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.

Kündigungsbutton: zahlreiche Abmahnungen

Kündigungsbutton: zahlreiche Abmahnungen

Seit Juli 2022 besteht eine Pflicht, Verbrauchern das Kündigen online abgeschlossener Verträge zu erleichtern. Die Verbraucherzentrale Bayern hat 840 Webseiten daraufhin untersucht und erhebliche Mängel festgestellt, die zu 154 Abmahnungen wegen Rechtsverstößen geführt haben. In einigen Fällen wird es zu Gerichtsverfahren kommen.

In zahlreichen Fällen war der vorgeschriebene Kündigungsbutton gar nicht vorhanden, in anderen Fällen war er versteckt und nicht wie gesetzlich gefordert „gut auffindbar“. Verstöße lagen auch gegen die Pflicht vor, eine gut lesbare Schaltfläche mit der Aufschrift „jetzt kündigen“ oder einer gleichwertigen Bezeichnung vorzuhalten. *Tobias Haar* (ur@ix.de)

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

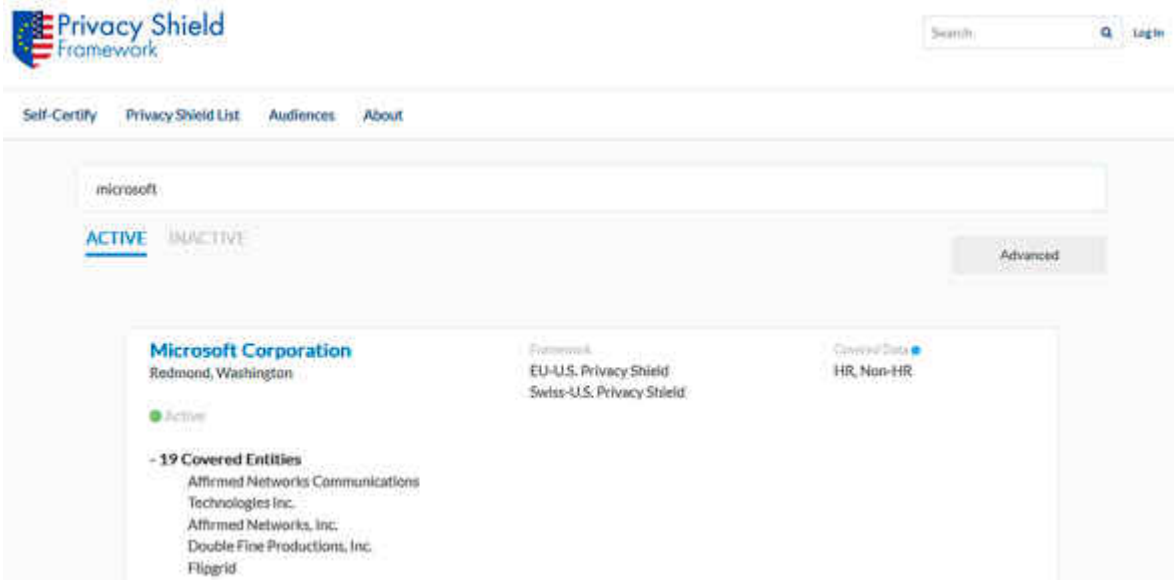
Seit dem Amtsantritt Joe Bidens in den USA und dem Angriff Russlands auf die Ukraine sind weitere Einflüsse auf künftige Regulierung maßgeblich geworden. Vor allem eine Frage treibt Politiker in Brüssel um: Auf wen wird man sich in Zukunft verlassen können? Ihre naheliegende Antwort: Auf als stabil

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.

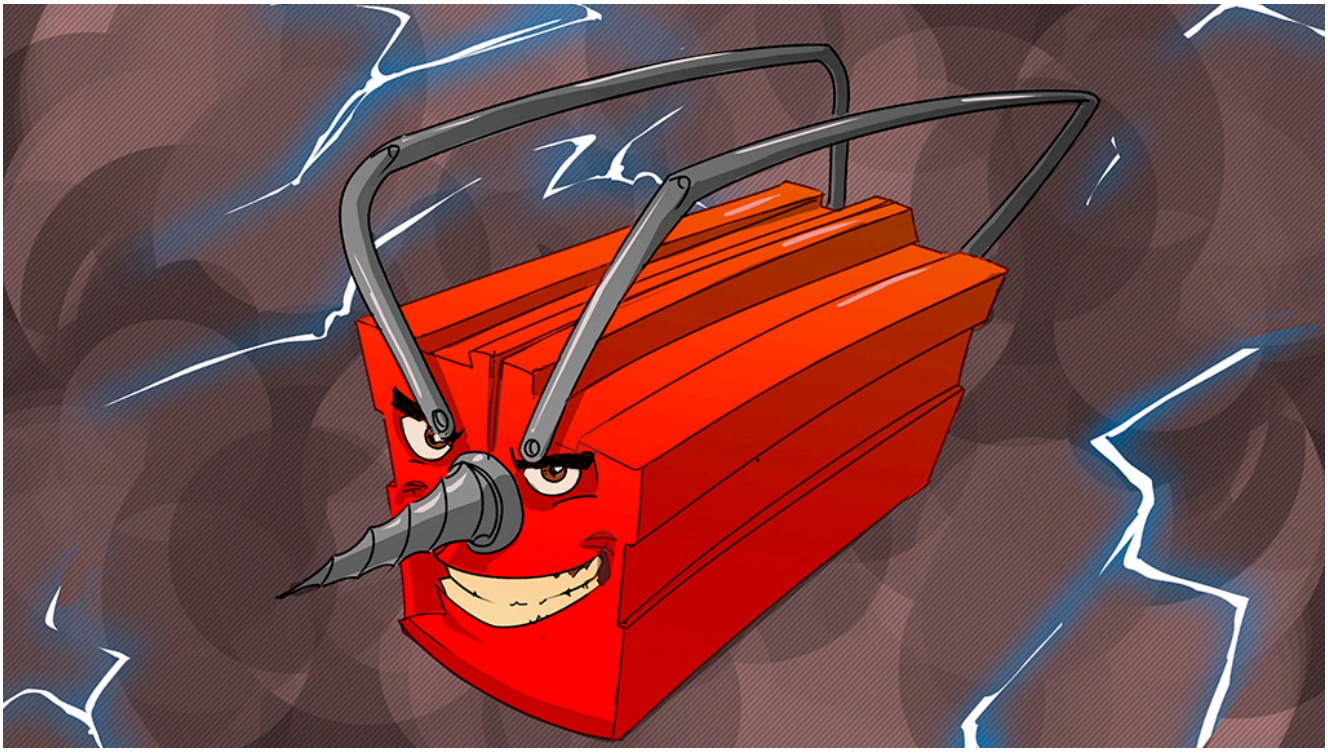
Bei einigen Gesetzgebungsvorhaben ist unklar, ob sie tatsächlich den gewünschten, großen Unterschied machen können. Zugleich lauern auch in den Brüsseler Schubladen der Kommissare immer wieder Ideen, die nicht unbedingt von tieferem Verständnis für die digitalpolitischen Debatten der vergangenen Jahrzehnte 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

Rechtliche Unsicherheiten bei Hacking-Werkzeug



Kommt drauf an, wozu

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bei…

Kommt drauf an, wozu

Rechtliche Unsicherheiten bei Hacking-Werkzeug

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen

Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bein vor Gericht?

Von Verena Ehrl

Der Theaterautor und Sprachliebhaber Hans-Joachim Haecker brachte die Dual-Use-Problematik bereits 1968 in einem Gedichtchen seines Bandes „Insonderheit“ unter dem Eindruck des internationalen Wettrüstens scherzhaft auf den Punkt:

„Insonderheit die Abwehrwaffen
sind für die Abwehr wie geschaffen.
Auch kann man mit geschickten Händen
sie für den Angriff gut verwenden.“

Die Waffen, mit denen Akteure innerhalb der IT-Welt hantieren, eignen sich zum Eindringen in Systeme, zum Überwinden von Sicherungsmaßnahmen, zum Spionieren und Manipulieren. Dieselben Werkzeuge können aber dazu dienen, unterschiedliche Ziele zu erreichen. In der Hand eines Administrators, der ein System, für das er verantwortlich ist, Penetration Tests („Pentests“) aussetzt, kann etwa das Software-Tool „Mimikatz“ legalen Einsatz finden (S. 24). Es ebnet allerdings ebenso gut Angreifern den Weg bei illegalen Aktionen, indem es ihnen Zugangsdaten für die Übernahme eines Netzwerks offenbart. Auf diese Ambivalenz bezieht sich das Schlagwort „Dual Use“ im Zusammenhang mit Hackerausrüstung.

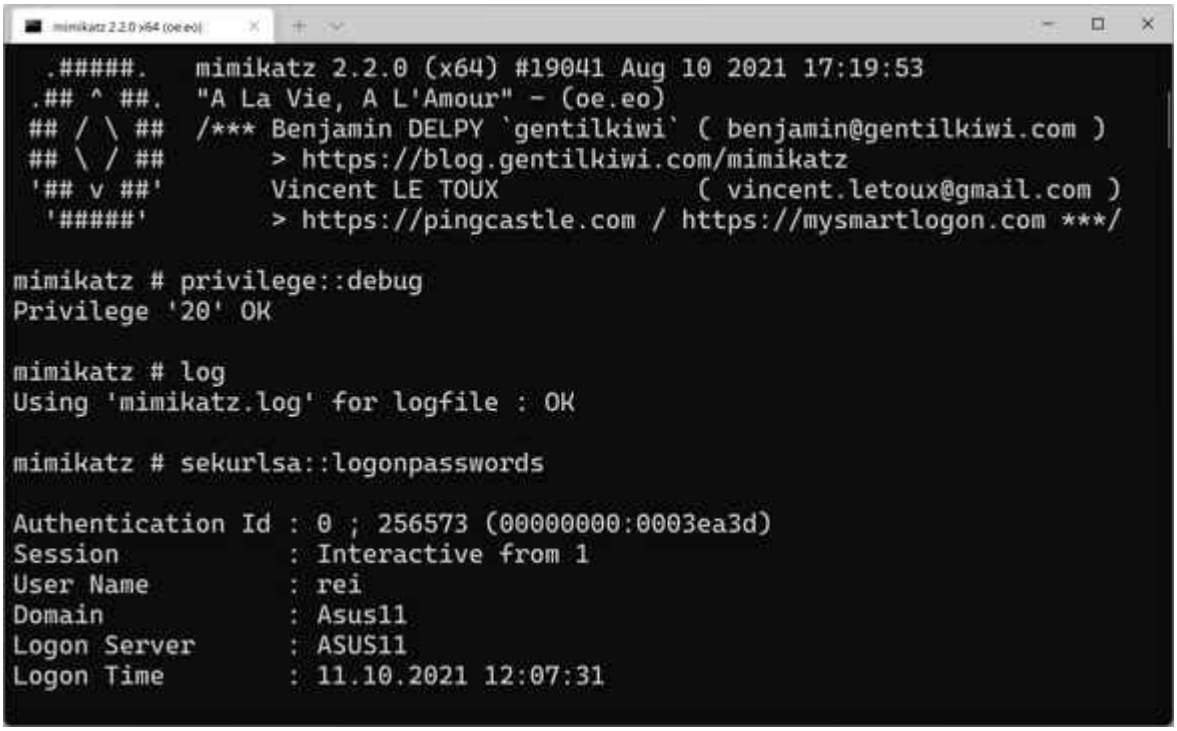
Nicht immer erscheinen die Werkzeuge, um die es geht, so spektakulär wie die Hacking-Gadget-Hardware, mit der c’t sich in Ausgabe 18/2017 befasst hat [1]. Sehr oft steht vielmehr bloße Software im Mittelpunkt, die loggt, sucht, entschlüsselt, ausliest, analysiert und speichert (S. 16, 18, 24 und 39). Die rechtlichen Fragen, vor die ein Anwender gestellt ist, sind jedoch grundsätzlich die gleichen wie bei den Spionagegerätchen [2]: Wo liegt die rote Linie, jenseits

der man sich auf illegalem Terrain bewegt? Was sagt das geltende Recht zum Umgang mit potenziell gefährlichen und schadenträchtigen Tools?

Dass es „Güter mit doppeltem Verwendungszweck“ gibt, die sich gleichermaßen für legales und illegales Tun eignen, beschäftigt nicht zuletzt den europäischen Gesetzgeber. Am 9. September 2021 ist die Neufassung der sogenannten Dual-Use-Verordnung in Kraft getreten [3].

Sie betrifft „Güter einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können“. Es gibt durchaus Softwareentwicklungsprojekte, die man mit etwas Fantasie in den Betrachtungshorizont der Verordnung rücken kann.

Ziel der Dual-Use-Verordnung ist die Exportkontrolle. Die kann bereits relevant werden, wenn Forschung und Produktentwicklung mit Partnerunternehmen in bestimmten außereuropäischen Ländern stattfinden und dabei schadenträchtige Software im Spiel ist.



Mimikatz ist ein typisches Beispiel für ein Hackerwerkzeug, das auch verantwortungsvollen Admins wertvolle Dienste leistet, wenn es ums Aufspüren von Schwachstellen im eigenen Netz geht.

Neu im Blick der europäischen Rechtssetzungsorgane und der zur Umsetzung verpflichteten Mitgliedsstaaten sind Länder, welche die Todesstrafe praktizieren oder in denen Menschenrechtsverletzungen wie Folter auf staatliches Geheiß stattfinden. Wer etwa potenziell gefährliche Software ins nichteuropäische Ausland transferieren will, braucht dazu eine vorherige Genehmigung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Diese Behörde entscheidet in jedem Einzelfall, ob der Transfer zulässig ist oder nicht.

Zweierlei Paar Schuhe

Abseits der von der Verordnung erfassten Transferproblematik sind Dual-Use-Softwarewerkzeuge rechtlich schwer zu fassen. Weder ihr Erwerb noch ihr Besitz ist grundsätzlich untersagt. Straf- und Zivilrecht melden sich erst dann, wenn jemand diese Tools einsetzt, um Rechtsbrüche zu begehen. Derjenige riskiert dann eine Strafe oder er sieht sich zivilrechtlichen Ansprüchen ausgesetzt – oft droht ihm beides.

Nicht alles, was jemand rechtswidrig tut, ist auch strafbar. Mit dem Strafrecht geht der Staat gegen von ihm untersagtes Verhalten vor, dabei sind Strafermittlungsbehörden im Spiel, es gibt Beschuldigung und Anklage. Im Zivilrecht stehen hingegen gleichberechtigte Streitparteien einander gegenüber. Dabei gibt es Kläger und Beklagte, die Gerichte entscheiden über Ansprüche, welche die Parteien gegeneinander geltend machen. Vertragspflichten und Schadenersatzansprüche sind typisches zivilrechtliches Geschäft.

Durch Software kann ein Anwender sich Ärger in beiden Rechtsbereichen einhandeln. Ein gutes Beispiel für die rechtliche Gratwanderung dabei sind die bereits angesprochenen Pentests. Sie haben die Aufgabe, Schwachstellen in Konfiguration, Hard- und Software von Servern, Routern und Arbeitsplätzen im Netz aufzuzeigen. Ein Mitarbeiter, der einen solchen Test im Auftrag eines zuständigen Entscheiders für das betroffene Netz durchführt, bewegt sich damit auf der legalen

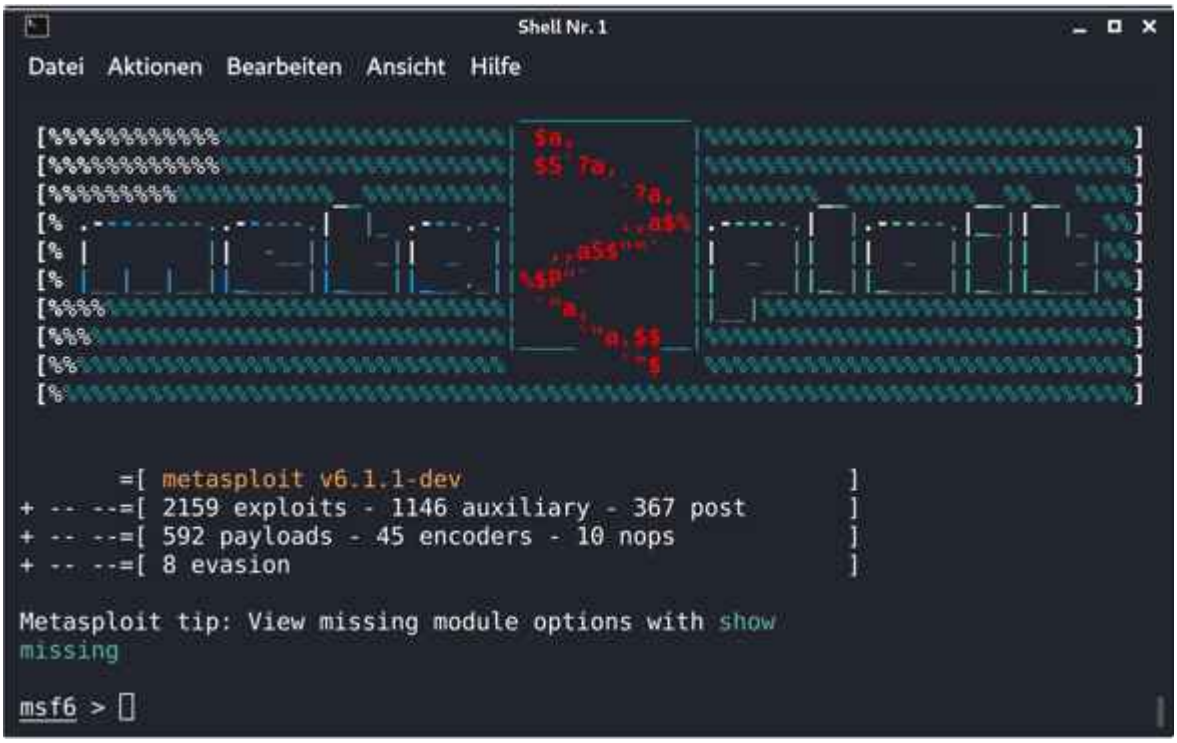
Seite. Wenn allerdings etwa ein Cybersecurity-Dienstleister einen Pentest unaufgefordert und ohne Erlaubnis bei einem potenziellen Kunden durchführt, um diesen als Auftraggeber zu gewinnen, setzt er sich strafrechtlicher Verfolgung wegen Datenveränderung oder Computersabotage aus.

Wesentlich sind dabei die Paragrafen 303a und 303b des Strafgesetzbuchs (StGB), die sich mit virtueller Sachbeschädigung befassen. Damit hat der Gesetzgeber 1986 eine Regelungslücke beim Straftatbestand der Sachbeschädigung (§ 303 StGB) geschlossen. Die klassische Sachbeschädigung setzt einen körperlichen Gegenstand voraus – das lässt Daten und beispielsweise Festplatten, die funktionsfähig bleiben, aber deren Inhalt gelöscht oder verschlüsselt wurde, außen vor.

§ 303a StGB stellt die unbefugte Veränderung von Daten unter Strafe. Dort heißt es in Absatz 1: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

Bereits der Versuch ist strafbar; dasselbe gilt wie beim Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) auch fürs „Vorbereiten“ einer rechtswidrigen Datenveränderung – beispielsweise durch Bereitstellen von Software, deren „Zweck die Begehung einer solchen Tat ist“ (§ 202c Abs. 1 Nr. 2 StGB).

Als Daten in diesem Sinne gelten nach § 202 StGB „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“, also nicht etwa Papiernotizen.



Das modulare Pentesting-Tool Metasploit ist bei Security-Experten beliebt, es lässt sich aber auch für echte Angriffe missbrauchen.

§ 303b StGB, der sogenannte Hackerparagraf, ist der Computersabotage gewidmet. Er steht in direktem Zusammenhang mit seinem Nachbarn, der die Datenveränderung betrifft, und lautet: „Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, … erheblich stört, … wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“

Wenn es um die Datenverarbeitung eines Unternehmens respektive einer Behörde geht, stehen Freiheitsstrafen bis zu fünf Jahren im Raum. In besonders schweren Fällen riskieren Täter sogar bis zu zehn Jahren Gefängnis. Der Paragraf grenzt die Wege, auf denen die strafbare Datenverabeitungsstörung bewirkt wird, näher ein: Unter Nr. 1 fasst er die Störung durch Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (siehe § 303a Abs. 1). Unter Nr. 2 erscheint die Dateneingabe und -übermittlung mit der Absicht, jemand anderem einen Nachteil zuzufügen. Unter Nr. 3 schließlich geht es darum, dass eine Datenverarbeitungsanlage oder ein Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder

verändert wird. Auch hierbei sind wie bei der Datenveränderung bereits Versuch und Vorbereitung strafbar.

Dass es nur ums Stören von Datenverarbeitungen von „wesentlicher Bedeutung“ geht, soll Bagatellfälle aus dem Blick der Strafjustiz nehmen.

Erpressungstrojaner vor Gericht

Im April 2021 hat der Bundesgerichtshof (BGH) einen Fall entschieden, der die Verteilung von Ransomware betraf – also das Einschleusen von Verschlüsselungstrojanern zu Erpressungszwecken [4]. Dabei stufte das Gericht unter anderem das Anbringen einer Eintragung in der Windows-Registry, die das automatische Laden einer Schadsoftware beim Rechnerstart bewirkte, als strafbare Datenveränderung ein. Zugleich sah der BGH in diesem Fall auch eine Computersabotage nach § 303b StGB.

Der Angeklagte war Mitglied einer Cybercrime-Bande mit Sitz in der Ukraine. Diese hatte mit ihren Ransomware-Angriffen von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro erpressen können.

Schadsoftware ähnlicher Art mit einer vorgesehenen Entsperrmöglichkeit hätte aber auch im Rahmen eines Pentests in einem lokalen Netz durchaus legal verwendet werden können. Ein Unternehmen hätte damit etwa seine Mitarbeiter auf deren Vorsicht testen können, was das Anklicken unbekannter Inhalte betrifft.

Computersabotage am Arbeitsplatz

Das mutwillige Stören des Datenverarbeitungsbetriebs kann nicht nur strafrechtliche, sondern auch arbeitsrechtliche Auswirkungen haben. Mitarbeiter, die aus Wut oder infolge von Rachegedanken gegen ihren Arbeitgeber Datenvandalismus im

Unternehmensnetz betreiben, riskieren eine fristlose Kündigung.

Das geschah 2019 einem als Key-Account-Manager beschäftigten Arbeitnehmer nach einer heimlichen Löschaktion auf dem Unternehmensserver seines Arbeitgebers. Nach einer Abmahnung war ihm zuvor ein Aufhebungsvertrag angeboten worden. Daraufhin löschte er 8 GByte an Daten, darunter Kalkulationssoftware, Umsatzmeldungen, Vorlagen für Preislisten und Wettbewerbsanalysen für bestimmte Produkte. Die Daten konnten später wiederhergestellt werden. Der Verdacht fiel auf ihn. Gegen die fristlose Kündigung , die er wenig später erhielt, wehrte er sich zunächst erfolgreich. In der Berufungsinstanz jedoch unterlag er vor dem Landesarbeitsgericht (LAG) Baden-Württemberg im September 2020 [5]. Sein Arbeitgeber hatte einen 93seitigen Vergleich des Datenbestands im fraglichen Verzeichnis vor und nach der Löschaktion vorgelegt.

Das Gericht sah die fristlose außerordentliche Kündigung als begründet an: Das unbefugte vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers tauge ebenso wie das Vernichten von Verwaltungsvorgängen grundsätzlich als „wichtiger Grund“ für eine solche Kündigung im Sinne des § 626 Abs. 1 BGB. Dabei komme es nicht unbedingt darauf an, ob sich der Arbeitnehmer nach § 303a StGB oder § 303b StGB strafbar gemacht habe. Es sei auch nicht entscheidend, ob und mit welchem Aufwand ein Teil der gelöschten Daten wiederhergestellt werden konnte oder ob der Arbeitgeber diese Daten für den weiteren Geschäftsablauf tatsächlich benötigte. Vielmehr gehöre es zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehre oder unmöglich mache.

In der Hand von Angreifern kann auch der Fern Wifi Cracker, mit dem man Drahtlosnetze auf Sicherheitslücken abklopft, zum Werkzeug für eine Straftat werden.

Wenn der Admin spioniert

Dass es bei der strafrechtlichen Bewertung von Hacker-Aktivitäten nicht so sehr um die benutzten Werkzeuge als vielmehr um Zweck und Absicht des Einsatzes geht, illustriert auch ein Fall, den 2020 der BGH in letzter Instanz entschied [5]. Zwei Männer mussten sich wegen des Ausspähens von Daten (§ 202a StGB) verantworten. Einer davon leitete die Stabsstelle eines Apothekerverbandes und betrieb daneben ein gesundheitspolitisches Informationsportal im Internet. Der

zweite Angeklagte arbeitete als Systemadministrator am Berliner Standort des Bundesgesundheitsministeriums (BMG) und war nebenbei als Callboy tätig – daher rührte auch die Bekanntschaft der beiden Männer.

Der Admin hatte jahrelang Zugriffsrecht auf alle E-Mail-Accounts seiner Dienststelle und versorgte den Portalbetreiber mit so gewonnenen Interna aus dem Ministerium. Nachdem das Ministerium den unbeschränkten Mailzugriff der Administratoren im Hause als Sicherheitsmangel erkannt hatte, wurde es für den Mann schwieriger – er verlegte sich schließlich auf einen unter den Admins bekannten Notfalltrick, mit dem er sich selbst von Fall zu Fall die nötigen Zugriffsrechte verschaffte. Er lieferte dem Portalbetreiber auf Datenträger kopierte E-Mail-Inhalte nach Wunsch und kassierte dafür insgesamt rund 1000 Euro. Sein Kunde war besonders an E-Mails der Minister und Staatssekretäre sowie einiger Abteilungs- und Referatsleiter interessiert. In den weitergereichten Mails ging es unter anderem um Gesetzesvorhaben, die für das Publikum des Portals besonders interessant waren.

Das Landgericht (LG) Berlin verurteilte die Männer im April 2019 wegen gemeinschaftlichen Ausspähens von Daten nach § 202a StGB und sah in der Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten zudem die Überwindung einer Zugangssicherung nach § 202a Abs. 1 StGB. Die gegen das landgerichtliche Urteil eingelegte Revision wies der BGH weitgehend ab, lediglich den einzuziehenden Geldbetrag setzte er niedriger an als die Vorinstanz.

Die Bundesrichter beschäftigten sich vor allem damit, ob Daten im Sinn des §202a Abs. 1 StGB überhaupt als gesichert gelten können, wenn ein Admin mithilfe seiner Kenntnisse darauf zugreifen kann. Die Antwort: Es genüge, wenn getroffene Vorkehrungen den Zugriff auf Daten zumindest deutlich erschweren. Die Sicherung von E-Mail-Accounts durch Passwörter reiche aus. Dabei brauche der Systembetreiber nur den Zugriff Unbefugter zu berücksichtigen, aber nicht die

Zugriffsmöglichkeit durch Eingeweihte oder Experten. Es sei nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt – wenn dieser etwa ein Administrator ist, der den tatsächlichen Zugriff auf die Daten hat.

Als Überwinden der Zugangssicherung nach § 202a StGB können dem Gericht zufolge auch Handlungen gelten, die nicht besonders anspruchsvoll oder aufwendig sind. Wenn jemand durch Insiderkenntnisse oder Ähnliches eine Absicherung schnell und leicht ausschalten kann, zähle das rechtlich ebenso, als hätte sich jemand durch raffinierte technische Werkzeuge Zugriff verschafft. Nur wenn eine Durchbrechung des Schutzes für jedermann ohne Weiteres möglich sei, werde der Tatbestand nicht erfüllt.

Wer den Schaden hat …

Wie bereits gesagt, ist strafrechtliche Verfolgung nicht das Einzige, was der illegale Einsatz von Hacking-Tools nach sich ziehen kann: Wenn dabei ein Schaden entsteht, hat der Geschädigte einen Anspruch auf Schadenersatz gegen den Verursacher. Schäden durch IT-Störmanöver können sehr hoch sein – wenn etwa durch den Ausfall von Unternehmensservern Arbeitsprozesse lahmgelegt werden. Auch der Ausfall der Netzkommunikation kann enorme Umsatzeinbußen und damit hohe wirtschaftliche Schäden bedeuten. Für Anspruchsteller im Zivilrecht ist wichtig, dass jede Streitpartei alles, was für ihre Sache spricht, selbst gerichtsfest beweisen muss. Das kann bei Schäden durch Hackertools etwa den Nachweis eines Hackerangriffs und die zweifelsfreie Benennung des Angreifers betreffen. Außerdem ist auch nachzuweisen, dass der Angriff tatsächlich den geltend gemachten Schaden hervorgerufen hat.

Wenn ein Täter bereits strafrechtlich wegen einer Computerstraftat zulasten eines Geschädigten verurteilt worden ist, hat jener es anschließend vergleichsweise leicht, seine Ansprüche gegen den Verurteilten zivilrechtlich geltend zu machen: Das Urteil des Strafgerichts hat selbst bereits

Indizwirkung, zudem kann der Kläger die im Strafverfahren erhobenen Beweise zu seinen Gunsten nutzen.

Ein dritter, bislang noch nicht genannter Bereich, der durch unrechtmäßigen Einsatz von Hackertools berührt werden kann, ist der Datenschutz. Wo bei einem Angriff personenbezogene Daten im Spiel sind, geht es nicht bloß um wirtschaftliche Schäden, sondern möglicherweise auch um die massenhafte Verletzung des informationellen Selbstbestimmungsrechts der Betroffenen. Wer es also als Pentester mit realen Datenbeständen zu tun hat, tut gut daran, die Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) sorgfältig zu beachten. *(psz@ct.de)*

1. Literatur

2. Ronald Eikenberg, David Wischnjak, Böse und billig: Hacking-Gadgets, Gefahr durch angriffslustige Hardware, c’t 18/2017, S. 62 und S. 64
3. Verena Ehrl, Elektronische Übeltäter, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c’t 18/2017, S. 78
4. Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20.5.2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck: heise.de/s/N76o
5. BGH, Beschluss vom 8.4.2021, Az. 1 StR 78/21: heise.de/s/rmDJ
6. LAG Baden-Württemberg, Urteil vom 17.9.2020, Az. 17 Sa 8/20: heise.de/s/MXBL
7. BGH, Beschluss vom 13.5.2020, Az. 5 StR 614/19: heise.de/s/Zvpw

101 Rechtsfehler im Online-Marketing – Folge II

“101 Rechtsfehler im Online-Marketing –

Teil 2 ” – websiteboosting.com

Im Online-Marketing kann man bekanntlich viele teure Fehler machen. Für viele Marketer besonders mysteriös sind rechtliche Mängel. In den folgenden Heften wollen wir den häufigsten Fehlern auf den Grund gehen und jeweils kurz darstellen, was man alles falsch machen kann – und wie es besser geht. …
Im Online-Marketing kann man bekanntlich viele teure Fehler machen. Für viele Marketer besonders mysteriös sind rechtliche Mängel. In den folgenden Heften wollen wir den häufigsten Fehlern auf den Grund gehen und jeweils kurz darstellen, was man alles falsch machen kann – und wie es besser geht. In Folge 2 geht es um Social Media und Display-Werbung.

Unzureichende Sensibilisierung von Mitarbeitern für Social Media

Ein Hauptproblem bei Social-Media-Auftritten kleiner und mittlerer Unternehmen ist die unzureichende Schulung der Kolleg:innen, die die Accounts mitbetreuen. Es würde schon helfen, wenn den Mitarbeiter:innen bewusst wäre, dass Facebook & Co keine Spielwiese sind, auf der man Dinge ausprobieren kann, die für die Website „zu gefährlich“ erscheinen.

Zu spät bei Account-Namen

Es ist für Unternehmen um ein Vielfaches günstiger, sich die einschlägigen Aliase bei neuen sozialen Netzwerken jeweils zu reservieren oder durch entsprechende Dienstleister reservieren zu lassen, als später mühsam die Accounts kaufen oder einklagen zu müssen. Dies gilt insbesondere für Start-ups und Unternehmen ohne starke Marken.

Facebook, Twitter und Co: fehlendes

Impressum

Auch bei Twitter und Facebook muss ein Impressum vorhanden sein, wenn die Social-Media-Plattformen geschäftsmäßig genutzt werden. In Konzernen ist es wichtig, sich genau zu überlegen, welche Gesellschaft Betreiberin der Social-Media-Profile sein soll.

Fehlende Datenschutzinformation für Facebook-Page

Jede professionelle Facebook-Seite braucht eine Datenschutzinformation. Aus dieser muss sich ergeben, dass die Seite aus datenschutzrechtlicher Sicht gemeinsam mit Facebook betrieben wird. Außerdem sollte darin beschrieben sein, wie die Nutzer:innen ihre Rechte – etwa auf Auskunft und Löschung – geltend machen können.

Fehlende Einwilligung bei Mitarbeiterfotos

Wer Angestellte auf Fotos oder in Videos auf Social-Media-Präsenzen präsentieren möchte, sollte vorher schriftlich die Einwilligung einholen oder gleich eine Art Model-Release-Vertrag mit den jeweiligen Beschäftigten schließen. Wichtig ist, dass denjenigen, die das nicht möchten, kein Nachteil entsteht.

Firmenevents auf Facebook & Co

Wer vorhat, Firmenevents – wenn diese denn irgendwann einmal wieder stattfinden können – in sozialen Netzwerken zu bebildern, muss dafür sorgen, dass die Abgebildeten davon wenigstens wissen. Am besten ist es, schon bei der Einladung darauf hinzuweisen und auch am Veranstaltungsort entsprechende

Aushänge zu machen. Wer sich nicht auf Facebook sehen möchte, hat ein Widerspruchsrecht. Wichtig ist in jedem Falle: Augenmaß bei der Auswahl der Bilder.

Selbstbewertungen

Nur weil die Wahrscheinlichkeit, entdeckt zu werden, gering scheint, heißt das nicht, dass Unternehmen sich selbst positiv bewerten sollten. Es ist als Schleichwerbung wettbewerbswidrig. Auch eine Incentivierung positiver Bewertungen durch eigene Mitarbeiter:innen sollte unterbleiben. Im Übrigen kommt insbesondere systematische Selbstbeweihräucherung meist doch heraus, sei es über ausgeschiedene Kollegen, verärgerte Agenturen oder deren Mitarbeiter.

Rabatt gegen Bewertungen

Die Rechtsprechung sieht es außerordentlich kritisch, wenn Kunden Vorteile für die Abgabe einer Bewertung geboten werden. Evident rechtswidrig ist das Versprechen eines Rabatts für eine positive Bewertung. Vertragliche Vereinbarungen, etwa in AGB, negative Bewertungen zu unterlassen, sind unwirksam.

Werbung mit Preisen in Social Media ohne Pflichthinweis

Die Preisangabenverordnung gilt natürlich auch auf Facebook und Instagram. Wer dort gegenüber Privatleuten mit Preisen wirbt, muss mitteilen, dass die Preise inklusive Mehrwertsteuer sind und ob gegebenenfalls Versandkosten hinzukommen.

Anzeigen auf Facebook ohne Pflichtangaben

Auch Werbung in sozialen Netzwerken ist Werbung. Gibt es spezielle branchenspezifische Regeln für die Ausgestaltung von Werbung, müssen diese auch auf Twitter und Facebook eingehalten werden.

Laxer Umgang mit beleidigenden Kommentaren

Unternehmen sind für Nutzerkommentare verantwortlich, sobald sie Kenntnis davon haben. Enthalten etwa die Kommentare von YouTube-Videos Beleidigungen oder falsche Behauptungen, sind Unterlassungsansprüche der Betroffenen die Folge. Zensurvorwurf hin oder her: Rechtswidrige Kommentare müssen gelöscht werden, sobald der Betreiber der Seite davon Kenntnis erlangt.

Verwendung von User-Fotos ohne ausreichende Rechte

Es ist unzulässig, Fotos von Nutzer:innen zu verwenden, ohne dass diese damit einverstanden sind. Die Fotograf:innen haben stets das Recht zu bestimmen, ob und wo ihre Fotos veröffentlicht werden. Im Zweifel braucht es also eine ausdrückliche Erklärung von User:innen, wenn deren Fotos in Sovial-Media-Präsenzen von Unternehmen eingesetzt werden sollen.

Influencer-Marketing ohne

Werbekennzeichnung

Jede nicht ohne Weiteres als solche erkennbare Werbung muss gekennzeichnet werden. In Verträgen mit Influencern müssen Unternehmen auf Transparenz drängen, um als Auftraggeber nicht selbst verklagt zu werden.

Unscheinbare Werbekennzeichnung von Influencern

Die Rechtsprechung ist streng und verlangt eine deutliche Kennzeichnung von Influencer-Marketing als Werbung. Ein unscheinbares #ad am Ende einer Wolke aus Hashtags genügt nicht. Besser ist eine deutliches #Werbung oder #sponsored.

Anbieten von Glücksspielen

Die Grenze zwischen erlaubtem Gewinnspiel und verbotenem Glücksspiel sind teilweise fließend. Man muss also darauf achten, dass das Marketing keine Spiele veranstaltet, bei denen die Spieler einen finanziellen Einsatz leisten müssen, um teilnehmen zu können. Einen Like oder Kommentar zu hinterlassen, zählt allerdings nicht als geldwerter Einsatz, der ein Gewinnspiel zu einem illegalen Glücksspiel macht.

Unzureichende Teilnahmebedingungen bei Gewinnspielen

Es gibt keinen Zwang, für jedes Gewinnspiel Teilnahmebedingungen vorzusehen. Allerdings empfiehlt sich das häufig, um die gesetzlichen Pflichtangaben unterzubringen. Diese sollten dann alle wesentlichen Angaben zu dem Gewinnspiel enthalten.

Verwendung von Gewinnspieldaten zu Werbezwecken

Die Tatsache, dass jemand an Ihrem Gewinnspiel teilgenommen hat, rechtfertigt nicht, dieser Person Werbung zuzusenden. Die Nutzung von Daten zu Werbezwecken setzt in aller Regel eine Einwilligung des Betroffenen voraus. Ob man die Teilnahme an einem Gewinnspiel von der Erteilung einer Werbeeinwilligung abhängig machen darf (Kopplung), wird unterschiedlich bewertet. Die Datenschutzbehörden sind eher kritisch.

Werbung in Direktnachricht ohne Einwilligung

Für die Direktwerbung in sozialen Netzwerken gelten die gleichen Regeln wir für die Werbung per E-Mail. Es ist unzulässig, werbende Direktnachrichten zu versenden, ohne dass der Empfänger zuvor eingewilligt hat.

Custom Audience ohne Nutzereinwilligung

Für das Re-Targeting von Nutzern über soziale Netzwerke braucht man in der Regel eine Einwilligung der Nutzer. Dies gilt nach Ansicht der Datenschutzbehörden auch für den Einsatz des Facebook-Pixels.

Direkteinbindung von Social-Plug-ins auf der Website

Datenschützer halten die Einbindung des Like-Buttons und anderer Plug-ins für rechtswidrig, weil eine Übermittlung personenbezogener Daten unmittelbar an das soziale Netzwerk erfolge, ohne dass der Nutzer eingewilligt habe. Drittinhalte

sollten wo möglich mit datensparsamen Varianten integriert werden.

Anreicherung von CRM-Daten um Informationen aus Social Media

Sollen Daten aus dem eigenen Customer-Relationship-Management-System mit Daten zusammengeführt werden, die über Social-Media-Monitoring erhoben wurden, setzt dies praktisch immer die Einwilligung des Betroffenen voraus. Fehlt diese, liegt ein Datenschutzverstoß vor.

Getarnte Displaywerbung

Beachten Sie das Gebot der Trennung von Werbung und redaktionellem Inhalt. Wenn sich nicht aus dem Banner unmittelbar ergibt, dass es Werbung ist, muss das Werbemittel als Anzeige gekennzeichnet sein.

Datenerhebung in interaktiven Bannern

Werden personenbezogene Daten über interaktive Banner erhoben, ohne dass der Betroffene dies erkennen kann, ist dies ein Datenschutzverstoß. Jedenfalls bedarf es einer Datenschutzinformation. Vorsicht ist geboten bei zu vielen Pflichtfeldern – es gilt das Gebot der Datenminimierung.

B2C-Bannerwerbung mit Nettopreisen

Werden in Bannern Preise für bestimmte Produkte angegeben, muss es sich dabei um Gesamtpreise handeln. Es ist ein Verstoß gegen die Preisangabenverordnung und damit wettbewerbswidrig, wenn zu den angegebenen Preisen noch weitere Kosten hinzutreten.

Umgehung von Pop-up-Blockern

Werden Pop-ups technisch so ausgestaltet, dass sie herkömmliche Pop-up-Blocker umgehen, ist dies eine unzumutbare Belästigung.

Gekaufte Advertorials

Werbung ist stets von redaktionellen Inhalten zu trennen. Wird Unternehmen die Möglichkeit gegeben, sich im Rahmen eines Advertorials werblich darzustellen, muss die Werbung als Anzeige gekennzeichnet werden.

Fake-Bewertungen

Es ist zwar üblich, aber klar wettbewerbswidrig, vermeintlich objektive Produktbewertungen in Online-Portalen abzugeben. Wenn Mitarbeiter einer PR-Agentur Produkte von Kunden in Online-Portalen lobend erwähnen oder der Verlag auf Amazon eine geschönte Rezension eines eigenen Buches verfasst, ist dies als Schleichwerbung wettbewerbswidrig.

Fehlende Einwilligung beim Targeting

Werden personenbezogene Daten für Targeting-Maßnahmen verwendet, bedarf es häufig einer Einwilligung, jedenfalls aber einer transparenten Information des Nutzers.

Targeting: fehlendes Opt-out

Auch wenn keine Einwilligung erforderlich sein sollte (etwa bei einfachem Re-Targeting), muss dem Nutzer die Möglichkeit gegeben werden, der Profilbildung (auch unter Pseudonym) zu widersprechen. Es bedarf also einer Opt-out-Möglichkeit. In der Praxis geschieht dies in der Regel durch Setzen eines Opt-

out-Cookies.

Location Based Messages ohne Einwilligung des Nutzers

Wenn Sie mit mobilen Nachrichten werben, müssen Sie die Einwilligung des Empfängers haben – sowohl für die Zusendung von Werbung als auch für die Nutzung der Standortdaten.

Kundenprofile im Mobile Targeting

Die Bildung umfangreicher Nutzerprofile bedarf nach der Rechtsprechung einer Einwilligung der Betroffenen. Dies gilt jedenfalls, wenn Daten, die auf der Website erhoben werden, mit Klardaten des Betroffenen zusammengeführt werden. Werden Nutzerprofile etwa bei der mobilen Werbung mit Log-in-Daten des Nutzers abgeglichen, um noch mehr Informationen über einen konkreten User zu erhalten, ist das ein Datenschutzverstoß, wenn keine Einwilligung des Nutzers vorliegt.

---

101 Rechtsfehler im Online-Marketing – Teil 4

101 Rechtsfehler im Online-Marketing –

Teil 4 – websiteboosting.com

Im Online-Marketing kann man bekanntlich viele teure Fehler machen. Für viele Marketer besonders mysteriös sind rechtliche Mängel. In den folgenden Heften wollen wir den häufigsten Fehlern auf den Grund gehen und jeweils kurz darstellen, was man alles falsch machen kann – und wie es besser geht. In.…
Im Online-Marketing kann man bekanntlich viele teure Fehler machen. Für viele Marketer besonders mysteriös sind rechtliche Mängel. In den folgenden Heften wollen wir den häufigsten Fehlern auf den Grund gehen und jeweils kurz darstellen, was man alles falsch machen kann – und wie es besser geht. In Folge 4 geht es um typische Rechtsfehler im Online-Shop.

Fehlende Anpassung an geändertes E-Commerce-Recht

Kaum ein Rechtsgebiet ist so häufigen Änderungen unterworfen wie das Fernabsatzrecht. E-Commerce-Unternehmer müssen sich ständig über diese Änderungen auf dem Laufenden halten und die eigene Website, AGB und Datenschutzinformation anpassen. Dies gilt umso mehr, als Übergangsfristen oft nicht eingeräumt werden. Vom Tag des Inkrafttretens eines neuen Gesetzes muss dieses von den Unternehmern daher in der Regel beachtet werden.

Falsche oder fehlende Widerrufsbelehrung im B2C-Bereich

Im Online-Handel muss jedem Verbraucher das Recht zugestanden werden, den Kauf ohne Angabe von Gründen rückgängig zu machen. Über dieses Widerrufsrecht ist der Verbraucher zu informieren. An Inhalt und Form der Belehrung werden strenge Anforderungen gestellt, die vielfach ignoriert werden. Es ist empfehlenswert, die vom Gesetzgeber zur Verfügung gestellte Musterbelehrung zu verwenden. Ohne anwaltliche Hilfe sollte

davon nicht abgewichen werden.

Fehlendes Widerrufsrecht bei digitalen Inhalten

Ein Widerrufsrecht besteht auch für den Download von E-Books, Computerspielen, Apps, Musik oder Filmen. Der Verbraucher hat also 14 Tage nach dem Download Zeit, sich den Vertragsschluss noch einmal zu überlegen. Dies bedeutet auch, dass der Anbieter die Kunden über das Bestehen dieses Rechts ordnungsgemäß informieren muss.

Fehlender Hinweis auf Nichtbestehen eines Widerrufsrechts

Von der Pflicht, im B2C-E-Commerce ein Widerrufsrecht einzuräumen, gibt es viele Ausnahmen. Besteht eine Ausnahme, muss der Verbraucher darauf hingewiesen werden. Dabei genügt es zwar, einen Standardtext unterhalb der Widerrufsbelehrung anzubringen. Einen solchen Passus muss der Händler aber anbringen.

Unnötiges vertragliches Widerrufsrecht

Wer bei der Formulierung von AGB und Widerrufsbelehrung nicht aufpasst, räumt auch solchen Kunden ein Widerrufsrecht ein, bei denen das nicht notwendig ist. Das ist zwar nicht abmahnfähig, aber unnötig. So können dann etwa gewerbliche Besteller zu den gleichen Konditionen an ein Widerrufsrecht gelangen wie Privatkunden. Auch wenn eigentlich Ausnahmen gelten, kann aus Versehen ein Widerrufsrecht eingeräumt werden.

Unklare Situation bei Rücksendung der Ware

Der Verbraucher muss eindeutig seinen Widerruf erklären. Die Zurücksendung der Ware soll nach dem Gesetz dafür nicht genügen. Wird in den AGB oder auf dem Retourenschein nicht ausdrücklich klargestellt, dass die Rücksendung als Ausübung des Widerrufsrechts aufgefasst wird, ist bei jeder einfachen Rücksendung unklar, was der Kunde eigentlich wollte.

Fortlassen des Widerrufsmusters

So absurd es auch klingen mag: Das Gesetz verlangt, dass jedem privaten Online-Kunden ein Muster zur Verfügung gestellt wird, das der Verbraucher verwenden kann, um seinen Widerruf zu erklären. Wird dieses gesetzliche Muster weggelassen, drohen Abmahnungen.

Unvollständige Verbraucherinformation

Das Fernabsatzrecht sieht eine scheinbar endlose Anzahl von Umständen vor, über die der Verbraucher im Detail zu informieren ist. Wird auch nur eine dieser Informationen nicht mitgeteilt, ist die Verbraucherinformation unvollständig, mit der Folge, dass der Shop-Betreiber abgemahnt werden kann.

Fehlende Angaben zu Herstellergarantien

Zu den Pflichtinformationen gehören zum Beispiel Angaben zu bestehenden Garantien. Noch ist gerichtlich nicht geklärt, ob dazu auch Herstellergarantien gehören, auf die der Händler keinen Einfluss hat. Dennoch sollte man solche Garantien jedenfalls dann bei dem jeweiligen Produkt verlinken, wenn mit

einer Garantie geworben wird.

Unzutreffende Produktbilder

Anzugeben sind auch die wesentlichen Merkmale der Ware. Ein Teil dieser Pflicht lässt sich über geeignete Fotografien erledigen. Hierbei ist aber Vorsicht geboten. Auf den Bildern müssen die Produkte sein, die auch verkauft werden. Ein häufiger Fehler ist, dass daneben auch weitere Gegenstände abgebildet werden, die – aus Sicht des Kunden – womöglich im Preis enthalten sind.

Unzureichende Versandkostenangaben

Häufig fehlen konkrete Angaben zu Versandkosten. Sind Versandkosten abhängig von Menge oder Gewicht, muss sich dies aus der Versandkostenangabe eindeutig ergeben. Unterscheiden sich die Kosten für den Versand der Ware ins Ausland, muss auch dies klar und deutlich auf der Website angegeben sein. Insbesondere bei Auslandsversandkosten wird oft nachlässig gehandelt.

Fehlende Angabe der verfügbaren Zahlungsmittel

Online-Händler müssen schon vor Vertragsschluss auf der Website angeben, auf welchem Wege der Verbraucher bezahlen kann. Das wird häufig übersehen, lässt sich aber auch durch Einbindung entsprechender Logos lösen.

Unzureichende Angabe von Lieferzeiten

Ebenfalls ein häufiger Fehler sind unkonkrete Angaben zur Belieferung. Das Gesetz sieht vor, dass konkrete Angaben zu

machen sind, wann mit einer Lieferung zu rechnen ist. Angaben wie „Fremdbelieferung“, „Lieferung auf Nachfrage“ oder „nachbestellt“ genügen nicht den strengen Anforderungen. Zulässig ist dagegen die Angabe von Circa-Fristen (Abschnitt 5.2.7).

Fehlende Informationen bei digitalen Inhalten

Werden E-Books, Apps oder Software oder der Zugang zu Musik oder Video-Portalen verkauft, muss über die technische Funktionsweise der Inhalte und etwaige Urheberrechtsschutzmechanismen informiert werden. Der Anbieter ist auch dazu verpflichtet, darüber zu informieren, mit welcher Hard- und Software die erworbenen digitalen Inhalte kompatibel sind.

Fehlende Angaben zur Sprache des Kundendienstes

Ein beliebter Fehler bei der Erweiterung des Online-Shops auf ausländische Märkte ist, dass zwar die Website in verschiedenen Sprachen angeboten wird, sodass Bestellungen auch ausschließlich in der fremden Sprache möglich sind. Gleichzeitig wird Support jedoch nur auf Englisch und Deutsch angeboten. In diesem Fall ist in der jeweils anderen Sprache auf den Umstand gesondert hinzuweisen, dass es keinen Kundendienst in dieser Sprache gibt.

Link zur EU-Streitbeilegungsplattform

Die Europäische Union hat eine Online-Plattform ins Leben gerufen, die eine einfache, effiziente, schnelle außergerichtliche Lösung für Streitigkeiten zwischen

Verbrauchern und Händlern bieten soll. Auf diese Plattform muss jeder B2C-E-Commerce-Händler verlinken.

Fehlende Pflichtangaben im Warenkorb

Die wesentlichen Merkmale der Ware müssen im Warenkorb noch einmal wiedergegeben werden. Ein bloßer Link auf die Produktdetailseite soll nicht genügen. Viele Richter interpretieren das recht weit und wollen zum Beispiel auch das Material oder die genaue Größe im Warenkorb noch einmal sehen.

Fehlende Übermittlung der Informationen in Textform

Sämtliche Informationen, die vor Vertragsschluss zu erbringen sind, müssen dem Verbraucher auch auf einem dauerhaften Datenträger, d. h. auf Papier oder per E-Mail zugehen. Hierin liegt einer der wesentlichen Fehler bei den Verbraucherinformationen. Alle Pflichtangaben müssen dem Kunden dauerhaft vorliegen. Die Möglichkeit der Speicherung von der Website genügt nicht.

Fehlende oder veraltete Datenschutzerklärung

Jeder Online-Shop braucht eine Datenschutzinformation. Diese Datenschutzerklärung muss ein lebendes Dokument sein. Wird ein neues Tool oder ein neuer Dienstleister eingesetzt, muss das in aller Regel in der Datenschutzinformation vermerkt werden.

Fehlende Verlinkung der

Datenschutzinformation

Die Information über die Datenverarbeitung muss erfolgen, bevor die Daten erhoben werden. Deshalb empfiehlt es sich, die Datenschutzerklärung transparent an zentraler Stelle (zum Beispiel in der Fußzeile des Shops) zu verlinken.

Zusammenkopierte AGB

Allgemeine Geschäftsbedingungen sind der Standardvertrag des Händlers mit seinen Kunden. Einfach AGB der Konkurrenz zu übernehmen ist schon deshalb keine gute Idee, weil dessen Situation eine andere sein kann als die eigene. Zudem sind allgemeine Geschäftsbedingungen häufig urheberrechtlich geschützt, sodass eine Kopie auch ein Urheberrechtsverstoß sein kann. Es ist gar nicht so selten, dass AGB an sich überflüssig sind. Wer einen B2C-Online-Shop für Textilien betreibt, wird in AGB kaum zulässige Abweichungen vom Gesetz vereinbaren können. Dann kann man auf AGB auch gleich verzichten.

Veraltete AGB

Das Recht ändert sich häufig. Gerade erst ist das Gesetz über faire Verbraucherverträge verkündet worden, das etwa für Aufrechnungen und Kündigungsbestimmungen in AGB neue Regeln festlegt. Diese müssen jeweils aktuell umgesetzt werden. Auch neue obergerichtliche Urteile führen manchmal zu Anpassungsbedarf.

Verwendung identischer AGB im Multi-Channel-Marketing

Es kann problematisch sein, die gleichen allgemeinen Geschäftsbedingungen und Widerrufsbelehrungen in verschiedenen Vertriebsformen einzusetzen. Wird z. B. über das

Zustandekommen des Vertrages belehrt, muss diese Belehrung auf eBay anders aussehen als im Online-Shop. Wird zudem auch über den stationären Handel oder etwa über Vertriebspartner verkauft, sind unter Umständen weitere Anpassungen notwendig.

Vertragsannahme statt Bestellbestätigung

Online-Händler sind verpflichtet, dem Verbraucher den Eingang der Bestellung per E-Mail zu bestätigen. Bisweilen wird aber keine Bestellbestätigung („Ihre Bestellung ist bei uns eingegangen“), sondern gleich eine Vertragsbestätigung („Vielen Dank für die Bestellung der Ware, die wir so schnell wie möglich versenden werden“) versandt. Das ist nachteilig, weil die Möglichkeit wegfällt, zu prüfen, ob der Bestellung etwa eine fehlerhafte Preisauszeichnung im Shop zugrunde liegt.

Nichtbeachtung von Spezialgesetzen

Für eine Vielzahl von Artikeln bestehen spezielle gesetzliche Regelungen. Diese gelten oft unabhängig von der konkreten Vertriebsform und regeln die Werbung für die besonderen Produkte oder auch die Einzelheiten des Produktvertriebs. Jeder Händler sollte sich bei seinem Interessenverband oder einem Rechtsanwalt erkundigen, welche speziellen Regelungen zu beachten sind.

Verstöße gegen das Textilkennzeichnungsgesetz

Eine typische Regelung, die oft übersehen wird, ist die Textilkennzeichnungsverordnung. Danach muss bei der Bewerbung sämtlicher Textilien eine Angabe der Textilfaseranteile erfolgen. Spezialversender sind darauf eingerichtet. Doch auch

wer beispielsweise als Add-on zu Merchandising-Zwecken T-Shirts vertreibt, muss die Pflichtangaben in die Werbung aufnehmen.

Kostenpflichtige Rufnummer für Kundenhotline

Die für den Kunden anfallenden Kosten für Hotlines zu Vertragsfragen dürfen den Grundtarif nicht übersteigen. Solche Kundenhotlines dürfen daher keine teuren Mehrwertrufnummern sein. Werden verschiedene Hotlines betrieben, sollte klargestellt werden, welche Rufnummer welchem Zweck dient.

Überhöhte Kosten für bestimmte Zahlungsmittel

Das Gesetz reguliert die Kosten, die dem Verbraucher für den Einsatz bestimmter Zahlungsmittel abverlangt werden dürfen. Zum einen muss es stets eine kostenfreie gängige Möglichkeit der Bezahlung geben. Zum anderen dürfen die verlangten Zusatzkosten für die Bezahlform nicht den Betrag übersteigen, den der Händler für den Einsatz des jeweiligen Zahlungsmittels hat.

Untergeschobene Zusatzleistungen

Wer seinen Kunden neben der Hauptleistung im Bestellprozess weitere zusätzliche Leistungen verkaufen möchte, muss den Kunden dies ausdrücklich bestätigen lassen. Der Kunde muss also jeweils ein Häkchen anklicken müssen, um die Zusatzleistung zu buchen.

Nichterstattung von Versandkosten

im Falle des Widerrufs

Dem Verbraucher sind die Kosten für einen Standardversand der Ware vom Händler zum Kunden zu erstatten, wenn der Kunde den Kaufvertrag widerruft. Etwaige Versandkostenpauschalen sind also mit dem Kaufpreis der Ware zu erstatten. Wer das nicht tut, handelt wettbewerbswidrig und kann abgemahnt werden.

Nettopreise in Bannern

Es ist unproblematisch, in Werbebannern mit Preisen zu werben. Werden in einer Werbung, die sich jedenfalls auch an Verbraucher richtet, Preise angegeben, müssen dies jedoch Gesamtpreise sein, zu denen weder Steuern noch sonstige Gebühren oder Kosten hinzukommen. Andernfalls handelt es sich um einen Verstoß gegen die Preisangabenverordnung.

Fehlende Grundpreisangabe

Messbare Waren, die in bestimmten Mengen abgefüllt werden, müssen auch im Online-Shop mit einer Grundpreisangabe versehen werden. Hier muss dem Verbraucher also ein Preis pro Maßeinheit (Kilogramm, Liter etc.) mitgeteilt werden. Fehlt eine solche Angabe bei einzelnen Artikeln oder erfolgt die Angabe nicht unmittelbar bei der Beschreibung der Ware, ist dies in der Regel wettbewerbswidrig und kann von Konkurrenten abgemahnt werden.

Unzureichende Bevorratung bei Sonderangeboten

Es ist unzulässig, ein Sonderangebot zu bewerben, wenn die Ware nicht für einen Mindestzeitraum zu den beworbenen Konditionen erhältlich ist. Daran ändert auch ein dezenter Hinweis „Nur solange der Vorrat reicht“ nichts.

Unzulässiges Werben mit Gütesiegeln

Mit Gütesiegeln darf nur werben, wenn der Prüfprozess für das jeweilige Siegel abgeschlossen und dem Händler formal das Recht eingeräumt wurde, das Siegel auf der Website zu verwenden. Klar irreführend ist auch die Werbung mit einem selbst kreierten Siegel, wenn dies einen offiziellen Eindruck erwecken soll.

Umgang mit Verbraucherbestellungen in B2B-Shops

Der rechtssichere Betrieb eines B2B-Online-Shops setzt einen wirksamen Ausschluss von Verbrauchern voraus. Dabei genügt es nicht, auf die Website oder in die AGB zu schreiben, dass Verträge nur mit Unternehmen geschlossen würden. Erforderlich ist vielmehr, dass kontrolliert wird, dass der Vertragspartner tatsächlich ein Unternehmer ist. Auf eine entsprechende Angabe des Kunden darf der Händler aber vertrauen. Nachprüfungen sind nicht erforderlich.

Sorglosigkeit im Cross-Border-Vertrieb

Händler, die über Ländergrenzen hinweg Online-Vertrieb betreiben, müssen sich bewusst sein, dass sie dadurch unter Umständen ausländisches Recht zur Anwendung bringen. Auch bei der Erstellung von allgemeinen Geschäftsbedingungen muss darauf geachtet werden. Hier ergeben sich aus Sicht des Versandhändlers Gestaltungsspielräume, die genutzt werden sollten.

Nutzung von Kundendaten für Werbe-

E-Mails

Ein weitverbreiteter Irrglaube ist die Annahme, bestehende Kundendaten aus Online-Shop-Bestellungen könnten für die Versendung von Newslettern genutzt werden, ohne dass eine ausdrückliche Einwilligung des Kunden erforderlich ist. Zwar gibt es hier ein Schlupfloch, dessen Voraussetzungen in § 7 Abs. 3 UWG geregelt sind. Die Anforderungen sind jedoch hoch. Von der Ausnahme Gebrauch machen kann nur, wer es explizit darauf anlegt.

Reaktivierungskampagnen ohne Einwilligung

Dementsprechend sind auch Reaktivierungskampagnen von Bestandskunden regelmäßig nur bei Vorliegen einer Einwilligung der Kunden zulässig. Dies gilt übrigens auch für gewerbliche Kunden.

Werbung in Transaktions-E-Mails

Der Bundesgerichtshof hat entschieden, dass Werbung in Transaktions-E-Mails (z. B. Bestellbestätigungen oder Autoresponder) nur zulässig ist, wenn der Empfänger eine Werbeeinwilligung erteilt hat.

E-Mails an Warenkorbabbrecher

Es ist unzulässig, ohne Einwilligung per E-Mail Aufforderungen an potenzielle Kunden zu senden, einen zuvor abgebrochenen Kauf abzuschließen.

Bitten um Feedback per E-Mail

Auch Feedbackanfragen werden von der Rechtsprechung für Werbung gehalten. Daher sind auch solche E-Mails

einwilligungsbedürftig. Es bedarf also einer Einwilligung oder die Voraussetzungen der Bestandskundenwerbung nach § 7 Abs. 3 UWG müssen eingehalten werden.

E-Mail-Adresse zur Kontaktaufnahme

Markt + Trends | IT-Recht & Datenschutz

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende

klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Das Landgericht Düsseldorf hat erneut bestätigt, dass eine kommerzielle Webseite eine **E-Mail-Adresse zur Kontaktaufnahme** durch Internetnutzer enthalten muss (LG Düsseldorf, Beschluss vom 17.08.2022 – 12 O 219/22). Bei Verstößen können Webseitenbetreiber auf Basis der Regelung des § 5 Telekommunikationsgesetz erfolgreich abgemahnt werden.

Neueste Entwicklungen im Datenschutzrecht

Markt + Trends | IT-Recht & Datenschutz

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden erfahren Sie, wie ein sogenannter Bl…

Das Arbeitsgericht Baden-Württemberg hat zu zwei **Fragen des Auskunftsrechts** nach der Datenschutz-Grundverordnung entschieden (ArbG Baden-Württemberg, Urteil vom 10.08.2022, 2 Sa 16/21 ab Rdnr. 96). Zum einen genügt nach dessen Auffassung eine Auskunftserteilung per E-Mail, da die DSGVO keine besondere Form hierfür vorgibt. Zum anderen stellte das Gericht klar, dass der Auskunftsverpflichtete sich des Datenschutzbeauftragten als Erfüllungsgehilfen bedienen darf.

Wegen der **missbräuchlichen Verwendung von Grundbuchdaten** hat

der Datenschutzbeauftragte Baden-Württembergs ein Bußgeld in Höhe von 55 000 Euro verhängt. Ein Vermessungsingenieur hatte von seiner gesetzlichen Erlaubnis zur Einsicht in Grundbücher Gebrauch gemacht und die dadurch gewonnenen Erkenntnisse an einen Bauträger übermittelt. Dieser wiederum hat den Eigentümern Kaufangebote für ihre Grundstücke unterbreitet. Beide beteiligten Parteien mussten einen Teil des Bußgeldes bezahlen.

Ein Bußgeld von über 500 000 Euro hat der Berliner Datenschutzbeauftragte verhängt, weil er in der **Bestellung eines Datenschutzbeauftragten** in einem E-Commerce-Konzern einen Interessenkonflikt sieht. In dieser Unternehmensgruppe war eine Person zum Datenschutzbeauftragten ernannt worden, die gleichzeitig in zwei weiteren Unternehmen als Geschäftsführer tätig war. Diese Unternehmen waren noch dazu Auftragsdatenverarbeiter für das betroffene Unternehmen.

Das Bundesamt für Arzneimittel und Medizinprodukte hat seine Prüfkriterien für den **Datenschutz für digitale Gesundheitsanwendungen** überarbeitet. Sie sind Grundlage für die Zertifizierung der Datenschutzkonformität entsprechender Medizinprodukte. Konkret geht es dabei um Apps auf Rezept, die seit etwa zwei Jahren von Ärzten verschrieben werden können. Neben diesen digitalen Gesundheitsanwendungen hat das Amt als

erste EU-Behörde nun auch digitale Pflegeanwendungen in den Geltungsbereich aufgenommen. In die Überarbeitung waren der Bundesdatenschutzbeauftragte sowie das Bundesamt für Sicherheit in der Informationstechnik eingebunden.

Der bekannte IT-Rechtsprofessor Thomas Hoeren aus Münster hat gemeinsam mit Mitarbeitenden der Forschungsstelle des DFN-Vereins eine **überarbeitete Musterdatenschutzerklärung** veröffentlicht (siehe ix.de/zcph). Sie darf von allen Webseitenbetreibern als Mustertext herangezogen und verwendet werden. Allerdings weisen die Autoren darauf hin, dass sie keine Gewähr für Richtigkeit und Vollständigkeit übernehmen, und warnen vor einem unbedachten Übernehmen. *Tobias Haar* (ur@ix.de)