IT-Recht 2023: Viele neue EU-Regeln

IT-Recht 2023: Viele neue EU-Regeln

Im kommenden Jahr muss sich die IT-Welt mit etlichen neuen rechtlichen Regulierungen auseinandersetzen, viele davon auf EU-Ebene. Unter anderem sollen die Internetgiganten stärker an die Leine genommen werden. Aber auch kleine Unternehmen müssen handeln.
Im kommenden Jahr muss sich die IT-Welt mit etlichen neuen rechtlichen Regulierungen auseinandersetzen, viele davon auf EU-Ebene. Unter anderem sollen die Internetgiganten stärker an die Leine genommen werden. Aber auch kleine Unternehmen müssen handeln.

Es gibt einen Grund, warum auf EU-Ebene derzeit viele Gesetzgebungsvorhaben im IT-Bereich forciert werden: die im Frühjahr 2024 anstehende Europawahl. Insbesondere die EU-Kommission möchte bis dahin möglichst alle ihre in der Agenda „Priorities 2019 – 2024 – A Europe fit for the digital age“

gesetzten Ziele erreichen. Die Amtszeit der derzeitigen Kommission endet mit der Legislaturperiode des Europäischen Parlaments. Anschließend wird eine neue EU-Kommission gebildet, die sich dann eine neue IT-Rechts-Agenda geben dürfte.

2023 werden zunächst zahlreiche EU-Gesetze in Kraft treten, die bereits im Jahr 2022 beschlossen wurden. Hierzu zählt der **Digital Markets Act (DMA),** der am 1. November 2022 in Kraft getreten und ab dem 2. Mai 2023 wirksam ist. Er sieht vor, dass es auf Plattformen der Gatekeeper im Internet fair zugeht, wie es auf einer Webseite der EU-Kommission heißt. Anhand objektiver Kriterien wird festgestellt, ob es sich bei einer Onlineplattform um einen solchen Gatekeeper handelt. Relevant sind dabei insbesondere die wirtschaftliche Position und die Nutzerzahlen.

Der DMA sieht vor, dass Gatekeeper künftig diskriminierungsfrei ihre Plattformen für den Absatz von Waren und Dienstleistungen durch Dritte zur Verfügung stellen müssen. Dies gilt auch für die dabei von Nutzern auf der Plattform hinterlassenen Daten. Eigene Waren und Dienstleistungen darf der Gatekeeper dabei nicht bevorzugen, auch darf er Nutzer nicht vom Deinstallieren von Apps abhalten. Außerhalb der Plattform darf er Nutzer nicht ohne deren Einwilligung bewerben. Die Bußgelder können bis zu 20 Prozent des weltweiten Jahresumsatzes betragen.

Länderübergreifende Dienste

Beim **Digital Services Act (DSA)** hat sich die EU auf eine längere Frist zwischen dem Inkrafttreten am 16. November 2022 und dem Wirksamwerden am 17. Februar 2024 verständigt. Hintergrund hierfür sind die zahlreichen und teils tiefgreifenden Vorgaben für sehr viele Unternehmen, die Leistungen rund um das oder im Internet anbieten. Im Wesentlichen geht es bei der Regulierung darum, Verbraucher und ihre Grundrechte besser zu schützen, einen einheitlichen

Rechtsrahmen zu schaffen und – vor allem auch für kleinere Serviceanbieter, KMU oder Start-ups – den Zugang zu EU-weiten Märkten zu vereinfachen. Nicht zuletzt liegt ein Schwerpunkt des DSA auf der Minderung systemimmanenter Risiken wie Manipulation oder Desinformation (siehe ix.de/zqe9).

Neben den üblichen Folgen bei Rechtsverstößen wie wettbewerbsrechtlichen Abmahnungen, einstweiligen Verfügungen und dergleichen sieht der DSA Bußgelder von bis zu sechs Prozent des weltweiten Jahresumsatzes des Anbieters vor. Betroffen vom DSA sind „vermittelnde Online-Dienste“. Hierzu zählen Vermittlungsdienste mit einem eigenen Infrastrukturnetz, etwa Internetanbieter, DNS-Registrierstellen und Hosting-Dienste im Bereich Cloud und Webhosting. Erfasst sind des Weiteren Onlineplattformen wie Onlinemarktplätze, App-Stores oder Social-Media-Plattformen. Der DSA sieht in den Regelungen zum Anwendungsbereich keine Ausnahmen für nicht kommerzielle Anbieter vor. Also dürften Mastodon und gegebenenfalls auch Wikipedia unter den Anwendungsbereich fallen.

Die betroffenen Unternehmen sind gut beraten, das Jahr 2023 zur Vorbereitung zu nutzen. Es gilt, die Compliance mit dem DSA zu schaffen, die AGB anzupassen und womöglich auch die angebotenen Leistungen selbst [1].

Der DSA wird in Fachkreisen auch als „Biest“ bezeichnet, denn die Vorgaben sind sehr weitreichend. Neben Tech-Giganten dürften beispielsweise auch einzelne geschäftliche WLAN-Betreiber betroffen sein. Mit Abmahnungen bei DSA-Verstößen ist ab Februar 2024 zu rechnen. Diese Abmahnwelle könnte deutlich größere Ausmaße annehmen als die derzeitige bei der Verwendung dynamischer Google-Fonts.

Kryptoregulierung verspätet sich

Eigentlich sollte die Verordnung **Markets in Crypto-Assets (MiCA)** bereits 2022 verabschiedet werden und in Kraft treten.

Überraschend vertagte das EU-Parlament die Beschlussfassung jedoch auf 2023. Inhaltlich bestand weitgehend Einigkeit zwischen EU-Rat, -Kommission und -Parlament. MiCA regelt die „digitale Darstellung eines Wertes oder eines Rechts, das elektronisch transferiert und gespeichert werden kann“, wenn dafür „die Distributed-Ledger-Technologie oder eine vergleichbare Technologie verwendet“ wird. Non-Fungible Tokens (NFT) sind nach derzeitigem Stand als Ergebnis längerer Diskussionen auf Gesetzgebungsebene nicht von der Verordnung betroffen. Die Verordnung ist Teil des EU-Pakets zur Digitalisierung des Finanzwesens.

Die MiCA-Verordnung soll EU-weit Krypto-Assets regulieren. Sie nimmt Emittenten und Dienstleister in den Fokus. Neben dem Anlegerschutz durch Transparenz- und Offenlegungspflichten stehen unter anderem die Verhinderung von Marktmissbrauch und Geldwäsche im Raum. Für zahlreiche Dienstleistungen wird zukünftig die Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erforderlich sein. Die Anforderungen ähneln denen an Finanzinstitute.

Kryptodienstleister müssen ihren Sitz und mindestens einen Geschäftsleiter in der EU haben. Sie müssen die BaFin über das Unternehmen sowie dessen Gesellschafter und Geschäftsleiter umfassend informieren. Die Geschäftsleiter müssen zudem fachlich geeignet und zuverlässig, die Geschäftsorganisation muss ordnungsgemäß und angemessen sein. Maßnahmen gegen Geldwäsche und die ausreichende Organisation der Compliance sind ebenso vorgeschrieben wie ein professionelles Beschwerdemanagement und die Pflicht, eigene Vermögenswerte von denen der Kunden zu trennen.

Sichere Standards für vernetzte Produkte

Am 15. September 2022 hat die EU-Kommission einen ersten Entwurf für einen **Cyber Resilience Act (CRA)** vorgestellt, der nun durch das Gesetzgebungsverfahren und die Abstimmungen zwischen EU-Kommission, -Rat und -Parlament läuft. Das Gesetz

soll gemeinsame Cybersicherheitsstandards für vernetzte Geräte und Dienste („Produkte mit digitalen Anteilen“) festlegen und damit spürbar zur Bekämpfung von Cyberkriminalität beitragen. Mit seiner Verabschiedung ist 2023 zu rechnen, 24 Monate nach Inkrafttreten wird es wirksam. Auf Hersteller solcher Produkte kommt aber bereits nach 12 Monaten eine Berichtspflicht zu, wenn in einem Produkt mit digitalen Elementen eine aktiv ausgenutzte Sicherheitslücke auftritt.

Die geplanten Regelungen reichen von der Pflicht von Herstellern und Dienstleistern, ein angemessenes Niveau an Cybersicherheit einzuhalten, bis hin zum Verkaufsverbot für Produkte mit bekannten Schwachstellen. Produkte sollen nur noch in Verkehr gebracht werden, wenn sie im Sinne von Security by Default konfiguriert sind. Zudem müssen Angriffsflächen und mögliche Auswirkungen von Attacken systemseitig begrenzt sein.

Für kritische Produkte sollen zwei Kategorien eingeführt werden. Die Anforderungen an die Compliance mit den CRA-Vorgaben sollen für Hersteller von Desktop- und Mobilgeräten, virtualisierten Betriebssystemen, Ausstellern digitaler Zertifikate, Allzweck-Mikroprozessoren, Kartenlesegeräten, Robotersensoren, intelligenten Zählern und IoT-Geräten jeglicher Art, Routern und Firewalls für den industriellen Einsatz deutlich höher sein als für andere Produkte mit digitalen Inhalten. Der CRA-Entwurf sieht Bußgelder bis 15 Millionen Euro beziehungsweise 2,5 Prozent des weltweiten Jahresumsatzes vor. In ersten Stellungnahmen warnen Branchenvertreter davor, kleine und mittlere Unternehmen durch allzu hohe und kostspielige Sicherheitsanforderungen vom Markt auszuschließen.

Auf Finanzunternehmen kommen bereits 2023 im Bereich Cybersicherheit zahlreiche Hausaufgaben zu. Am 10. November 2022 hat das EU-Parlament den **Digital Operational Resilience Act (DORA)** verabschiedet. Ziel ist es, bestehende Standards für die Cybersicherheit zu vereinheitlichen. Das soll die

digitale Betriebsstabilität von EU-Finanzunternehmen gewährleisten. Geplant ist ein detailliertes und umfassendes Rahmenwerk. DORA soll nach einer Umsetzungsfrist von zwei Jahren wirksam werden. Die Vorgaben gelten damit zum Jahreswechsel 2024/2025 (zu DORA siehe separaten Artikel ab Seite 92).

Lange erwartet: die NIS2-Richtlinie

Knapp zwei Jahre nach dem Kommissionsvorschlag hat ebenfalls im November 2022 das EU-Parlament der NIS2-Richtlinie zugestimmt. Die noch ausstehende Zustimmung durch die EU-Staaten gilt in Fachkreisen als Formsache. **NIS2** steht für die überarbeitete zweite Fassung der 2016 verabschiedeten **Directive on Security of Network and Information Systems.** Richtlinien sind anders als Verordnungen oder Acts durch die EU-Mitgliedsstaaten in nationales Recht umzusetzen. Ihr Ziel ist die Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

Geplant ist, durch NIS2 den Anwendungsbereich der bisherigen NIS1-Richtlinie drastisch auszuweiten. Unternehmen mit mehr als 50 Mitarbeitern und einem Jahresumsatz von mehr als 10 Millionen Euro sollen künftig unter NIS2 fallen, wenn sie in einem kritischen Sektor tätig sind. Auch die Auflistung, was als kritischer Sektor einzustufen ist, soll signifikant erweitert werden. Danach fallen künftig etwa auch Hersteller von Medizingeräten, Labore, Cloud-Provider, Rechenzentren und Content-Delivery-Netzwerke darunter. Zum etwas schwächer regulierten „wichtigen Sektor“ zählen künftig der gesamte industrielle Sektor, Hersteller von Computern sowie die Branchen Maschinenbau und Mobility.

Die von vielen lange ersehnte NIS2-Richtlinie weitet den Geltungsbereich ihres Vorgängers erheblich aus. Zahlreiche weitere Branchen gelten nun als „kritischer Sektor“.
Betroffene Unternehmen müssen Risikoanalyse- und Sicherheitskonzepte für die Informationssysteme, die Bewältigung von Zwischenfällen, die Offenlegung von Schwachstellen sowie die Gewährleistung der Sicherheit in der Lieferkette schaffen. Die Aufsichtsmaßnahmen und Durchsetzungsanforderungen der nationalen Behörden sollen strenger gefasst werden. Der Bußgeldrahmen soll 10 Millionen Euro oder bis zu zwei Prozent des weltweiten Jahresumsatzes umfassen.

Binnen 18 Monaten nach Inkrafttreten sollen die Mitgliedsstaaten die NIS2-Richtlinie umgesetzt haben. Betroffene Unternehmen müssen sich also auf erheblich verschärfte Vorgaben in puncto Cybersicherheit ab 2024 oder spätestens 2025 einstellen. Angesichts des Mangels an Fachkräften in diesem Bereich und des benötigten Vorlaufs für eine Compliance mit den NIS2-Vorgaben müssen sich die Verantwortlichen in Unternehmen spätestens ab 2023 mit der konkreten Umsetzung beschäftigen. Auf Betreiber kritischer Infrastrukturen kommt am 1. Mai 2023 auf jeden Fall eine bereits beschlossene Pflicht nach dem BSI-Gesetz zu. Sie sind

dann verpflichtet, Systeme zur Angriffserkennung zu verwenden.

Ein weiteres Großprojekt der EU ist der **Artificial Intelligence Act (AI Act).** Nachdem die EU-Kommission bereits im April 2021 einen ersten Gesetzentwurf vorgelegt hat, fand erst im Oktober 2022 die erste Plenarsitzung des EU-Parlaments dazu statt. Ein Grund für die lange Dauer des Verfahrens dürften die über 3000 Änderungsvorschläge sein, mit denen sich das Parlament bei der Regulierung des Einsatzes von künstlicher Intelligenz befassen muss. Die EU beabsichtigt mit dem AI Act einen einheitlichen Rechtsrahmen für vertrauenswürdige KI-Systeme zu schaffen sowie einheitliche Regeln für die Entwicklung, Vermarktung und Verwendung von KI innerhalb der EU im Einklang mit ihren Werten und den Grundrechten.

Schwieriges Ringen um Kompromisse

In Details ist der AI Act sehr umstritten. Der Anwendungsbereich, aber auch der Einsatz biometrischer Erkennungssysteme und ihr potenzieller Missbrauch stehen neben anderen Aspekten im Mittelpunkt der Diskussion. Ein Kompromissvorschlag sieht vor, Behörden in Drittstaaten vom AI Act auszunehmen, wenn sie künstliche Intelligenz im Rahmen von Vereinbarungen über internationale oder justizielle Zusammenarbeit verwenden und ein Angemessenheitsbeschluss der EU-Kommission nach der DSGVO vorliegt. Ausnahmen wird es sicher für die militärische Nutzung und womöglich auch für Forschung und Entwicklung geben. Der EU-Rat fordert zudem eine Beschränkung des Anwendungsbereichs auf maschinelles Lernen.

Angst vor kollektiver biometrischer Überwachung

Strittig ist, welche Ausnahmen es für das pauschale Verbot von Echtzeit-Fernerkennungssystemen zur biometrischen Identifizierung von Personen im öffentlichen Raum geben soll.

Einige EU-Parlamentarier haben Sorge, dass die Zulassung der Identifizierung von Entführungsopfern und Kriminellen sowie zur Abwehr von unmittelbar drohenden Terroranschlägen zur Überwachung der Gesellschaft quasi durch die Hintertür führen kann. Vereinzelte Forderungen sehen vor, das Verbot auch auf den privaten Bereich auszudehnen und auch durch Streichung des „Echtzeit-Erfordernisses“ eine nachträgliche Identifizierung zu untersagen.

Der AI Act wird einen risikobasierten Regelungsansatz verfolgen. KI-Systeme sollen in die vier Kategorien minimales, geringes, hohes oder unannehmbares Risiko eingestuft werden. Im unteren Bereich stehen Transparenzanforderungen und sektorale Regulierungen im Raum. Erfasst werden beispielsweise Systeme, die mit Menschen interagieren oder Emotionen anhand biometrischer Daten erkennen, sowie Systeme, die Inhalte erzeugen oder manipulieren. Unter Letzteres würden auch Deepfakes, also realistisch wirkende Medieninhalte fallen, die durch KI-Systeme geändert oder verfälscht wurden.

Für KI-Systeme mit hohem Risiko sind hohe Anforderungen an das Risikomanagement, die Datenqualität und die technische Dokumentation vorgesehen. Eine hochrangige Expertengruppe soll hierfür Mindestanforderungen gemäß definierten Ethik-Leitlinien festlegen. Diskutiert wird darüber hinaus eine Konformitätsbewertung, die vor Einsatz des betreffenden KI-Systems positiv ausfallen muss.

Als unannehmbar riskante KI-Systeme werden die genannten biometrischen Systeme zur Fernidentifizierung, aber auch Social Scoring durch Behörden (wie bereits in China praktiziert) sowie manipulative Systeme mittels Techniken der unterschwelligen Beeinflussung Schutzbedürftiger eingestuft. Für sie ist ein generelles Verbot vorgesehen. Verstöße gegen den AI Act sollen durch beträchtliche Bußgelder geahndet werden. Diskutiert wird über einen Rahmen von bis zu 30 Millionen Euro oder sechs Prozent des weltweiten Jahresumsatzes.

US-EU-Datenschutz, die Dritte!

Was noch? Spannend wird sein, ob die EU-Kommission aller Kritik zum Trotz im Frühjahr 2023 einen sogenannten Angemessenheitsbeschluss gemäß Artikel 45 der Datenschutz-Grundverordnung fassen wird, der dem Datenschutz in den USA „ein angemessenes Schutzniveau“ bescheinigt. Seit der Europäische Gerichtshof in seinem viel beachteten Schrems-II-Urteil den **EU-US Privacy Shield** kassiert hat, ist die Übermittlung personenbezogener Daten aus der EU in die USA deutlich erschwert.

Im Oktober 2022 hatte US-Präsident Biden eine Executive Order unterzeichnet, mit der ein angemessenes Datenschutzniveau aus EU-Sicht geschaffen werden soll. Zahlreiche Datenschützer wie der scheidende Landesdatenschutzbeauftragte Baden-Württembergs Stefan Brink, aber auch der Datenschutzaktivist Max Schrems zweifeln daran, dass die Executive Order ausreicht. Der EuGH dürfte erneut mit der Rechtslage befasst werden. Ein Ende der Gemengelage ist nicht absehbar.

Ungeachtet dessen dürften die von Unternehmen getroffenen Maßnahmen und Verträge auch weiterhin nicht den Bestimmungen der DSVGO entsprechen. Seit Ende 2022 gelten neue Vorgaben für die Standardvertragsklauseln. Sie sind derzeit eine der wenigen Möglichkeiten, den Datentransfer in die USA rechtskonform auszugestalten. Die Datenschutzbehörden dürften 2023 mit einer Durchsetzung der Änderungen beginnen und gegebenenfalls signifikante Bußgelder verhängen.

Um die in den letzten Jahren heftig diskutierte **E-Privacy-Verordnung** ist es zuletzt sehr ruhig geworden. Sie soll die DSGVO ergänzen und weiter gehende Rahmenbedingungen für den Umgang mit personenbezogenen Daten im Bereich der elektronischen Kommunikation schaffen. In erster Linie soll es Regelungen etwa zu Cookies oder Trackern geben. Diskutiert werden auch Vorgaben für Direktmarketing und Teilnehmerverzeichnisse. Ob die Verordnung nun endlich 2023

das Licht der Welt erblicken wird, ist allerdings mehr als fraglich. Aber selbst wenn, dürfte sie nicht vor 2025 wirksam werden.

Weniger wegwerfen, mehr reparieren

Mitte November 2022 haben sich die EU-Mitgliedsstaaten und die EU-Kommission auf neue **Ecodesign-Vorgaben** geeinigt. Sie sollen 2023 formal verabschiedet und nach einer Umsetzungsfrist von 21 Monaten wirksam werden. Eingeführt werden soll ein **Recht auf Reparatur.** Hersteller von Smartphones, Tablets und Co. müssen danach Reparaturanleitungen und für die Dauer von sieben Jahren bestimmte Ersatzteile wie Displays und Batterien verfügbar halten. Software-Updates müssen fünf Jahre lang bereitgestellt werden. Sie dürfen die Geräteperformance nicht beeinträchtigen. Schließlich sollen die Rechte von Dienstleistern gestärkt werden, die Gerätereparaturen anbieten.

2023 dürfte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine neue Fassung ihres Rundschreibens **Mindestanforderungen an das Risikomanagement (MaRisk)** veröffentlichen. Es wird die derzeit gültige Fassung dieses Rundschreibens vom August 2021 ersetzen. Aus IT-Sicht interessant sind die Diskussionen rund um IT-Sicherheit und IT-Zugang zu Handelsplattformen aus dem Homeoffice. Infolge der Coronapandemie haben zahlreiche Finanzdienstleister gefordert, den strengen Ansatz aufzuweichen, dass beispielsweise ihr Aktienhandel nur „in Geschäftsräumen“ stattfinden darf. Letztlich haben Änderungen in der MaRisk zahlreiche Auswirkungen auf die im Finanzwesen eingesetzten IT-Systeme. Relevant ist hier auch das 2021 überarbeitete Rundschreiben **Bankaufsichtsrechtliche Anforderungen an die IT,** kurz **BAIT,** das die MaRisk konkretisiert. Womöglich steht auch dieses 2023 zur Überarbeitung an.

Weitergehen dürfte es 2023 auch mit den Vorbereitungen für einen **European Chips Act,** der die Wettbewerbsfähigkeit und

Resilienz der Chipindustrie in der EU signifikant stärken soll. Am 24. September 2023 wird zudem der **Data Governance Act (DGA)** wirksam, der am 23. September 2022 in Kraft trat. Sein Ziel ist die Schaffung eines erleichterten Rahmens für die gemeinsame Nutzung von Daten. Ein europäisches Datenaustauschmodell soll zur Förderung der künstlichen Intelligenz einen Datenaustausch zwischen verschiedenen Branchen über Ländergrenzen hinweg ermöglichen. Bürger sollen ihre personenbezogenen Daten für bestimmte Zwecke spenden können. Zudem soll der Zugang zu Daten der öffentlichen Hand erleichtert werden. Datenvermittlungsdienste müssen in einem Register aufgeführt sein, damit interessierte Bürger sich von deren Vertrauenswürdigkeit überzeugen können.

Weiter voranschreiten dürfte 2023 auch die CSAM-Verordnung, die die EU-Kommission im Mai 2022 vorgelegt hat. **CSAM** steht für **Child Sexual Abuse Material,** also Kinderpornografie. Hosting- und Kommunikationsanbieter sollen danach Risikoeinschätzungen vornehmen und Maßnahmen zur Risikoreduzierung treffen. Sie werden dabei überwacht durch nationale Aufsichtsbehörden, denen besondere Befugnisse etwa in Bezug auf die Sicherstellung und Sperrung entsprechender Inhalte zustehen sollen.

Zu erwartende Neuerungen im IT-Recht 2023			
Kürzel	Name	in Kraft ab/seit	wirksam ab
AI Act	Artificial Intelligence Act	voraussichtlich 2023, spätestens 2024 (auch ein Scheitern ist nicht auszuschließen)	voraussichtlich nicht vor 2025, nach aktuellem Stand 24 Monate nach Inkrafttreten

Zu erwartende Neuerungen im IT-Recht 2023			
Kürzel	Name	in Kraft ab/seit	wirksam ab
CRA	Cyber Resilience Act	2023	24 Monate nach Inkrafttreten; einige erste Pflichten jedoch bereits 12 Monate nach Inkrafttreten
CSAM	„Child Sexual Abuse Material“-Verordnung	voraussichtlich 2023	voraussichtlich 6 Monate Umsetzungsfrist ab Inkrafttreten
DGA	Data Governance Act	23. September 2022	24. September 2024
DMA	Digital Markets Act	1. November 2022	2. Mai 2023
DORA	Digital Operational Resilience Act	verabschiedet am 10. November 2022; Inkrafttreten 20 Tage nach Veröffentlichung im EU-Amtsblatt	Jahreswechsel 2024/2025
DSA	Digital Services Act	16. November 2022	17. Februar 2024
	Ecodesign-Vorgaben, „Recht auf Reparatur“	2023	21 Monate Umsetzungsfrist ab Inkrafttreten
ECA	European Chips Act	voraussichtlich 2023	noch in Diskussion
ePVO	E-Privacy-Verordnung	eventuell 2023	nicht vor 2025

Zu erwartende Neuerungen im IT-Recht 2023			
Kürzel	Name	in Kraft ab/seit	wirksam ab
	EU-US Privacy Shield 2.0	eventuell 2023	
LksG	Lieferkettengesetz	1. Januar 2023	mit Inkrafttreten
MaRisk; BAIT	Mindestanforderungen an das Risikomanagement; Bankaufsichtsrechtliche Anforderungen an die IT	voraussichtlich 2023	
MiCA	Markets in Crypto-Assets	2023	18 Monate nach Inkrafttreten; voraussichtlich 2024
NIS2	Directive on Security of Network and Information Systems	voraussichtlich 2023, benötigt noch Zustimmung der EU-Staaten	voraussichtlich 2024, spätestens 2025

Abuse-Material: finden, löschen, berichten

Verfahren und Techniken zum Aufspüren kinderpornografischer Inhalte sollen bestimmten Vorgaben entsprechen, so datenschutzfreundlich und so wenig fehleranfällig wie möglich sein. Weitere Vorgaben soll ein noch zu schaffendes EU Centre on Child Sexual Abuse (EU Centre) veröffentlichen. Zusätzlich gibt es für die verantwortlichen Unternehmen Berichtspflichten. Sie müssen entsprechende Inhalte löschen oder den Zugang zu ihnen effektiv unterbinden, wenn die Inhalte außerhalb der EU gehostet werden. Die Aufsichtsbehörden können Anordnungen treffen, denen unverzüglich Folge zu leisten ist.

App-Stores werden verpflichtet, den Download von Apps zu verhindern, die Kinder „einem hohen Risiko der Anwerbung […] aussetzen können“. Das EU Centre steht dabei den Dienstanbietern, den einzelstaatlichen Ermittlungsbehörden sowie Europol, den EU-Mitgliedsstaaten und den Opfern beratend und unterstützend zur Seite. Wann die CSAM-Richtlinie verabschiedet werden wird, ist offen. Zuletzt hatten sich der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss kritisch geäußert. Sie werten die geplanten Regelungen als nicht vereinbar mit der Datenschutz-Grundverordnung und den freiheitlichen Grundrechten. Die emotionale Diskussion wird 2023 fortgesetzt werden.

Ab 1. Januar 2023 gilt das **Lieferkettengesetz,** zunächst für Unternehmen mit mehr als 3000 und ab 2024 auch für Unternehmen mit weniger als 1000 Beschäftigten. Es gilt zwar nicht ausschließlich für die IT-Branche, allerdings versprechen sich Marktbeobachter dort ein Umsatzwachstum, geht es doch um Automatisierung, Platform as a Service, Supply-Chain-Management sowie Blockchain-Technologien. Ungeachtet der gesetzlichen Vorgaben dürfte die Diskussion um Diversifizierung der Beschaffung von Produkten, Rohstoffen und dergleichen auch 2023 anhalten.

Fazit

Aus IT-rechtlicher Sicht wird es das Jahr 2023 in sich haben. Die EU ist sehr umtriebig und wird zahlreiche Gesetzesvorhaben umsetzen. Auf Unternehmen aller Branchen kommen zahlreiche neue Vorgaben zu, etwa bei der Cybersicherheit. Einige der Gesetzeswerke werden erst in den Jahren 2024 oder 2025 greifen. Zur Vorbereitung bleibt Unternehmen dennoch wenig Zeit. Denn ab Wirksamwerden der verschärften Vorgaben greifen signifikante Bußgelder nach dem Vorbild der Datenschutz-Grundverordnung. In manchen Fällen drohen auch Abmahnungen durch Verbände und Konkurrenten.

Ein Neujahrswunsch vieler betroffener Unternehmen für 2023

dürfte allerdings nicht in Erfüllung gehen: Es steht nicht zu erwarten, dass es vor der Europawahl 2024 noch zu einer Überarbeitung und Änderung der Datenschutz-Grundverordnung kommen wird. Hoffen darf man aber auf einen EU-US Privacy Shield 2.0 für die rechtssichere Übermittlung personenbezogener Daten in die USA. Hierzu wie auch in anderen Bereichen wird es auch im kommenden Jahr interessante und bedeutsame Gerichtsurteile geben, nicht zuletzt des Europäischen Gerichtshofs. Prosit 2023! (ur@ix.de)

1. Quellen
2. Tobias Haar; EU will digitale Märkte regulieren; iX 9/2022, S. 80
3. Die im Text angesprochenen Gesetzesvorhaben sind über ix.de/zqe9 zu finden.

Tobias Haar

ist Rechtsanwalt mit Schwerpunkt IT-Recht bei Vogel & Partner in Karlsruhe. Er hat zudem Rechtsinformatik studiert und hält einen MBA.

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

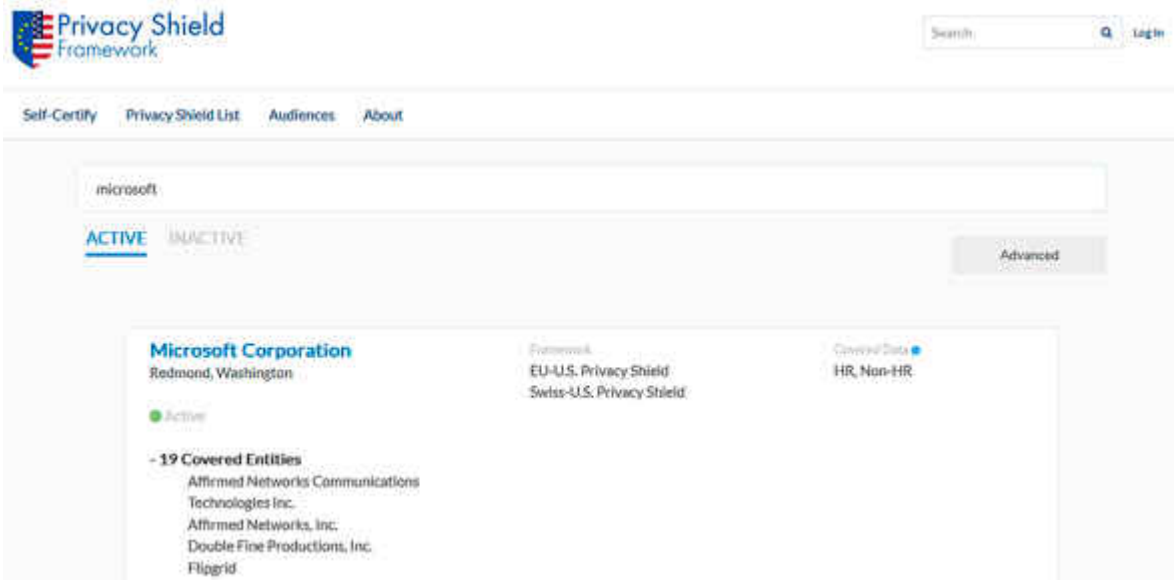
Seit dem Amtsantritt Joe Bidens in den USA und dem Angriff Russlands auf die Ukraine sind weitere Einflüsse auf künftige Regulierung maßgeblich geworden. Vor allem eine Frage treibt Politiker in Brüssel um: Auf wen wird man sich in Zukunft verlassen können? Ihre naheliegende Antwort: Auf als stabil

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

EU – Umgang mit Daten

Europäisches Trommelfeuer

Wie die EU den Umgang mit Daten revolutionieren will

Europa soll zum Vorbild für die digitale Gesellschaft werden. Dazu zündet die EU ein wahres Feuerwerk an Gesetzen. Sie sollen die Dominanz der US-Unternehmen brechen und europäischen Firmen einen besseren Zugang zu Daten verschaffen. Die geplanten Regulierungen stellen sogar die DSGVO in den Schatten, wie unsere Übersicht zeigt, und werden die Gesellschaft wohl nachhaltig verändern.

Von Joerg Heidrich

kompakt

- Ab Mitte 2023 reguliert der Digital Markets Act europaweit die Geschäftspraktiken von Onlineplattformen, ab 2024 greift der Digital Services Act.
- Der Data Governance Act und der Data Act sollen vor allem den Umgang mit nicht personenbezogenen Daten regeln, die nicht unter die DSGVO fallen.
- Firmen sollen ihre Daten künftig mit Treuhändern teilen, ein AI Act verbietet KI-Systeme in besonders risikoreichen Einsatzgebieten.

Mit viel Pathos kündigte die EU-Kommission Anfang 2020 in einer Art Manifest ihre neue Datenstrategie an. Die EU könne zu einem Vorbild für eine Gesellschaft werden, die „dank Daten in der Lage ist, in der Wirtschaft wie im öffentlichen Sektor bessere Entscheidungen zu treffen“. Um eine weltweit führende

Rolle in der Datenwirtschaft zu übernehmen, müsse man unverzüglich handeln und die vielfältigen Probleme regulatorisch angehen, die von der Konnektivität über die Datenverarbeitung und -speicherung bis hin zur Cybersicherheit reichen.

Hierfür sei es nötig, die Voraussetzungen für den Umgang mit Daten zu verbessern und für die Gesellschaft „Pools mit hochwertigen Daten“ aufzubauen. Diese sollen nicht nur die Produktivität von Firmen steigern und deren Wettbewerbsfähigkeit verbessern, sondern auch den Bereichen Gesundheit, Umwelt und öffentliche Dienste zugutekommen. Zugleich will man die digitale Wirtschaft fördern, damit sie mit Firmen aus den USA und China mithalten kann.

Um diese ambitionierten Ziele zu erreichen, hat die Kommission seit der Ankündigung ein ganzes Bündel aus Gesetzen auf den Weg gebracht. Juristen erwarten gar ein neues Rechtsgebiet, das Datenrecht. Im Fokus der Diskussion steht etwa ein halbes Dutzend dieser Vorhaben. Sie haben das Potenzial, die Gesellschaft nachhaltig zu verändern.

Digital Services Act

Dies gilt insbesondere für den Digital Markets Act (DMA) und den Digital Services Act (DSA). „Acts“ sind Verordnungen, die – wie beispielsweise die DSGVO – unmittelbar als europäisches Recht gelten. Im Gegensatz zu Richtlinien müssen Gesetzgeber in den einzelnen europäischen Ländern sie nicht erst in nationales Recht umsetzen.

EU-Binnenmarktkommissar Thierry Breton kündigte mit den neuen EU-Verordnungen „das Ende des Wilden Westens" im Internet an. *Bild: Virginia Mayo/Pool AP/dpa*

Der DSA tritt ab 2024 in Kraft und wendet sich insbesondere an Anbieter von Onlinediensten und sozialen Medien. Er verpflichtet diese, in kurzer Zeit gegen rechtswidrige Inhalte vorzugehen. Besonders strenge Anforderungen gibt es für jene großen Onlineplattformen und Suchmaschinen, die im Monat von mehr als 45 Millionen Menschen genutzt werden. Aufgrund ihrer Reichweite sollen deren Anbieter „systemische Risiken" eindämmen, die sich etwa aus der Verbreitung rechtswidriger Inhalte ergeben. Dazu zählen Desinformation oder Wahlmanipulation, Cybergewalt gegen Frauen sowie jugendgefährdende Inhalte. Die EU-Kommission sieht darin einen wichtigen Schritt „zur Verteidigung europäischer Werte wie Demokratie und Rechtsstaatlichkeit" im virtuellen Raum. Der DSA wird damit zum EU-weiten Nachfolger des deutschen Netzwerkdurchsetzungsgesetzes (NetzDG), welches bereits jetzt Social-Media-Angebote reguliert.

In die Pflicht nimmt der DSA auch Onlinemarktplätze. Sie haben dafür zu sorgen, dass über ihre Plattformen keine gefährlichen

oder illegalen Produkte wie Markenfälschungen angeboten werden. Das Gesetz sieht dazu neue Mechanismen vor, die es Usern ermöglichen, illegale Inhalte zu melden. Die Plattformen müssen zudem mit „vertrauenswürdigen Hinweisgebern“ zusammenarbeiten, die ihnen helfen sollen, verbotene Inhalte zu ermitteln und zu entfernen.

Der DSA regelt ferner bestimmte Formen der Werbung. Hier war sogar ein grundsätzliches Verbot von Werbetracking in der Diskussion, der Ansatz konnte sich jedoch nicht durchsetzen. Das Gesetz enthält allerdings ein Verbot irreführender Werbepraktiken, zum Beispiel gezielt auf Kinder ausgerichtete Werbung oder solche, die auf sensiblen Daten wie Religionszugehörigkeit, sexueller Ausrichtung oder politischer Meinung basiert. Dies wird die werbetreibende Industrie vor große Herausforderungen stellen.

Nach den neuen Vorschriften sind auch sogenannte Dark Patterns verboten. Onlineplattformen dürfen Nutzer nicht mehr täuschen oder manipulieren beziehungsweise „ihre Fähigkeit, freie und fundierte Entscheidungen zu treffen“ beeinträchtigen oder behindern.

Digital Markets Act

Der DMA kommt etwas früher und gilt bereits ab der zweiten Jahreshälfte 2023. Seine Vorschriften ergänzen das Wettbewerbsrecht und sollen die Macht der marktbeherrschenden Digitalkonzerne einschränken. Auf deren Plattformen, den sogenannten Gatekeepern, soll es zukünftig durch gesetzliche Regulierung fairer zugehen.

Welche Unternehmen unter diese Einstufung fallen, legt die Kommission explizit fest. Erfasst werden mit hoher Sicherheit Unternehmen wie Airbnb, Alphabet, Apple, Amazon, Meta und Microsoft. Dass es sich dabei um amerikanische Konzerne handelt, ist kein Zufall. Die gesamte Digitalstrategie der EU beruht darauf, es amerikanischen Unternehmen schwerer zu

machen und so die digitale Wirtschaft im europäischen Raum zu stärken. Aber auch die Verbraucher sollen geschützt werden, indem Firmen ihre Nutzerdaten nicht mehr über Plattformgrenzen hinweg zusammenführen dürfen.

Den Gatekeepern ist es zukünftig untersagt, ihre eigenen Dienste oder Produkte höher zu gewichten als die von anderen geschäftlichen Nutzern ihrer Plattform. Dies dürfte etwa Amazon oder Alphabet treffen, denen Kritiker häufig vorhalten, eigene Angebote gegenüber Dritten zu bevorzugen.

Weitere Regelungen sollen sogenannte Lock-In-Effekte verhindern. Die als Gatekeeper eingestuften Plattformen müssen ihre Angebote kompatibel zu denen von Wettbewerbern gestalten. In der Vergangenheit musste etwa Microsoft bereits hohe Strafen zahlen, weil es unter Windows seinen Edge-Browser gegenüber anderen Browser bevorzugt hatte.

Verstößt ein Gatekeeper gegen die Vorschriften des DMA, so kann dies für ihn sehr teuer werden. Die neue Vorschrift sieht Geldstrafen vor, die bis zu 10 Prozent Gesamtumsatzes betragen, die das Unternehmen im vorhergehenden Geschäftsjahr weltweit erzielt hat. Bei wiederholten Verstößen können die Strafen sogar bis zu 20 Prozent des Umsatzes betragen. Im Fall von Amazon wären das aktuell bis zu 94 Milliarden US-Dollar.

Die dänische EU-Kommissarin für Wettbewerb, Margrethe Vestager, gilt als treibende Kraft hinter dem Digital Markets Act, der wettbewerbswidrige Praktiken der großen US-Konzerne eindämmen soll. *Bild: Oliver Berg/dpa*

Umstrittene Interoperabilität

Die geplante Regulierung von Messenger-Diensten trifft bei kleineren Anbietern eher auf Ablehnung. Künftig müssen sich Platzhirsche wie WhatsApp und iMessage dafür öffnen, auch Nachrichten von Wettbewerbern zu empfangen. Kleinere Anbieter wie Signal oder Threema sperren sich jedoch gegen das Vorhaben. Die Firmen sehen nämlich durch die Pläne der EU die vertrauliche und sichere Kommunikation über ihre Apps bedroht. So fürchtet der Betreiber von Signal, dass die Zusammenarbeit mit den dominanten Messengern letztlich die Privatsphäre des eigenen Angebots verschlechtert. Die Mitbewerber hätten dann Zugriff auf Metadaten und könnten diese für ihre Zwecke nutzen. Daher haben beide Anbieter bereits angekündigt, auf eine Zusammenschaltung mit WhatsApp & Co. zu verzichten.

Laut Digital Markets Act müssen Gatekeeper wie WhatsApp sich für Konkurrenten öffnen, wenn diese das fordern. Anbieter wie Threema und Signal wollen davon jedoch keinen Gebrauch machen. *Bild: Threema*

Trainingsdaten für KI

Während der DMA und der DSA primär Plattformen und größere Onlinedienste regulieren, betrifft der zweite wichtige Teil der EU-Strategie den Umgang mit Daten. Für personenbezogene Daten gilt die Datenschutz-Grundverordnung (DSGVO) bereits seit 2018. Allerdings gibt es eine Vielzahl von Daten, die nicht unter die DSGVO fallen, insbesondere solche, die von Maschinen stammen und für das Training neuronaler Netze genutzt werden. Hier setzen zwei weitere Gesetzesvorhaben der EU an: der Data Governance Act (DGA) und der Data Act (DA).

Den DGA verabschiedeten die EU-Gremien bereits im Mai 2022. Er soll im September 2023 in Kraft treten. Ziel des Gesetzes ist es, dem öffentlichen Sektor den Zugang zu Daten zu erleichtern und ein „vertrauenswürdiges Umfeld“ für die Forschung sowie für innovative Dienste und neue Produkte zu schaffen.

Der DGA geht bei der Weitergabe von Daten an den öffentlichen Sektor sehr weit. Der Regelung liegt der Gedanke zugrunde, dass auch geschützte Daten der Gesellschaft zugutekommen sollen, wenn sie beispielsweise durch öffentliche Förderung generiert oder gesammelt wurden. Firmen sollen beispielsweise Geschäftsgeheimnisse, personenbezogene Daten und durch Rechte des geistigen Eigentums geschützte Werke übertragen. Dies gilt allerdings nur für Daten, die sich bereits „im Besitz öffentlicher Stellen“ befinden. Dort vorhandene Daten können etwa für Forschungszwecke im öffentlichen Interesse weiterverarbeitet werden.

Faire Datenbroker

Der DGA soll darüber hinaus ein neues und potenziell revolutionäres Geschäftsmodell etablieren: Es sollen Datenvermittlungsdienste entstehen, die eine sichere Umgebung bieten, in der Unternehmen oder Einzelpersonen Daten austauschen. Unternehmen sollen ihre Daten teilen können, ohne Missbrauch oder einen Wettbewerbsnachteil befürchten zu müssen.

Die Vermittlungsdienste bieten nur eine Plattform an und sind ansonsten neutrale Akteure. Die von ihnen vorgehaltenen Daten dürfen sie nicht zu eigenen Zwecken nutzen. Erstaunlicherweise müssen sie aber keinen Sitz innerhalb der EU haben, sondern dürfen sich auch außerhalb der EU niederlassen.

Auf Basis der neuen Regulierung sollen Dienste entstehen, die einen Handel mit persönlichen Daten ermöglichen. Der Gesetzgeber sieht solche Datainteremediären als Schlüssel für eine neu entstehende Datenwirtschaft. Genannt werden als Beispiel Daten-Wallets, also Apps, mit deren Hilfe der Einzelne in die Nutzung seiner Daten einwilligt und dadurch auch Geld verdienen oder sonstige Vorteile erlangen kann.

Daten für alle

Der dritte Bereich des Data Governance Acts bildet das Konzept des Datenaltruismus ab. Die EU will es Privatpersonen und Unternehmen erleichtern, der Gesellschaft Informationen für Ziele im allgemeinen Interesse zur Verfügung zu stellen. Hierzu zählen beispielsweise Daten für Forschungszwecke im Bereich der Medizin, des Klimawandels oder um öffentliche Dienstleistungen zu verbessern.

Allerdings ist es gar nicht so einfach, eine datenaltruistische Organisation zu werden. Die Stellen müssen neben hohen Anforderungen an ihre technische Ausstattung und Transparenz auch umfangreiche Berichtspflichten erfüllen, sobald sie in ein Verzeichnis aufgenommen wurden.

Den wohl radikalsten Ansatz hinsichtlich des Umgangs mit Daten verfolgt die Europäische Kommission derzeit mit dem Data Act (DA). Dieser befindet sich allerdings noch in einer recht frühen Phase des Gesetzgebungsverfahrens und wird nicht vor 2024 in Kraft treten. Der Grundgedanke des Data Act liegt darin, bislang weitgehend ungenutzte Potenziale von Daten auszuschöpfen und dadurch die europäische Wirtschaft zu fördern.

Zu diesem Zweck verpflichtet der DA Unternehmen dazu, ihre eigenen Daten zugänglich zu machen und Dritten zur Verfügung zu stellen. Dabei geht es in erster Linie nicht um personenbezogene Informationen, sondern um Maschinendaten, insbesondere aus Industrieanlagen, medizinischen Geräten, IoT- oder Smart-Home-Prozessen. Gerade kleine und mittlere Unternehmen (KMU) können auf solche Daten bislang nicht zugreifen oder sie zusammenführen, wodurch ihnen erhebliche Wettbewerbsnachteile bei der Entwicklung innovativer Geschäftsfelder entstehen.

Daten vergesellschaften

Der Data Act regelt zahlreiche, noch nicht abschließend diskutierte Voraussetzungen, unter denen Unternehmen verpflichtet werden können, ihre Informationen zu teilen. Zugleich soll er festlegen, wer unter welchen Umständen auf diese Daten zugreifen darf. Das können auch öffentliche Stellen sein, sofern sie ein erhebliches Interesse nachweisen, etwa im Rahmen der Bekämpfung einer Pandemie. Der DA soll so eine Art „freien Datenmarkt“ für nicht-personenbezogene Nutzungsdaten schaffen, auf dem diese gehandelt und weitergeben werden. Unter bestimmten Voraussetzungen sollen auch Vergütungen fließen.

Die Unternehmen, bei denen die begehrten Daten entstehen und in deren Rechte eingegriffen werden soll, reagieren nicht gerade begeistert auf den Vorstoß der EU-Kommission. So kritisiert beispielsweise der Bundesverband der Deutschen Industrie (BDI) in einer Stellungnahme bereits den Ansatz der Regulierung im DA. Man zweifele an der „Notwendigkeit eines solchen breit gelagerten Eingriffs in die Grundprinzipien der Datenwirtschaft in noch jungen Märkten”.

Die Kommission hält den Eingriff jedoch für notwendig, damit die europäische Wirtschaft mithilfe eines solchen Datenbinnenmarkts wettbewerbsfähig gegen eine sich rasant entwickelnde internationale Konkurrenz bleibt. Wie weit der Data Act jedoch in seiner finalen Form gehen wird, ist angesichts des langen Weges durch die Mühlen der europäischen Gesetzgebung noch offen.

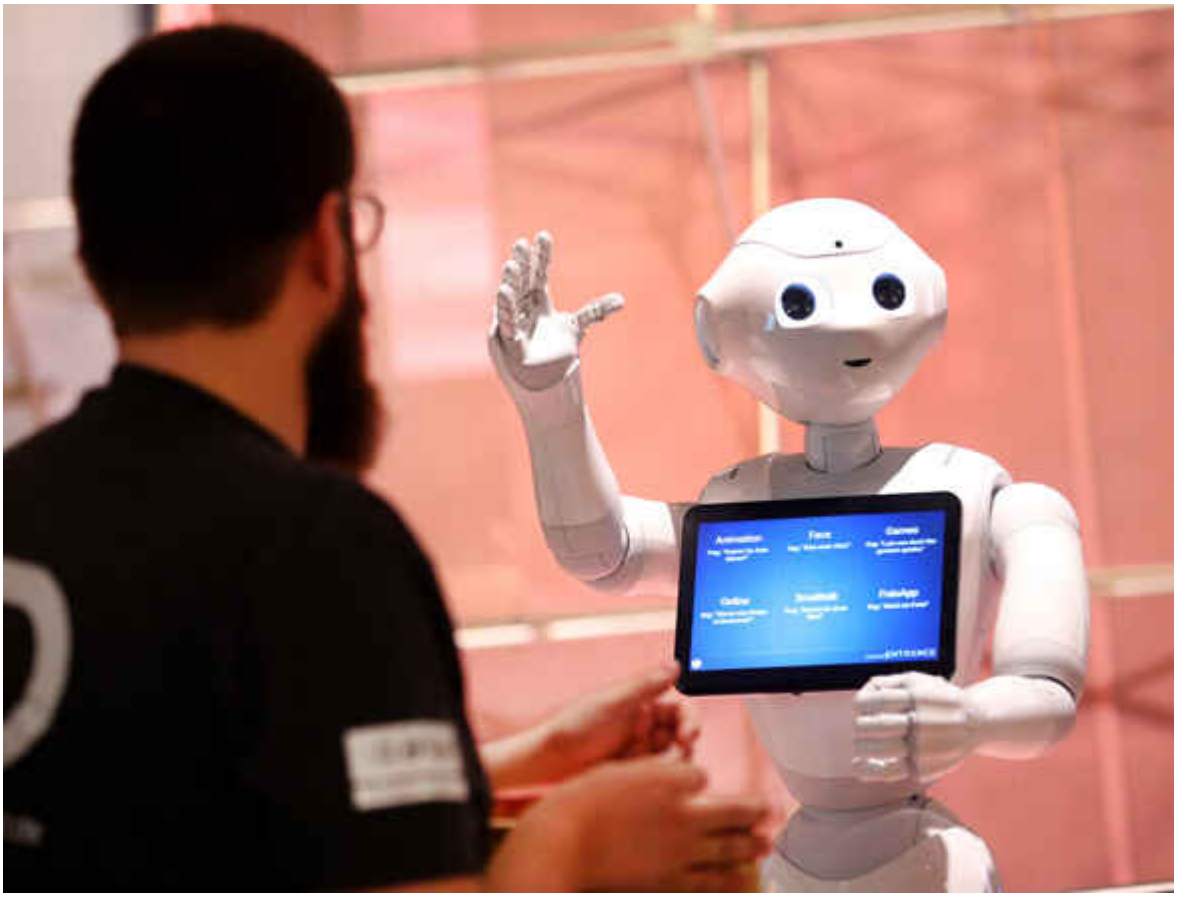
KI im Zaum halten

Erwähnenswert ist in diesem Zusammenhang auch der Artifical Intelligence Act, der ebenfalls noch in einer sehr frühen Phase der Gesetzgebung hängt und nicht vor 2024 zu erwarten ist. Der AI Act soll einen europaweit einheitlichen rechtlichen Rahmen schaffen, in dem Unternehmen und

Institutionen sichere und vertrauenswürdige Systeme mit künstlicher Intelligenz entwickeln und einsetzen.

Im Kern der vorliegenden Fassung steht dabei ein Stufensystem, das die KI-Anwendungen in verschiedene Risikoklassen mit daraus resultierenden Vorgaben einteilt. In die strengste Kategorie des „Inakzeptablen Risikos“ fallen vier Praktiken, die der Gesetzgeber als klare Bedrohung bewertet und grundsätzlich verbietet.

Hierzu gehören Social Scoring, also die „Klassifizierung der Vertrauenswürdigkeit natürlicher Personen auf der Grundlage ihres sozialen Verhaltens“ ebenso wie das sogenannte Nudging, die unterschwellige Beeinflussung einer Person außerhalb des Bewusstseins. Ebenfalls verbieten wollen die Initiatoren das „Ausnutzen der Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters oder ihrer Behinderung“. Zumindest teilweise wollen sie außerdem untersagen, biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zur Strafverfolgung zu nutzen. Erstaunlicherweise nicht in dieser Gruppe finden sich naheliegende Bedrohungen durch autonome Waffensysteme, die ihre Ziele mithilfe von künstlicher Intelligenz auswählen.



Der AI Act teilt KI-Systeme in Risikostufen ein und verbietet künftig beispielsweise deren Einsatz beim Social Scoring. *Bild: Roland Weihrauch/dpa*

Anwendungen, die als potenziell bedrohlich eingestuft werden, fallen in die Kategorie „Hohes Risiko“. Nutzt jemand Algorithmen für derartige Bereiche, so muss er zahlreiche Voraussetzungen erfüllen und die Sicherheit der Anwendung nachweisen. Hierzu zählt etwa, natürliche Personen biometrisch zu identifizieren und zu kategorisieren, ferner die Strafverfolgung, die Rechtspflege sowie die Verwaltung und der Betrieb kritischer Infrastrukturen.

Für Angebote im Bereich des „begrenzten Risikos“ gelten vor allem Transparenzverpflichtungen. Hierunter fallen zum Beispiel Chatbots, die dann als solche gekennzeichnet werden müssen. Nutzer sollen informierte Entscheidungen treffen können, ob sie diese Angebote nutzen wollen. Nicht reguliert werden KI-gestützte Prozesse mit „minimalem Risiko“ wie KI-gestützte Videospiele oder Spamfilter, da von ihnen nur eine geringe Gefahr für die Sicherheit und Rechte der Nutzer

ausgehe.

Der AI Act sieht in seinem derzeitigen Stadium weiterhin vor, dass die von einer KI getroffenen Entscheidungen „transparent und fair“ sein müssen. Das könnte in einigen Bereichen, in denen etwa Deep Neural Networks zum Zuge kommen, sehr schwierig werden, weil die trainierten Netzwerke zum Teil Tausende Variablen einbeziehen. Aber auch bei diesem Entwurf kann es noch zu erheblichen Änderungen im Rahmen des Gesetzgebungsverfahrens kommen.

Fazit

Die Grundgedanken der ambitionierten Datenstrategie der EU-Kommission sind nachvollziehbar und im Grundsatz auch sinnvoll. Die Liste von geplanten oder bereits umgesetzten Gesetzen ist sogar noch weitaus länger als hier dargestellt.

Es ist allerdings fraglich, ob man ein hochgradig disruptives und dynamisches Umfeld tatsächlich einer so weitgehenden staatlichen Regulierung unterwerfen und diese mit den Rechten von Bürgern und Unternehmen in Einklang bringen kann. Ungeklärt ist beispielsweise das Verhältnis der DSGVO zu den vielen neuen Acts, denen ein allzu rigider Datenschutz in vielen Bereichen im Weg stehen wird. Schließlich ist es ja ein Ziel der Regulierungen, die internationale Wettbewerbsfähigkeit der europäischen Wirtschaft zu verbessern, indem man ihr den Zugang zu Daten erleichtert. Zudem überschneiden sich viele der neuen Grundverordnungen in zahlreichen Punkten. Zu befürchten ist daher, dass ein regulatorisches Dickicht entsteht, welches auf Jahre zu einer großen Rechtsunsicherheit führt. *(hag@ct.de)*

Die wichtigsten EU-Gesetzesinitiativen	
Name	Wichtigste Regelungen
Digital Markets Act (DMA)	– reguliert den Wettbewerb und insbesondere große Unternehmen – verpflichtet Gatekeeper zu fairem Wettbewerb – fordert Interoperabilität zwischen Anbietern (Messenger)
Digital Services Act (DSA)	– verlangt sicheren digitalen Raum ohne rechtswidrige Inhalte – fordert von Onlinemarktplätzen eine Überwachung der Angebote – verbietet bestimmte Werbepraktiken, etwa gezielte Ansprache von Kindern
Data Governance Act (DGA)	– reguliert Verfügbarkeit von Daten für den öffentlichen Sektor – schafft Basis für Datenvermittlungsdienste und Datenaltruismus
Data Act (DA)	– fördert die Wirtschaft durch stärkere Datennutzung – regelt Voraussetzungen, unter denen Firmen ihre Daten teilen müssen – strebt einen freien Datenmarkt für nicht-personenbezogene Daten an
Artificial Intelligence Act (AIA)	– reguliert den Rahmen und die Entwicklung künstlicher Intelligenz – teilt KI-Anwendungen in Risikoklassen mit bestimmten Beschränkungen ein

Datenstrategie der EU-Kommission: ct.de/ynr9