyrisico's zijn.

https://www.ftm.nl/artikelen/controversiele-sleepnetmethode-om-fraude-in-arme-wijken-op-te-sporen-voorlopig-stopgezet#popup-form