Die Tech-Ideen der EU: Gut gemeint, aber …

Europa will klarere Regeln im Internet, die Marktmacht der Tech-Unternehmen eindämmen, die Strafverfolgung stärken. Das sind hehre Absichten – die aber grossen Schaden anrichten könnten. Eine Einordnung der wichtigsten Vorstösse.

Von Adrienne Fichter und Patrick Seemann, 21.04.2022

Spätestens als Margrethe Vestager zur Wettbewerbskommissarin ernannt worden ist, hat es sich abgezeichnet: Die Europäische Union will Big Tech zähmen – und das Internet an sich stärker regulieren. Das globale Netz soll ein bisschen europäischer werden.

Darum tüfteln Brüssels Beamte an vielen verschiedenen Vorstössen in Sachen Datenschutz, Cybersecurity, Marktfreiheit und Tech-Industrie. Viele davon werden erst in einigen Monaten verabschiedet. Doch schon jetzt ist klar, dass die Bilanz durchzogen sein wird.

Die EU setzt einige Impulse, die tatsächlich mehr Rechtssicherheit oder auch Arbeitsplätze und Wertschöpfung schaffen könnten. Doch ausgerechnet dort, wo Europa in der Vergangenheit eine Pionierrolle einnahm, bei den digitalen Bürgerrechten, könnten sich gewisse neue Ideen verheerend auswirken.

Was bringt wirklich Mehrwert – und was vor allem Kollateralschäden? Wir machen einen Zwischenhalt und ordnen die wichtigsten Regulierungen ein, die im Moment verhandelt werden.

1. Digital Markets Act

Worum es geht: Am 24. März haben sich das Europäische Parlament und der EU-Rat nach langen Diskussionen auf einen gemeinsamen Entwurf für den Digital Markets Act (DMA) geeinigt. Der DMA ist Teil eines Bündels von Regulierungen, mit dem die EU die Dominanz der grossen Online-Plattformen und Tech-Unternehmen brechen will. Dies auch als politische Konsequenz zahlreicher kartellrechtlicher Verfahren der EU gegen Google, Apple und Amazon. Die Grundidee: Die Big-Tech-Unternehmen sollen gezwungen werden, ihre geschützten Gärten, also geschlossene Datenuniversen, aufzubrechen.

Die wichtigsten Punkte:

– Die Gesetzgeber störten sich insbesondere daran, dass neu gekaufte Smartphones oft vorinstallierte Apps der Hersteller favorisieren (und auch deren Datentracker, die alles mitverfolgen). Dies geht auf Deals zwischen Betriebssystem-Anbietern, Smartphone-Herstellerinnen, Werbeunternehmen und App-Entwicklern zurück. Nun soll es einfacher werden, die vorinstallierten Standard-Apps für E-Mail und Webbrowsing durch Angebote von Dritten zu ersetzen.

- Der DMA untersagt den Unternehmen, ihre Marktmacht und ihr Insiderwissen zu ihrem eigenen Vorteil auszunutzen. So wird es beispielsweise Google in Zukunft verboten, eigene Produkte oder Angebote bei den Suchresultaten zu bevorzugen. Ausserdem darf der E-Commerce-Riese Amazon die aus seinem Marktplatz gewonnenen Daten nicht zur Entwicklung eigener Produkte nutzen.
- Neu dürfen die grossen Internetplayer Daten aus verschiedenen Quellen nur mit ausdrücklicher Nutzereinwilligung zusammenführen. Dieses Verbot zielt auf das Unternehmen Meta und die Zusammenführung von Instagram, Facebook oder Whatsapp. Eine fehlende Zustimmung darf die User nicht von der Nutzung der Apps ausschliessen.
- Grosses Gewicht wird dabei auf die sogenannte Interoperabilität zwischen verschiedenen Messenger-Plattformen und -Diensten gelegt. Was bedeutet: Der Versand von Nachrichten soll analog zum technischen Standard der E-Mail möglich werden. Wer beispielsweise nur Facebook Messenger nutzt, soll trotzdem auch Nachrichten an Whatsapp- oder iMessage-Kontakte verschicken können, ohne dass dadurch die End-to-End-Verschlüsselung der Nachricht verloren geht. Diese Interoperabilität wird für die Grosskonzerne wie Meta und Apple verpflichtend. In einer zweiten Phase soll diese Regelung dann auch für Gruppenchats und für Sprach- und Videotelefonate gelten.

Betroffen von den neuen Regeln sollen grosse Anbieter sein. Als «gross» definiert die EU dabei Unternehmen mit einem Jahresumsatz von mindestens 7,5 Milliarden Euro im europäischen Wirtschaftsraum oder einer Marktkapitalisierung von mindestens 75 Milliarden Euro. Zusätzlich müssen sie monatlich mindestens 45 Millionen aktive Nutzer aus der EU aufweisen.

Bei Nichteinhaltung der neuen Regeln drohen drakonische Strafen, die Rede ist von bis zu 10 Prozent des weltweit erzielten Umsatzes bei einem ersten Regelbruch und einer Steigerung auf bis zu 20 Prozent im Fall von Wiederholungen.

Was wir davon halten: Der DMA ist ein Gesetz, das gegen die Gesetzmässigkeiten des Internets antritt. Wegen des sogenannten Netzwerkeffekts begünstigt die Digitalisierung die Bildung von Datenmonopolen: Je mehr meiner Freunde und Bekannten sich auf einem Netzwerk tummeln, desto (vermeintlich) besser wird der Dienst für mich. Bezahlt wird mit den persönlichen Daten, der Dienst wird personalisiert und verbessert. Dies erschwert natürlich den Markteintritt kleinerer Anbieter. Der DMA versucht also letztlich, marktwirtschaftliche Grundprinzipien und Wettbewerb zu verteidigen.

Regeln, die beispielsweise das privilegierte Hervorheben eigener Produkte in Suchergebnissen verbieten, nützen den Bürgerinnen. Ebenfalls weitgehend im Sinne der Nutzer sind Regeln, welche die Installation von alternativen Apps ermöglichen.

Spannend und gleichzeitig umstritten dürfte allerdings die Umsetzung der Interoperabilität werden. Noch ist unklar, ob und wie sich die Kommunikation zwischen Whatsapp und Signal datenschutzkonform realisieren lässt. Der DMA legt hierzu nur die rechtlichen Voraussetzungen fest. Schon rein die Tatsache, dass die von Mark Zuckerberg bereits 2019 angekündigte interne Zusammenführung der Messenger-Plattformen von Facebook, Whatsapp und Instagram noch immer nicht umgesetzt worden ist, zeigt, dass für so ein Unterfangen einige technische Stolpersteine zu überwinden sind (auch wenn der Hauptgrund für die Verzögerung politischer Natur ist). Denn die End-to-End-Verschlüsselung der Kommunikation, wie sie auf Whatsapp existiert (niemand ausser der Senderin und dem Empfänger kann die Nachricht mitlesen), ist aufgrund von unterschiedlichen tech-

nischen Protokollen nicht direkt kompatibel mit dem unverschlüsselten Facebook Messenger.

Falls es klappt, könnte der DMA im schlimmsten Fall unfreiwillig Marktmacht zementieren, weil die Interoperabilität nur für die Grossen vorgeschrieben ist und sie sich auf diese Weise gegenseitig stärken.

Ich will es genauer wissen: Was sind die konkreten Probleme bei der geplanten Interoperabilität?

Es gilt folgende Problematik zu lösen: Für den Transfer zwischen Messengern müssen die Daten zuerst einmal entschlüsselt und anschliessend im Zielmessenger neu verschlüsselt werden. Die End-to-End-Verschlüsselung wird damit gebrochen, die Nachrichten können auf dem Transportweg mitgelesen werden (technisch würde man von einem «Person in the middle»-Angriff sprechen). Um ein stark vereinfachtes Beispiel zu machen: Nehmen wir an, die französische und die schweizerische Post schreiben unterschiedliche Briefumschläge vor und weigern sich, Umschläge des anderen zu transportieren. Innerhalb der Schweiz ist das Briefgeheimnis gewährleistet, bei einem Briefversand nach Frankreich müsste der Schweizer Brief an der Grenze geöffnet und der Inhalt in ein französisches Couvert gelegt werden. Wer immer diese Aufgabe wahrnimmt, kann dabei problemlos sämtliche Briefe mitlesen.

Es gibt Ansätze, wie man diese Problematik entschärfen könnte: Am einfachsten liesse sich dies mittels einer spezifischen Messenger-App realisieren, die auf dem Smartphone des Benutzers läuft und sowohl mit Whatsapp wie auch mit iMessage kommuniziert.

Da aber nur die grossen Internetanbieter und damit de facto nur Apple und Meta gezwungen sind, unter dem DMA eine Schnittstelle nach aussen anzubieten, könnte das Gesetz ironischerweise deren Marktmacht eher verstärken. Messenger wie Signal und Threema fallen nicht unter den DMA. Ausserdem gibt es keinen zusätzlichen Anreiz, auf andere Anbieter umzusteigen, weil man mit der Nutzung der Whatsapp-App auf der «sicheren Seite» ist und alle Leute erreicht.

Ebenfalls noch völlig unklar ist die Thematik der Metadaten und der Nutzerverzeichnisse beziehungsweise -adressen. Denn die Interoperabilität nützt ja letztlich wenig, wenn ich keinen Weg habe, meinen Gesprächspartner im anderen Messenger-Universum überhaupt zu finden. Grundsätzlich liesse sich dies über allgemeine Verzeichnisdienste (quasi ein «Adressbuch für alle Messenger») lösen. Dadurch würde aber am Datenschutz der Teilnehmerinnen zumindest geritzt.

Wie es weitergeht: Der Gesetzesentwurf gelangt jetzt in die parlamentarische Beratung, es ist aber davon auszugehen, dass sich an den zentralen Punkten nicht mehr viel ändern wird. Schliesslich ist der Entwurf das Ergebnis langer Verhandlungen zwischen EU-Parlament und EU-Rat.

Unter Berücksichtigung aller Fristen kann der DMA Anfang 2023 in Kraft treten, eine Umsetzung der neuen Regeln ist etwa 2024 zu erwarten.

2. Gesetz zur Chat-Kontrolle

Worum es geht: Während die EU mit dem DMA-Paket bezüglich Wettbewerbsvielfalt und Datenschutz unter dem Strich eine progressive Reform einleitet, zeichnet sich beim geplanten Gesetzespaket gegen

Kindesmissbrauch eine Entwicklung in die Gegenrichtung ab. Der Gesetzestext selbst wird zwar noch hinter verschlossenen Türen verhandelt, bekannt geworden ist allerdings der Inhalt eines internen Prüfberichts der EU-Kommission. Er gibt Hinweise auf die geplanten Regeln.

Diesem Bericht zufolge sollen die Anbieter von Messenger-Diensten wie Whatsapp durch das Gesetzespaket gegen Kindesmissbrauch dazu verpflichtet werden, Chat-Inhalte auf entsprechendes Bild- und Textmaterial zu durchsuchen und bei Verdachtsfällen mit den Strafermittlungsbehörden zusammenzuarbeiten. Die Idee ist nicht neu: Schon vor zwei Jahren wollte die Kommission eine Chat-Kontrolle einführen – damals unter dem Vorwand der Terrorbekämpfung.

Was wir davon halten: Man kann es drehen oder wenden, wie man möchte: Ein wie auch immer ausgestaltetes Durchsuchen sämtlicher privater Chats (das heisst ohne konkreten Verdacht) stellt einen unverhältnismässigen und massiven Eingriff in die Privatsphäre dar und stellt alle Nutzerinnen unter Generalverdacht.

Die EU-Kommission stellt sich auf den Standpunkt, dass aufgrund der Datenmenge ein solches Durchsuchen zwingend automatisiert erfolgen muss und «nur» als problematisch erkannte Inhalte durch Ermittlungsbehörden eingesehen werden können. Doch das macht die Sache nicht besser: Aus einer guten Absicht folgt zwangsläufig eine Massenüberwachungsarchitektur.

Ich will es genauer wissen: Warum gefährdet das Chat-Kontrolle-Gesetz den Datenschutz?

Es gibt mehrere Gründe, weshalb das angedachte EU-Gesetz grosse Kollateralschäden anrichten wird:

Eine Überwachung der Nachricht «unterwegs» zwischen Senderin und Empfängern (also zum Beispiel auf den Servern von Whatsapp) wäre nur durch Aufbrechen der End-to-End-Verschlüsselung möglich, mit entsprechenden Nachteilen und Risiken für sämtliche Chat-Benutzer.

Das automatisierte Scannen von Inhalten direkt bei der Eingabe oder beim Empfang einer Nachricht (wenn sie also noch oder wieder unverschlüsselt auf dem Gerät der Benutzerin liegt) wurde letztes Jahr bereits einmal von Apple angekündigt und stiess umgehend auf massive Kritik bei Sicherheitsexpertinnen und Datenschutzspezialisten. Nachdem Apple zuerst versucht hatte, der Kritik mit einer nachgebesserten Version entgegenzuwirken, wurde das Vorhaben einige Monate später in der Schublade versorgt. Kernpunkte der Kritik waren, dass diese Art von Scanning zu fehleranfällig ist und zu vielen ungerechtfertigten Verdachtsfällen führen würde. Auch könnte das Scanning, unbemerkt von der Benutzerin, auf weitere Themen ausgedehnt werden und Ermittlungsbehörden Zugriff auf praktisch alle Nachrichten geben.

Hinzu kommt, dass die heute bekannten automatischen Inhalts-Scans insbesondere von Bildern und Videos stark fehleranfällig sind. Algorithmen müssen ständig «nachjustiert» werden, um möglichst genau zwischen akzeptablen und nicht akzeptablen Inhalten zu unterscheiden. Die dazu notwendigen Trainingsdaten sind aber schwierig zu bekommen (da es ja gerade darum geht, die Algorithmen mit illegalen Inhalten zu trainieren). Auch zeigt sich, dass sich solche Algorithmen oft mit einfachen Mitteln austricksen lassen (wie sich zum Beispiel auf Youtube zeigt, wo trotz urheberrechtlichem «Content Filtering» diverse im Kino aufgezeichnete Filme, die nachher auf dem Videoportal publiziert worden sind, nicht gefiltert werden).

Wie es weitergeht: Erwartet wurde die Veröffentlichung des Gesetzestexts am 30. März. Die Kommission verschob den Termin kurzfristig auf den 27. April 2022. Grund: eine vernichtende (und inzwischen geleakte) Stellungnahme eines Überprüfungsausschusses der Europäischen Kommission. Deren Verfasserinnen sagen, eine solche allgemeine Überwachung sei vermutlich rechtswidrig und in der Praxis sehr anfällig für Fehler. Es ist anzunehmen, dass diverse EU-Bürgerrechtsorganisationen versuchen werden, die relevanten Paragrafen vor der Verabschiedung wieder aus dem Gesetz zu kippen.

3. Verbindliche staatliche EU-Webzertifikate

Worum es geht: Wenn Sie sich auf der E-Banking-Webseite einer Bank einloggen, um eine Transaktion zu überweisen, vertrauen Sie darauf, dass die Domain «NameIhrerBank.com» auch tatsächlich Ihrer Bank gehört und dass Ihre Daten von dort transportverschlüsselt an die richtige Adresse gelangen. Niemand sollte diese mitlesen können. Denn nur so können Sie sicher sein, dass Sie Ihre Zugangsdaten und Kreditkartenangaben nicht direkt in die Hände von Cyberkriminellen legen.

Dieses Vertrauen wird durch ausgestellte Webzertifikate sichergestellt. Diese belegen, dass sich hinter dem Inhaber der Domain «NameIhrerBank.com» tatsächlich Ihre Bank verbirgt. Diese Zertifikate werden wiederum von Zertifizierungsstellen ausgehändigt (etwa «Let's Encrypt» von der Internet Security Research Group) und müssen zwingend von den Browsern anerkannt werden. Ist dies nicht der Fall, wird die Webseite beispielsweise im Firefox-Browser als unsicher markiert. Die Folge? Beim Aufruf der Webseiten wird ein Warnhinweis angezeigt.

Die bisherige Zertifizierungspraxis ist ein Zusammenspiel von mehreren Akteurinnen: Über die Regeln von Webseiten-Authentifizierung stimmen sich die Zertifizierungsstellen und Browser in spezifischen Foren immer ab, unlautere *trust service provider* werden von den Browseranbietern ausgeschlossen.

Nun möchte die EU im Rahmen der aktuellen eIDAS-Verordnung einen Standard für den Umgang mit Webzertifikaten schaffen. Die Browser würden verpflichtet, die von den europäischen Zertifizierungsstellen ausgestellten «Qualified Website Authentication Certificates QWAC» jederzeit anzuerkennen.

Was wir davon halten: Der Vorstoss birgt grosse Gefahren. Die EU zwingt damit allen ihre Deutungshoheit über die Webzertifikate auf. Und zwar unabhängig davon, ob diese Zertifikate den Qualitäts- und Sicherheitsrichtlinien der Internetbrowser entsprechen und wie gut die *trust service provider* dabei arbeiten. Damit wird ein bewährtes System aufs Spiel gesetzt: Denn Google, Apple, Mozilla und Microsoft prüfen heute im Rahmen von «Root-Programmen», ob die Zertifizierungsstellen die Vorgaben einhalten. Die IT-Zivilgesellschaft warnt daher vor diesem Vorstoss: Ein offener Brief von namhaften 38 Sicherheitsforscherinnen (darunter auch Vertreterinnen der Schweizer Hochschule ETH) kritisiert den betreffenden Artikel 45 Absatz 2 in der eIDAS-Reform.

Die von der EU vorgesehenen QWAC-Zertifikate hätten sich aufgrund technischer Schwächen im digitalen Zertifikate-Ökosystem nicht durchgesetzt, schreiben die Experten. Würde deren Einsatz vorgeschrieben, so würde dies «die Online-Sicherheit verschlechtern, ohne jeglichen Mehrwert für

Konsumenten und Unternehmen», schreibt die Mozilla-Stiftung. Die qualitativ ungenügenden Zertifikate würden Einfallstore für Hackerinnen schaffen. Ausserdem könnte dieser Eingriff Schule machen und autoritäre Staaten dazu animieren, lokalen Unternehmen unsichere Zertifikate aufzuzwingen. (In der Vergangenheit haben Kasachstan und Mauritius mit ähnlichen Zertifikateverordnungen versucht, ihre Bürgerinnen zu überwachen.)

Wie es weitergeht: Erstaunlich ist, dass das umstrittene Vorhaben erst jetzt die gebührende Aufmerksamkeit erhält, denn die EU-Kommission präsentierte die Zertifikatereform bereits im Juni 2021. Bis zum Juni 2022 können Änderungen im EU-Parlament zur gesamten eIDAS-Reform eingebracht werden. Die Netzgemeinschaft hofft nun darauf, dass die EU-Abgeordneten nochmals über die Bücher gehen und sich zumindest mit den Browser-Anbietern einig werden, wie Qualitätskriterien und Regeln der digitalen Identität miteinander in Einklang gebracht werden können. Das Parlament dürfte allenfalls noch einige Änderungen an der Reform vornehmen.

4. Regulierung von Root-Servern und DNS

Worum es geht: Das Internet – letztlich das globale Zirkulieren von Datenpaketen – funktioniert dank viel Goodwill, Freiwilligkeit und Selbstverpflichtungen. Das *Domain Name System,* also die Auflösung von URLs in IP-Adressen, ist dabei eine der grössten gemeinsamen internationalen Errungenschaften. Die insgesamt 13 weltweit verteilten Root-Server spielen dabei eine wichtige Rolle: Sie kontrollieren die sogenannten Top-Level-Domains (.com; .org; .ch; .de).

Die EU begann sich vor zwei Jahren für die Systemrelevanz von Root-Servern zu interessieren. In der neuen Netz- und IT-Sicherheitsrichtlinie NIS-2 wird verlangt, dass den Anbieterinnen dieser Dienste mehr Berichts- und Sicherungspflichten auferlegt werden. Hacks auf kritische Infrastrukturen sollen schnell gemeldet werden. Das Ziel: Informations- und Netzsicherheit.

Die ursprüngliche Idee der EU-Kommission war es, die 13 Root-Server einer Art Aufsichtsbehörde zu unterwerfen. Dies, obwohl nur 2 davon in Europa stehen, die Mehrheit wird in den USA betrieben. Ausserdem sollen DNS-Resolver ebenfalls unter die Richtlinie fallen. Damit sind Dienste gemeint, die eine aufgerufene Webadresse in eine IP-Adresse umwandeln und auflösen. Auch sie unterliegen Meldepflichten. Ebenso sollen alle Inhaberinnen von Webadressen registriert und deren Daten überprüft werden.

Was wir davon halten: Das Zusammenspiel der sehr autonomen Root-Server funktioniert seit den Achtzigerjahren reibungslos. Der globale Konsens: Kein Land soll mit seinen politischen Entscheidungen das einheitliche globale DNS-Root-System gefährden können. Das Begehren der Ukraine etwa, alle russischen .ru-Adressen zu sperren, wurde von den Root-Server-Betreibern wie auch von der offiziellen Netzverwaltung Icann abgelehnt. Es ist zwar löblich, dass die EU die kritische Bedeutung der Root-Server und DNS-Dienste anerkennt. Doch gleichzeitig ist es vollkommen absurd, autonome und unabhängige Root-Organisationen einem EU-Regelwerk unterwerfen zu wollen – schliesslich befinden sich darunter US-Einrichtungen wie etwa die University of Maryland oder die Nasa.

Auch eine Mehrheit des EU-Parlaments fand das Vorhaben gefährlich und entfernte den Begriff «Root-Server» aus dem Richtlinienentwurf. Ob die Regulierung kleiner und grosser DNS-Dienste mit umfangreichen

Berichtspflichten sinnvoll ist, ist fraglich. Sehr heikel ist vor allem, dass die Regulierung von DNS-Servern faktisch die Grundlage für ein EU-weites Blockieren von Webseiten schaffen würde (indem alle EU-Nutzer verpflichtet würden, EU-DNS-Server zu verwenden, und diese dann beispielsweise Domains mit angeblich terroristischen oder urheberrechtlich geschützten Inhalten nicht mehr auflösen dürften). Die EU würde damit den Runet-Plänen des autoritären Russland in nichts nachstehen. Ausserdem ist unklar, weshalb die Adressinhaberinnen von den Domaindienstleistern verifiziert werden müssen. Denn dies widerspricht auch einem anderen Grundsatz des Datenschutzregelwerks DSGVO: der Datensparsamkeit.

Wie es weitergeht: Die NIS-2-Richtlinie wird in den nächsten Monaten im Parlament, im Rat und in der Kommission beraten, im Juni 2022 soll sie dann durchs Parlament gebracht werden. Es ist gut möglich, dass die Debatte um die DNS-Dienste auch noch in der Öffentlichkeit ausgetragen wird.

5. Datenabkommen zwischen USA und EU

Worum es geht: US-Präsident Joe Biden und EU-Kommissionspräsidentin Ursula von der Leyen verkündeten Ende März, dass ein transatlantisches Datentransferabkommen in Griffweite liege. Zur Erinnerung: Im Juli 2020 wurde vom EU-Gerichtshof in Luxemburg – dank dem Aktivisten Max Schrems und seiner Organisation Noyb – das Privacy-Shield-Abkommen für ungültig erklärt. Anlass dafür war die seit Edward Snowdens Enthüllungen bekannte Massenüberwachung jeglicher unverschlüsselter digitaler Kommunikation, welche die Big-Tech-Unternehmen zur Weitergabe der Daten von europäischen Bürgerinnen an die USA zwingt.

Diese Weitergabe verstösst gegen die europäische Datenschutzverordnung und hatte die Aufkündigung des Abkommens zur Folge. Die Schweiz zog kurz darauf nach: Der eidgenössische Datenschutzbeauftragte erklärte das schweizerisch-amerikanische Pendant (US Swiss Privacy Shield) ebenfalls für nicht mehr gültig.

Seither sind in der Theorie alle täglichen Datenflüsse illegal: Jeder in der EU und in der Schweiz verfasste Tweet hatte seither streng genommen keine gültige rechtliche Grundlage mehr. Dieses Vakuum schaffte massive Rechtsunsicherheit für europäische Internetnutzerinnen – und auch für alle Unternehmen, die etwa Microsoft Cloud und andere amerikanische Produkte für ihre tägliche Datenverarbeitung nutzen.

Offenbar gibt es nun einen politischen Konsens: Die USA sichern zu, den Zugriff von US-Geheimdiensten wie der NSA auf persönliche Daten von EU-Bürgern «auf das zu beschränken, was zum Schutz der nationalen Sicherheit notwendig und verhältnismässig ist». Ausserdem dürfen EU-Bürgerinnen ihre Rechte dank eines neuen Beschwerdemechanismus gerichtlich einfordern. Wie, ist noch unklar.

Was wir davon halten: Das neue Datentransferabkommen ist dem Vernehmen nach bisher lediglich eine *executive order* des aktuellen Präsidenten. Es handelt sich also um eine politische Zusicherung, dass die Daten nicht massenhaft abgesaugt werden und an die Sicherheitsbehörden gelangen. Technische Schranken, die den Abfluss der Daten der EU-Bürgerinnen zuhanden der US-Sicherheitsbehörden verhindern sollen, sind nicht vorgesehen. Die weitreichenden Überwachungsbefugnisse der NSA mit dem FISA-Gesetz (Section 702) bleiben unangetastet. Auch scheint von der Leyens Verhandlungserfolg symbolischer Natur zu sein, denn der Konsens hat

offenbar nicht ausreichend Rückhalt in Brüssel. Die USA hätten sich zu wenig bewegt in den Verhandlungen, schreibt der österreichische «Standard». Kritiker wie Aktivist Schrems bleiben daher wohl zu Recht skeptisch und verlangen nicht weniger als ein «No Spy»-Abkommen.

Wie es weitergeht: Bisher existiert das Bekenntnis zu einem transatlantischen Datenabkommen: präsidiale Worte. Die Ausarbeitung des Wortlauts wird demnächst präsentiert. Aktivist Schrems hat bereits angekündigt, das neue Abkommen genau zu prüfen und gegebenenfalls ein drittes Mal vor Gericht zu ziehen.

6. European Chips Act

Worum es geht: Der European Chips Act ist eine Investitionsoffensive, um die technologische Souveränität Europas zu stärken: Die EU-Kommission will die eigene Halbleiterbranche fördern. Bis 2030 sollen 20 Prozent der weltweiten Halbleiterproduktion in Europa erfolgen. Das wird insgesamt rund 48 Milliarden Euro kosten. Die Idee ist die Ansiedlung von sogenannten Fabs von Herstellern wie TSMC (Taiwan) und Intel (USA): Fabriken mit fortschrittlichster Fertigungstechnik für Chips von 2 Nanometern, die Milliarden von Transistoren enthalten. Ein solcher Chip ist sehr leistungsfähig und kann besonders viele Operationen ausführen (er soll ausserdem die Akkuzeit von Handys verlängern).

Was wir davon halten: In Zeiten von US-chinesischen Handelskonflikten sowie internationalen Embargos und Sanktionen ist es grundsätzlich sicherlich eine kluge Idee, in technologische Unabhängigkeit zu investieren – und so die Abhängigkeit von ausländischen Zulieferern gerade für die kritische Infrastruktur zu verringern. Mit Regulatorien, Bussen und Datenschutzregeln allein baut man schliesslich noch keine eigene Tech-Industrie auf.

Doch es ist fraglich, ob die EU dabei auf das richtige Pferd setzt. Branchenverbände wie ZVEI oder der Thinktank Neue Verantwortung finden den Fokus auf Chips mit 2-Nanometer-Strukturen illusorisch und warnen vor einer Fehlinvestition. Den Rückstand gegenüber den viel billigeren Produzentinnen im Ausland erachten sie als unaufholbar.

Ein weiterer Risikofaktor: der aktuelle Krieg. Die Chipfabriken verbrauchen Strom, und die steigenden Gas- und Ölpreise könnten die Pläne der EU ebenfalls stark verteuern. Die europäischen Chiphersteller loben – vielleicht wenig überraschend – die Pläne und die vorgesehenen Fördermittel. Zugute kommt dem EU-Plan, dass viele Zulieferer wie der niederländische Hersteller von Lithografiesystemen ASML und deutsche Firmen wie Jenoptik bereits in Europa beheimatet sind.

Es gibt, mit anderen Worten, Argumente dafür und dagegen: Die industriepolitische Investition der EU zur Ankurbelung der Chipindustrie könnte sich auszahlen – oder auch nicht. Der Ausgang ist derzeit noch ungewiss.

Wie es weitergeht: Der European Chips Act liegt nun im Parlament und braucht noch grünes Licht von den Regierungen der EU-Länder (Ministerrat).

Und jetzt nochmal eine Runde

Im Bereich Internet und Politik galt die EU im weltweiten Vergleich vor allem auf einem Gebiet als Vorreiterin: bei der Privatsphäre ihrer Bürger und

dem Datenschutz. Das Datenschutzregelwerk DSGVO entwickelte sich zu einem Exportschlager und Trendsetter. Es wurde von anderen Ländern wie beispielsweise Japan kopiert und hat bei den Big-Tech-Unternehmen tatsächlich zu Neuerungen geführt.

Doch dieses Mal schneiden einige der Ideen aus Brüssel ausgerechnet in diesem historisch starken Bereich schlecht ab.

Wie so oft, wenn es um «mehr Sicherheit» geht, sind die neuen Vorschläge zwar gut gemeint. Sie wollen der Bekämpfung von Kinderpornografie dienen. Oder sicheren Internetverkehr garantieren. Doch wie ebenfalls oft bringen solche gut gemeinten Vorstösse letztlich nicht mehr, sondern weniger Sicherheit – und liefern Cyberkriminalität und eine potenzielle Massenüberwachungsinfrastruktur gleich mit.

Auch die bisherigen Vorschläge zur Interoperabilität könnten letztlich bei mangelhafter Umsetzung das Gegenteil von dem bewirken, was sie eigentlich wollen. Sie könnten den Kleinen schaden und den Grossen nützen – und das ebenfalls bei weniger Datenschutz als zuvor.

Es ist zu hoffen, dass man in Brüssel nochmals eine Runde dreht – und vielleicht etwas weniger macht. Das dafür auf kluge Art und Weise.