Digital Services Act für Meta, X & Co.

Online-Riesen an der Leine

Die größten Plattformen und Suchmaschinen in Europa müssen sich seit Ende August den Regeln des Digital Services Act unterwerfen. Nutzer können seitdem beobachten, wie die US-Konzerne allmählich die Vorgaben zur Inhaltemoderation und Transparenz umsetzen.

EU-Vorschriften zu mehr Cybersicherheit

Die Europäische Union bringt im Rahmen ihrer Digitalstrategie zwei wichtige Gesetze auf den Weg: den Cyber Resilience Act (CRA) sowie die sogenannte NIS2-Richtlinie.Da wir immer digitaler werden, muss auch immer mehr Wert auf Onlinesicherheit, oder wie es auf Neudeutsch heißt, Cybersecurity, gelegt werden.

Die EU-Kommission hat am 15. September 2022 einen Entwurf des CRA vorgeschlagen, der noch vom europäischen Parlament und vom Rat angenommen werden muss.

Recht auf Updates durch den CRA

Mit dem CRA werden erhöhte Sicherheitspflichten auf Hersteller, Vertreiber, Importeure und Händler von IT-Produkten zukommen. Dazu zählen insbesondere geplante Meldepflicht für aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle. Durch die Vorgaben des CRA sollen sicherere Hardware- und Softwareprodukte gewährleistet werden.

Zu den dabei erfassten Produkten zählt jedes Software- oder Hardwareprodukt sowie seine Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die separat in Verkehr gebracht werden. Er ist anwendbar auf „Produkte mit digitalen Elementen“, also auf solche Produkte, die ohne ihre digitalen Elemente nicht sinnvoll genutzt werden können (z. B. Smartphones). Der CRA teilt die Produkte mit digitalen Elementen in drei Kategorien ein:

- Standardkategorie
- kritische Klasse I
- kritische Klasse II

In die Standardkategorie fallen voraussichtlich gut 90 Prozent aller Produkte, wie z. B. Textverarbeitung, Fotobearbeitung oder Festplatten. Zum CRA gehören verschiedene Anhänge. Darin, nämlich in Anhang III, werden die kritischen Produkte mit digitalen Elementen der Klassen I und II aufgeführt. Zur kritischen Klasse I zählen u. a. Software für Identitätsmanagementsysteme, Browser, Passwortmanager, Antivirensoftware, VPN-Lösungen, Netzwerkmanagementsysteme, Werkzeuge zur Verwaltung der Netzwerkkonfiguration, Systeme zur Überwachung des Netzwerkverkehrs, Verwaltung von Netzwerkressourcen, Systeme zur Verwaltung von Sicherheitsinformationen und -ereignissen (SIEM), Update-/Patch-Verwaltung (einschließlich Bootmanager), Systeme zur Verwaltung der Anwenderkonfiguration, Software zur Verwaltung mobiler Geräte, Firewalls, Router/Modems, Anwenderspezifische integrierte Schaltungen (ASIC) oder auch Industrielle Automatisierungs- und Steuerungssysteme (IACS). Zur kritischen Klasse II zählen hingegen insbesondere Betriebssysteme für Server, Desktops und mobile Geräte, Infrastrukturen für öffentliche Schlüssel und Aussteller digitaler Zertifikate, Hardwaresicherheitsmodule (HSM), sichere Kryptoprozessoren, Smartcards, Smartcard-Lesegeräte und Token oder auch Geräte des industriellen Internets der Dinge.

Folgende Pflichten sollen zukünftig auf die vom Anwendungsbereich des CRA erfassten Unternehmen zukommen:

- Berücksichtigung der Cybersicherheit schon in der Planungs-, Entwurfs- und Entwicklungsphase sowie auch in der Produktions-, Liefer- und Wartungsphase („Security by Design“)
- umfangreiche Dokumentationspflichten in Bezug auf Cybersicherheitsrisiken
- Meldepflicht für aktiv ausgenutzte Schwachstellen und Vorfälle
- Überwachungs- und Beseitigungspflichten von Schwachstellen während der erwarteten Produktlebensdauer

(max. fünf Jahre)
- Pflicht zur Lieferung von klaren und verständlichen Gebrauchsanweisungen
- Pflicht zur Bereitstellung von bestimmten Pflichtinformationen (u. a. Name, Anschrift und Kontaktdaten des Herstellers, Typen-, Chargen-, Versions- bzw. Seriennummer, Verwendungszweck, Art der technischen Sicherheitsunterstützung, die der Hersteller anbietet, sowie der Zeitpunkt, bis zu dem sie geleistet wird)
- Pflicht zur Bereitstellung von Sicherheitsupdates für jedenfalls fünf Jahre

Ganz konkret und unabhängig von der jeweiligen Kategorie müssen Produkte mit digitalen Elementen zudem immer einer Risikobewertung unterzogen werden.

Unter die Produkte mit digitalen Elementen im Sinne des CRA fallen jedoch weder „Produkte mit digitalen Inhalten“ noch „digitale Produkte“. Die Erstgenannten zeichnen sich dadurch aus, dass der digitale Teil des Produkts für dessen Funktionsfähigkeit nicht von zentraler Bedeutung ist (z. B. Kühlschrank mit Bestellfunktion via App). Bei den „digitalen Produkten“ handelt es sich um rein digitale Produkte (z. B. Apps oder Musikdateien). Der CRA hat folglich einen sehr weit gefassten Anwendungsbereich, von dem nur ein paar spezifische Produktkategorien ausgenommen werden, wie beispielsweise Medizinprodukte. Software, die als Dienstleistung angeboten wird, also Software-as-a-Service-bzw. Cloudleistungen, wird ebenfalls gesondert geregelt.

Sichere Infrastrukturen durch NIS2

Speziell auf den Bereich der sogenannten kritischen Infrastruktur (KRITIS) zielt die NIS2-Richtlinie ab. Es geht also um den besseren Schutz von Stromversorgung, Wasserwerken oder Telekommunikationsleitungen. Es soll ein Höchstmaß an

Ausfallsicherheit gewährleistet werden, um beispielweise Strom-Blackouts oder Störungen der Trinkwasserversorgung für die Bevölkerung möglichst zu vermeiden oder jedenfalls so schnell und gut wie möglich auf derartige Störungen reagieren zu können.

In Deutschland ist mit Blick auf den KRITIS-Sektor bereits 2015 das IT-Sicherheitsgesetz (IT-SiG) in Kraft getreten. Darin war auch eine Änderung des damaligen § 13 Telemediengesetz (TMG) enthalten, der in einem Absatz 7 die Pflicht für alle Websitebetreiber zur Absicherung ihrer Websites mit sich brachte (z. B. durch Verschlüsselung nach dem Stand der Technik per SSL-/TLS-Zertifikat). Diese Norm findet sich nach der letzten Änderung des TMG nun in § 19 Abs. 4 des Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG). Seit Mai 2021 ist nunmehr das zweite IT-Sicherheitsgesetz (IT-SiG2) in Kraft, welches sowohl den Adressatenkreis als auch den Pflichtenkatalog der KRITIS-Betreiber merklich erweitert hat.

Aber auch auf EU-Ebene tut sich einiges. 2016 ist die 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 (kurz: NIS-Richtlinie) in Kraft getreten. Sie ist der europäische Rahmen für Cybersecurity im KRITIS-Bereich und soll ein hohes Sicherheitsniveau für Netzwerke und Informationssysteme sicherstellen.

Seit dem Jahr 2021 wird die NIS-Richtlinie überarbeitet. Ihr Nachfolger, die sogenannte NIS2-Richtlinie, soll den bestehenden Rechtsrahmen modernisieren, um die Herausforderungen des zunehmenden Grades an Digitalisierung und der stetig wachsenden Bedrohungen für die Cybersicherheit meistern zu können. Nach Inkrafttreten der NIS2-Richtlinie muss diese noch in das jeweilige nationale Recht der EU-Mitgliedsstaaten umgesetzt werden. In NIS2 wird zwischen

kritischen und wichtigen Einrichtungen unterschieden:

- *Kritische Einrichtungen:* Energie (Strom, Fernwärme und Fernkälte, Erdöl, Erdgas und Wasserstoff); Verkehr (Luft, Schiene, Wasser und Straße); Bankenwesen; Finanzmarktinfrastrukturen; Gesundheitswesen; Herstellung pharmazeutischer Erzeugnisse (einschließlich Impfstoffe und kritischer Medizinprodukte); Trinkwasserversorgung; Abwasserwirtschaft; digitale Infrastrukturen (Internetknoten, DNS-Anbieter, Anbieter von Clouddienstleistungen, Anbieter von Rechenzentrumsdiensten, Netze zur Bereitstellung von Inhalten, öffentliche elektronische Kommunikationsnetze und elektronische Kommunikationsdienste,…); öffentliche Verwaltung; Weltraum.
- *Wichtige Einrichtungen:* Post- und Kurierdienste; Abfallwirtschaft; Chemikalien; Lebensmittel; Herstellung anderer Medizinprodukte, von Computern, Elektronik und Kraftfahrzeugen sowie Maschinenbau; Anbieter digitaler Dienste (Onlinemarktplätze, Onlinesuchmaschinen und Plattformen der sozialen Netzwerke).

Sowohl die kritischen als auch die wichtigen Einrichtungen müssen u. a. folgende Cybersecurity-Maßnahmen treffen:

- Erlass und Umsetzung von Richtlinien für Risiken und Informationssicherheit
- Umsetzung von Maßnahmen zur Prävention, Detektion und Bewältigung von Cybersecurity-Vorfällen (Sicherheitspannen)
- Ergreifen von Maßnahmen zum Business Continuity Management (BCM) inkl. Backup- bzw. Krisenmanagement
- Gewährleistung der Sicherheit bei der Beschaffung von IT- und Netzwerksystemen
- Beachtung von Vorgaben für Kryptografie bzw. Verschlüsselung

- Umsetzung angemessener Maßnahmen zur Zugangskontrolle
- Einsatz sicherer Sprach-, Video- und Textkommunikation
- Einsatz gesicherter Notfallkommunikationssysteme

Durch die NIS2-Richtlinie wird der Aspekt der Cybersecurity zukünftig in der gesamten Lieferkette zu berücksichtigen sein. Außerdem sollen die Aufsicht und die Zusammenarbeit zwischen den Behörden und den von NIS2 betroffenen Betreibern innerhalb der EU vertieft werden. Die Sanktionen bei Verstößen gegen die NIS2-Vorgaben sollen durch die einzelnen EU-Mitgliedsstaaten selbst geregelt werden. Allerdings wird von Seiten des EU-Gesetzgebers bestimmt, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen. Gegen kritische Einrichtungen sollen Geldbußen mit einem Höchstbetrag von mindestens 10 Mio. Euro oder von mindestens 2 Prozent des gesamten weltweit erzielten Vorjahresumsatzes verhängt werden können. Bei Sanktionen gegen wichtige Einrichtungen soll der Höchstbetrag mindestens 7 Mio. Euro oder 1,4 Prozent des Vorjahresumsatzes betragen.

Praxistipp

Neben dem CRA und NIS2 beinhaltet die Strategie der EU noch weitere Gesetze, die den Umgang mit digitalen Daten regeln sollen. Dazu zählen insbesondere der Data Governance Act (DGA) zur Förderung der Weiterverwendung von Daten des öffentlichen Sektors, der Digital Markets Act (DMA) und der Digital Services Act (DSA) zur Regulierung großer Onlineplattformen, der Artificial Intelligence Act (AIA) zur Regulierung von Künstlicher Intelligenz (KI) oder auch der Data Act (DA) zur besseren Weiterverwendung von Unternehmensdaten. Bei diesen Rechtsakten handelt es sich nicht um bloße Zukunftsmusik, denn der DMA ist bereits seit dem 1. November 2022 in Kraft. Der DGA wird ab dem 24. September 2023 anwendbar sein, der DSA bereits ab dem 2. Mai 2023.

- Michael Rohrlich hat als Rechtsanwalt und Fachautor seinen

Kanzleisitz in Würselen, Nähe Aachen. Seine beruflichen Schwerpunkte liegen auf dem Gebiet des Onlinerechts sowie des gewerblichen Rechtsschutzes. Weitere Infos zu den Themen aus den Rechtsbeiträgen sowie Gesetze und Gerichtsentscheidungen bietet er unter www.rechtssicher.info an.

Wie die EU ihre Digitalstrategie vorantreibt

Im Regulierungsrausch

Nationale Regierungen müssen sich daran gewöhnen: Relevante Gesetze werden zunehmend in Brüssel geschrieben. Gerade in der Digitalpolitik schleudert die Kommission einen Verordnungsvorschlag nach dem anderen heraus, um Versäumnisse aufzuholen und Zukunftstechnologien frühzeitig zu regulieren. Das kl…

Wie die EU ihre Digitalstrategie vorantreibt

Nationale Regierungen müssen sich daran gewöhnen: Relevante Gesetze werden zunehmend in Brüssel geschrieben. Gerade in der Digitalpolitik schleudert die Kommission einen Verordnungsvorschlag nach dem anderen heraus, um Versäumnisse aufzuholen und Zukunftstechnologien frühzeitig zu regulieren. Das klappt manchmal, ist aber auch oft widersprüchlich.

Von Falk Steiner

kompakt

- Die EU zieht im digitalen Bereich immer mehr Kompetenzen an sich und übernimmt auch Aufsichtsfunktionen.
- Insbesondere zu den USA ist die Beziehung kompliziert, weil sich die großen Tech-Konzerne nur ungern an die Regeln der lukrativen europäischen Märkte anpassen.
- Einige Pläne, vor allem der CSAM-Act, schießen deutlich über das Ziel hinaus und werden 2023 für heftige Konflikte zwischen den Mitgliedsstaaten sorgen.

Das dritte Jahrzehnt des 21. Jahrhunderts müsse zur „digitalen Dekade“ werden. Dies hatte EU-Kommissionspräsidentin Ursula von der Leyen in ihrer „Rede zur Lage der Europäischen Union“ im September 2020 angekündigt – und direkt Taten folgen lassen. Bereits ein Jahr später war ein Konzept erkennbar, inklusive neu entwickelter Instrumente, um den digitalen Fortschritt zu messen.

Beispielsweise hat die Kommission den „Index für die digitale Wirtschaft und Gesellschaft“ (DESI) geschaffen, der Fortschritte bei den Zielmarken für 2030 in jedem EU-Mitgliedsstand abbildet und damit Wettbewerb der Staaten untereinander anfacht. In einem jährlichen Bericht über den

„Stand der digitalen Dekade“ bewertet die Kommission außerdem die Fortschritte, beispielsweise bei der Digitalisierung von Verwaltungsakten.

Vor allem aber hat die Kommission, die als einziges EU-Organ Gesetze entwerfen und vorschlagen darf, ein wahres Feuerwerk an neuen Regelwerken fürs Digitale auf die Schiene gesetzt [1]. Einige der Gesetzentwürfe stehen bereits davor, umgesetzt zu werden, bei anderen suchen Kommission, EU-Parlament und Europäischer Rat noch Kompromisse. Und die Lust auf mehr Regulierung ist in Brüssel noch lange nicht verflogen – auch fragwürdige Ideen sind auf dem Weg.

Der Brüssel-Effekt

Den Startschuss für die digitale Dekade gab die EU eigentlich schon im Mai 2018: Damals wurde die EU-Datenschutz-Grundverordnung (DSGVO) wirksam. Sie setzt bis heute die Grenzen dafür, wie Unternehmen und Behörden Daten von EU-Bürgern nutzen dürfen – auch für alle nachfolgenden Gesetze. Die EU-Kommission hatte darauf gesetzt, mit der DSGVO nationale Datenschutzgesetze abzulösen und einheitliche Regelungen für den gesamten Binnenmarkt zu schaffen. Dies gilt mittlerweile als Erfolgsmodell, weshalb viele neue Vorhaben als für alle 27 Mitgliedsstaaten verbindliche Verordnungen daherkommen statt als schwächere Richtlinien.

Denn die DSGVO hat gezeigt: Als Absatzmarkt ist die EU mit ihren fast 450 Millionen kaufkräftigen Einwohnern für viele Unternehmen zu wichtig, um sie zu ignorieren – unter anderem auch für Amazon, Apple, Meta, Google und die anderen großen Akteure. Wer in Europa Profite machen will, muss sich ihren Regeln unterwerfen. Ob bei Anschlussbuchsen, Ladegeräten, im Daten-, Wettbewerbs- und Kartellrecht, bei der Plattformgesetzgebung, IT-Sicherheit oder KI-Regulierung: Nationale Regeln sind an vielen Stellen mittlerweile schlicht zu unbedeutend.

Dieser sogenannte Brüssel-Effekt führt dazu, dass Europa immer mehr Kompetenzen an sich zieht – und das mit Unterstützung der Mitgliedstaaten. Die meisten davon haben begriffen, dass sie alleinstehend wenig ausrichten können. Mit der Kraft der EU lockt eine mächtige Verhandlungsposition.

Komplizierte Beziehung

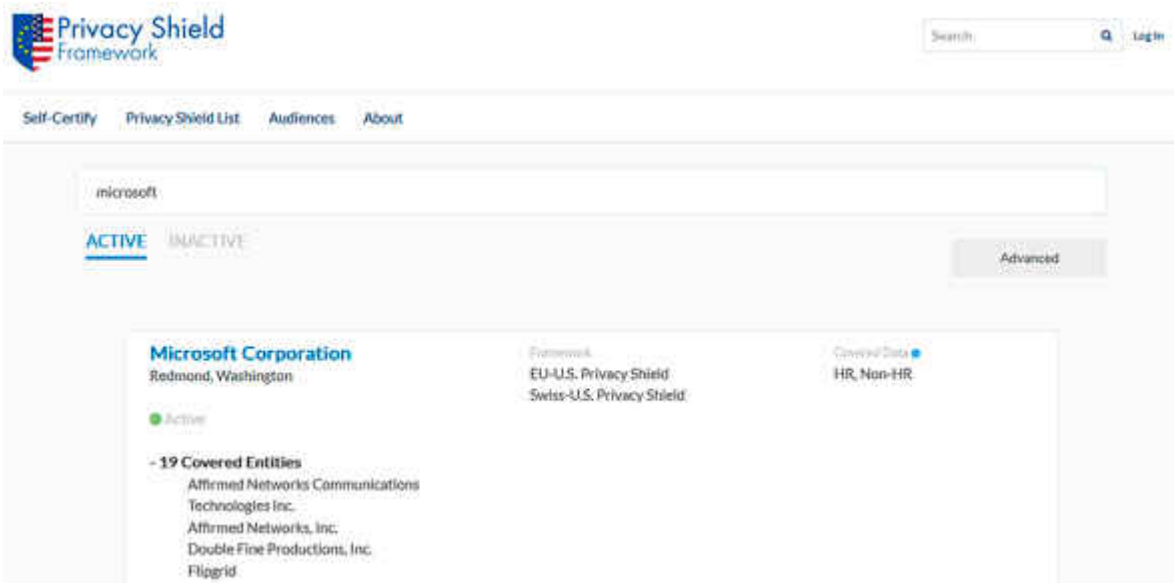
Seit dem Amtsantritt Joe Bidens in den USA und dem Angriff Russlands auf die Ukraine sind weitere Einflüsse auf künftige Regulierung maßgeblich geworden. Vor allem eine Frage treibt Politiker in Brüssel um: Auf wen wird man sich in Zukunft verlassen können? Ihre naheliegende Antwort: Auf als stabil erachtete Demokratien überall in der Welt. Seit Monaten führen EU-Politiker auf vielen Ebenen Gespräche und loten aus, wie sich „die Guten“ dieser Welt untereinander besser vernetzen können, um resilienter gegen böswillige Akteure zu werden.

Handelsabkommen wie CETA mit Kanada, das lange auf Eis lag, sollen nun doch kommen. Vorteilhaft: Auch in den USA gibt es durchaus Lust auf mehr Regulierung. Das ist nicht zuletzt der wachsenden Macht chinesischer Staatsunternehmen, aber auch der einheimischen Kritik am Gebaren einiger US-Konzerne geschuldet.

Aber nicht nur mit Investitionen, auch regulatorisch versucht die EU den Schulterschluss mit den USA. Der eigentliche Lackmustest für die neu belebten transatlantischen Beziehungen steht noch bevor: Im Frühjahr 2023 wird die EU-Kommission über den Transfer personenbezogener Daten in die USA entscheiden. Der erwartete Angemessenheitsbeschluss als Nachfolgeregelung des gescheiterten Privacy Shields ist elementar für Wirtschaft und Nutzer auf beiden Seiten des Atlantiks. Denn wenn keine neue, sichere Rechtsgrundlage geschaffen wird, dürfen viele US-Unternehmen nicht mehr mit den persönlichen Daten von EU-Bürgern arbeiten.

Salesforce, Amazon, Google, Apple, Meta und Microsoft könnten

für EU-Daten zur Tabuzone werden. Meta etwa warnt immer wieder davor, dass möglicherweise das EU-Geschäft eingestellt werden müsste – ein Milliardenmarkt würde dem Konzern verloren gehen. Damit das nicht passiert, müssten die USA die Sicherheit von EU-Daten auch gegenüber den US-Nachrichtendiensten verbessern und die Hürden für Zugriffe höher legen. Bislang liegt aber lediglich ein Vorschlag seitens der US-Regierung vor, der bessere Beschwerdemöglichkeiten vorsieht. Dafür hat US-Präsident Biden Anfang Oktober ein Dekret unterzeichnet, und die EU-Kommission muss nun entscheiden, ob das ausreicht [2].



Auf Eis: Viele US-Konzerne wie Microsoft haben sich zwar selbst für den EU-US-Datentransfer zertifiziert, dürfen sich aber derzeit nicht darauf berufen.

Parallel dazu ist die EU bemüht, sich US-Unternehmen als Spielfeld für die sogenannten Zukunftsmärkte im IT-Sektor zu präsentieren. Das ist kein leichtes Unterfangen, denn gerade hier reguliert sie exzessiv herum: Um die KI-Verordnung (AI-Act), die zumindest besonders kritische KI-Anwendungen mit strikteren Regeln versehen soll, wird seit dem Amtsantritt Ursula von der Leyens 2020 gerungen. Bereits seit Frühjahr 2021 liegen die Vorschläge der Kommission auf dem Tisch. Es geht nur zäh voran: Das Parlament und die Mitgliedstaaten suchen nach Lösungen, während KI-Anwendungen in immer mehr Endgeräte und Anwendungen Einzug halten.

Die strittige Haftung für automatisierte Entscheidungen hat man nun aus der Verordnung herausgenommen: Für KI im engeren Sinne und für den Einsatz im Rahmen marktgängiger Produkte und Dienstleistungen hat die Kommission Ende September neue Regelungsvorschläge unterbreitet. Sie sollen gewährleisten, dass von KI-Entscheidungen unrechtmäßig Benachteiligte ihre Betroffenheit auch nachweisen können. Bei der begründeten Annahme, dass ein Unternehmen nicht alle Regeln eingehalten hat, soll in einigen Fällen eine „Vermutungsregel“ zugunsten der Betroffenen greifen – für Anwälte könnte da ein weiteres interessantes Geschäftsfeld entstehen.

Alles für die Kinder?

Wo sogenannte KI nach dem Willen der Kommission entgegen aller Bedenken intensiv zum Einsatz kommen soll, ist beim Kampf gegen Missbrauchsdarstellungen von Kindern im Internet. Als Sammelbegriff für dieses Material hat sich auch hierzulande das US-amerikanische Akronym CSAM (Child Sexual Abuse Material) etabliert. Ein im Mai 2022 vorgestellter Gesetzentwurf wird deshalb auch kurz CSAM-Verordnung genannt. Dieses Vorhaben der EU-Innenkommissarin steht inhaltlich stark in der Kritik: Mit dem Gesetz könnten Plattformanbieter wie Apple, Meta, Microsoft und Google dazu verpflichtet werden, automatisiert nach CSAM-Inhalten zu fahnden und mutmaßliche Treffer an ein europäisches Zentrum zur Bekämpfung derartiger Inhalte zu melden. Bislang tun das einige auf Grundlage einer befristeten Erlaubnis bereits heute. Microsoft etwa durchforstet seinen Cloud-Speicher OneDrive auf CSAM-Material hin und sperrt deshalb bisweilen unberechtigt Nutzerkonten [3].

Bürgerrechtler stellen denn auch immer wieder infrage, dass die KI-gestützten Filter CSAM-Abbildungen ausreichend zuverlässig erkennen. Sie sehen die Gefahr von Falschverdächtigungen für größer an als den Nutzen, zumal die Pflicht nach den Plänen der Kommission auch Anbieter

verschlüsselter Chats träfe – was zu einem heftigen Eingriff ins Grundrecht auf vertrauliche Kommunikation führen würde [4]. Zudem könnten Strafverfolgungsbehörden laut Kommissionsvorschlag Zugangsanbieter dazu verpflichten, Sperren gegen Websites einzurichten, die nicht genug gegen derartige Inhalte unternehmen. Da der Vorschlag technikneutral formuliert ist, bezieht er sich nicht nur auf klassische Webseiten: auch Betreiber anderer digitaler Kommunikationswege, etwa Tor-Hoster, könnten davon betroffen sein.

Gegenwind aus Deutschland: Bürgerrechtsorganisationen sammeln gemeinsam auf der Petitionsplattform Campact Unterschriften gegen die geplante CSAM-Verordnung der EU-Kommission.
Das Vorhaben gilt insbesondere in Deutschland als politisch heißes Eisen. In der Bundesregierung hat sich Bundesinnenministerin Nancy Faeser (SPD) grundsätzlich dafür ausgesprochen, die FDP-geführten Digital- und Justizministerien dagegen. Auch im Europaparlament gibt es Widerstand vor allem aus Reihen von FDP, Grünen und Piraten gegen die dort unter dem Begriff Chatkontrolle laufenden Pläne der Kommission. Ob das Parlament den Plan im Gesetzgebungsprozess stoppen oder doch nur abmildern kann, wird sich frühestens 2023 entscheiden.

Sicherheit vor allzu wilden Politikerideen lässt sich nicht verordnen – sehr wohl aber mehr Cybersicherheit für Endgeräte und kritische Infrastruktur: Für beide Themen liegen

Vorschläge auf dem Tisch. Die überarbeitete Netzwerk- und Informationssicherheits-Richtlinie NIS ist bereits unter Dach und Fach – die Mitgliedstaaten müssen sie nun in nationales Recht umsetzen. Für Deutschland bringt sie vergleichsweise wenig Änderungen mit sich, dennoch werden 2023 einige Änderungen am IT-Sicherheitsgesetz fällig, um dem genauen Wortlaut der Revision zu entsprechen.

Anders sieht es mit dem Cyber Resilience Act (CRA) genannten Kommissionsvorschlag vom Herbst 2022 aus – es stehen harte Verhandlungen zwischen Kommission, Parlament und Rat an. Unter anderem geht es um Anforderungen an netzwerkfähige Endgeräte, die nicht von Spezialregeln (etwa für kritische Infrastruktur) umfasst sind. Die Kommission begreift ihren Vorschlag als Antwort etwa auf die Erfahrungen mit dem Mirai-Botnetz, das eine große Zahl nicht gesicherter Webcams für DDoS-Attacken missbrauchte. Mit dem CRA sollen Anbieter von derlei Produkten von Betroffenen in die Pflicht genommen werden können. Halten sie sich nicht an definierte Sicherheitskriterien, haften sie für Schäden – so zumindest der Plan der EU, der im kommenden Jahr verabschiedet werden soll.

Notdürftige Reparaturen

Die Eile, mit der die Kommission einige der Gesetzeswerke derzeit unkoordiniert durch die Institutionen peitscht, führt zu jeder Menge neuer Probleme. Zum Beispiel die Cookie-Problematik: Sie ist bis heute auf EU-Ebene nicht abschließend gelöst – ein echtes Ärgernis für alle Beteiligten, sowohl Unternehmen als auch Verbraucher. Die Kommission hatte geplant, dass die sogenannte E-Privacy-Verordnung eindeutige Regeln vorgibt. Doch die steckt seit über vier Jahren im Prozess fest und wurde von der DSGVO überholt, aus der nun Datenschutzbehörden notgedrungen Regeln ableiten müssen, die nicht drinstehen. Die Gemengelage aus DSGVO und noch gültiger, überalterter E-Privacy-Richtlinie lässt zu viel Interpretationspielraum – eine umfassende Lösung gibt es

bislang nicht, nur notdürftige Reparaturen [5].

Gegen irreführende Techniken bei Einwilligungsbannern („Dark Patterns“) hat die EU zuletzt auf Drängen der Europaparlamentarier in den ab April 2024 wirksamen Digital Services Act (DSA) eine Regelung aufgenommen. Das deutsche Digitalministerium erarbeitet parallel auf Grundlage des deutschen Telemedien-Teledienste-Datenschutzgesetzes (TTDSG) eine Regelung für die zentralisierte Einwilligungsverwaltung. Von der erhofft sich die Ampelregierung, einen großen Knoten in der Debatte um die E-Privacy-Verordnung vorbildhaft durchschlagen zu können, sodass sie irgendwann doch noch kommen kann – mit einem halben Jahrzehnt Verspätung [6].

Viele der zuletzt verabschiedeten oder derzeit im Beratungsprozess steckenden Gesetzgebungen zeigen aber auch, dass die EU dazulernt: Während mit der DSGVO noch versucht wurde, starke und unabhängige Aufsichtsbehörden in den Mitgliedstaaten zu schaffen, plant die Kommission neuere Vorschläge deutlich zentralistischer – und das teils auf ausdrücklichen Wunsch der EU-Staaten, vertreten durch den Europäischen Rat. Denn wenn im Binnenmarkt eine der Behörden nicht mitspielt, entsteht ein exekutiver Flaschenhals, wie die irische Datenschutz-Aufsichtsbehörde DPC mit ihrer laxen Verfolgung von Datenschutzverstößen immer wieder belegt.

Mit dem DSA und dem Digital Markets Act (DMA) hat die EU nun bereits zwei Gesetze verabschiedet, bei denen die Kommission im kommenden Jahr das Aufsichtsregime zusammensetzt. Geplant ist ein Zusammenspiel nationaler und europäischer Aufsichtsbehörden. Für die extrem großen Player am Markt wird die EU-Kommission selbst als Aufsicht fungieren.

Bei der Plattformaufsicht im DSA muss sich insbesondere Deutschland umsortieren. Das umfangreiche Gesetzeswerk verändert unter anderem den Mechanismus, wann und wie Plattformbetreiber im Netz bei rechtswidrigen Inhalten eingreifen müssen. Was in Deutschland bislang über das

Netzwerkdurchsetzungsgesetz (NetzDG) geregelt war, wird ab 2024 vom DSA überschrieben. Und der geht in Teilen sogar über das hinaus, was das umstrittene NetzDG vorgibt. Damit werden im kommenden Jahr Änderungen am deutschen Recht nötig, die auch die Nutzer von sozialen Medien betreffen.

Zankapfel Traffic-Kosten

Überrascht waren im Mai 2022 Beobachter und Regulierungsbehörden, als Kommissionsvizepräsidentin Margrete Vestager und der Binnenmarktkommissar Thierry Breton einen neuen Vorstoß unternahmen, einige Anbieter im Netz künftig mehr für die Infrastruktur zahlen zu lassen. Kern der Debatte: Sehr wenige Akteure verursachen einen Großteil des Datenverkehrs im Netz – tragen in der Wahrnehmung der ausbauenden Telekommunikationsunternehmen und der EU-Kommission aber zu wenig der entstehenden Kosten. Insbesondere geht es um den Breitbandausbau in der Fläche, den viele Mitgliedstaaten teuer subventionieren.

Wer soll das bezahlen? Nach Wünschen zweier EU-Kommissare sollen Streaminganbieter wie Netflix an den Kosten für den Glasfaserausbau in der Fläche beteiligt werden. *Bild: Deutsche*

Telekom
Zwei unvereinbare Positionen prallen aufeinander: Die Anbieter von Streamingdiensten wie Netflix oder Amazon, deren hochauflösende Videos statistisch große Teile des Verkehrs verursachen, argumentieren damit, dass erst ihre Angebote teure Netzzugänge und den weiteren Ausbau attraktiv machen würden. Einige der Telekommunikationsanbieter wiederum argumentieren, dass diese ohne die Breitbandzugänge keine Umsätze generieren könnten.

Derzeit überarbeitet die EU die Richtlinie zur Reduzierung der Breitbandkosten. Im Laufe des Jahres 2022 rückten Vestager und Breton von ihrem Plan zwar nicht ab – von einem schnellen Abschluss der Revision ist seit dem Herbst aber nicht mehr die Rede. Stattdessen soll nun in einem geregelten Prozess ermittelt werden, ob tatsächlich finanzielle Ungleichgewichte bestehen und ob sich daraus Handlungsbedarf ergibt. Dieses Vorgehen hatten auch die nationalen Regulierungsbehörden verlangt.

Eine breite Koalition aus Mitgliedstaaten, Verbraucherschützern und Europaparlamentariern hatte davor gewarnt, mit dieser Debatte ein altes Fass wieder aufzumachen: Sollten nicht doch einzelne Dienste gegen Bezahlung bevorzugt werden? Dies würde einen Eingriff in die eigentlich garantierte Netzneutralität bedeuten. Danach sieht es politisch derzeit zumindest nicht aus, doch ein Streit im kommenden Jahr scheint vorprogrammiert.

Bilanz

Im Frühjahr 2024 wählen die EU-Bürger ihr Parlament neu. Offen ist, ob die Von-der-Leyen-Kommission danach die „Digitale Dekade“ weiter umsetzen darf. Einen großen Teil der EU-Digitalstrategie hat sie tatsächlich bereits 2022 auf den Weg gebracht – doch viele der Puzzlestücke sind entweder noch in Arbeit oder werden bereits von neueren Entwicklungen überrollt.

Bei einigen Gesetzgebungsvorhaben ist unklar, ob sie tatsächlich den gewünschten, großen Unterschied machen können. Zugleich lauern auch in den Brüsseler Schubladen der Kommissare immer wieder Ideen, die nicht unbedingt von tieferem Verständnis für die digitalpolitischen Debatten der vergangenen Jahrzehnte zeugen. Und je stärker der außenpolitische Druck wird, desto größer ist die Gefahr, dass auch sicherheitspolitische Ideen wie die Vorratsdatenspeicherung, automatische Inhaltsfilterungen und Websperren in Brüssel Anklang finden.

Bislang ist die Bilanz der aktuellen EU-Kommission durchwachsen. Während sie mit ihrer KI-Gesetzgebung und im Datenrecht vor vielen anderen Initiativen in der Welt liegt und Standards setzt, bei der IT-Sicherheit endlich auch wenig smarte Endgeräte und deren Hersteller in den Blick nimmt, droht in anderen Bereichen Chaos: Neue Regeln allein machen die digitale Welt noch kein bisschen besser. *(hob@ct.de)*

1. Literatur

2. Joerg Heidrich, Europäisches Trommelfeuer, Wie die EU den Umgang mit Daten revolutionieren will, c’t 18/2022, S. 168
3. Holger Bleich, Privacy Shield 2.0, Neues EU-US-Datentransfer-Abkommen nimmt erste Hürde, c’t 23/2022, S. 32
4. Greta Friedrich, Ein Foto – und alles ist weg, Microsoft sperrt Kunden unangekündigt für immer aus, c’t 24/2022, S. 104
5. Holger Bleich, Massenüberwachung durch die Hintertür, Wie ein EU-Kinderschutzgesetz die Presse- und Meinungsfreiheit massiv einschränken könnte, c’t 13/2022, S. 144
6. Holger Bleich, Löcher stopfen per Verordnung, Die bizarre Tracking-Regulierung in Deutschland, c’t 16/2022, S. 34
7. Holger Bleich, Cookie-Banner adieu?, Eine

Rechtsverordnung soll Cookie-Abfragen eindämmen, c’t 20/2022, S. 38