AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

www.austrian-law-journal.at
DOI: 10.25364/01.9:2022.2.4

Das Inverkehrbringen von Produkten mit digitalen Elementen nach dem Vorschlag der EU-Kommission für eine Verordnung über horizontale Cybersicherheitsanforderungen

Matthias Zußner ,* Graz

Abstract: Die EU-Kommission hat vor Kurzem den Vorschlag für ein Cyberresilienzgesetz vorgelegt, mit dem horizontale Verpflichtungen für wirtschaftliche Akteure u.a. im Zusammenhang mit dem Inverkehrbringen von Produkten mit digitalen Elementen eingeführt werden sollen.

Im vorliegenden Beitrag werden diese Bestimmungen erstmals in eingehender Form systematisiert und darüber hinaus einer kritischen Würdigung unterzogen.

Keywords: Cyberresilienzgesetz; Cybersicherheit; digitale Souveränität; Produkte mit digitalen Elementen.

I. Einleitung

Die EU-Kommission hat einen Entwurf für eine Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen vorgelegt (Cyberresilienzgesetz; im Folgenden kurz CRG-E[1]),[2] der derzeit in aller Munde ist[3] – häufiger freilich unter seinem englischen Titel „Cyber Resilience Act". Der Grund hierfür ist leicht verständlich, würde seine Um-

* Mag. Dr. Matthias Zußner ist Universitätsassistent (Post Doc) am Institut für Öffentliches Recht und Politikwissenschaften der Universität Graz.

1 Die Abkürzung steht für „Cyberresilienzgesetz-Entwurf".

2 Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.

3 S stellvertretend für Medienberichterstattungen https://www.promedianews.de/business/cyber-resilience-act-der-eu-umfasst-importeure/ (19.12.2022).

Fundstelle: *Zußner,* Das Inverkehrbringen von Produkten mit digitalen Elementen nach dem Vorschlag der EU-Kommission für eine Verordnung über horizontale Cybersicherheitsanforderungen, ALJ 2022, 180-197 (http://alj.uni-graz.at/index.php/alj/article/view/292).

setzung doch bedeuten, dass erstmals horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen eingeführt würden, die nicht nur Hersteller, sondern auch Importeure sowie Händler von Produkten mit digitalen Elementen von der Entwicklung bis zum Ende deren Lebenszyklus unmittelbar anwendbaren cybersicherheitsrechtlichen Verpflichtungen unterwerfen.[4] Die entsprechenden Vorschriften würden sich dabei außerordentlich gut in den bestehenden politischen Rahmen der neuen EU-Cybersicherheitsstrategie[5] einfügen, als dessen bislang tragende Säulen die Richtlinie zur Netz- und Informationssicherheit[6] (NIS-RL bzw – wohl bald: – NIS-2-RL[7]) sowie der Rechtsakt zur Cybersicherheit[8] gelten.[9] Denn die vorgeschlagene Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen würde bestehende Sicherheitslücken schließen, welche die bisherigen cybersicherheitsrechtlichen Unionsvorschriften bislang mit ihrem bereichsspezifischen und vertikalen Ansatz noch geltungsbereichsbezogen offen lassen.[10]

In einer immer stärker vernetzten Welt stellen Produkte mit digitalen Elementen freilich nicht erst seit heute erhebliche Einfallstore für breitflächige Cyberattacken, etwa auf kritische Infrastrukturen, dar.[11] Schon bislang schaden sie aber nicht nur der Sicherheit im Allgemeinen und (mit-)verursachen global betrachtet (geschätzte) jährliche Kosten der Cyberkriminalität iHv ca 5,5 Billionen EUR. Vielmehr wirken sie sich auch nachteilig auf das Funktionieren des Binnenmarkts für Produkte mit digitalen Elementen aus, weil sich ein „fragmentierte[r] [Rechts-]Rahmen mit möglicherweise voneinander abweichenden nationalen Vorschriften abzeichne[t]", der insgesamt für eine unbefriedigende Rechtsunsicherheit für Hersteller, Importeure oder Händler sowie „[un-]gleiche Wettbewerbsbedingungen" sorgen könnte.[12]

---

4 *Albrecht*, Cyber Resilience Act der EU-Kommission – Vorschlag für einheitliche Sicherheitsanforderungen an digitale Produkte, GWR 2022, 313 (313); s aber auch *Nwankwo*, European Commission's Initiative on Cyber Resilience Act: A New Height for Cybersecurity in the EU, ZD-Aktuell 2022, 01253; *Chiara*, The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. An introduction, Int. Cybersecur. Law Review 2022, 255 (257 ff).

5 Weitere Informationen abrufbar unter https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (19.12.2022).

6 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl 2016/194, 1.

7 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148; weiterführend *Kipker/Birreck/Niewöhner/Schnorr*, NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie, MMR 2021, 214.

8 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl L 2019/151, 15.

9 *Chiara*, The IoT and the new EU cybersecurity regulatory landscape, International Review of Law, Computers & Technology 2022, 118 (119 ff).

10 *Kipker*, Der EU „Cyber Resilience Act" kommt – und mit ihm die umfassendsten Compliance-Pflichten in der IT-Sicherheit, die es jemals gab, MMR-Aktuell 2022, 452009.

11 ErwGr 2 ff zum CRG-E; *Kipker*, MMR-Aktuell 2022, 452009.

12 Begründung des Vorschlags: COM(2022) 454 final; s auch ErwGr 3 zum Rechtsakt zur Cybersicherheit.

Der vorliegende Beitrag nimmt vor diesem Hintergrund ausgehend von Fragen des Anwendungsbereichs des CRG-E jene vorgeschlagenen Vorschriften über horizontale Cybersicherheitsanforderungen genauer in den Blick, die – in sehr unübersichtlicher und bislang im Schrifttum[13] noch nicht hinreichend klar dargestellter Weise – das Bereitstellen bzw das Inverkehrbringen am Markt betreffen. Ganz willkürlich erfolgt diese Auswahl freilich nicht, denn gerade die genannten Vorschriften verbinden Sicherheits- und Binnenmarktinteressen, die der Verordnungsvorschlag verfolgt, in jener Weise, welche die vorgeschlagene Verordnung erst kompetenzrechtlich legitimieren sollen.[14] Noch dazu sind sie auch praktisch von höchster Relevanz, weil sie von den relevanten Wirtschaftsakteuren in den meisten Fällen während des gesamten Produktlebenszyklus unter relativ hoher Strafandrohung zu beachten sind,[15] dh – vereinfacht ausgedrückt – darüber entscheiden, ob ein Produkt überhaupt am Markt platziert werden bzw bleiben darf.

Am Ende des Beitrags steht eine kurze kritische Würdigung des Mehrwerts, die die rechtlichen Voraussetzungen der Bereitstellung bzw des Inverkehrbringens von Produkten mit digitalen Elementen aus der Sicht des Verfassers mit sich bringen würden.

II. (Weiter) Anwendungsbereich

Aufgrund der Gefahren der beschrieben Lücken im System des unionalen Cybersicherheitsrechts hat die Kommission im CRG-E vorgeschlagen, dass diese für ein „breites Spektrum digitaler Produkte und zugehöriger Nebendienstleistungen" anwendbar sein, sich diese also auch auf „‚materielle digitale Produkte' (drahtlos und drahtgebunden) sowie nicht eingebettete Software" beziehen soll.[16] Konkret wird in Art 2 Abs 1 CRG-E festlegt, dass die Verordnung für Produkte mit digitalen Elementen gilt, deren bestimmungsgemäße oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Eine solche „logische" Verbindung wäre eine „virtuelle Darstellung einer Datenverbindung, die über eine Softwareschnittstelle hergestellt wird". Datenverbindungen, die „mit physikalischen Mitteln wie elektrischen oder mechanischen Schnittstellen, Drähten oder Funkwellen hergestellt" werden, gelten als „physisch".[17]

Als konsequente Folge des Umstandes, dass der Anwendungsbereich des CRG-E auch durch den Verwendungszweck bzw die (zumindest vorhersehbare) Verwendungsmöglichkeit für Datenverbindungen mit einem anderen Gerät oder Netzwerken mitabgegrenzt wird, gelten nicht nur Software- oder Hardwareprodukte als Bestandteile eines Produkts mit digitalen Elementen, sondern auch jene Datenfernverarbeitungslösungen, einschließlich entsprechender

---

13 Am bislang eingehendsten *Chiara*, Int. Cybersecur. Law Review 2022, insb 260 ff.

14 Damit geben sie dem Verordnungsvorschlag auch seine kompetenzrechtliche Legitimation nach Art 114 AEUV; vgl auch zur Begründung des Vorschlags: COM(2022) 454 final.

15 Zu dem „strengen Sanktionsregime" s auch *Kipker*, MMR-Aktuell 2022, 452009.

16 *Kipker*, MMR-Aktuell 2022, 447353.

17 Art 3 Nr 10 und 11 CRG-E.

Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden sollen, aber funktional eine Einheit mit den grundlegenden Software- oder Hardwarekomponenten bilden, weil sie für die Integration in ein elektronisches Informationssystem bestimmt sind.[18,19]

Ausdrücklich ausgeschlossen ist wegen nationalen Sicherheitsinteressen die Anwendung gemäß Art 2 Abs 5 CRG-E für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für militärische Zwecke entwickelt wurden oder die ausschließlich für die Verarbeitung von Verschlusssachen konzipiert sind.[20]

Weil entsprechende Rechtsgrundlagen eigene Produktanforderungen festlegen, die bereits ein ausreichendes Cybersicherheitsniveau über den gesamten Produktlebenszyklus hinweg gewährleisten und außerdem entsprechende Konformitätsbewertungsverfahren vorgesehen sind, sind gemäß Art 2 Abs 2 CRG-E auch solche Produkte mit digitalen Elementen vom Anwendungsbereich ausgenommen,[21] auf die entweder die Verordnung (EU) 2017/745 über Medizinprodukte[22], die Verordnung (EU) 2017/746 über In-vitro-Diagnostika[23] oder die Verordnung (EU) 2019/2144 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge[24] Anwendung finden. Soweit Produkte nach der Verordnung (EU) 2018/1139 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt zertifiziert worden sind, ist der

18 Art 3 Nr 8 CRG-E.

19 Art 3 Nr 1 CRG-E; vgl auch *Albrecht*, GWR 2022, 313.

20 Vgl Art 52 CRG-E (Vertraulichkeit).

21 Zum „interplay between the New Legislative Framework and IoT cybersecurity" *Chiara*, International Review of Law, Computers & Technology 2022, 122 ff.

22 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl L 2017/117, 1.

23 Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission, ABl L 2017/117, 176.

24 Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates und zur Aufhebung der Verordnungen (EG) Nr. 78/2009, (EG) Nr. 79/2009 und (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates sowie der Verordnungen (EG) Nr. 631/2009, (EU) Nr. 406/2010, (EU) Nr. 672/2010, (EU) Nr. 1003/2010, (EU) Nr. 1005/2010, (EU) Nr. 1008/2010, (EU) Nr. 1009/2010, (EU) Nr. 19/2011, (EU) Nr. 109/2011, (EU) Nr. 458/2011, (EU) Nr. 65/2012, (EU) Nr. 130/2012, (EU) Nr. 347/2012, (EU) Nr. 351/2012, (EU) Nr. 1230/2012 und (EU) 2015/166 der Kommission, ABl L 2019/325, 1.

Anwendungsbereich des CRG-E ebenfalls ausgeschlossen.[25,26]

Alle sonstigen Produkte mit digitalen Elementen, auf die die generalklauselartige Definition des Geltungsbereich in Art 2 Abs 1 iVm 3 Nr 1 CRG-E anwendbar ist,[27] unterfallen dem Anwendungsbereich dieses CRG-E. Damit ist freilich nicht ausgeschlossen, dass diese Produkte auch Sicherheitsrisiken mit sich bringen, für die der CRG-E keine rechtliche Antwort bereithält. Soweit Sicherheitsrisiken bestehen, die durch den CRG-E nicht erfasst werden und für die es auch keine speziellen harmonisierten Sicherheitsanforderungen gibt, gelten daher ausdrücklich die Vorgaben des allgemeinen EU-Produktsicherheitsrechts[28] (Art 7 CRG-E). Sofern Produkte mit digitalen Elementen dem Anwendungsbereich dieser CRG-E unterfallen, schließt das umgekehrt nicht aus, dass spezielle Produktsicherheitsvorschriften die Anliegen des CRG-E bereits hinreichend gewährleisten. Um entsprechende Doppelgleisigkeiten zu vermeiden, ist im CRG-E die Möglichkeit vorgesehen, dass der Anwendungsbereich des CRG-E oder bestimmte Teile desselben auf entsprechende Produkte durch delegierte Rechtsake der Kommission ausgeschlossen werden können.[29] Zentrale Voraussetzung hierfür ist, dass eine solche Einschränkung oder ein solcher Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und mit den sektorspezifischen Vorschriften dasselbe Schutzniveau erreicht wird, wie es diese Verordnung für entsprechende Sicherheitsrisiken gewährleistet.[30]

In bestimmten Fällen sieht Art 18 CRG-E ausdrücklich eine Konformitätsvermutung hinsichtlich der grundlegenden Anforderungen in Anhang I vor, womit aber gerade keine Ausnahme entsprechender Produkte vom Anwendungsbereich des CRG-E verbunden ist.[31]

Soweit der Anwendungsbereich des CRG-E eröffnet ist, dh für das entsprechende Produkt auch nicht durch delegierte Rechtsakte ausgeschlossen wurde, wird im CRG-E mit Wirkung

---

25 Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates, ABl L 2018/212, 1.

26 Art 2 Abs 3 CRG-E.

27 Obwohl der Anwendungsbereich nach Art 2 Abs 1 CRG-E als sehr weit(reichend) qualifiziert werden kann, bezieht er sich grundsätzlich nicht auf Dienstleistungen wie Cloud-Computing Dienste oder Cloud-Dienstmodelle wie Software-as-a-Service (SaaS), es sei denn, es wären solche Datenfernverarbeitungslösungen betroffen, „die sich auf ein Produkt mit digitalen Elementen beziehen und als entfernt stattfindende Datenverarbeitung verstanden werden, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wird und ohne die das Produkt mit digitalen Elementen eine seiner Funktionen nicht erfüllen könnte“ (ErwGr 9 zum CRG-E).

28 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die allgemeine Produktsicherheit, zur Änderung der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 87/357/EWG des Rates und der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates, COM/2021/346 final.

29 Beachte Art 50 CRG-E.

30 S zu alledem Art 2 Abs 4 CRG-E.

31 Siehe dazu noch unten V.

auf die Konformitätsbewertung nach anderen Sekundärrechtsakten der Union[32] die rechtliche Vermutung aufgestellt, dass Produkte mit digitalen Elementen, die mit den Vorgaben des vorliegenden CRG-E konform sind, bestimmte Anforderungen der entsprechenden anderen Sekundärrechtsakte jedenfalls erfüllen: Dies betrifft zunächst Hochrisiko-KI-Systeme iSd Art 6 des KI-Gesetzes.[33] Art 8 des CRG-E sieht vor, dass die Cybersicherheitsanforderungen des Art 15 KI-Gesetz als erfüllt gelten, sofern jenes Produkt mit digitalen Elementen, dass zugleich als Hochrisiko-KI-System gilt, den Anforderungen des Anhang I zum CRG-E entspricht und dasselbe Schutzniveau erreicht wird. Begleitend wird für entsprechende Hochrisiko-KI-Systeme außerdem vorgesehen, ob sich das Konformitätsbewertungsverfahren diesfalls nach Art 43 KI-Gesetz oder nach den Regeln dieses CRG-E richtet,[34] will heißen: ob ein Konformitätsverfahren nach dem CRG-E unterbleiben kann und nur ein Konformitätsbewertungsverfahren nach Art 43 KI-Gesetz durchgeführt zu werden braucht. Das Konformitätsbewertungsverfahren nach dem CRG-E muss nur dann weiterhin durchgeführt werden, wenn für das kritische Produkt mit digitalen Elementen, welches zugleich als Hochrisiko-KI-System gilt, nach Maßgabe des KI-Gesetzes ein rein internes Konformitätsbewertungsverfahren[35] durch den Hersteller durchzuführen wäre.[36]

Maschinenprodukte, die nach dem Vorschlag für eine Maschinenverordnung[37] in deren und zugleich in den Anwendungsbereich des CRG-E fallen, sollen bei entsprechendem Nachweis dieser Aspekte durch eine nach dem CRG-E ausgestellte EU-Konformitätserklärung als konform mit den grundlegenden Gesundheits- und Sicherheitsanforderungen nach Anhang III zur (vorgeschlagenen) Maschinenverordnung gelten.[38]

III. Grundanforderungen an das Inverkehrbringen von Produkten mit digitalen Elementen

Der CRG-E sieht vor, dass Produkte mit digitalen Elementen nur unter bestimmten Voraussetzungen auf dem Markt bereitgestellt, dh in Verkehr gebracht, werden dürfen. Diese Grundanforderungen werden durch Art 5 CRG-E festgelegt und betreffen einerseits technische Anforderungen an das Produkt mit digitalen Elementen, die Art und Weise, wie diese Produkte bereitgestellt werden sowie das Bereitstellungsverfahren an sich. Sie gelten sowohl für schlichte, als auch für „kritische" Produkte mit digitalen Elementen iSd Art 6 CRG-E.

---

32 *Chiara*, Int. Cybersecur. Law Review 2022, 266 ff.
33 *Kipker*, MMR-Aktuell 2022, 452009.
34 Vgl Art 8 Abs 2 und 3 CRG-E.
35 Vgl Art 24 Abs 1 iVm Anhang VI des CRG-E.
36 Vgl abermals Art 8 Abs 3 CRG-E.
37 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Maschinenprodukte, COM/2021/202 final.
38 Art 9 CRG-E.

Konkret setzt die Bereitstellung von Produkten mit digitalen Elementen ganz allgemein voraus, dass diese – erstens – den grundlegenden Anforderungen des ersten Abschnitts in Anhang I genügen, welcher seinerseits Sicherheitsanforderungen in Bezug auf die Eigenschaften von digitalen Produkten mit digitalen Elementen vorgibt. Zunächst wird dort festgelegt, dass Produkte mit digitalen Elementen so konzipiert, entwickelt und hergestellt werden müssen, dass sie gemessen an den Risiken, die von ihnen ausgehen, ein angemessenes Cybersicherheitsniveau erreichen. Sind ausnutzbare Schwachstellen bekannt, ist dieses Sicherheitsniveau – im Umkehrschluss – nicht erreicht. Das angemessene Cybersicherheitsniveau muss jedenfalls unter Nutzung der Standardkonfiguration garantiert sein und insoweit eine Abweichung von der sicheren Standardkonfiguration möglich ist, muss das Produkt jederzeit in seinen „ursprünglichen", dh sicheren, Zustand zurückversetzt werden können. Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme müssen jedenfalls durch geeignete Kontrollmechanismen vor unbefugtem Zugriff geschützt sein. Durch technische Vorkehrungen minimiert werden müssen weiters die Gefahr der Manipulation von Daten oder Systemfunktionen, mögliche Beeinträchtigungen der Datensicherheit sowohl von nicht personenbezogenen als auch von personenbezogenen Daten, potentielle Angriffsflächen auf das Produkt bzw dessen Funktionen und die möglichen Folgewirkungen eines tatsächlichen Angriffs. Außerdem sind die Verfügbarkeit wesentlicher Funktionen gegen Überlastungsangriffe auf Server sowie die Eindämmung solcher Angriffe zu gewährleisten. Ferner sind sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Systemvorgänge bereitzustellen. Sichergestellt werden muss schließlich auch, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Aktualisierungen und die Benachrichtigung der Nutzer über verfügbare Aktualisierungen.[39]

Zweitens müssen die Produkte mit digitalen Elementen vor ihrer Bereitstellung ordnungsgemäß installiert worden sein sowie gewartet und bestimmungsgemäß oder unter vernünftigerweise vorhersehbaren Umständen verwendet sowie gegebenenfalls aktualisiert werden können.[40]

Drittens müssen bestimmte prozedurale Vorkehrungen bzw Begleitmaßnahmen bereits im Zusammenhang mit dem Bereitstellungsprozess eingehalten werden.[41] Die entsprechenden Pflichten sind im zweiten Abschnitt des Anhanges I des CRG-E genannt und richten sich an

[39] Aufzählung Abschnitt 1 des Anhanges I des CRG-E.

[40] Art 5 Nr 1 CRG-E.

[41] Art 5 Nr 2 CRG-E.

die Hersteller von Produkten mit digitalen Elementen. Diese müssen die einzelnen Kompetenzen des Produkts mit digitalen Elementen in einer Stückliste[42] und in einem gängigen maschinenlesbaren Format aufzählen und entsprechende Schwachstellen ermitteln und dokumentieren. Sind Schwachstellen vorhanden, müssen diese nach Möglichkeit bereits vor der Bereitstellung behoben werden und muss vor dem Bereitstellen jedenfalls eine Strategie für eine koordinierte Offenlegung von Schwachstellen erarbeitet werden. Außerdem muss es eine Kontaktadresse für die Meldung der in einem Produkt mit digitalen Elementen entdeckten Schwachstellen geben.

Produkte, welche die drei genannten Produktanforderungen nicht erfüllen, dürfen von vornherein nicht von einem Hersteller oder Importeur auf dem Markt bereitgestellt, dh in Verkehr gebracht, werden.[43] Auch der Importeur hat dies vor dem Inverkehrbringen zu überprüfen.[44]

IV. Sonstige (versteckte) Voraussetzungen für das Inverkehrbringen von Produkten mit digitalen Elementen

Es finden sich zahlreiche weitere allgemeine Voraussetzungen für das Bereitstellen bzw das Inverkehrbringen von Produkten mit digitalen Elementen verstreut in den Art 10 ff CRG-E. Welche Voraussetzungen das sind, hängt davon ab, wer das Produkt mit digitalen Elementen bereitstellt. In der Tat wird ein breites Spektrum an Stakeholdern das neue Regelwerk einhalten müssen.[45]

A. Hersteller

Die meisten Verpflichtungen adressieren den Hersteller. Bevor diese ein Produkt mit digitalen Elementen in Verkehr bringen, müssen sie nach Art 23 iVm Anhang V des CRG-E eine technische Dokumentation erstellt haben, die eine systematische Bewertung der Cybersicherheitsrisiken enthält.[46] Die Bewertung muss alle relevante Cybersicherheitsaspekte des Produkts mit digitalen Elementen, einschließlich der Schwachstellen, von denen Kenntnis besteht, sowie alle von Dritten bereitgestellten einschlägigen Informationen enthalten.[47] Die technische Dokumentation enthält alle einschlägigen Daten oder Einzelheiten darüber, wie der Hersteller sicherstellt, dass das Produkt mit digitalen Elementen und die vom Hersteller festgelegten

---

42 Art 10 Abs 15 CRG-E: Die Kommission kann im Wege von Durchführungsrechtsakten das Format und die Elemente der Software-Stückliste gemäß Anhang I Abschnitt 2 Nummer 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 51 Absatz 2 genannten Prüfverfahren erlassen.

43 Art 10 Abs 1, Art 13 Abs 1 CRG-E.

44 Art 13 Abs 1 CRG-E.

45 *Chiara*, Int. Cybersecur. Law Rev 2022, 261.

46 Art 10 Abs 7 CRG-E.

47 Art 10 Abs 5 CRG-E.

Verfahren den grundlegenden Anforderungen in Anhang I genügen sowie (zumindest) die in Anhang V genannten Angaben.[48]

Im Zeitpunkt des Inverkehrbringens von Produkten mit digitalen Elementen müssen die Hersteller weiters bereits geeignete Strategien und Verfahren bzw entsprechende Konzepte zur Offenlegung, Bearbeitung und Behebung von (System-)Schwachstellen ausgearbeitet haben.[49] Außerdem müssen die Hersteller gewährleisten, dass den Produkten mit digitalen Elementen die in Anhang II des CRG-E genannten Informationen und Anleitungen in elektronischer Form oder in Papierform beigefügt sind[50] und dass die Konformität von Produkten mit digitalen Elementen auch bei einer Serienherstellung sichergestellt bleibt.[51]

Eine weitere – und zugleich wohl eine der wichtigsten – Voraussetzungen, die im Zeitpunkt des Inverkehrbringens eines Produkts mit digitalen Elementen durch den Hersteller vorliegen muss ist, dass ein positives Konformitätsbewertungsverfahren gemäß Art 24 CRG-E vom Hersteller oder von einem schriftlich benannten Bevollmächtigten iSd Art 12 CRG-E durchgeführt wurde, eine sogenannte EU-Konformitätserklärung gemäß Art 20 CRG-E ausgestellt sowie eine CE-Kennzeichnung nach den Art 22 f CRG-E gut sichtbar, leserlich und dauerhaft auf dem Produkt mit digitalen Elementen angebracht wurde.[52] Die EU-Konformitätserklärung muss ihrerseits entweder dem Produkt mit digitalen Elementen beigegeben werden oder – unter entsprechender Angabe in den Anleitungen und Informationen gemäß Anhang II – über eine Internetadresse abgerufen werden können bzw dort einsehbar sein.[53] Alle letztgenannten Aufgaben kann auch ein schriftlich benannter Bevollmächtigter durchführen,[54] dennoch müssen sie bereits im Zeitpunkt des Inverkehrbringens vorliegen.

B. Einführer (Importeur)

Bevor Importeure ein Produkt mit digitalen Elementen in Verkehr bringen, haben diese sicherzustellen, dass der Hersteller ein geeignetes Konformitätsbewertungsverfahren nach Art 24 CRG-E durchgeführt und die technische Dokumentation erstellt hat. Außerdem muss der Importeuer sicherstellen, dass das Produkt mit digitalen Elementen mit der in Art 22 CRG-E genannten CE-Kennzeichnung versehen ist und dem Produkt die Informationen und Gebrauchsanleitungen nach Anhang II des CRG-E in leicht verständlicher Sprache beigefügt sind.[55]

Das zulässige Inverkehrbringen durch den Importeur setzt weiters voraus, dass der Importeur nicht annimmt bzw annehmen muss, dass ein Produkt mit digitalen Elementen oder die

48 Art 23 Abs 1 CRG-E.
49 Art 10 Abs 6 CRG-E.
50 Art 10 Abs 10 CRG-E.
51 Art 10 Abs 9 CRG-E.
52 Art 23 Abs 1 CRG-E.
53 Art 10 Abs 11 CRG-E.
54 Vgl Art 12 Abs 1 CRG-E.
55 Art 13 Abs 2, 5 CRG-E.

vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht (mehr) genügen. In diesem Fall ist das Inverkehrbringen erst (wieder) zulässig, wenn die Konformität dieses Produkts und der vom Hersteller festgelegten Verfahren mit den grundlegenden Anforderungen in Anhang I (wieder) hergestellt ist.[56]

Außerdem setzt ein zulässiges Inverkehrbringen des Produkts mit digitalen Elementen durch den Importeur voraus, dass entweder auf der Verpackung oder in den beigelegten Unterlagen entweder der Name, der eingetragene Handelsname oder die eingetragene Handelsmarke sowie die Postanschrift und die E-Mailadresse angegeben sind.[57]

Schon im Zeitpunkt des Inverkehrbringens des Produkts mit digitalen Elementen muss der Importeur ein Exemplar der EU-Konformitätserklärung für die Marktüberwachungsbehörden bereithalten und diesen ab diesem Zeitpunkt auf deren Verlangen eine technische Dokumentation vorlegen können.[58] Außerdem muss der Importeuer bereits im Zeitpunkt des Inverkehrbringens des Produkts mit digitalen Elementen die Namen und Anschriften aller Wirtschaftsakteure vorweisen können, von denen er Produkte mit digitalen Elementen bezogen hat.[59]

Nimmt ein Importeur wesentliche Änderungen an dem Produkt mit digitalen Elementen vor, muss er u.a. vor dem Inverkehrbringen des Produkts bzw soweit abgrenzbar hinsichtlich der betroffenen Teile alle Voraussetzungen erfüllen, die auch für den Hersteller gelten.[60] Gleiches gilt für den Importeur, wenn er ein Produkt mit digitalen Elementen unter seinem eigenen Namen oder seiner eigenen Marke in Verkehr bringt.[61]

C. Händler

Bevor Händler ein Produkt mit digitalen Elementen auf dem Markt bereitstellen müssen diese überprüfen, ob das Produkt mit digitalen Elementen vom Hersteller mit einer CE-Kennzeichnung versehen wurde, dem Produkt vom Hersteller verständliche Anleitungen und Informationen iSd Anhangs II des CRG-E beigelegt wurden, die EU-Konformitätserklärung dem Produkt vom Hersteller beigelegt oder im Internet einsehbar gemacht wurde und – soweit das Produkt von einem Importeur bezogen wurde – die Kontaktdaten des Importeurs von diesem beigefügt wurden.[62]

---

56 Art 13 Abs 3 CRG-E.
57 Art 13 Abs 4 CRG-E.
58 Art 13 Abs 7 CRG-E.
59 Art 17 CRG-E.
60 Art 16 CRG-E.
61 Art 15 CRG-E.
62 Art 14 Abs 2 CRG-E.

Sind diese Anforderungen erfüllt darf der Händler das Produkt mit digitalen Elementen grundsätzlich in Verkehr bringen. Hat der Händler aber bzw muss dieser Grund zur Annahme haben, dass ein Produkt mit digitalen Elementen oder die vom Hersteller festgelegten Verfahren den grundlegenden Anforderungen in Anhang I nicht genügen, darf der das entsprechende Produkt nicht (mehr) in Verkehr bringen.[63]

Nimmt ein Händler wesentliche Änderungen an dem Produkt mit digitalen Elementen vor, muss er u.a. vor dem Inverkehrbringen des Produkts bzw soweit abgrenzbar hinsichtlich der betroffenen Teile alle Voraussetzungen erfüllen, die auch für den Hersteller gelten.[64] Gleiches gilt für den Händler, wenn er ein Produkt mit digitalen Elementen unter seinem eigenen Namen oder seiner eigenen Marke in Verkehr bringt.[65]

Außerdem muss der Händler bereits im Zeitpunkt des Inverkehrbringens des Produkts mit digitalen Elementen die Namen und Anschriften aller Wirtschaftsakteure vorweisen können, von denen er Produkte mit digitalen Elementen bezogen hat.[66]

V. Konformität des Produkts

Wie *Rudolf von Jehring* gesagt hat, ist „[d]ie Form … die geschworene Feindin der Willkür" und damit „die Zwillingsschwester der Freiheit".[67] Das trifft im Allgemeinen aber etwa nicht nur auf die Idee grundrechtlicher Eingriffsvorbehalte zu, nach denen die Form der Rechtsgrundlage über die Zulässigkeit des staatlichen Eingriffs in entsprechende Freiheitssphären (mit-)entscheiden soll, sondern gilt sinngemäß auch für Verfahren zur ex-ante Überprüfung der Einhaltung spezifischer, insbesondere grundrechtskonkretisierender, Rechtsvorschriften *inter privatos*.

Wie bereits oben[68] ausgeführt wurde, ist für jedes Produkt mit digitalen Elementen vor seinem Inverkehrbringen u.a. ein Konformitätsbewertungsverfahren durchzuführen, worin die Übereinstimmungen mit den Vorgaben nach Anhang I überprüft wird, das positiv ausfallen muss und mit der Ausstellung einer EU-Konformitätsbewertung durch den Hersteller[69] endet. Sie steht damit am Ende jedes Konformitätsbewertungsverfahren für Produkte mit digitalen Elementen und hat in ihrem Aufbau dem Muster in Anhang IV zu entsprechen und die in den einschlägigen Konformitätsbewertungsverfahren gemäß Anhang VI angegebenen Elemente zu enthalten.

---

63 Art 14 Abs 4 CRG-E.

64 Art 16 CRG-E.

65 Art 15 CRG-E.

66 Art 17 CRG-E.

67 Hier zitiert nach *Jhering*, Geist des römischen Rechts auf den verschiedenen Stufen seiner Entwicklung, Zweiter Theil, Zweite Abteilung, Dritte, verbesserte Auflage (1875) 470.

68 Oben IV.A.

69 Art 10 Abs 7 CRG-E.

In bestimmten Fällen sieht Art 18 CRG-E ausdrücklich eine Konformitätsvermutung hinsichtlich der grundlegenden Anforderungen in Anhang I vor, was im Konformitätsbewertungsverfahren materiell-rechtlich zu berücksichtigen ist und dieses damit stark vereinfacht. Das gilt allgemein für Produkte mit digitalen Elementen und den vom Hersteller festgelegten Verfahren, die mit (Teilen von) harmonisierten EU-Normen übereinstimmen und die im Amtsblatt der EU veröffentlicht wurden[70] oder die mit den technischen Spezifikationen nach Ar 19 CRG-E übereinstimmen.[71]

Speziell ist eine entsprechende Konformitätsvermutung dann vorgesehen, wenn eine EU-Konformitätserklärung oder ein Cybersicherheitszertifikat im Rahmen eines gemäß der Verordnung (EU) 2019/881[72] angenommenen und von der Kommission nach Art 18 Abs 4 CRG-E im Wege von Durchführungsrechtsakten ausgewiesenen europäischen Systems für die Cybersicherheitszertifizierung ausgestellt wurde.[73] Die Konformitätsvermutung ersetzt aber nicht einmal dann, wenn sie bei einem Produkt mit digitalen Elementen zur Gänze zum Tragen kommt, die Durchführung eines (förmlichen) Konformitätsbewertungsverfahren nach Art 24 CRG-E.

Nach Art 24 iVm Anhang VI stehen grundsätzlich drei verschiedene Arten von Konformitätsbewertungsverfahren auf der Grundlage entsprechender Modul(-abläufe) zur Verfügung: Gewählt werden kann zwischen dem sog „internen Kontrollverfahren“ (Typ 1), der „internen Fertigungskontrolle zur Überprüfung der Konformität mit einem EU-Baumuster“, welches im Rahmen eines EU-Baumusterprüfverfahren ausgestellt wurde (Typ 2) sowie einer „Konformitätsbewertung auf der Grundlage einer umfassenden Qualitätssicherung“ (Typ 3).

Während beim „internen Verfahren“ alle Verfahrensschritte einschließlich der Prüfung der Konformität vom Hersteller selbst aufgrund des Modul A des Anhanges VI durchgeführt werden (Anhang VI Modul A), sind in den beiden anderen Konformitätsbewertungsverfahren andere Stellen involviert.

Einer „internen Fertigungskontrolle zur Überprüfung der Konformität mit einem EU-Baumuster“, die der Hersteller – in einem zweiten Schritt – selbst durchführt (Anhang VI Modul C), geht – in einem ersten Schritt – eine EU-Baumusterprüfung voraus (Anhang VI Modul B). Bei dieser untersucht eine notifizierte Stelle[74] die technische Konzeption und Entwicklung eines Produkts und die vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen

70 Art 18 Abs 1 CRG-E.

71 Art 18 Abs 2 CRG-E.

72 Rechtsakt zur Cybersicherheit (Fundstelle: FN 8).

73 Art 18 Abs 3 CRG-E.

74 Siehe noch unten bei FN 77 und 78.

und prüft und bescheinigt allenfalls, dass ein Produkt mit digitalen Elementen den grundlegenden Anforderungen in Anhang I Abschnitt 1 des CRG-E genügt und dass der Hersteller die grundlegenden Anforderungen in Anhang I Abschnitt 2 CRG-E erfüllt. Diese Bescheinigung erfolgt durch die Ausstellung einer EU-Baumusterprüfbescheinigung, die ihrerseits die Grundlage für eine „interne Fertigungskontrolle auf der Grundlage von Modul C ist und bei dem der Hersteller – wie bereits beschrieben – die Konformität des Produkts mit einem EU-Baumuster selbst bescheinigt, in dem er eine EU-Konformitätserklärung ausstellt.

Demgegenüber ist das Konformitätsbewertungsverfahren auf der Grundlage einer umfassenden Qualitätssicherung (Anhang VI Modul H) zwar nicht formal zweigeteilt. Der Hersteller muss aber bei der notifizierten Stelle seiner Wahl die Bewertung seines Qualitätssicherungssystems für die betreffenden Produkte mit digitalen Elementen beantragen. Diese Bewertung fällt (nur) dann positiv aus, wenn das Qualitätssicherungssystem die Konformität des Produkts mit den grundlegenden Anforderungen in Anhang I Abschnitt 1 und die Konformität der vom Hersteller festgelegten Verfahren zur Behandlung von Schwachstellen mit den grundlegenden Anforderungen in Anhang I Abschnitt 2 gewährleistet. Die Konformitätserklärung des Produkts auf der Grundlage des geprüften Qualitätssicherungssystems hat der Hersteller jedoch abermals selbst vorzunehmen.

Eine Einschränkung der Wahlmöglichkeit zwischen den drei Verfahren besteht nur insoweit, als das „interne“ Verfahren grundsätzlich dann nicht gewählt werden darf, wenn ein sog „kritisches“ Produkt mit digitalen Elementen iSd Art 6 CRG-E vorliegt, dh solche Produkte, die zu einer der in Anhang III zum CRG-E angeführten Kategorie gehören und die dort unter Berücksichtigung des mit diesen Produkten verbundenen Cybersicherheitsrisikos in zwei Klassen, nämlich die Klassen I und II, unterteilt werden. Zur Klasse I zählen u.a. Software für Identitätsmanagementsysteme, eigenständige und eingebettete Browser, Passwort-Manager, Netzmanagementsysteme. Zur – risikoreicheren – Klasse II etwa Public-Key-Infrastrukturen, die Aussteller digitaler Zertifikate, Firewalls, Angriffserkennungs- und/oder Präventionssysteme für den industriellen Einsatz, Router, Modems für die Internetanbindung oder sichere Kryptoprozessoren (um jeweils nur Beispiele zur Illustration zu nennen).

Art 6 Abs 4 CRG-E bestimmt nun zwar, dass kritische Produkte mit digitalen Elementen generell den Konformitätsbewertungsverfahren nach Art 24 Abs 2 und 3 CRG-E unterliegen sollen. Und das würde die Durchführung eines internen Verfahrens (auf der Grundlage von Modul A gemäß Anhang VI) ausschließen. Art 24 CRG-E sieht aber – als speziellere Norm zum Konformitätsverfahren – die Wahlmöglichkeit auch eines internen Verfahrens in jenen Fällen vor, in denen ein kritisches Produkt der Klasse I betroffen ist. Dies gilt aber nur dann, wenn der Hersteller oder sein Bevollmächtigter bei der Bewertung der Konformität eines kritischen Produkts mit digitalen Elementen – wenn auch nur – der Klasse I des Anhanges III sowie bei

der Umsetzung der Verpflichtungen des Anhanges I[75] entweder unionsrechtlich harmonisierte Normen, gemeinsame Spezifikationen oder europäische Systeme für die Cybersicherheitszertifizierung gemäß Art 18 anwenden kann.[76]

Der Vollständigkeit halber sei an dieser Stelle erwähnt, dass die im Rahmen zweier Konformitätsbewertungsverfahrenstypen jeweils einbezogene notifizierte (Konformitätsbewertungsstelle eine solche ist, die von einer notifizierenden Behörde[77] auf Antrag notifiziert wurden[78] und hierfür die Anforderungen des Art 29 CRG-E erfüllen müssen.

VI. Allgemeine Vorschriften mit Relevanz (auch) für die Sicherung der Einhaltung der Regeln über das Inverkehrbringen von Produkten mit digitalen Elementen

Die Marktüberwachung und Kontrolle von Produkten mit digitalen Elementen wird von zumindest einer Marktüberwachungsbehörde durchgeführt, die auf der Grundlage der Verordnung (EU) 2019/1020[79] vom jeweiligen Mitgliedstaat für die Zwecke des CRG-E benannt wurde[80] und die in relevanten Fällen mit der ENISA und anderen Stellen nach den Vorschriften der Art 45 f CRG-E zusammenarbeitet. Gemeinsame Tätigkeiten der Marktüberwachungsbehörden mehrerer Mitgliedstaaten sind vorgesehen (Art 48 CRG-E).

Nach Art 53 CRG-E haben die Mitgliedstaaten Vorschriften über Sanktionen zu erlassen, die bei Verstößen der Wirtschaftsakteure gegen diese Verordnung zu verhängen sind, und alle für die Durchsetzung der Sanktionen erforderlichen Maßnahmen zu treffen.

Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sei. Nach Abs 3 leg cit soll bei Nichteinhaltung der grundlegenden Anforderungen in Anhang I oder Verstößen gegen die in den Artikeln 10 und 11 festgelegten Pflichten, sogar Geldbußen von bis zu 15 000 000 EUR oder – im Falle von Unternehmen und wenn der Betrag höher ist – von bis zu 2,5 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Bei Verstößen gegen andere Pflichten aus dieser Verordnung werden Geldbußen von bis zu 10 000 000 EUR oder – im Falle von Unternehmen und sofern der Betrag höher ist – von bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt.

---

75 Der Normtext spricht von der „Festlegung" entsprechender Verfahren.

76 Umkehrschluss aus Art 24 Abs 2 CRG-E.

77 Art 26 ff CRG-E.

78 Art 32 CRG-E.

79 Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011, ABl L 2019/169, 1.

80 Art 41 Abs 1 und 2 CRG-E.

VII. Kritische Würdigung und Schlussgedanken

Wie gezeigt worden ist, sollen die Vorschriften der von der EU-Kommission vorgeschlagenen Verordnung Lücken in der Cybersicherheitsarchitektur der Union schließen, dabei aber keine Doppelgleisigkeiten für Konformitätsbewertungsverfahren von Produkten aufgrund ein und desselben Maßstabes erzeugen. Zugleich sollen sie eine Fragmentierung des produktbezogenen Rechts der Mitgliedstaaten betreffend horizontale Verpflichtungen von Wirtschaftsakteuren im Bereich der Cybersicherheit verhindern. Mit dem vorliegenden CRG-E soll also – neben der DSGVO oder dem (vorgeschlagenen) KI-Gesetz – nicht nur ein weiterer Schutzschirm vor speziellen faktischen Gefahren der Digitalisierung aufgespannt werden. Durch die Harmonisierung der horizontalen Cybersicherheitsanforderungen im Verordnungsrang soll vielmehr auch ein Beitrag zum Aufbau jener Voraussetzungen geleistet werden, die einen leichteren Austausch von Produkten mit digitalen Elementen am Binnenmarkt vorantreiben sollen. In Art 4 Abs 1 CRG-E wird vor diesem Hintergrund sogar ausdrücklich festgeschrieben, dass die Mitgliedstaaten in den von der vorgeschlagenen Verordnung erfassten Aspekten nicht die Bereitstellung von Produkten mit digitalen Elementen behindern dürfen, die den Bestimmungen des CRG-E entsprechen.

Betrachtet man die genannten Zielsetzungen des CRG-E kritisch, besteht dabei gar nicht so sehr die erst jüngst von *Kipker*[81] hervorgehobene Gefahr einer unsystematischen Überregulierung, wonach der Rechtsakt zur Cybersicherheit[82] und konkret die darin enthaltenen Vorschriften über den Zertifizierungsrahmen für die Cybersicherheit (Art 46 ff) im Gefüge der EU-Cybersicherheitsarchitektur ihren Eigenstand verlören oder erst behaupten müssten. Denn der Rechtsakt zur Cybersicherheit bezieht sich zwar lediglich auf (Komponenten) von „Netz- und Informationssystem[-en]“ iSd NIS-RL[83] und sein Konformitätsbewertungsverfahren hat anders als der CRG-E einen rein risikobasierten Ansatz.[84] Schon in Anbetracht der allgemeinen Konformitätsbewertung des Art 18 CRG-E kann nun aber ein funktionierender Zertifizierungsrahmen für die Cybersicherheit die Handhabung der Konformitätsbewertung nach dem CRG-E für solche Produkte erheblich entlasten, die sowohl in den Anwendungsbereich des Gesetzes zur Cybersicherheit als auch in den des CRG-E fallen, soweit sich die Anforderungen decken. Wenn nämlich ein Produkt mit digitalen Elementen den Vorgaben des Gesetzes zur Cybersicherheit entspricht, müssen nur mehr sonstige Anforderungen an das Inverkehrbringen von Produkten mit digitalen Elementen nach dem CRG-E geprüft werden.[85] Der CRG-E verdrängt daher diesbezüglich keineswegs die eigene Bedeutung des Rechtsaktes zur Cybersicherheit, sondern schließt nur die offene Flanke seines bereichsspezifischen und vertikalen Ansatzes.

---

81 *Kipker*, MMR-Aktuell 2022, 452009.
82 FN 8.
83 Vgl Art 2 Nr 2 Rechtsakt zur Cybersicherheit iVm Art 4 Nr 1 Richtlinie (EU) 2016/1148 (NIS-RL).
84 Vgl die Sicherheitsziele in Art 51 Rechtsakt zur Cybersicherheit.
85 Allgemein oben V.

Die eigentliche Kritik am CRG-E betrifft zunächst kompetenzrechtliche Fragen, stützt sich der CRG-E doch wie alle anderen Rechtsakte der Union zur Cybersicherheit auf Art 114 AEUV.[86] Nach Art 114 AEUV ist die Union ermächtigt, Rechtsakte zu erlassen, die der Verwirklichung der Ziele des Binnenmarkts dienen, dh entweder relevante Hemmnisse bei der Ausübung der Grundfreiheiten abbauen oder spürbare Wettbewerbsverzerrungen verhindern sollen.[87] Beides kann zwar auch präventiv erfolgen, es muss aber belegt bzw plausible begründet werden können, dass negative Effekte für den Binnenmarkt nicht nur mittelbar und hypothetisch sind.[88] Durch die Harmonisierung technischer Spezifikationen von Produkten mit digitalen Elementen wird nun zwar zunächst idS der Eindruck erweckt, der CRG-E wäre ein notwendiger Baustein für die Verwirklichung eines Binnenmarkts für solche Produkte. Umgekehrt wird aber von der Kommission gerade nicht bestritten, dass es bereits einen Markt für Produkte mit digitalen Elementen gibt, ist doch eine Grundprämisse der Begründung des CRG-E, dass die Zahl von solchen Produkten kontinuierlich steigt.[89] Unterschiedliche Rechtslagen in den Mitgliedstaaten haben die Entstehung dieses Marktes also bislang nicht aufgehalten. Dass dieser noch nicht oder nur „suboptimal funktioniert"[90] oder dass der Wettbewerb auf diesem Markt verfälscht wäre, wird in der Begründung des CRG-E nicht einmal angesprochen. Vielmehr wird darin lediglich vermutet, dass es in den Mitgliedstaaten bald einen „*möglicherweise* voneinander abweichenden" Cybersicherheitsrechtsrahmen geben kann und dass der CRG-E einen Beitrag für (möglichst) „gleiche "Wettbewerbsbedingungen schaffen soll.[91] Es ist dagegen aber rechtlich notwendig zu begründen, warum die Nichterlassung des CRG-E zu einer spürbaren Wettbewerbsbeeinträchtigung führt. Rechtsangleichung allein ist auch im Lichte der Binnenmarktkompetenz nach Art 114 AEUV kein „Selbstzweck":[92] Erstens setzt das Funktionieren von Wettbewerb auf einem Markt nicht zwingend und nicht immer alleine die Herstellung eines (voll-)harmonisierten Rechtsrahmens voraus; sonst hätte Art 114 AEUV überhaupt keine inneren Grenzen. Zweitens würden sich Tatbestandsvoraussetzungen und Rechtsfolge des Art 114 AEUV ineinander auflösen, wenn die Ermächtigung zur Rechtsharmonisierung allein von Wirkungen abhängig wäre, die mit *jeder* Rechtsharmonisierung einhergingen: nämlich der Geltung des gleichen Rechts für alle im erfassten Harmonisierungsbereich.[93]

---

86 *Deutsch/ Eggendorfer*, 50.1. IT-Sicherheit, in *Taeger/ Pohle (Hrsg)*, Computerrechts-Handbuch (37. Lfg 2022) Rn 243.
87 *Korte* in *Calliess/ Ruffert* (Hrsg), EUV/AEUV[6] (2022) Art 114 AEUV Rn 41 ff, 44 ff.
88 *Schröder* in Streinz (Hrsg), EUV/AEUV[3] (2018) Art 114 AEUV Rn 42, 43.
89 Begründung des Vorschlags: COM(2022) 454 final.
90 *Schröder* in Streinz, EUV/AEUV[3] Art 114 AEUV Rn 19, 20.
91 Begründung des Vorschlags: COM(2022) 454 final (Hervorhebung nicht im Original).
92 *Korte* in *Calliess/ Ruffert* (Hrsg), EUV/AEUV[6] Art 114 AEUV Rn 2.
93 *Korte* in *Calliess/ Ruffert* (Hrsg), EUV/AEUV[6] Art 114 AEUV Rn 2, 45.

Das primäre Ziel, an dem die Zulässigkeit des CRG-E im Lichte des Art 114 AEUV zu messen ist, bleibt so gesehen der Schutz vor Sicherheitsgefahren durch Produkte mit digitalen Elementen, die aber nachdem, was wir bislang wissen, weniger den Markt, sondern die digitale Souveränität der Union und ihrer Bewohner herausfordern.[94] Dass rechtstechnisch am Produkt mit digitalen Elementen angeknüpft und im CRG-E wirtschaftlichen Akteuren sanktionsbewehrte Verpflichtungen auferlegt werden, mag diesen Umstand in subtiler Weise verdecken, ändert aber nichts an dem Umstand, dass insbesondere mit den Vorschriften über das Inverkehrbringen von Produkten mit digitalen Elementen nach dem derzeitigen Stand des CRG-E gestützt auf Art 114 AEUV eine innere Sicherheitspolitik der Union im Gewand marktrechtlicher Vorschriften umgesetzt werden soll.[95] Der Schutz der inneren Sicherheit der Union liegt nun aber in der Kompetenz der Mitgliedstaaten.[96] Ist er primäres Ziel eines Rechtsaktes, darf dieser nicht auf Art 114 AEUV gestützt werden. Insofern bleiben mE Zweifel an der Kompetenzkonformität des CRG-E zurück.

Sieht man von dieser formell-rechtlichen Problematik ab, verspricht der CRG-E durch die Einführung von staatlich überwachten Konformitätsbewertungsverfahren in inhaltlicher Hinsicht gewiss mehr Transparenz bezogen auf die Frage, wie Produkte mit digitalen Elementen eigentlich funktionieren[97] und könnte sich von daher mit als Inspirationsquelle für die zukünftige nähere Regulierung von digitalen Wirtschaftsgütern und der durch sie unterstützten Dienstleistungen erweisen. Die oben unter IV. systematisierten Verpflichtungen, welche grundsätzlich in abgestufter Form vor allem die Hersteller, zum Teil aber auch die Importeure und nicht zuletzt auch die Händler von Produkten mit digitalen Elementen treffen, könnten aber je nach Fallkonstellation auch vom Hersteller über die Importeure auf die Händler durchschlagen. Kurz zusammengefasst ist dies dann der Fall, wenn die Selbstkonformitätsprüfung des Vormannes in der Lieferkette vom Hintermann nicht ausreichend hinterfragt wird.[98] Angesichts der unterschiedlichen Ausgangslage und des produktbezogenen Kenntnisstandes von Herstellern, Importeuren und Händlern in der Lieferkette begegnet dieser Umstand – vor allem im Verhältnis Importeur und Händler – nicht nur gleichheitsrechtlichen Bedenken (Art 20 GRC). Vor allem aus der Perspektive des einfachen Händlers erweist sich der entsprechende Regulierungsrahmen über das Inverkehrbringen von Produkten mit digitalen Elementen vor dem Hintergrund des durch das CRG-E vorgegebenen Sanktionsregimes zudem auch als intensiver Eingriff in die unternehmerische Freiheit (Art 16 GRC). Denn das mögliche Durchschlagen der Verpflichtungen des Herstellers in Verbindung mit dem Aufwand, den die Selbstkonformitätsüberprüfung des CRG-E fordert, stellt das Inverkehrbringen

94 Joint Communication of the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 5 ff; s aber auch https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (19.12.2022).

95 Vgl die vielen Hinweise auf die sicherheitspolitische Dimension des CRG-E in der Begründung des Vorschlags: COM(2022) 454 final.

96 Art 4 Abs 2 Satz 2 EUV.

97 S aber Art 52 CRG-E, der die nötige vertrauliche Behandlung der dabei gewonnenen Informationen im Verhältnis zu Dritten gewährleistet.

98 S oben IV.B. und IV.C.

von Produkten mit digitalen Elementen angesichts der beschriebenen tatsächlichen Unsicherheiten über das CRG-E-konforme Handeln des Vormannes unter ein beträchtliches unternehmerisches Risiko. Es ist also nicht allein die „Bürokratie“,[99] sondern auch die ungleiche und unverhältnismäßige Verteilung von strafsanktionsbewehrter Verantwortung, die man am CRG-E im Lichte primärrechtlicher Vorgaben kritisieren muss.

Ungeachtet der geübten Kritik am CRG-E ist dessen Kernidee in einer Gesamtzusammenschau rechtspolitisch natürlich zu begrüßen: Seine unterstützende Rolle für den Aufbau der digitalen Souveränität der Union und ihrer Mitgliedstaaten wäre an sich enorm. Denn die horizontalen Anforderungen an die Cybersicherheit von digitalen Produkten würden nicht nur dabei helfen, jene Cyberattacken, die die politische Souveränität der Union herausfordern, oder Produkte aus Drittstaaten abzuwehren, mit denen diese Problematik bis dato buchstäblich in die Union (mit-)importiert wird.[100] Vielmehr würde der mittels der vorgeschlagenen Verordnung harmonisierte Rechtsrahmen eben auch den Aufbau eines eigenen unionalen Markts für Produkte mit digitalen Elementen von europäischen Herstellern unterstützen, welche zunächst der Rechtsgewalt nationaler und unionaler Behörden und Gerichte wegen der territorialitätsbezogenen Anknüpfbarkeit idR vollständig zugänglich sind und in der Folge jene Cyberbedrohungen, die nach wie vor von manchen außereuropäischen Produkten am europäischen Markt ausgehen, durch neuen Wettbewerb von diesem verdrängen.[101]

Das Cyberresilienzgesetz birgt also ausgehend von seinen Vorschriften über das Inverkehrbringen von Produkten mit digitalen Elementen viele Chancen in sich. Zunächst die Chance, ausgehend von den kompetenzrechtlichen Bedenken gegen seine Umsetzung allgemein über eine Nachjustierung der Kompetenzverteilung zwischen der Union und ihren Mitgliedstaaten im Kontext der digitalen Transformation nachzudenken. Dann aber auch die Chance, ausgehend von seinen Vorschriften über das Inverkehrbringen von Produkten mit digitalen Elementen die allgemeine Frage nach einer gerechteren Verteilung von Verantwortung zwischen verschiedenen Akteuren zu stellen. Nicht zuletzt ist der Plan, dass die Union cyberresilienter wird und zu diesem Zweck auch horizontale Verpflichtungen im Zusammenhang mit dem Inverkehrbringen von Produkten mit digitalen Elementen einführen will, aber auch eine Chance, die Rolle des Einzelnen beim Aufbau digitaler – und damit dem Erhalt politischer – Souveränität in der Union besser verstehen zu lernen.

---

99 *Kipker*, MMR-Aktuell 2022, 452009.

100 Vgl auch *Wu*, Sovereignty Fever: The Territorial Turn of Global Cyber Order, ZaöRV 2021, 651 (657 ff).

101 Damit der CRG-E nicht umgekehrt „als mitgliedstaatliches Mittel des Protektionismus für eigene Hersteller und Produkte missbraucht w[erden] kann“ (so zu Recht ein Bedenken von *Kipker*, MMR-Aktuell 2022, 452009), sieht der Vorschlag der Kommission ein eigenes neues Behördenkooperationsnetzwerk zur Sicherung der Gleichmäßigkeit des Vollzugs des CRG-E vor (oben VI.).