Prof. mr. C.D.J. Bulten, prof. dr. B.P.F. Jacobs & prof. mr. C.J.H. Jansen[1]

Cybersecurity: Chefsache?!

Ondernemingsrecht 2021/79

De Cyber Security Raad (CSR) publiceerde op 6 mei 2021 een alarmerend advies aan de Nederlandse regering, getiteld 'Nederlandse Digitale Autonomie en Cybersecurity'. De CSR wees op drie acute gevaren: het verder toenemen van cyberbedreigingen, een te grote afhankelijkheid van de Nederlandse economie van China en de Verenigde Staten op het gebied van digitale technologieën ('techkolonialisme') en de te grote afhankelijkheid van Nederlandse bedrijven van buitenlandse techbedrijven (zoals Microsoft, Google, Apple en IBM) wat betreft de afname van digitale diensten en de opslag van data. Digitale autonomie, de strategische autonomie in het digitale domein, staat volgens de CSR onvoldoende op de agenda van de politiek, de wetenschap en het bedrijfsleven. DNB, de AFM en de Europese Unie onderschrijven de oproep van de CSR tot continue aandacht voor de vergroting van de cyberweerbaarheid van (financiële) ondernemingen. Cyberbedreigingen via digitale communicatienetwerken nemen namelijk toe. Zij raken bedrijven hard en kunnen resulteren in grote schade. Zonder een betrouwbare digitale infrastructuur dreigt het risico van bedrijfsstilstand. De auteurs onderzoeken naar aanleiding van het advies van de CSR de vraag wat de taak van het bestuur en de RvC van vennootschappen op het gebied van cybersecurity moet zijn, mede in het licht van de toenemende zorg om digitale autonomie. Een van hun conclusies is dat de verantwoordelijkheid voor digitale autonomie 'Chefsache' (zaak van de CEO) is.

1. Inleiding

De 'machine' versterkt sinds de 19e eeuw de menselijke werkkracht, als '*force multiplier*'. In de huidige tijd versterkt zij ook de menselijke denkkracht. Veel ondernemingen, niet alleen financiële, hebben een digitale transformatie doorgemaakt. Internet maakt onlosmakelijk deel uit van het dagelijkse functioneren van Nederlandse bedrijven en instellingen. Het verwerken van (digitale) persoonsgegevens is voor veel organisaties een essentieel onderdeel van hun activiteiten. Zij kunnen niet meer zonder ICT. Dit geldt niet alleen voor financiële instellingen. Maersk, bekend als containervervoerder, is tegenwoordig bijvoorbeeld meer een techbedrijf met schepen dan een rederij.[2] Een bank is eigenlijk geen bank meer, maar een informatieverwerker die ook bankproducten verkoopt.[3] Een van de grootste uitdagingen voor bestuurders en commissarissen is het realiseren van een optimale beveiliging van hun digitale infrastructuur en van de gegevens die zij daarmee verwerken. Op het gebied van digitale veiligheid bestaan er drie basisprincipes: integriteit, vertrouwelijkheid en beschikbaarheid.[4] Helaas staan deze principes steeds meer onder druk door cyberbedreigingen, van zowel criminele als statelijke actoren. Er gaat bijna geen dag voorbij of de media berichten over verminderde beschikbaarheid, verlies aan vertrouwelijkheid of het niet langer betrouwbaar zijn van gegevens door uit onzorgvuldig gedrag ontstane datalekken, bewuste hacks, sabotage of diefstal (denk aan ransomware). Digitale spionage en afpersing zijn volwassen vormen van criminaliteit geworden, met een voor criminelen aantrekkelijke verhouding tussen mogelijke opbrengst en pakkans. De coronaepidemie heeft het belang van digitale transacties voor ondernemingen versterkt, waarbij zekerheid nodig is bij authenticatie (met wie heb ik van doen), bij digitale ondertekening, en bij online overleg en besluitvorming, bijvoorbeeld in vergaderingen van directie, RvC of aandeelhouders.

De Cyber Security Raad (CSR)[5] publiceerde onlangs een alarmerend advies aan de Nederlandse regering, getiteld 'Nederlandse Digitale Autonomie en Cybersecurity' (6 mei 2021), dat leidde tot flinke koppen in Nederlandse kranten. *Het Financieele Dagblad* schreef bijvoorbeeld op 14 mei 2021 op de voorpagina 'Nederland verliest controle op beveiliging van het internet'. De CSR wees op drie acute gevaren: het verder toenemen van cyberbedreigingen, een te grote afhankelijkheid van de Nederlandse economie van China en de Verenigde Staten op het gebied van digitale technologieën ('techkolonialisme') en de te grote afhankelijkheid van Nederlandse bedrijven van buitenlandse techbedrijven (zoals Microsoft, Google, Apple en IBM) wat betreft de afname van digitale diensten en de opslag van data. De CSR constateert voorts dat de aanpak van cybersecurity vooral technisch en reactief van aard is geweest en nauwelijks nog geschiedt vanuit het bredere perspectief van strategische autonomie, dat wil zeggen het vermogen en de middelen om beslissingen te kunnen nemen en uit te voeren aangaande essentiële aspecten

1 Claartje Bulten is hoogleraar Ondernemingsrecht, Bart Jacobs hoogleraar Computerbeveiliging en Corjo Jansen hoogleraar Rechtsgeschiedenis & Burgerlijk recht aan de Radboud Universiteit Nijmegen.

2 *Het Financieele Dagblad* 27 mei 2021, p. 18-19.

3 Zie bijv. ING Group, *Annual Report 2020*, p. 11: '(…) we made further progress towards our strategic ambition to become a data-driven digital leader.', https://www.ing.com/Investor-relations/Shareholders-meeting/Annual-General-Meeting.htm.

4 CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie? (CSR Advies 2021, nr. 3), p. 5. Volgens de CSR ook wel genoemd de CIA van cybersecurity: Confidentiality, Integrity, Availability.

5 Zie www.cybersecurityraad.nl. Deze Raad met een publieke, private en wetenschappelijke samenstelling adviseert het kabinet over cyberveiligheid. Een van de auteurs (BJ) is lid van de raad.

van de langetermijn-toekomst in economie, maatschappij en rechtsstaat. Digitale autonomie, de strategische autonomie in het digitale domein, staat onvoldoende op de politieke agenda en 'overwegingen van digitale economie' worden 'niet structureel meegenomen bij het opstellen van beleid en wetgeving'.[6] Volgens de CSR is een aantal acties op korte termijn noodzakelijk. Een daarvan is: 'Verhoog bewustwording van het belang van strategische autonomie in cybersecurity'. Hij zegt hierover:

> "Het belang van strategische autonomie in cybersecurity is tot nog toe onvoldoende onderkend op alle relevante niveaus van de Nederlandse overheid, politiek, bedrijfsleven en wetenschap, maar ook bij onze belangrijkste partners in de EU. Digitale autonomie begint met kennis en begrip zodat alle partijen acties kunnen ondernemen om de digitale gevaren te elimineren of te minimaliseren."[7]

De voorzitter van de Europese Commissie, Ursula von der Leyen, heeft sinds haar aantreden het belang van Europese soevereiniteit en digitale autonomie benadrukt, bijvoorbeeld in haar eerste grote rede voor het Europese parlement in november 2019.[8] Deze nadruk is voortgekomen uit ontwikkelingen op het gebied van 5G, quantumtechnologie, cloudopslag en clouddiensten en is versterkt door gebleken corona-afhankelijkheden (mondkapjes, medicijnen, vaccins) en door de bestaande geopolitieke instabiliteit.

Vijf jaar geleden, in 2016, vroegen twee van ons – mede naar aanleiding van een door de CSR in 2015 uitgebrachte 'Cybersecurity guide for boardroom members' – in dit tijdschrift om aandacht voor en bewustwording bij bestuurders en commissarissen voor vraagstukken van cyberveiligheid.[9] In deze bijdrage doen wij dat opnieuw, omdat cyberdreigingen via digitale communicatienetwerken toenemen. Zij raken bedrijven en instellingen steeds harder en (kunnen) resulteren in grote schade. Digitale autonomie is de verantwoordelijkheid van de overheid, de private sector én de kennisinstellingen.[10] Deze drie partijen moeten samenwerken op basis van het besef van nut en noodzaak van digitale autonomie voor het Nederlandse kennis-ecosysteem. Digitale autonomie raakt ondernemingen in de kern van hun functioneren en in de kern van hun concurrentievermogen. Hun bedrijfsvoering is afhankelijk van de integriteit, vertrouwelijkheid en beschikbaarheid van hun digitale infrastructuur. Zonder betrouwbare digitale infrastructuur dreigt het risico van bedrijfsstilstand, (digitale) afhankelijkheid van (onbetrouwbare) partijen, reputatieschade, spionage, e.d. Dat dit laatste risico reëel is, blijkt uit recente berichtgeving over KPN en Huawei. Op de NOS-website valt te lezen dat het Chinese technologiebedrijf Huawei in het verleden vrije toegang had tot het mobiele netwerk van KPN en alle telefoongesprekken (onder meer van de toenmalige minister-president) kon afluisteren. Een van de conclusies van het onlangs pas bekend geworden rapport waarop de NOS zijn berichtgeving baseerde, was: 'Het voortbestaan van KPN Mobiel is ernstig in gevaar.'[11] De AIVD en MIVD wijzen regelmatig op de omvang van digitale spionage en op de daaruit voortvloeiende aantasting van het Nederlandse verdienvermogen.[12] Digitale autonomie raakt bovendien juridische kwesties als mogelijke buitenlandse overnames van voor Nederland vitale vennootschappen, de diefstal en bescherming van intellectueel eigendom en de (on)mogelijkheid om een cyberverzekering af te sluiten.

2. De taak van het bestuur en de raad van commissarissen (RvC) op het gebied van cybersecurity

Het bestuur is belast met het besturen van de vennootschap. Onder besturen begrijpt de wet (voor beursgenoteerde bedrijven) in ieder geval het bepalen van het beleid en de strategie van de vennootschap.[13] Het dient deze taak in het belang van de vennootschap en de met haar verbonden onderneming op zorgvuldige en behoorlijke wijze te vervullen. Risicobeheersing is een taak die van wezenlijk belang is voor het bestuur van de vennootschap. Risico's op het gebied van cybersecurity maken daar een steeds groter deel van uit. Het bestuur is verantwoordelijk voor het identificeren en beheersen van deze risico's.[14] De RvC heeft naast zijn werkgeversfunctie tot taak toezicht te houden op het beleid van het bestuur en de algemene gang van zaken in de vennootschap en de met haar verbonden onderneming (toezichtfunctie) en het bestuur bij de vervulling van zijn functie met raad ter zijde te staan

6 CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity', p. 5 (definitie strategische autonomie), p. 7. Zie over digitale autonomie: L. Moerel & P. Timmers, *Reflecties over digitale soevereiniteit*, Preadvies Staatsrechtconferentie 2020; en L. Faesen, T. van Schie, M. Rademaker, P. Timmers & M. Veenendaal, *Soevereiniteit en Digitale Autonomie* (februari 2012).

7 CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity', p. 12.

8 Zie https://ec.europa.eu/info/sites/info/files/president-elect-speech-original_en.pdf, en daarin bijvoorbeeld: '(…) we must have mastery and ownership of key technologies in Europe'.

9 Zie eerder: J.A.M. Hermans, 'Cyber Security: een relevant onderwerp voor iedere bestuurder', in: M. Lückerath, B. Bier, H. van Ees & M. Kaptein (red.), *Jaarboek Corporate Governance 2014-2015*, Deventer: Kluwer 2014, p. 233 e.v. Zie ook C.D.J. Bulten & C.J.H. Jansen, 'De taak van de commissaris in een digitale wereld: de noodzaak van awareness van cyber security', *Ondernemingsrecht* 2016/74.

10 Op 6 april 2021 publiceerde de CSR het Adviesrapport 'Integrale Aanpak voor Cyberweerbaarheid' (CSR Advies 2021, nr. 2).

11 'Huawei kon gesprekken KPN-klanten afluisteren', bericht op NOS-website, zaterdag 17 april 2021, gebaseerd op berichtgeving in *de Volkskrant* op basis van een geheim rapport van Capgemini uit 2010.

12 Zie recent 'Veiligheidsdiensten slaan alarm om Chinese cyberdreiging in Nederland', *Het Financieele Dagblad* 10 februari 2021. En: 'De Chinese staat is iedere dag bezig om Nederlandse bedrijven aan te vallen', aldus de directeur van de MIVD generaal-majoor Swillens, *Het Financieele Dagblad* 11 februari 2021.

13 Zie het sinds 1 mei 2021 uitgebreide art. 2:129 lid 1 BW.

14 Art. 2:8 BW, art. 2:9 BW en art. 2:129/239 lid 5 BW. Zie *Asser/Van Solinge & Nieuwe Weme 2-IIb, NV en BV. Corporate Governance*, Deventer: Wolters Kluwer 2019/121 en 141 (onder a en c).

(adviesfunctie).[15] Het toezicht omvat mede de risico's die zijn verbonden aan de activiteiten van de onderneming en de naleving van wet- en regelgeving.[16] Op het gebied van de interne risicobeheersings- en controlesystemen van de vennootschap bereidt de (eventueel ingestelde) auditcommissie de besluitvorming van de RvC voor. Zij behoort zich – volgens best-practice-bepaling 1.5.1 van de Nederlandse Corporate Governance Code 2016 – te richten op het toezicht op het bestuur ten aanzien van: 'iii. de toepassing van informatie- en communicatietechnologie door de vennootschap, waaronder risico's op het gebied van cybersecurity'. Deze bepaling richt zich primair op de Nederlandse beursfondsen als adressanten van de Corporate Governance Code 2016. Bestuur en RvC van niet-beursgenoteerde bedrijven kennen volgens ons eenzelfde taakopdracht ten aanzien van cybersecurity. Cybersecurity is immers niet beperkt tot beursgenoteerde bedrijven, maar raakt in potentie ieder bedrijf met een internetverbinding. Zoals wij hierboven al opmerkten, vallen de implementatie en het onderhoud van adequate risicobeheersings- en controlesystemen binnen de bestuurstaak. Dit staat expliciet in best-practice-bepaling 1.2.2 van de Code 2016.[17] De specifieke risicofunctie op het terrein van cybersecurity moet hieronder begrepen worden. De praktijk herkent dit als de *second line of defence*, waarin de specifieke risicofuncties de eerste laag (kortgezegd: het management) ondersteunen met coördinatie en het goede gebruik van de systemen.[18] Dat voor een vennootschap een adequaat risicobeheersings- en controlesysteem leidt tot betere digitale veiligheid en cybersecurity lijkt een overbodige constatering, maar het is niettemin goed de aandacht hierop te vestigen.

De noodzaak van een (pro)actief beleid op het gebied van digitalisering (zonder welke een bedrijf in deze moderne communicatiemaatschappij niet overleeft) en cyberweerbaarheid heeft geleid tot een verzwaring van de zorgplicht van de bestuurders en de commissarissen, mede vanwege het belang van ICT voor het functioneren van de meeste ondernemingen. Een zorgvuldig handelend bestuur moet een weldoordachte strategie hebben ontwikkeld op het gebied van *cybersecurity* om schade te voorkomen door schendingen van de integriteit, vertrouwelijkheid of beschikbaarheid van data en andere vormen van misbruik.[19] Bovendien moet die strategie via regelmatige oefeningen getest worden en zo nodig aan veranderde omstandigheden worden aangepast. Een behoorlijke taakvervulling brengt ook met zich dat het bestuur dit beleid – gelet op de snelle ontwikkelingen op digitaal gebied – regelmatig monitort en aanscherpt. Het moet aangesloten zijn op (sectorale) knooppunten voor informatieuitwisseling en meldingen en voldoende capaciteit georganiseerd hebben om adequaat op meldingen te kunnen reageren. Een bijkomend risico voor bestuurders (en commissarissen) van bedrijven is de steeds groter wordende afhankelijkheid van hun bedrijf van de digitale infrastructuur die in handen is van een beperkt aantal vooral Amerikaanse bedrijven (zoals Microsoft, Apple, IBM en Google). De afhankelijkheid van de *cloud* in de bedrijfsvoering van veel bedrijven en instellingen kan leiden tot aansprakelijkheden, omdat buitenlandse bedrijven onderworpen zijn aan, en eigen regels gebruiken op het gebied van, privacy, afgifte van data en gegevensbeheer.[20]

Wij wijzen erop dat de verwezenlijking van digitale weerbaarheid raakvlakken heeft met een brede discussie die in 2020 en 2021 al het nodige stof heeft doen opwaaien in ondernemingsrechtelijk Nederland: het pleidooi voor de invoering van een zorgplicht voor bestuurders en commissarissen van Nederlandse kapitaalvennootschappen op het gebied van het maatschappelijk verantwoord ondernemen. Digitale autonomie, zorg om cyberveiligheid en privacy raken de *governance* van bedrijven en instellingen, net zoals transparante verslaglegging en diversiteit in de samenstelling van raden van bestuur en commissarissen. Zij bepalen mede wat een onderneming in de Nederlandse (en Europese) samenleving kan en wil bereiken en zij betreffen de impact en de reputatie van een bedrijf in de samenleving. Zij zijn tevens relevant voor de langetermijnwaardecreatie waarop het bestuur van een beursvennootschap zich moet richten (*good governance* of goed bestuur).[21] Moerel schrijft in haar Preadvies uit 2019 dat de impact van digitale innovaties op privacy moet worden beoordeeld vanuit risico's voor individuen en daarmee de

15 Art. 2:140/250 lid 2 BW. Gemakshalve laten wij het onderscheid one-tier- en two-tier-board buiten beschouwing. Het moge duidelijk zijn dat hetgeen wij schrijven voor bestuur en RvC, mutatis mutandis geldt voor de bestuurders van een one-tier-board. Over de verschillen (in het algemeen) tussen de RvC en de niet-uitvoerende bestuurders verwijzen wij naar N. Kreileman, *De niet-uitvoerende bestuurder in een one tier board* (diss. RU) (Serie VHI deel 168), Deventer: Kluwer 2020.

16 *Asser/Van Solinge & Nieuwe Weme 2-IIb* 2019/289 (onder b).

17 Principe 1.2 Code 2016 luidt: 'De vennootschap beschikt over adequate interne risicobeheersings- en controlesystemen. Het bestuur is verantwoordelijk voor het identificeren en beheersen van de risico's verbonden aan de strategie en de activiteiten van de vennootschap.' Zie ook *Asser/Van Solinge & Nieuwe Weme 2-IIb* 2019/141 onder a.

18 Zie DBBW, *Corporate Governance in Nederland, Een praktische handleiding bij de nieuwe Corporate Governance Code*, Den Haag: Boom juridisch 2017, p. 38-40; en R. van Esch, *Handboek Legal Risk Management. De jurist als proactieve risicobeheerder*, Deventer: Den Hollander 2017, p. 85 e.v.

19 Bijv. de casus bij Stichting Open Nederland, de organisatie die regelt dat mensen zich kunnen laten testen voor evenementen. De Stichting had haar e-mailbeveiliging niet op orde, zodat in haar naam phishing-e-mails konden worden verstuurd naar iedereen. Zie 'Testorganisatie in de fout met gebrekkige e-mailbeveiliging', *Het Financieele Dagblad* 29 mei 2021, p. 11.

20 Het niet optreden van een raad van commissarissen van een NV of BV in geval van onacceptabele risico's of een inadequaat beheers- en controlesysteem kan bijvoorbeeld worden aangemerkt als onbehoorlijk toezicht. Zie *Asser/Van Solinge & Nieuwe Weme 2-IIb* 2019/289 (onder i).

21 Zie over de recente discussie: J.W. Winter e.a., 'Naar een zorgplicht voor bestuurders en commissarissen tot verantwoordelijke deelname aan het maatschappelijk verkeer', *Ondernemingsrecht* 2020/86 en de kritische reactie van H.J. de Kluiver, 'Over de verantwoordelijke onderneming. Naar een Paradise by the dashboard light?', *Ondernemingsrecht* 2020/126; en recent W. Oostwouder & T. Spronk, 'Naar een maatschappelijke zorgplicht voor bestuurders en commissarissen bij NV's en BV's? Over een belangwekkend voorstel met een aantal onvoldoende doordachte consequenties', *NJB* 2021/1395, p. 1580 e.v. Zie voorts de reacties in *Ondernemingsrecht* 2021 afl. 1 met een antwoord op de reacties van Winter c.s. (*Ondernemingsrecht* 2021/6).

maatschappij als geheel. Een risicobeoordeling vanuit het bedrijf zelf op een jurisdictie-per-jurisdictie-basis volstaat niet meer.[22]

Tot slot over de taak van het bestuur en de RvC. Zoals uit ons stuk uit 2016 al blijkt, loopt de financiële sector met specifieke bepalingen op het terrein van digitale veiligheid voorop. Dat is niet gewijzigd. DNB heeft eind 2020 het document *Visie op Toezicht 2021-2024* gepubliceerd. Dit document biedt een overzicht van de prioriteiten die DNB in 2021 stelt in haar toezicht op financiële instellingen. Een van de speerpunten is technologische vernieuwing. Daaronder begrijpt DNB de beveiliging van data en IT-infrastructuur tegen cyberaanvallen, die 'continue investering in weerbaarheid vergt'. Instellingen en dienstverleners moeten – aldus DNB – kunnen aantonen dat zij hun informatiebeveiliging op orde hebben. Zij roept daarnaast de financiële instellingen op regelmatig hun weerbaarheid te testen. 'Verhoging van het kennisniveau van bestuursleden en commissarissen op het gebied van IT- en cyberrisico's is nodig om de toenemende risico's te beheersen.'[23]

Ook de AFM heeft het zorgdragen voor cyberveiligheid door bedrijven die onder haar toezicht vallen zichtbaar op de agenda staan. In haar eind 2019 gepubliceerde 'Principes voor informatiebeveiliging' staan de verwachtingen van de AFM ten aanzien van het gewenste gedrag van financiële ondernemingen en accountantsorganisaties op het terrein van informatiebeveiliging.[24] Uit principe 2 'De onderneming richt een governance structuur in die effectieve informatiebeveiliging mogelijk maakt', volgt volgens de AFM onomwonden dat het bestuur verantwoordelijk is. Het heeft ook de expertise om deze verantwoordelijkheid te nemen. Sterker nog: de AFM verwacht dat de belangrijkste informatiebeveiligingsrisico's, dreigingen en incidenten bij het bestuur van de onderneming bekend zijn. Ook al zijn de gepubliceerde principes van de AFM toegesneden op financiële ondernemingen en accountantsorganisaties, deze inhoudelijke beschrijving van de bestuurstaak geldt volgens ons voor het bestuur in het algemeen. Wel valt op dat de RvC ongenoemd blijft.

De Europese Commissie vervolmaakt de trits. In september 2020 verscheen haar Digital Finance Package met daarin de Digital Finance Strategy. Die strategie behelst voorstellen voor het borgen van cyberveiligheid onder het acroniem 'DORA', Digital Operational Resilience Act. Onder deze vlag publiceerde de Europese Commissie gelijktijdig met haar strategie een Voorstel voor een verordening betreffende digitale operationele veerkracht voor de financiële sector.[25] De (voorgestelde) Verordening is direct van toepassing op een groot aantal financiële ondernemingen, variërend van kredietinstellingen tot handelsplatformen en 'derde aanbieders van ICT-diensten'. Onder 'digitale operationele veerkracht' verstaat de Europese Commissie: het vermogen van een financiële entiteit om haar operationele integriteit uit technologisch oogpunt op te bouwen, te waarborgen en te evalueren, door direct of indirect via gebruik van diensten van derde ICT-aanbieders te voorzien in het volledige scala van ICT-gerelateerde capaciteiten die nodig zijn voor de beveiliging van de netwerk- en informatiesystemen waarvan een financiële entiteit gebruikmaakt, en die de permanente verlening van financiële diensten en de kwaliteit ervan ondersteunen. Deze uitgebreide definitie bevat elementen die we ook in de algemeen omschreven best-practice-bepalingen van de Nederlandse Code 2016 ontwaren. Artikel 4 van de voorgestelde Verordening bevat de taken en verplichtingen van het leidinggevend orgaan, waar voor Nederlandse bedrijven zowel het bestuur als de RvC onder vallen. Het verbaast niet dat de (uiteindelijke) verantwoordelijkheid voor het kader voor ICT-risicobeheer bij bestuur en RvC is neergelegd.[26] De uiteindelijke verantwoordelijkheid is het overkoepelende beginsel van een alomvattende aanpak met een voortdurende betrokkenheid van het leidinggevend orgaan, aldus de considerans. Een sterk bewustzijn van cyberrisico's moet op elke bedrijfslaag en bij alle personeelsleden worden bevorderd. Een strikte cyberhygiëne is vereist. Dit vraagt een centrale en actieve rol van het bestuur en de RvC. In negen uitgesplitste deeltaken (onder a tot en met i) voor bestuur en RvC wijst de Verordening vervolgens onder meer op de vaststelling van duidelijke taken en verantwoordelijkheden en de bepaling van het passende risicotolerantieniveau voor het ICT-risico.

De Verordening vereist daarnaast uitdrukkelijk dat de leden van het leidinggevend orgaan (lees: bestuur en RvC) regelmatig specifieke opleidingen volgen, teneinde voldoende kennis en vaardigheden te verwerven en te onderhouden om ICT-risico's en de gevolgen daarvan voor de activiteiten van de financiële entiteit te begrijpen en te beoordelen.[27] Men is er in Brussel blijkbaar niet helemaal gerust op dat het bestuur en de RvC van financiële ondernemingen voldoende geëquipeerd zullen zijn en blijven op het terrein van cybersecurity.

22 L. Moerel, 'Reflecties over de impact van de digitale revolutie op corporate governance van Nederlandse beursgenoteerde ondernemingen', in: *Onderneming, digitalisering en data*, Preadvies Vereeniging 'Handelsrecht' 2019, Zutphen: Paris 2019, § 2.2.9.

23 DNB, *Visie op Toezicht 2021-2024*, p. 16. Dit aandachtspunt komt niet uit de lucht vallen. Zie C.D.J. Bulten & C.J.H. Jansen, 'De taak van de commissaris in een duurzame wereld', *Ondernemingsrecht* 2019/69, p. 367 (rechterkolom). Wij wijzen nog op AFM, *Trendzicht 2021* (november 2020), p. 19 waar zij opmerkt zorgen te hebben over en dus extra aandacht te hebben voor het gebruik van *Distributed Ledger Technology* (DLT) voor onder meer dataopslag door middel van cryptografie, waaraan risico's kleven die volgens de AFM niet helemaal kunnen worden beheerst.

24 Zie https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging.

25 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014, COM(2020) 595 final. De Verordening is ten tijde van het schrijven van dit artikel in behandeling bij de EU-Raad.

26 Zie de toelichting, p. 10 en de considerans, overweging 36 en 37 van de voorgestelde Verordening.

27 Zie art. 4 lid 4 van de voorgestelde Verordening.

3. De bestuurder en commissaris en digitale autonomie

Het advies van de CSR over digitale autonomie en cybersecurity moet – als de talloze incidenten uit het recente verleden dit niet al hebben gedaan – de alarmbellen doen rinkelen bij bestuurders en commissarissen. Bedrijven en instellingen kunnen, zoals de CSR schrijft, bijdragen aan het verwezenlijken van digitale autonomie, dat wil zeggen het realiseren van een zo groot mogelijke autonomie op het gebied van integriteit, vertrouwelijkheid en beschikbaarheid van informatie in hun bedrijfsvoering, waaronder in het bijzonder de bescherming van het eigen intellectuele eigendom, en daarmee van het eigen verdienvermogen en van de eigen autonomie. Zij kunnen en moeten investeren in technologische innovatie om hun cyberweerbaarheid te vergroten en hun afhankelijkheid van (al dan niet betrouwbare) buitenlandse partijen te verminderen en leveringszekerheid te vergroten, met name in bijzondere tijden. Het belang voor Nederlandse bedrijven om controle te behouden over de externe partijen, die hun gegevens verwerken, neemt bovendien toe. Veel gegevens worden door de bijna monopoliepositie van Amerikaanse techbedrijven verwerkt in de VS.

Het Hof van Justitie van de EU heeft in juli 2020 in *Schrems II* geoordeeld dat persoonsgegevens niet meer in de VS mogen worden verwerkt, omdat het Amerikaanse rechtssysteem vanwege de 'US Surveillance programmes' en het feit dat EU-burgers geen mogelijkheid hebben om naar de rechter te stappen, de persoonsgegevens van EU-burgers onvoldoende beschermt. Het feit dat de Amerikaanse en Chinese overheden zichzelf een wettelijke basis hebben verschaft voor toegang tot gegevens die opgeslagen zijn bij hun nationale leveranciers van ICT-diensten en gegevensopslag dient niet alleen bezien te worden vanuit privacyperspectief. Hun inlichtingendiensten hebben nadrukkelijk ook een taak op het gebied van economische spionage. Volgens het Hof moeten Nederlandse bedrijven zich ervan vergewissen dat het ontvangende land een aan de EU gelijkwaardige bescherming van gegevens kent. De precieze betekenis van deze uitspraak van het Hof is nog onduidelijk, maar zeker is wel dat Europese rechters zich op het gebied van bescherming van persoonsgegevens steeds strenger uitlaten.[28] Ook de Nederlandse toezichthouder wijst volgens krantenberichten in een recent (en blijkbaar vertrouwelijk) advies het gebruik van diensten van Google in het onderwijs af.[29] Tekenend is verder dat de Nederlandse overheid voor de hosting bij de apps CoronaMelder en CoronaCheck welbewust gekozen heeft voor Nederlandse leveranciers, om iedere discussie over cloud en jurisdictie te vermijden.

4. Van advies op papier naar verantwoordelijkheid en actie

Wat betekent de aandacht voor de vergroting van cyberweerbaarheid concreet voor bedrijven en instellingen?[30] Wij geven dit voor de overzichtelijkheid aan in een aantal *bullets*:

Bestuur en toezicht

- Beleg de verantwoordelijkheid voor digitale autonomie op het hoogst mogelijke niveau van het bedrijf, maak het 'Chefsache' (CEO).
- Zorg voor voldoende kennis bij bestuur en RvC op het terrein van digitale autonomie en cybersecurity.[31]
- Maak digitale autonomie en cyberveiligheid tot een zelfstandig terugkerend punt op de agenda van het bestuur en de RvC en ontwikkel een continu, proactief en in de overige bedrijfsprocessen geïntegreerd beleid op het gebied van cyberveiligheid en -weerbaarheid.
- Stimuleer de verdere ontwikkeling van kennis en innovatie op het gebied van digitale autonomie op nationaal en Europees gebied als onderdeel van de permanente educatie van bestuur en commissarissen.
- Adresseer de (overige) taken uit art. 4 lid 1 onder (a) tot en met (i) van de voorgestelde Verordening digitale operationele veerkracht voor bestuur én RvC.

Verankering in de bedrijfsprocessen

- Maak cyberrisico's onderdeel van de 'risk appetite' van een bedrijf en oefen, test en evalueer – indien relevant – de cyberweerbaarheid in het kader van het *Own Risk and Solvency Assessment* (ORSA).
- Verwerk digitale autonomie als aandachtspunt in het *compliancecharter*.
- Maak digitale autonomie een apart aandachtspunt in de bestaande rapportages.

Gegevensbescherming en dataopslag

- Wees kritisch bij de selectie van een (buitenlandse) partij voor de ontwikkeling en het beheer van de onderliggende technische systemen en netwerken. Controleverlies ligt op de loer en daarmee inbreuken op privacy en informatieveiligheid.
- Wees kritisch op, maak afspraken met en bied tegenspel aan de partij die verantwoordelijk is voor het transport en de opslag van vertrouwelijke data.

28 HvJ EU 16 juli 2021, C-311/18, ECLI:EU:C:2020:559 (*Schrems II*). In de zaak draaide het om de uitleg van art. 44 e.v. AVG. De standaardclausules, op grond waarvan Amerikaanse bedrijven moeten voldoen aan een aantal beschermingsmaatregelen bij de verwerking van persoonsgegevens, zijn vermoedelijk onvoldoende in het licht van de privacybescherming.

29 Zie 'Toezichthouder maant scholen, universiteiten en Justitie om met Google te stoppen', *Het Financieele Dagblad* 7 juni 2021.

30 Grotendeels geïnspireerd op het CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity', p. 13.

31 Ter illustratie: Moerel (a.w., § 2.2.12) verwijst naar een MIT Sloan-onderzoek dat laat zien dat bedrijven met minimaal drie *digital-savvy*-boardmembers significant betere financiële resultaten laten zien. Niets minder dan een win-winsituatie dus.

- Check of het nodig is om persoonsgegevens in de VS te laten verwerken en onderzoek alternatieven binnen de EU. Stimuleer de ontwikkeling en het gebruik van een eigen ICT-infrastructuur in Nederland en de EU.

Hopelijk maken deze acties (die ongetwijfeld investeringen vragen) een bedrijf of instelling weerbaarder tegen cyberbedreigingen. Een *chief information security officer* kan helpen de cyberrisico's in kaart te brengen en maatregelen voor te bereiden. Gelet op het toenemende belang van cyberweerbaarheid voor bedrijven en de daarmee verband houdende risico's moet echter de CEO voor de digitale autonomie van het bedrijf verantwoordelijk zijn, net zoals de minister-president volgens de CSR in haar adviezen verantwoordelijk moet zijn voor de digitale autonomie van Nederland.

5. Afrondend

Digitale autonomie is een complex vraagstuk, dat het functioneren van steeds meer bedrijven en instellingen rechtstreeks raakt. Cyberbedreigingen zullen in de nabije toekomst verder toenemen. Zij kunnen voor bedrijven enorme schadeposten opleveren (als bijvoorbeeld de productie stilvalt door een hack, bedrijfsinformatie of intellectueel eigendom wordt gestolen of enorme boetes dreigen door privacyschendingen). Het feit dat digitale autonomie vaak het niveau van een individueel bedrijf of instelling overstijgt, mag niet tot gevolg hebben dat bestuurders en commissarissen het initiatief op dit gebied aan de overheid laten. Dit artikel is een actualisering – naar aanleiding van recente gebeurtenissen en de groeiende zorgen bij de CSR – van ons eerdere stuk in *Ondernemingsrecht* over 'awareness' bij bestuur en RvC van bedrijven en instellingen voor vraagstukken van cyberveiligheid. Kennelijk is die bewustwording nog onvoldoende geweest (zie ook de opmerking van DNB in *Visie op Toezicht 2021-2024*). Wij roepen (opnieuw) bestuurders (in het bijzonder de CEO) en commissarissen (in het bijzonder de voorzitter van de RvC en de voorzitter van de audit- en riskcommissie) op cyberveiligheid serieus te nemen en over te gaan tot het nemen van concrete maatregelen om een zo hoog mogelijk niveau van cybersecurity te verwezenlijken en volledig compliant te zijn met de regels op het gebied van privacybescherming (zoals neergelegd in onder meer de AVG). Kort en goed: Cybersecurity is Chefsache!