De ontwikkeling van cyberveiligheid in Europa

Voorstel voor de Cyber Resilience Act

Nynke Brouwer & Minke Reijneveld[1]

In dit artikel wordt het voorstel voor de Cyber Resilience Act (CRA) besproken. Daarnaast wordt ingegaan op de inpassing van de CRA in het regelgevend kader dat ziet op productveiligheid, digitale beveiliging, veiligheid en aansprakelijkheid. Eerst wordt daartoe het voorstel zelf op hoofdlijnen besproken. Met het voorstel wordt beoogd dat producten met digitale elementen die in de EU op de markt worden gebracht veilig(er) zijn, dat fabrikanten verantwoordelijk blijven voor de cyberbeveiliging gedurende de hele levenscyclus van een product en dat consumenten de nodige bescherming genieten. Vervolgens wordt besproken hoe de CRA zich verhoudt tot productveiligheids- en productaansprakelijkheidswetgeving. Daarna wordt ingegaan op de vraag hoe de CRA zich verhoudt tot andere EU-wetgeving en voorstellen waarnaar de CRA verwijst, namelijk de Algemene verordening gegevensbescherming (AVG), en de voorstellen voor de AI-verordening en de herziene Netwerk- en informatiebeveiligingsrichtlijn (NIS 2-richtlijn).

1. Inleiding

Het gebruik van producten met digitale elementen neemt overal toe. Deze apparaten combineren hardware- en software-elementen, waardoor een fysiek product verbonden is met het internet. De voorbeelden zijn talrijk: routers en modems, slimme meters, netwerkbeheersystemen, software voor toegang op afstand, maar ook huishoudelijke en bedrijfsmatige of industriële apparaten zoals de slimme koelkast of voorraadbeheer in winkels (Internet of Things). Er is op dit moment geen (Europese) wetgeving die bepaalt dat fabrikanten of producenten digitale producten moeten beveiligen.[2] Hoewel dit natuurlijk niet betekent dat digitale producten altijd onvoldoende beveiligd zijn, wil de Europese wetgever minimumeisen vaststellen om het beveiligingsniveau te harmoniseren.

Een belangrijke oorzaak van succesvolle cyberaanvallen is namelijk de onvoldoende beveiliging in digitale producten en ondersteunende diensten. Het Cybersecuritybeeld Nederland 2022 concludeert dat de onveiligheid van ICT-producten en diensten de achilleshiel vormt van de digitale weerbaarheid, en dat de marktdynamiek de beheersing van digitale risico's compliceert.[3] Een cyberincident in een omgeving waar zich veel verbonden producten bevinden kan grote gevolgen hebben, zowel in de zin van zuivere vermogensschade, als ook in de zin van schade aan zaken of zelfs aan personen. Deze onveilige producten resulteren daardoor in hoge kosten voor de maatschappij.

Om dit probleem aan te pakken, heeft de Europese Commissie op 15 september 2022 een voorstel voor de Cyber Resilience Act (CRA) gepubliceerd.[4] Deze concept-CRA bevat cyberbeveiligingsbepalingen voor fabrikanten, ontwikkelaars en distributeurs van producten met digitale elementen. Deze bepalingen moeten ervoor zorgen dat producten met digitale elementen die in de EU op de markt worden gebracht veilig(er) zijn, fabrikanten verantwoordelijk blijven voor de cyberbeveiliging gedurende de hele levenscyclus van een product en consumenten de nodige bescherming genieten.[5]

Als het voorstel voor de CRA wordt goedgekeurd door het Europees Parlement, zal de CRA na 24 maanden in werking treden. Voor de inwerkingtreding van de CRA is geen nationale wetgeving vereist. Wel is er in het voorstel op bepaalde punten ruimte voor nationale bepalingen om nadere uitvoering aan de CRA te geven.

De CRA zal moeten worden ingepast in een reeds bestaand regelgevend kader van productveiligheid, zoals de Richtlijn inzake algemene productveiligheid, die op dit moment eveneens wordt herzien.[6] Bovendien dient de CRA zich ook te verhouden tot andere EU-wetsvoorstellen en wetten die eveneens zien op digitale beveiliging, veiligheid

en aansprakelijkheid. Zo kan de CRA bijvoorbeeld samenlopen met onder meer de Algemene verordening gegevensbescherming (AVG) en de aankomende AI-Verordening.

In dit artikel bespreken wij het voorstel voor de CRA op hoofdlijnen (par. 2). Vervolgens trachten wij de concept-CRA zoveel mogelijk te plaatsen binnen het kader van de huidige wetgeving en andere recente EU-wetsvoorstellen, namelijk de herziene productaansprakelijkheidsrichtlijn, de NIS 2-richtlijn, de AVG, de AI-Verordening en de verschillende richtlijnen en voorstellen die zien op productveiligheid. De afstemming en samenloop van deze verschillende wetten zijn nog punten van zorg en kritiek, en juist daarom is het belangrijk om te kijken hoe deze regelgeving zich tot elkaar verhoudt (par. 3). Vervolgens gaan wij in par. 4 in op de eerste ontvangst van deze eerste versie van de CRA en de eerste reacties hierop, bijvoorbeeld van de Tweede Kamer en de European Data Protection Supervisor (EDPS). Wij ronden af met een korte schets van de toekomst van de CRA (par. 5).[7]

2. De CRA op hoofdlijnen

2.1 Doelstelling

De Europese Commissie ziet de kosten die gepaard gaan met cyberincidenten als een groot probleem. Volgens de Europese commissie kan de CRA die kosten met € 290 miljard per jaar verlagen. Het doel van de CRA is dan ook voornamelijk om de interne markt te beschermen tegen onveilige producten met digitale elementen.

De CRA heeft vier specifiek geformuleerde doelstellingen:[8]

i) ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen verbeteren vanaf de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus;
ii) zorgen voor een samenhangend cyberbeveiligingskader, waardoor naleving voor hardware- en softwarefabrikanten gemakkelijker wordt;
iii) de beveiligingskenmerken van producten met digitale elementen transparanter maken; en
iv) bedrijven en consumenten in staat stellen om producten met digitale elementen veilig te gebruiken.

Om deze doelen te bereiken, bevat de CRA regels voor het in de handel brengen van producten met digitale elementen, om zo de cyberbeveiliging van dergelijke producten te waarborgen.[9] De CRA formuleert cybersecurityeisen voor het ontwerp, de ontwikkeling en de productie van producten met digitale elementen.[10] Daarnaast bevat de CRA vereisten voor de procedures inzake de respons op kwetsbaarheden, zodat fabrikanten de cyberbeveiliging van hun producten gedurende de hele levenscyclus kunnen waarborgen.[11] De CRA bevat ook een hoofdstuk over toezicht en handhaving.[12]

2.2 Toepassingsbereik

De CRA zal van toepassing worden op producten met digitale elementen waarvan – kort gezegd – het beoogde gebruik een verbinding met een apparaat of netwerk omvat.[13] Dit geldt niet voor producten die al worden gereguleerd door sectorale wetgeving, zoals medische hulpmiddelen, en voor producten die uitsluitend zijn ontwikkeld voor nationale veiligheid of militaire doeleinden.[14] Producten met digitale elementen zijn: *'elk software- of hardwareproduct en de oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht'*.[15] Software wordt kort omschreven als de computercode, en hardware als een (deel van een) fysiek elektronisch informatiesysteem dat digitale gegevens kan verwerken.[16] De CRA is in beginsel niet van toepassing op Software-as-a-Service (SaaS).[17]

De CRA zal van toepassing worden op producten met digitale elementen waarvan – kort gezegd – het beoogde gebruik een verbinding met een apparaat of netwerk omvat

Het grootste deel van de verplichtingen uit de CRA richt zich tot fabrikanten. Daarnaast bevat de CRA ook bepalingen met verplichtingen voor importeurs en distributeurs.

Auteurs

1. Mr. dr. N.M. Brouwer en mr. dr. M.D. Reijneveld zijn beiden werkzaam als advocaat bij Stibbe. Zij zijn tevens beiden als *fellow* verbonden aan het Onderzoekcentrum Onderneming en Recht (OO&R) van de Radboud Universiteit Nijmegen.

Noten

2. ENISA, *Opinion Consumers and IoT security*, 2019.
3. NCTV, 'CSBN 2022', Bijlage bij *Kamerstukken II* 2021/22, 26643, nr. 891.
4. Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020 COM (2022) 454 Final. In het Nederlands wordt naar de CRA ook wel verwezen als Cyberweerbaarheidsverordening of de Verordening inzake cyberweerbaarheid. In dit artikel gebruiken wij de afkorting CRA.
5. Voorstel CRA, Achtergrond van het voorstel, toelichting bij de CRA: Motivering en doel van het voorstel.
6. Huidige Richtlijn inzake algemene productveiligheid: Richtlijn 2001/95/EG van 3 december 2001. Op dit moment ligt er een voorstel om deze richtlijn te vervangen door een verordening: voorstel voor een Verordening van het Europees Parlement en de Raad inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 87/357/EEG van de Raad en Richtlijn 2001/95/EG van het Europees Parlement en de Raad, COM(2021) 346 final 2021/0170 (COD).
7. In het vervolg van dit artikel verwijzen wij steeds naar de 'CRA'. Wij merken volledigheidshalve op dat wij daarmee doelen op het eerste gepubliceerde voorstel voor een CRA en zodoende een conceptversie van de CRA.
8. Voorstel CRA, Achtergrond van het voorstel, toelichting bij de CRA: Motivering en doel van het voorstel.
9. Art. 1 sub a CRA.
10. Art. 1 sub b CRA.
11. Art. 1 sub c CRA.
12. Art. 1 sub d CRA.
13. Art. 2 lid 1 CRA.
14. Art. 2 lid 2 sub a-c CRA.
15. Art. 3 sub 1 CRA.
16. Art. 3 sub 6 jo. art. 3 sub 7 CRA.
17. Overweging 9 CRA.

© Jorg Greuel / Getty Images

2.3 Verplichtingen voor fabrikanten

2.3.1 Essentiële eisen voor cyberbeveiliging

De verplichtingen voor fabrikanten zijn te verdelen in *ex ante* verplichtingen (voorafgaand aan het op de markt brengen van de producten) en *ex post* verplichtingen (verplichtingen gedurende de levensduur van het product). De CRA introduceert hiermee een wettelijke verplichting tot *security by design*.

Fabrikanten zullen een product met digitale elementen alleen in de handel mogen brengen, indien het is ontworpen, ontwikkeld en geproduceerd overeenkomstig de in de bijlage bij de CRA opgenomen essentiële eisen.[18] De CRA bevat daarmee voor alle producten met digitale elementen basisvoorwaarden op het gebied van cyberbeveiliging.

De cyberbeveiligingseisen waaraan fabrikanten zullen moeten voldoen, vallen in drie onderdelen uiteen:

i) producten met digitale elementen moeten zodanig worden ontworpen, ontwikkeld en geproduceerd dat zij een passend niveau van cyberbeveiliging waarborgen op basis van de risico's;[19]
ii) producten met digitale elementen worden geleverd zonder bekende kwetsbaarheden;[20]
iii) op basis van een verplichte risicobeoordeling moeten, indien van toepassing, producten met digitale elementen voldoen aan een aantal verplichtingen, zoals: levering met een standaard beveiligde configuratie; de vertrouwelijkheid van opgeslagen, verzonden of anderszins verwerkte (persoons)gegevens, bijvoorbeeld door middel van encryptie; en de minimalisering van gebruikte (persoons)gegevens.[21]

Naast cyberbeveiligingseisen (*ex ante*) zullen fabrikanten moeten voldoen aan eisen met betrekking tot de behandeling van kwetsbaarheden (*ex post*). Fabrikanten zullen bijvoorbeeld kwetsbaarheden moeten vaststellen en documenteren, beveiligingsupdates verstrekken voor kwetsbaarheden in verband met de risico's die zijn verbonden aan producten met digitale elementen, informa-

Naast cyberbeveiligingseisen (*ex ante*) zullen fabrikanten moeten voldoen aan eisen met betrekking tot de behandeling van kwetsbaarheden (*ex post*)

tie verstrekken over verholpen kwetsbaarheden en ervoor zorgen dat beveiligingsupdates onverwijld en kosteloos worden verspreid, vergezeld van informatie over te nemen maatregelen voor gebruikers.[22] De verplichting om beveiligingsupdates uit te brengen zal gelden gedurende de verwachte levensduur van het product, of gedurende vijf jaar vanaf het in de handel brengen, indien dat korter is.[23]

Met deze verplichtingen wil de Europese Commissie twee concrete problemen aanpakken: een gebrek aan beveiligingsupdates en een gebrek aan transparantie over kwetsbaarheden die fabrikanten en/of derden vinden in producten met digitale elementen.

2.3.2 Conformiteitsbeoordeling

De fabrikant zal zelf moeten beoordelen of een product met digitale elementen voldoet aan de hierboven omschreven vereisten.[24] Om dat te beoordelen moet de fabrikant een conformiteitsbeoordeling uitvoeren van zowel de cyberbeveiligingsrisico's[25] als de procedures voor respons op kwetsbaarheden.[26] De CRA schrijft daarvoor de verschillende methodes voor. Indien een product conform is, dient de fabrikant een EU-conformiteitsverklaring op te stellen[27] en een CE-markering aan te brengen op het product.[28] Deze systematiek maakt dat de fabrikant verantwoordelijk is voor het vaststellen en verklaren dat het product voldoet aan alle vereisten.

Deze werkwijze is niet uniek. Ook bij AI-systemen met een hoog risico wordt gewerkt met CE-markeringen, net als bij veel andere industriële productgroepen. Als voorwaarde geldt altijd dat een product pas mag worden verhandeld binnen de Europese Economische Ruimte als het product een CE-markering heeft die aangeeft dat het overeenstemt met de relevante gezondheids-, veiligheids-, prestatie- en milieueisen.[29]

Sommige producten vormen vanwege de aard van hun functie of het beoogde gebruik ervan in gevoelige omgevingen een verhoogd risico. Met betrekking tot deze *kritieke* producten met digitale elementen gelden daarom nadere voorwaarden. De CRA bevat een lijst met kritieke producten, die door de Europese Commissie kan worden bijgewerkt.[30] Op dit punt heeft de Europese Commissie dus in feite zelf al een eerste risicobeoordeling gemaakt. Voor deze producten geldt een strengere conformiteitsbeoordelingsprocedure.

In het huidige voorstel van de CRA zijn in Klasse I producten opgenomen zoals software voor identiteits- en toegangsbeheer, browsers, wachtwoordbeheerders, kwaadaardige softwaredetectiesystemen, tools voor update- en patchbeheer en software voor toegang op afstand. Klasse II, de hoogste risicoklasse, bevat producten zoals besturingssystemen, uitgevers van digitale certificaten, routers en modems voor industrieel gebruik, smartcards en slimme meters.[31] Voor producten in klasse I geldt dat een derde partij moet worden betrokken bij het assessment, tenzij sprake is van geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelen[32] voor het betreffende product.[33] Voor producten in klasse II geldt dat altijd een derde partij bij de conformiteitsbeoordeling *moet* worden betrokken.[34] De EC geeft zelf aan te verwachten dat zo'n 90% van de markt bestaat uit niet-kritische producten die alleen een zelfbeoordeling nodig hebben.[35]

2.3.4 Documenteren en rapporteren

Het voorstel van de CRA schrijft voor dat fabrikanten systematisch en op een wijze die in verhouding staat tot de aard en de cyberbeveiligingsrisico's, zullen moeten documenteren over relevante cyberbeveiligingsaspecten met betrekking tot het product met digitale elementen.[36] Dat geldt ook voor kwetsbaarheden waarvan zij kennisnemen en alle relevante informatie die door derden wordt verstrekt. Bovendien moet de fabrikant, indien van toepassing, de risicobeoordeling van het product bijwerken. Fabrikanten zullen er verder voor moeten zorgdragen dat de producten met digitale elementen vergezeld gaan van gedetailleerde informatie en instructies,[37] die elektronisch of in fysieke vorm moeten worden verstrekt in een taal die de gebruikers makkelijk kunnen begrijpen.[38] De instructies moeten ook duidelijk, begrijpelijk en leesbaar zijn.

Daarnaast legt het voorstel voor de CRA een meldplicht ('rapportageverplichting') op aan fabrikanten.[39] Indien fabrikanten een actief gebruikte kwetsbaarheid in hun product ontdekken, of indien zich een incident voordoet dat gevolgen heeft voor de veiligheid van het product, zullen fabrikanten dit moeten melden aan ENISA, het EU-agentschap voor cyberbeveiliging. De melding moet onverwijld en uiterlijk binnen 24 uur na kennisneming worden gedaan.

18. Bijlage 1 bij voorstel voor een verordening van het Europees parlement en de raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020 (Hierna: Bijlage 1 CRA. Voor de overige bijlagen: Bijlage 2 CRA, etc.).

19. Afdeling 1 punt 1 Bijlage 1 CRA. Art. 5 sub 1 CRA bevat als aanvulling hierop wel het vereiste dat dit geldt onder de voorwaarde dat de producten op passende wijze worden geïnstalleerd, onderhouden en gebruikt voor het beoogde doel of in redelijkerwijs voorzienbare omstandigheden, en worden bijgewerkt indien dat van toepassing is.

20. Afdeling 1 punt 2 Bijlage 1 CRA.

21. Afdeling 1 punt 3 Bijlage 1 CRA. De verplichte risicobeoordeling is geregeld in artikel 10 lid 2 CRA.

22. Afdeling 2 Bijlage 1 CRA.

23. Art. 10 lid 6 CRA.

24. Art. 10 lid 1 CRA.

25. Art. 10 lid 3 jo. art. 23 CRA.

26. Art. 10 lid 6 jo. afdeling 2 punt 5 Bijlage I CRA.

27. Art. 20 jo. art. 10 lid 7 CRA.

28. Art. 22 jo. art. 10 lid 7 CRA.

29. Zie bijvoorbeeld Mededeling van de Commissie De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU (voor de EER relevante tekst) 2022/C 247/01 en besluit nr. 768/2008/eg van het Europees Parlement en de Raad van 9 juli 2008 betreffende een gemeenschappelijk kader voor het verhandelen van producten en tot intrekking van Besluit 93/465/EEG van de Raad.

30. Art. 6 jo. Bijlage 3 CRA.

31. Zie voor een volledig overzicht Bijlage 3 CRA.

32. Art. 18 CRA.

33. Module B+C of Module H, art. 24 lid 2 CRA.

34. Module B + C of Module H, Bijlage VI CRA. Zie art. 24 lid 4 en overweging 45 CRA.

35. Europese Commissie, *Cyber Resilience Act-Factsheet*, onder 'How the Cyber Resilience Act will work in practice', online via digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet, p. 3.

36. Art. 10 lid 10 CRA.

37. Bijlage 2 CRA.

38. Art. 10 lid 10 CRA.

39. Art. 11 CRA.

De fabrikant moet ook de gebruikers van het product onverwijld op de hoogte stellen van het incident en, indien nodig, van de corrigerende maatregelen die de gebruiker kan nemen om de gevolgen van het incident te beperken.[40]

2.4 Verplichtingen voor importeurs en distributeurs

Importeurs zullen uitsluitend producten met digitale elementen in de handel mogen brengen die voldoen aan de door de CRA gestelde cybersecurityeisen en ook alleen indien de door de fabrikant ingestelde processen aan de eisen uit de CRA voldoen.[41] Importeurs moeten ervoor zorgdragen dat een product met digitale elementen pas in de handel wordt gebracht als de fabrikant de juiste conformiteitsbeoordelingsprocedure heeft uitgevoerd, de fabrikant de technische documentatie heeft opgesteld, en het product met digitale elementen is voorzien van CE-markering en de vereiste informatie en instructies.[42] Importeurs moeten de relevante contactgegevens – hun naam, postadres en e-mailadres – opnemen op (de verpakking van) het product.[43]

Voor distributeurs gelden dezelfde eisen, maar zij zullen ook moeten controleren of de importeurs aan de verplichtingen hebben voldaan.[44] De CRA introduceert hiermee een getrapt systeem. Dat moet ervoor zorgen dat iedere schakel in de keten wordt gecontroleerd en daarmee het risico op cyberincidenten wordt geminimaliseerd.

De CRA introduceert een getrapt systeem dat ervoor moet zorgen dat iedere schakel in de keten wordt gecontroleerd en daarmee het risico op cyberincidenten wordt geminimaliseerd

Ook op importeurs en distributeurs zal een meldplicht komen te rusten: zij moeten de fabrikant onverwijld op de hoogte brengen van zwakke plekken in de cyberbeveiliging.[45] Als er sprake is van een aanzienlijk risico voor de cyberbeveiliging, moeten importeurs en distributeurs ook de nationale markttoezichtautoriteiten informeren.[46] In Nederland wordt de Rijksinspectie Digitale Infrastructuur (het voormalig Agentschap Telecom) de markttoezichtautoriteit.

2.4 Toezicht en handhaving: boetes

Het voorstel van de CRA bevat boetebevoegdheden voor de toezichthouders. Niet-naleving van de essentiële verplichtingen met betrekking tot *cybersecurity by design* kan leiden tot boetes van maximaal € 15 miljoen of 2,5% van de totale jaaromzet, indien dit bedrag hoger is.[47] Niet-naleving van andere verplichtingen binnen de CRA leidt tot administratieve boetes van maximaal € 10 miljoen of 2% van de wereldwijde jaaromzet, indien dit bedrag hoger zou zijn.[48] Daarnaast kan misleiding van markttoezichtautoriteiten door bijvoorbeeld het geven van onjuiste of onvolledige informatie leiden tot een boete van € 5 miljoen of 1% van de wereldwijde jaaromzet in het voorgaande belastingjaar, indien dit bedrag hoger zou zijn.[49]

Het voorstel geeft de lidstaten de vrijheid om andere doeltreffende, evenredige en afschrikkende sancties vast te stellen voor bedrijven die de CRA niet naleven.[50] Zij moeten deze regels en maatregelen wel aan de Commissie melden.[51] Nationale markttoezichtautoriteiten hebben daarnaast een verregaande bevoegdheid om het aanbieden van producten te verbieden of te beperken als de fabrikant, importeur, distributeur of een ander verantwoordelijk bedrijf niet aan de eisen blijkt te voldoen.[52] Ook de Europese Commissie kan maatregelen nemen voor producten met digitale elementen die een significant beveiligingsrisico inhouden, door bijvoorbeeld te gelasten om binnen een redelijke termijn producten uit de handel te nemen of terug te roepen.[53]

3. Verhouding tot andere richtlijnen en verordeningen

De CRA past binnen een groot pakket aan strategieën en wetsvoorstellen van de Europese Commissie. Het doel van al deze maatregelen is om Europa in digitaal opzicht klaar te stomen voor de toekomst. Binnen dit plan vallen veel wetsvoorstellen, die deels ook overlappen met de CRA. Deze samenloop van wetten kan leiden tot problemen, en het is dan ook goed om duidelijk af te stemmen hoe de CRA zich verhoudt tot andere wetgeving. Wij bespreken eerst hoe de CRA zich verhoudt tot productveiligheid- en productaansprakelijkheidswetgeving. Vervolgens gaan wij in op de vraag hoe de CRA zich verhoudt tot een aantal andere EU-wetten en -voorstellen waarnaar de CRA ook verwijst, namelijk de Algemene verordening gegevensbescherming (AVG), de AI-verordening en de herziene Netwerk- en informatiebeveiligingsrichtlijn (NIS 2-richtlijn).

3.1 De vormgeving van de digitale toekomst van Europa

Het wetsvoorstel van de CRA maakt deel uit van de uitgebreide EU-strategie *Shaping Europe's Digital Future*. Het doel van deze strategie is bijvoorbeeld om nieuwe mogelijkheden voor bedrijven te creëren, de ontwikkeling van betrouwbare technologie aan te moedigen, een open en democratische samenleving te bevorderen, een levendige en duurzame economie mogelijk te maken, klimaatverandering te bestrijden en de groene transitie te realiseren.[54]

Binnen deze strategie ontwikkelt de Commissie wetgeving op het gebied van gegevensbescherming, grondrechten, veiligheid, beveiliging en de interne markt.[55] Daarbinnen vallen veel wetgevingsvoorstellen, die op diverse aspecten zien. Voorbeelden zijn de Data Act[56] en Data Governane Act[57] binnen de Europese datastrategie, de DSA[58] en DMA[59] voor regulering van digitale diensten, de AVG[60] en E-privacy verordening[61] op het gebied van privacy en gegevensbescherming, de AI Act,[62] AI Liability Directive[63] en herziene productaansprakelijkheidsrichtlijn[64] met betrekking tot kunstmatige intelligentie en tot slot de herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2)[65] op het gebied van cybersecurity.

Ook de CRA valt onder de noemer van de digitale toekomst van Europa. Meer specifiek is de CRA deel van de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk.[66] Deze strategie schetst de risico's van steeds meer verbonden netwerk- en informatiesystemen, zoals cyberaanvallen, geopolitieke spanningen over het mondiale open internet en controle over technologieën, de veiligheid van onlinediensten[67] en een gebrek aan collectieve situationele kennis over cyberdreigingen binnen de EU.[68] Binnen deze strategie vallen de NIS 2-richtlijn, de CRA, de versterking van de rol van ENISA door de Cyberbeveiligingswet en de ontwikkeling van een EU-breed certificeringskader voor IT-producten en -diensten.[69]

3.2 Productveiligheid en productaansprakelijkheid voor digitale producten

De CRA is niet het enige wetsvoorstel dat betrekking heeft op het veiliger maken van (digitale) producten. Er kan onderscheid worden gemaakt tussen wetgeving die ziet op veiligheidsnormen *ex ante* (productveiligheid) en wetgeving die ziet op aansprakelijkheid voor onveilige producten *ex post* (productaansprakelijkheid). In beide domeinen werkt de Europese Commissie aan herziening van het juridisch kader.

3.2.1 Productveiligheid

De CRA bevat specifieke bepalingen voor cyberveiligheid. Uit artikel 7 en overweging 28 CRA leiden wij af dat de CRA in dit opzicht moet worden gezien als een *lex specialis* van de algemene Richtlijn inzake productveiligheid. Indien producten met digitale elementen veiligheidsrisico's met zich brengen die geen verband houden met cyberbeveiliging, vallen zij onder de algemene Richtlijn inzake productveiligheid, tenzij er bijvoorbeeld specifieke, sectorale regelgeving van toepassing is.[70] Ook die algemene productveiligheidsrichtlijn wordt op dit moment herzien, waarbij de bedoeling is dat dit een Verordening wordt: de Verordening inzake algemene productveiligheid (VAPV).[71] De CRA verwijst al naar deze nieuwe VAPV.[72] Het doel van de VAPV is om beter om te gaan met de risico's die voortvloeien uit nieuwe technologieën.[73] Het toepassingsgebied van de verordening wordt dan ook verruimd ten opzichte van de huidige richtlijn, zodat deze haar vangnetfunctie kan blijven behouden, indien risico's die

De CRA en de VAPV sluiten qua systematiek op elkaar aan: beide wetsvoorstellen bevatten vergelijkbare, getrapte verplichtingen voor fabrikanten, importeurs en distributeurs

40. Art. 11 lid 4 CRA.
41. Art. 13 lid 1 CRA.
42. Art. 13 lid 2 en lid 5 CRA.
43. Art. 13 lid 4 CRA.
44. Art. 14 CRA.
45. Art. 13 lid 6 CRA, art. 14 lid 4 CRA.
46. Art. 13 lid 9 CRA, art. 14 lid 6 CRA.
47. Art. 53 lid 3 CRA.
48. Art. 53 lid 4 CRA.
49. Art. 53 lid 5 CRA.
50. Art. 53 lid 1 CRA.
51. Art. 53 lid 2 CRA.
52. Art. 43 lid 4 CRA, art. 47 CRA.
53. Art. 45 lid 4 CRA.
54. Europese Commissie, *Shaping Europe's Digital Future*, Luxemburg: Publications Office of the European Union 2020.
55. Europese Commissie, 'Mededeling van de commissie aan het Europees parlement, de raad, het Europees economisch en sociaal comité en het comité van de regio's', Een Europese datastrategie, COM(2020) 66 final, par. 1.
56. Voorstel voor een verordening van het Europees Parlement en de Raad betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data (Dataverordening), COM(2022) 78 final.
57. Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (Datagovernanceverordening).
58. Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een ééngemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (Digitale-dienstenverordening).
59. Voorstel voor een verordening van het Europees Parlement en de Raad over betwistbare en eerlijke markten in de digitale sector (wet inzake digitale markten), COM(2022) 842 final.
60. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
61. Voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie) COM(2017) 010 final.
62. Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende de artificiële intelligentie (wet op de artificiele intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie COM(2021) 206 final.
63. Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de aanpassing van de regels inzake niet-contractuele civielrechtelijke aansprakelijkheid aan artificiële intelligentie (AI), COM(2022) 496 final.
64. Voorstel voor een richtlijn van het Europees Parlement en de Raad inzake aansprakelijkheid voor producten met gebreken, COM(2022) 495 final.
65. Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn.
66. Gezamenlijke mededeling aan het Europees Parlement en de Raad, 'De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk', JOIN(2020) 18 final. De cybersecuritystrategie is als zodanig weer onderdeel van de Digital Decade Strategy.
67. Zie ook Europese Commissie, Directorate-General for Communication, 'Speciale Eurobarometer 499: De houding van de Europeanen ten aanzien van cyberveiligheid (cybercriminaliteit)', version v1.00, 2020, (online).
68. Gezamenlijke mededeling aan het Europees Parlement en de Raad, De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk, JOIN(2020) 18 final, par. 1.
69. Europese Commissie, 'Cybersecurity Policies', online via digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.
70. Overweging 28 CRA; Richtlijn 2001/95/EG van het Europees Parlement en de Raad van 3 december 2001 inzake algemene productveiligheid.
71. Voorstel voor een verordening van het Europees Parlement en de Raad inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 87/357/EEG van de Raad en Richtlijn 2001/95/EG van het Europees Parlement en de Raad, COM(2021) 346 final 2021/0170 (COD).
72. Overweging 28 CRA, art. 7 CRA.
73. Toelichting op voorstel Verordening inzake algemene productveiligheid, punt 3.

voortvloeien uit nieuwe technologieën niet door specifiekere EU-wetgeving worden ondervangen.[74]

De CRA en de VAPV sluiten qua systematiek op elkaar aan: beide wetsvoorstellen bevatten vergelijkbare, getrapte verplichtingen voor fabrikanten, importeurs en distributeurs. Het getrapte systeem van verantwoordelijkheid en controleerbaarheid is niet nieuw en komt ook voor in de systematiek van wet- en regelgeving inzake productveiligheid die al van kracht is in de Europese Unie. Ook de systematiek omtrent de mogelijkheid voor een fabrikant om al dan niet de conformiteitsbeoordeling voor zijn product zelf uit te voeren is gebruikelijk.

Er bestaan ook meer specifieke productveiligheidsbepalingen, zoals bijvoorbeeld de Machinerichtlijn en de Richtlijn radioapparatuur.[75] Ook de Machinerichtlijn wordt momenteel aangepast. Er is een voorstel voor een Verordening betreffende machineproducten.[76] Deze verordening bevat veiligheidsbepalingen voor voornamelijk industrieel gebruikte machines. Het voorstel voor de verordening beoogt onder meer de risico's van opkomende technologieën beter te dekken.[77] De CRA geeft aan dat machineproducten kunnen vallen onder het toepassingsbereik van de CRA en de Machineverordening. Die producten worden geacht in lijn te zijn met de eisen uit de Machineverordening, als er een EU-conformiteitsverklaring op basis van de CRA voor het product is afgegeven.[78]

De Richtlijn radioapparatuur bevat veiligheidsvoorschriften voor radioapparatuur die op de interne markt wordt gebracht. Deze richtlijn bevat ook speciale cybersecurityvereisten die gelden voor IoT-apparaten, op basis van een gedelegeerde verordening.[79] Om overlap in de regelgeving te voorkomen, is het de bedoeling dat de Commissie de gedelegeerde verordening intrekt of wijzigt met betrekking tot de radioapparatuur die onder de CRA valt, zodat de CRA hierop van toepassing is.[80]

3.2.2 Productaansprakelijkheid

Hoewel de CRA ziet op productveiligheid en niet op aansprakelijkheid, bestaat er wel een zekere wisselwerking tussen de CRA en de Productaansprakelijkheidsrichtlijn. De CRA geeft aan dat de (huidige) algemene Productaansprakelijkheidsrichtlijn een aanvulling vormt op de CRA.[81] Die Productaansprakelijkheidsrichtlijn zorgt ervoor dat gelaedeerden schadevergoeding kunnen vorderen wanneer schade is veroorzaakt door producten met gebreken. De Productaansprakelijkheidsrichtlijn bevat een risicoaansprakelijkheid voor de fabrikant van een gebrekkig product dat schade veroorzaakt.

Ook in de wetgeving rondom (product)aansprakelijkheid vinden de nodige ontwikkelingen plaats. De Europese Commissie heeft bijvoorbeeld een voorstel voor herziening van de Richtlijn productaansprakelijkheid gepubliceerd. In dit voorstel wordt uitdrukkelijk bepaald dat personen die als gevolg van software of AI-systemen schade hebben geleden, vergoeding kunnen vorderen.[82] Om dat te bereiken, wordt verduidelijkt dat software, met inbegrip van AI-systemen,[83] een 'product' is zoals bedoeld in de Productaansprakelijkheidsrichtlijn.[84] De herziene richtlijn bepaalt ook wie aansprakelijkheid is voor fouten bij software-updates of bij algoritmes.[85] Het voorstel voor de herziening van de Productaansprakelijkheidsrichtlijn biedt bovendien ruimte voor schadevorderingen wanneer een gebrekkig product leidt tot verlies of corruptie van gegevens die niet uitsluitend beroepsmatig worden gebruikt.[86] Een voorbeeld daarvan is vergoeding voor uit een harde schijf verwijderde inhoud, inclusief kosten voor het terugwinnen of herstellen van die inhoud.[87] Dat is een uitbreiding ten opzichte van de huidige richtlijn, die enkel ziet op schade wegens overlijden, personenschade en (in beperkte mate) zaakschade.[88]

De herziene Productaansprakelijkheidsrichtlijn bepaalt verder expliciet dat ook cybersecurity-kwetsbaarheden een product 'gebrekkig' kunnen maken. De voorgestelde CRA creëert juist verplichtingen voor fabrikanten om kwetsbaarheden zoveel mogelijk te voorkomen, zowel vooraf door middel van beveiligingsmaatregelen, als achteraf door middel van beveiligingsupdates. Wanneer een gebrek aan veiligheid in een product bijvoorbeeld voortkomt uit een gebrek aan veiligheidsupdates nadat het product in de handel is gebracht, en hierdoor schade wordt veroorzaakt, kan de fabrikant aansprakelijk worden gesteld op basis van de Productaansprakelijkheidsrichtlijn.[89] De CRA bevat juist de verplichtingen voor fabrikanten met betrekking tot het verstrekken van dergelijke beveiligingsupdates.

De Productaansprakelijkheidsrichtlijn ziet niet op schadevergoeding voor inbreuken op grondrechten (bijvoorbeeld als de toepassing van AI leidt tot discriminatie). Voor die inbreuken is een ander wetsvoorstel gedaan: de richtlijn met betrekking tot niet-contractuele aansprakelijkheid voor AI.[90] Dit voorstel heeft tot doel uniforme regels vast te stellen voor toegang tot informatie en voor verlichting van de bewijslast met betrekking tot door AI-systemen veroorzaakte schade. De Europese Commissie geeft aan dat met betrekking tot AI het voorstel voor de herziene richtlijn productaansprakelijkheid en de AI-aansprakelijkheidsrichtlijn complementair zijn.[91] Het voorstel over de productaansprakelijkheid regelt dat AI-systemen en op AI gebaseerde goederen 'producten' zijn die onder het toepassingsbereik van het richtlijnvoorstel over productaansprakelijkheid vallen. De AI-aansprakelijkheidsrichtlijn ziet juist *niet* op productaansprakelijkheid, maar op schuldaansprakelijkheid uit onrechtmatige daad in andere gevallen, waarin de inzet van AI-systemen de schade heeft veroorzaakt.[92] Mogelijk kan bij de invulling van de verplichtingen ook in dit geval de CRA een rol spelen, hoewel de CRA op dit moment niet expliciet verwijst naar de AI-aansprakelijkheidsrichtlijn.

Hoewel de CRA ziet op productveiligheid en niet op aansprakelijkheid, bestaat er wel een zekere wisselwerking tussen de CRA en de Productaansprakelijkheidsrichtlijn

Hoewel het wetsvoorstel voor de CRA doet voorkomen dat het onderscheid altijd helder is en de verschillende wetten elkaar dus versterken of goed samenlopen, blijkt dat bij een nadere beschouwing toch niet altijd even simpel

3.3 Verhouding tot andere (voorgestelde) EU-wetgeving: NIS 2, AVG en AI-Verordening

Waar de CRA niet verwijst naar de aansprakelijkheidswetgeving, verwijst zij wel naar diverse andere wetten. Wij bespreken hieronder kort de verhouding tot de in de CRA genoemde wetgeving. Hoewel het wetsvoorstel voor de CRA doet voorkomen dat het onderscheid altijd helder is en de verschillende wetten elkaar dus versterken of goed samenlopen, blijkt dat bij een nadere beschouwing toch niet altijd even simpel.

3.3.1 NIS 2-Richtlijn

De CRA en de NIS 2-richtlijn (NIS 2) bevatten beide regels op het gebied van cyberbeveiliging. Terwijl de voorgestelde CRA betrekking heeft op *producten* met digitale elementen die op de markt worden gebracht, is de NIS 2-richtlijn gericht op het waarborgen van een hoog niveau van cyberbeveiliging van *diensten* in de – kort gezegd – kritieke infrastructuur.[93] De toepasselijkheid van NIS 2 is ook de reden dat SaaS niet valt onder de CRA: Software-as-a-Service wordt gezien als een *dienst*. Volgens de EC zal het kader uit NIS 2 ervoor zorgen dat '*technische specificaties en maatregelen die vergelijkbaar zijn met de essentiële cyberbeveiligingsvereisten van de verordening cyberweerbaarheid* [CRA; auteurs]*, ook worden ingevoerd voor het ontwerp, de ontwikkeling en de respons op kwetsbaarheden van software die als dienst wordt geleverd*'.[94] Het idee van de Uniewetgever lijkt dan ook dat dat beide wetten volledig complementair aan elkaar zijn.[95] Er is onzes inziens dan ook geen sprake van een *lex generalis* en een *lex specialis*, maar van twee wetten die naast elkaar in hiërarchie staan.

In theorie lopen de CRA en NIS 2 dan ook goed samen, omdat zij beide een eigen toepassingsgebied lijken te hebben dat niet overlapt. Hoewel dat in theorie klopt, zijn er wel punten waarop het onderscheid minder duidelijk is. Dat komt vooral omdat de uitsluiting van SaaS in de CRA niet absoluut is: de CRA is *wel* van toepassing op '*oplossingen voor gegevensverwerking op afstand die zijn gekoppeld aan een product met digitale elementen bedoeld voor normale gegevensverwerking op afstand, waarvoor de software is ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant van het betrokken product, bij gebreke waarvan een dergelijk product met digitale elementen een van zijn functies niet zou kunnen vervullen*'.[96] Dit lijkt te betekenen dat via een soort 'digitale natrekking' de software omslaat van dienst naar product, wanneer het product en de software zodanig met elkaar zijn verbonden dat het product een van zijn functies niet kan uitoefenen zonder de software, mits dezelfde fabrikant zowel het product met digitale elementen ontwikkelt als de software ontwikkelt of laat ontwikkelen.

In de CRA staat vervolgens dat in ieder geval cloudmodellen en cloudcomputerdiensten niet onder de CRA vallen,[97] maar dit laat heel veel ruimte voor andere SaaS-achtige oplossingen om wel onder het toepassingsbereik van de CRA te vallen. Dit maakt het in ieder geval behoorlijk ingewikkeld om vast te stellen wanneer precies sprake is van een product met digitale elementen waaraan

74. *Ibid*.
75. Richtlijn 2006/42/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende machines en tot wijziging van Richtlijn 95/16/EG (herschikking); Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG.
76. Voorstel voor een verordening van het Europees Parlement en de Raad betreffende machineproducten, COM(2021) 202 final. Ook dit voorstel is onderdeel van het plan inzake de digitale toekomst van Europa.
77. Europese Commissie, 'werkdocument van de diensten van de commissie Samenvatting van het Effectbeoordelingsverslag' Voorstel voor een verordening van het Europees Parlement en de Raad betreffende machines en werktuigen, SWD(2021) 83 definitief, p. 2-3.
78. Art. 8 CRA.
79. Gedelegeerde verordening (EU) 2022/30 van de Commissie van 29.10.2021 tot aanvulling van Richtlijn 2014/53/EU van het Europees Parlement en de Raad met betrekking tot de toepassing van de essentiele eisen als bedoeld in artikel 3, lid 3, punten d), e) en f), van die richtlijn.
80. Overweging 16 CRA.
81. Overweging 16 CRA.
82. Voorstel voor een richtlijn van het Europees Parlement en de Raad inzake aansprakelijkheid voor producten met gebreken, COM/2022/495 final (Herziene productaansprakelijkheidsrichtlijn).
83. Europese Commissie, 'Questions and answers on the revision of the Product Liability Directive', 28 september 2022.
84. Art. 4 sub 1 Herziene productaansprakelijkheidsrichtlijn.
85. Art. 10 lid 2 Herziene productaansprakelijkheidsrichtlijn.
86. Art. 4 sub 6 sub c Herziene productaansprakelijkheidsrichtlijn.
87. Overweging 16 Herziene productaansprakelijkheidsrichtlijn.
88. Art. 5 lid 1 jo art. 4 sub 6 Herziene productaansprakelijkheidsrichtlijn.
89. Overweging 16 CRA.
90. Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de aanpassing van de regels inzake niet-contractuele civielrechtelijke aansprakelijkheid aan artificiële intelligentie (AI), COM(2022) 496 final.
91. *Kamerstukken II* 2012/22, 22112, nr. 3549, 'BNC-fiche Richtlijn betreffende aanpassing civielrechtelijke aansprakelijkheidsregels voor kunstmatige intelligentie'.
92. Het voorstel moet bovendien worden bekeken in samenhang met het voorstel voor een AI-verordening voor de relevante definities en eisen aan AI-systemen.
93. Toelichting, Achtergrond van het voorstel onder 1 bij de CRA. Zie over de NIS 2-richtlijn uitgebreid N.M. Brouwer & J.J.H. van Mil, 'Cybersecurity in Europa. De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2)', *NJB* 2023/674, afl. 10, p. 748-757.
94. CRA, Toelichting, Achtergrond van het voorstel onder 1.
95. Overweging 5 en 9 CRA.
96. Overweging 9 CRA, art. 3 sub 2 CRA.
97. Overweging 9 CRA.

bepaalde software (onlosmakelijk) is verbonden, (en die daardoor in ieder geval valt onder de CRA, maar mogelijk ook nog onder NIS 2)[98] en wanneer sprake is van min of meer zelfstandige software als dienst, die niet valt onder de CRA maar onder NIS 2.

Er bestaat – mede hierdoor – veel discussie over de toepasselijkheid van de CRA op software en services. Nederland, Duitsland en Denemarken hebben bijvoorbeeld opgeroepen om SaaS wel toe te voegen aan de reikwijdte van de CRA.[99] Zij geven aan dat onderscheid tussen digitale producten, processen en diensten niet te maken is, omdat deze onderling vrijwel altijd onlosmakelijk verbonden zijn.[100] Dit zou ertoe leiden dat vrijwel alle software via de hierboven omschreven bepalingen over gegevensverwerking op afstand, alsnog onder het bereik van de CRA kan vallen. Bovendien geeft de focus op producten een te sterke nadruk aan verbondenheid met een fysiek product, terwijl de samenleving juist steeds meer afhankelijk wordt van een breed scala aan – al dan niet aan een product verbonden – softwareprocessen en -diensten.[101]

3.3.2 AVG

De CRA en de AVG lopen op verschillende manieren gelijk op. Allereerst bevatten beide bepalingen over certificering en zegels of merktekens om de naleving van de betreffende regelgeving aan te tonen. Bij de AVG gaat dit over certificeringsmechanismen voor gegevensbescherming en gegevensbeschermingszegels en -merktekens, om de naleving van die verordening bij verwerkingen door verwerkingsverantwoordelijken en verwerkers aan te tonen.[102] De voorgestelde CRA heeft betrekking op een breder gebied, namelijk cyberbeveiliging door middel van CE-certificering. Zo'n CE-certificering kan ook cyberbeveiligingsmaatregelen met betrekking tot persoonsgegevens omvatten, indien een product met digitale elementen ook persoonsgegevens verwerkt.

Er kan dan ook overlap bestaan tussen CE-certificering op basis van de CRA en certificering op basis van de AVG. Volgens de European Data Protection Supervisor (EDPS) moet deze samenloop worden verduidelijkt.[103] De voorgestelde CRA heeft volgens de EDPS niet de bedoeling om de toepasselijkheid van de AVG, en met name de taken van de toezichthouders, te beperken. Bovendien suggereert de EDPS dat in de CRA zou moeten worden benadrukt dat het verkrijgen van een cyberbeveiligingscertificaat *niet* garandeert dat ook AVG-*compliant* wordt gehandeld.[104] Ook moet er afstemming komen tussen de Europese Commissie, ENISA, de European Data Protection Board (EDPB), en de Europese organisaties voor standaardisering.[105] Hoewel dit valide punten zijn, lijken die deels al te worden ondervangen in de CRA. Zo staat in overweging 17 van de considerans dat de CRA geen afbreuk mag doen aan de AVG, '*met inbegrip van bepalingen betreffende de vaststelling van certificeringsmechanismen voor gegevensbescherming en van gegevensbeschermingszegels en -merktekens, om de naleving van die verordening bij verwerkingen door verwerkingsverantwoordelijken en verwerkers aan te tonen*'. Bovendien lijkt het evident dat een cyberbeveiligingscertificaat niet leidt tot AVG-compliance, aangezien de AVG niet alleen maar over beveiliging gaat.

Ten tweede lopen de AVG en de CRA gelijk op omdat ze allebei bepalingen bevatten inzake beveiliging van persoonsgegevens: de AVG door het beginsel van integriteit en vertrouwelijkheid en de verplichtingen inzake beveiliging van de verwerking;[106] de CRA omdat die algemene beveiligingsverplichtingen bevat die ook van toepassing zijn op producten met digitale elementen die persoonsgegevens verwerken. In de CRA staat hierover dat de CRA kan bijdragen aan een betere bescherming van persoonsgegevens en privacy '*door consumenten en organisaties te beschermen tegen cyberbeveiligingsrisico's*'.[107]

De Europese Commissie merkt over de bescherming van persoonsgegevens in de toelichting bij de CRA op dat naleving van de vereisten van vertrouwelijkheid, integriteit en beschikbaarheid van informatie, het gemakkelijker zal maken om de in de AVG vereiste beveiliging van persoonsgegevens na te leven.[108] De EDPS verwelkomt deze samenloop dan ook en stelt dat beide wetten elkaar kunnen versterken. Wel roept de EDPS op om *data protection by design and by default* (DPbDD)[109] als verplichting ook op te nemen in de CRA. Dit zou de naleving van dat beginsel uit de AVG vergemakkelijken en anderzijds zou het ervoor zorgen dat persoonsgegevens naar behoren worden beschermd, nu de AVG zich niet direct richt op fabrikanten.[110] Hoewel dit een terecht punt is, vragen wij ons wel af wat dit in concrete situaties zou betekenen. Een fabrikant verwerkt in de regel minder persoonsgegevens bij de ontwikkeling van een product – behalve als dat bijvoorbeeld nodig is om input te leveren voor een algoritme. Het is dan ook onduidelijk wat het zou betekenen voor een fabrikant als de bepalingen uit de AVG inzake DPbDD ook van toepassing worden op een partij die geen persoonsgegevens verwerkt, en daarmee in principe volledig buiten het toepassingsbereik van de AVG valt. Tegelijkertijd geeft het Europees Comité voor gegevensbescherming in het richtsnoer over DPbDD aan dat de verplichtingen inzake DPbDD ook relevant kunnen zijn voor producenten van producten, diensten en toepassingen, '*om producten te ontwikkelen die aan de AVG voldoen*'.[111] In die zin zou het voor de volledige bescherming van persoonsgegevens wel meerwaarde kunnen hebben om deze verplichting ook op te nemen in de CRA en fabrikanten zo te stimuleren in het gehele ontwikkelproces

Het zou voor de volledige bescherming van persoonsgegevens wel meerwaarde kunnen hebben om deze verplichting ook op te nemen in de CRA en fabrikanten zo te stimuleren in het gehele ontwikkelproces rekening te houden met DPbDD

rekening te houden met DPbDD. Wij zijn benieuwd of de Uniewetgever op dit punt de EDPS gaat volgen.

3.3.3 (Voorstel voor een) AI-Verordening

In producten met digitale elementen kan gebruik worden gemaakt van kunstmatige intelligentie. Voor zover dat het geval is, lopen de voorgestelde CRA en de AI-verordening derhalve samen. Gelet op de ruime definitie van AI-systemen in het voorstel voor de AI-verordening, zal dat geregeld het geval zijn.[112] Qua systematiek sluiten de CRA en de AI-Verordening redelijk op elkaar aan. De AI-verordening richt zich primair tot aanbieders, namelijk de producenten en ontwikkelaars die AI-systemen op de markt brengen.

De CRA bevat bijzondere bepalingen over AI-systemen met een hoog risico zoals gedefinieerd in de voorgestelde AI-verordening,[113] die ook vallen binnen het toepassingsgebied van de CRA. AI-systemen worden beschouwd als hoogrisicosystemen als ze (onderdeel van) een product zijn dat valt onder een van de harmonisatiewetten die zijn opgenomen in bijlage II van de AI-verordening of als ze zijn opgenomen in bijlage III van de AI-verordening.[114] In bijlage III staan bijvoorbeeld AI-systemen op het gebied van biometrische identificatie, beheer en exploitatie van kritieke infrastructuur, onderwijs, werkgelegenheid en toegang tot essentiële diensten. In bijlage II wordt verwezen naar tal van EU-wetten, zoals wetgeving inzake liften, radioapparatuur, kabelbaaninstallaties, medische hulpmiddelen en beveiliging van de burgerluchtvaart.[115]

Indien producten met digitale elementen, die ook kunnen worden aangemerkt als AI-systemen met een hoog risico, binnen het toepassingsbereik van de CRA vallen en voldoen aan de in de CRA voorgeschreven eisen, worden die producten geacht in overeenstemming te zijn met de in de AI-verordening vastgestelde cyberbeveiligingseisen.[116] In die zin wordt de CRA voor wat betreft de invulling van verplichtingen met betrekking tot de AI-verordening gebruikt om compliance met de AI-verordening aan te tonen, terwijl dat bijvoorbeeld ten aanzien van de AVG nadrukkelijk niet de bedoeling is.

Voor AI-systemen met een hoog risico die ook vallen onder het toepassingsbereik van de CRA, geldt de conformiteitsbeoordelingsprocedure uit artikel 43 AI-Verordening in plaats van de conformiteitsbeoordelingsprocedure uit de CRA.[117] Voor AI-systemen met een hoog risico, die onder de CRA gelden als *kritieke* producten met digitale elementen (omdat zij zijn opgenomen in bijlage III bij de CRA), geldt een afwijkend regime. Deze producten dienen niet alleen te worden beoordeeld conform de beoordelingsprocedure uit de AI-verordening, maar ook conform de conformiteitsbeoordeling uit de CRA voor zover het de essentiële eisen van de CRA betreft.[118] Hiermee lijkt het systeem van conformiteitsbeoordelingen op basis van de CRA en de AI-Verordening redelijk goed in elkaar te passen.

4. Eerste ontvangst van het voorstel

Een groot aantal partijen heeft zich inmiddels positief over het voorstel uitgelaten. De meeste partijen, waaronder de Raad van de Europese Unie, zijn vooral positief over het feit dat nu wordt gekomen tot harmonisering van het juridisch kader inzake cyberbeveiliging voor producten met digitale elementen.[119] Die harmonisatie beschermt de open en concurrerende interne markt en voorkomt dat lidstaten zelf afwijkende regels gaan vaststellen.[120] Het Nederlandse kabinet is eveneens positief, bijvoorbeeld over de keuze om horizontale cybersecuritywetgeving op te stellen met verplichtingen voor alle marktspelers van digitale producten, vooral ook omdat er op dit moment geen wetgeving met zo'n invalshoek bestaat. Het kabinet verwacht

De meeste partijen zijn vooral positief over het feit dat nu wordt gekomen tot harmonisering van het juridisch kader inzake cyberbeveiliging voor producten met digitale elementen

98. Mits sprake is van een essentiële of belangrijke entiteiten, zie Brouwer & Van Mil 2023. NIS 2 bevat geen verwijzingen naar de CRA en noemt SaaS ook slechts één keer. Uit de NIS 2-richtlijn volgt in ieder geval niet zonder meer dat de NIS 2-Richtlijn niet van toepassing is op software waarop ook de CRA van toepassing is.
99. Non-paper on the principles of a Cyber Resilience Act, bijlage bij Brief van Ministerie EZK van 21 oktober 2022 betreffende Nederlandse non-paper CRA en position paper AI Act.
100. *Ibid*, p.2.
101. *Ibid*, p. 3.
102. Art. 42 jo. art. 5 lid 2 AVG.
103. EDPS, Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, punt 15.
104. *Ibid*, punt 31 onder 9.
105. *Ibid*, punt 22.
106. Art. 5 lid 1 sub f jo. art. 32 AVG.
107. Overweging 17 CRA.
108. Toelichting op de CRA, hoofdstuk 3 'Evaluatie, raadpleging van belanghebbenden en effectbeoordeling'.
109. Art. 25 AVG.
110. EDPS, Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.
111. EDPB, 'Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen', 2020, rn. 1.
112. Art. 3 sub 1 AI-verordening: *'software die is ontwikkeld aan de hand van een of meer van de technieken en benaderingen die zijn opgenomen in de lijst van bijlage I en die voor een bepaalde reeks door mensen gedefinieerde doelstellingen output kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd.'*
113. Art. 6 AI-Verordening.
114. Art. 6 lid 1 en lid 2 AI-Verordening.
115. Zie over de rationale achter deze indeling en het verschil in oude- en nieuweaanpak-productveiligheidsrecht uitgebreid T. de Graaf & G. Veldt, 'Productveiligheid en aansprakelijkheid voor AI', *NJB* 2021/3173, afl. 43, p. 3534-3544, p. 3537 e.v.
116. Art 8 lid 1 CRA jo. art. 15 AI-Verordening.
117. Art. 8 lid 2 CRA.
118. Art. 8 lid 3 CRA.
119. General Secretariat of the Council, 'Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 – Progress Report, 14477/22 18 november 2022, punt 10.
120. Zie bijvoorbeeld Europees Parlement, EU cyber-resilience act Briefing, december 2022 (online).

dat de CRA een vangnet zal vormen met essentiële eisen voor *alle* producten met digitale elementen, waarbij dan ruimte kan blijven voor *lex speciali* met additionele voorwaarden voor specifieke producten en diensten.[121] De EDPS is, zoals al eerder besproken, met name positief over het feit dat de beginselen van beveiliging en dataminimalisatie als essentieel onderdeel van de EU-brede cyberbeveiligingseisen worden gezien.

Naast deze positieve receptie klinkt er uiteraard ook kritiek en leven er nog vele vragen. Zo is er kritiek op de onduidelijkheid van de reikwijdte van de CRA, met name doordat bijvoorbeeld het begrip 'product met digitale elementen' onvoldoende gespecificeerd is. Dit punt van kritiek is bepaald niet uniek voor de CRA. Ook bij andere wetsvoorstellen is te zien dat de reikwijdte vaak ruim of zelfs enigszins ongelimiteerd overkomt. Zo wordt bij de AI-Verordening een zeer ruime definitie van AI-systemen gehanteerd, waardoor ook algoritmes die weinig met AI van doen hebben onder de reikwijdte van de verordening vallen.[122]

Bij de CRA lijkt de onduidelijkheid vooral te zien op het onderscheid tussen producten met digitale elementen enerzijds en diensten anderzijds, omdat diensten niet vallen onder de CRA maar onder NIS 2, mits binnen de daarin aangewezen sectoren. Zoals wij hierboven al hebben aangeven, is het vaststellen van dit onderscheid echter minder eenvoudig dan het op het eerste oog lijkt, zeker door de enigszins vage toevoegingen over gegevensverwerkingen op afstand. Ook de Nederlandse overheid vraagt zich af hoe het onderscheid moet worden gemaakt tussen SaaS en andere softwaretoepassingen.[123] Het Nederlandse kabinet ziet graag als oplossing dat alle hard- en softwareproducten, inclusief alle losse software, binnen de definitie en daarmee binnen het bereik van de CRA komen te vallen.[124] De Raad van de Europese Unie lijkt ook al te veronderstellen dat SaaS in bepaalde gevallen wel onder de CRA kan vallen, en geeft aan dat verscheidene lidstaten meer duidelijkheid willen over de mate waarin SaaS eventueel wel onder het bereik van de CRA kan vallen.[125] Tegelijkertijd zijn er ook partijen – met name vertegenwoordigers van bedrijven – die aangeven het juist positief te vinden dat software als product wordt beschouwd en SaaS daardoor niet onder de reikwijdte valt.[126]

Deze vragen gelden niet alleen voor de verhouding tussen de CRA en NIS 2, maar ook voor de verhouding van de CRA tot andere Europese regelgeving. Deze verhouding kan, zoals wij hierboven al aangeven, leiden tot vragen. Het kabinet is dan ook van oordeel dat die relatie verdere duidelijkheid behoeft om duplicatie te vermijden en samenhang te garanderen.[127] Ook het Europees Economisch en Sociaal Comité meent dat er meer richtsnoeren moeten komen voor de precieze regels en procedures die in de praktijk gelden voor fabrikanten, omdat er overlap kan ontstaan tussen de CRA en andere wetgeving over (cyber)beveiliging.[128] Onzekerheid over de toepasselijke regelgeving, kan immers leiden tot rechtsonzekerheid voor fabrikanten.

Naast deze vragen over de samenhang met andere wetten binnen het wetgevend kader waarbinnen de CRA zich bevindt, bestaat er ook meer inhoudelijke kritiek op de CRA. Wij bespreken enkele in het oog springende punten.

Verschillende partijen plaatsen vraagtekens bij de kosten en (praktische) uitvoerbaarheid van de CRA

Verschillende partijen plaatsen vraagtekens bij de kosten en (praktische) uitvoerbaarheid van de CRA. Digital Europe meent dat het voorstel te ver gaat omdat zowel de industrie als overheden worstelen met krappe middelen voor de beveiliging van digitale producten. Digital Europe stelt dan ook voor om pragmatisch om te gaan met het wetsvoorstel om echte resultaten te bereiken.[129] Andere partijen geven aan dat het een enorme uitdaging voor ondernemingen en industrieën zal zijn om de CRA binnen 24 maanden te implementeren.[130] Wij kunnen ons voorstellen dat dit bijvoorbeeld geldt voor de certificeringsinstanties, die op dit moment nog niet lijken te bestaan. Voordat een volledige procedure is geïmplementeerd waarbij certificeringsinstanties de juiste certificaten kunnen uitgeven, zal enige tijd verlopen. Bovendien zullen de certificeringsinstanties veel werkdruk krijgen door de inwerkingtreding van de CRA, terwijl op dit moment geen zekerheid bestaat dat er tegen die tijd (voldoende) geschikte instanties zijn om dat werk te doen.[131] Ook Europarlementariër Groothuis maakt zich zorgen over de uitvoerbaarheid van de CRA en het effect daarvan op de innovatiekracht van Europa. Volgens hem kan het straks maanden duren voordat een product de Europese markt op mag. Hij wijst er onder meer op dat het lastig zal zijn om aan genoeg experts te komen die de uitgebreide review kunnen uitvoeren.[132]

Bovendien geeft Groothuis aan dat hij zorgen heeft over de effecten van de CRA op de veiligheid. Hij wijst erop dat de CRA de verplichting bevat om alle kwetsbaarheden te melden bij ENISA, die vervolgens die informatie verspreidt. Hierdoor bestaat een risico dat ook kwaadwillenden bij deze informatie kunnen, omdat een systeem voor *coordinated vulnerability disclosure* ontbreekt.[133] In de CRA is wel een verwijzing opgenomen naar de gecoördineerde bekendmaking van kwetsbaarheden, waarin staat dat ENISA de informatie doorstuurt naar het CSIRT van de betrokken lidstaat dat in het kader van die gecoördineerde bekendmaking is aangewezen.[134] Ook bevat de CRA de verplichting voor fabrikanten om een gecoördineerd beleid inzake openbaarmaking van kwetsbaarheden in te voeren om de melding van kwetsbaarheden te vergemakkelijken en te voorkomen dat gedetailleerde informatie over de kwetsbaarheden aan het publiek of derden wordt vrijgegeven voordat die kwetsbaarheden zijn verholpen.[135] Het zal van de ontwikkeling van dit beleid afhangen in hoeverre kwaadwillenden misbruik kunnen maken van het meldsysteem.

Ook de conformiteitsbeoordelingsprocedure krijgt kritiek. Hierbij staan (vertegenwoordigers van) het bedrijfsleven en (vertegenwoordigers van) consumenten tegenover elkaar. Bedrijven menen dat de procedure te ver gaat; consumentenorganisaties menen dat de procedure

Bedrijven menen dat de procedure te ver gaat; consumentenorganisaties menen dat de procedure juist niet ver genoeg gaat

juist niet ver genoeg gaat. Zo stelt Digital SME – de Europese alliantie van kleine en middelgrote ICT-bedrijven – dat het goed is dat producten met een laag risico alleen aan minimale eisen hoeven te voldoen, omdat dit de kosten beperkt.[136] De Raad sluit zich hierbij aan en geeft aan dat meer onderzoek moet worden gedaan naar de impact van de CRA op kleine bedrijven en startups.[137] BEUC – de Europese consumentenorganisatie – is juist van mening dat de behoeften van consumenten beter beschermd worden door nog duidelijker in te voegen dat een onafhankelijke beoordeling door een derde altijd nodig is voor bepaalde producten die grotere risico's voor de consument inhouden, zoals slimme systemen voor in huis.[138]

Ten slotte is er vanuit Nederland kritiek op de verregaande bevoegdheden van de Commissie om onder omstandigheden producten uit de handel te halen. Het kabinet stelt bijvoorbeeld dat onder meer onderzocht moet worden of dit op gespannen voet zou kunnen komen te staan met de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid.[139]

5. Tot besluit

Als wij ver uitzoomen en kijken naar het gehele kader van regulering voor producten in het algemeen, valt op dat tot kortgeleden het digitale domein grotendeels gevrijwaard bleef van strikte (veiligheids)voorschriften. Het is onzes inziens een goede ontwikkeling dat ook het digitale domein zal worden onderworpen aan strenge(re) veiligheidsnormen. Tegelijkertijd kan niet worden ontkend dat in het data- en digitaliseringsdomein in korte tijd enorm veel verschillende wetten worden voorgesteld. Voor bedrijven en organisaties kan het een behoorlijke uitdaging zijn om alle regelgeving tijdig te doorgronden en te implementeren. Daarnaast is niet altijd duidelijk hoe verschillende wetten zich tot elkaar verhouden.

De CRA vormt weer een extra stukje in de legpuzzel van Europese regelgeving op het gebied van cybersecurity. Deze nieuwe verordening bevindt zich nog in een vroeg stadium. De Europese Commissie heeft het wetsvoorstel op 15 september 2022 gepresenteerd. Op dit moment zijn verschillende commissies uit het Europees Parlement, waaronder de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE) en de Commissie interne markt en consumentenbescherming (IMCO) gevraagd om hun feedback op het voorstel.

Het is nog niet te voorspellen wanneer de CRA precies in werking zal treden en hoeveel wijzigingen nog zullen plaatsvinden in het vervolgproces. De eerste reacties zijn overwegend positief, maar plaatsen ook vraagtekens bij vrij fundamentele aspecten uit de CRA, zoals de reikwijdte en de uitvoerbaarheid. Hoewel er derhalve nog de nodige wijzigingen zijn te verwachten, is al wel duidelijk dat de CRA grote impact zal hebben op fabrikanten van producten met digitale elementen. •

121. *Kamerstukken II* 2021/22, 22112, nr. 3552, Brief van de Minister van Buitenlandse zaken over Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie, Fiche: Verordening Cyber Resilience Act, par. 3 onder b.

122. Art. 3 sub 1 AI-Verordening. Zie De Graaf & Veldt 2021.

123. *Kamerstukken II* 2021/22, 22112, nr. 3552, Brief van de Minister van Buitenlandse zaken over Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie, Fiche: Verordening Cyber Resilience Act, par. 3 onder b.

124. *Ibid*, par. 3 onder b; General Secretariat of the Council, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 – Progress Report, 14477/22 18 november 2022, punt 14. Zie ook: I. Tasheva & I. Kunkel, 'In a hyperconnected world, is the EU cybersecurity framework connected?', *European View* 2022/2, p. 186-195, 191.

125. General Secretariat of the Council, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 – Progress Report, 14477/22, 18 november 2022, punt 11.

126. Eurosmart, 'Eurosmart welcomes the proposal for a cyber resilience act', 20 sept 2022, online via eurosmart.com/eurosmart-welcomes-the-proposal-for-a-cyber-resilience-act/.

127. *Kamerstukken II* 2021/22, 22112, nr. 3552, Brief van de Minister van Buitenlandse zaken over Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie, Fiche: Verordening Cyber Resilience Act, par. 3 onder b.

128. EESC, Opinion Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 [COM(2022) 454 final – 2022/0272 (COD)], punt 1.7 en 3.7.

129. Digital Europe is een brancheorganisatie voor bedrijven en organisaties die in de digitale transitie zitten. Digital Europe, 'Cyber Resilience Act: a big step forward for digital resilience but too much too soon', online via digitaleurope.org/news/cyber-resilience-act-a-big-step-forward-for-digital-resilience-but-too-much-too-soon/.

130. Eurosmart, 'Eurosmart welcomes the proposal for a cyber resilience act', 20 september 2022, online via eurosmart.com/eurosmart-welcomes-the-proposal-for-a-cyber-resilience-act/.

131. EESC, Opinion Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 [COM(2022) 454 final – 2022/0272 (COD)], punt 3.9.

132. AG Connect, 'Waarom er grote zorgen zijn over nieuwe Europese cybersecurity-wetgeving', 15 november 2022, online via agconnect.nl/artikel/waarom-er-grote-zorgen-zijn-over-nieuwe-europese-security-wetgeving.

133. *Ibid*.

134. Art. 11 lid 1 CRA.

135. Overweging 36 CRA.

136. Digital SME, 'The European Commission launches new Cyber Resilience Act to secure IoT devices in Europe', 19 september 2022, online via digitalsme.eu/the-european-commission-launches-new-cybersecurity-resilience-act-to-secure-iot-devices-in-europe/.

137. General Secretariat of the Council, Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 – Progress Report, 14477/22 18 november 2022, punt 12.

138. Bureau Européen des Unions de Consommateurs (BEUC), 'Cybersecurity of connected products could improve significantly following Commission proposal', 15 september 2022 online via beuc.eu/press-releases/cybersecurity-connected-products-could-improve-significantly-following-commission.

139. Art. 4 lid 2 VEU.