Kommunikation & Recht

K&R
1 | Januar 2024
27. Jahrgang
Seiten 1 - 84

dfv Mediengruppe
Frankfurt am Main

Prof. Dr. Tobias Eggendorfer und RA Dr. Florian Schmidt-Wudy, MBA LL.M. (London)*

eIDAS 2.0 – „Sicherheit trotz und wegen Verschlüsselung“?

Kurz und Knapp

Der eIDAS 2.0-Entwurf der EU erlaubt staatlichen Instanzen Authentifizierungszertifikate auszustellen, die Webbrowser anerkennen müssen. Dies könnte - zumindest technisch - staatlichen Akteuren den Raum bieten, mittels Man-in-the-Middle-Angriffen verschlüsselte Kommunikation zu überwachen. Der Beitrag analysiert diese potentielle Entwicklung und betrachtet dabei insbesondere die technischen Implikationen sowie die möglichen Kollisionen mit bestehenden rechtlichen Rahmenbedingungen.

I. Einleitung

Die Europäische Kommission präsentierte im Juni 2021 einen Reformvorschlag für die existierende eIDAS-Verordnung, der eine substantielle Novellierung darstellt.[1] Zentraler Aspekt ist einerseits in Art. 6a des Reformvorschlags die Implementierung einer europäischen digitalen Identitätswallet, von der Kommission als EUid-Brieftasche bezeichnet, die es den Nutzern ermöglichen soll, ihre Identität sowohl online als auch offline zu verifizieren.[2] Die im Verlauf des legislativen Prozesses geplanten Modifikationen erstrecken sich jedoch weit über den Nachweis der Identität mittels digitaler Wallet hinaus. Art. 45 und Art. 45a des Reformvorschlags (nachfolgend als „eIDAS 2.0“ bezeichnet) in der aktuellen, indes noch nicht öffentlich zugänglichen Version (https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf), gestatten es staatlichen Stellen, eigene Qualifizierte Zertifikate für Website-Authentifizierung (nachfolgend als „QWACs“ bezeichnet) zu emittieren, die von Browser- und Softwareherstellern obligatorisch anerkannt werden müssen.[3] Was zunächst harmlos und sinnvoll erscheint, ermöglicht jedoch der EU, Zertifikate auszutauschen. Da diese Zertifikate ebenso die Grundlage sicherer Verschlüsselung zwischen zwei Systemen bilden, könnten Behörden auf diese Weise die Kommunikation unterbrechen und mitlesen. In der Domäne der IT-Sicherheit ist dies als Man-in-the-Middle-Angriff bekannt.[4] Mit anderen Worten, die Art. 45 und 45a des Reformvorschlags ermöglichen einen verborgenen Zugriff auf sämtliche abgesicherte Online-Kommunikation – eine „Hintertür“ für Massenüberwachung. Hinzu kommt erschwerend, dass diese Änderungen des Gesetzestextes bislang nicht öffentlich einsehbar sind, was Zweifel an einem transparenten Normsetzungsprozess aufkommen lässt.[5]

Diese eIDAS-2.0-Pläne erinnern an die einstige Forderung des damaligen Bundesinnenministers Horst Seehofer nach „Sicherheit trotz und wegen Verschlüsselung“.[6] Sein Anliegen war es, eine Hintertür in Verschlüsselungsmechanismen zu integrieren, die das Mitlesen verschlüsselter Kommunikation ermöglichen würde. Allerdings sollten nach seinem Wunsch Übeltäter diese Lösung nicht missbrauchen können. Kryptologen assoziierten dies unmittelbar mit einer schwachen Verschlüsselung, ähnlich der seinerzeitigen Export-RSA in den USA, einer fatalen Konstruktion.[7] Auch in Seehofers Konzept war das Ziel, eine technische Möglichkeit zum Entschlüsseln abgehörter Kommunikation zu schaffen. Doch die eIDAS-2.0-Hintertür wäre noch perfider, da sie scheinbar rechtmäßig über EU-Zertifikate realisiert würde, statt über offensichtliche Verschlüsselungsschwächungen, wie sie von Seehofer vorgeschlagen wurden.

Aktuell regt sich breiter Protest aus Wissenschaft und Zivilgesellschaft aus folgenden Gründen: Während bei realen Personalausweisen die Anreize von Regierungen, doppelte Identitäten zu schaffen, eher gering sind,[8] ist das Potenzial hier enorm: Zugriff auf alles, was bisher allgemein behördlichem Zugriff entzogen war. Ermittlungen wie z. B. im sog. EncroChat-Verfahren[9] wären künftig trivial, der technische Aufwand nahezu null. Generell hätten Behörden umfassenden Zugriff auf sämtliche Online-Kommunikation. Genau dieses Risiko rief bereits massiven Protest hervor.[10] Dem gegenüber stehen Lobbyverbände der EU, wie z. B. der European Signature Dialogue,[11] die in der aktuellen Fassung kein Problem sehen, ebenso wenig der Branchenverband BITKOM.[12]

Dieser Beitrag objektiviert das Thema unabhängig von politischen Einflüssen und unterzieht es einer ganzheitlichen technischen sowie rechtlichen Analyse.

---

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle Links zuletzt abgerufen am 14. 11. 2023.

1 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der VO (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM/2021/281 final, Verfahrensablauf abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=COM:2021:281:FIN.

2 *Busch*, in: Steege/Chibanguza, Metaverse, 2023, § 16 Rn. 20 ff.; *Britz/Indenhuck*, RDi 2023, 289 ff.; *Klink-Straub/Straub*, ZD-Aktuell 2023, 01126.

3 *Leisegang*, https://netzpolitik.org/2023/eidas-trilog-hunderte-wissenschaftlerinnen-und-dutzende-ngos-warnen-vor-massenueberwachung/; *Klink-Straub/Straub*, ZD-Aktuell 2023, 01126.

4 European Academics, Offener Brief zu eIDAS 2.0, https://nce.mpi-sp.org/index.php/s/cG88cptFdaDNyRr.

5 So auch https://last-chance-for-eidas.org/: „The introduction of this text so late in the legislative process and behind closed doors is also deeply concerning for democratic norms in Europe.“

6 Cybersicherheitsstrategie für Deutschland 2021, BMI, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf (dort 8.3.9); https://t3n.de/news/verschluesselung-whatsapp-signal-julia-reda-podcast-1332505/; https://www.sueddeutsche.de/wirtschaft/cybersicherheitsstrategie-seehofer-1.5332538. In IT-Sicherheitskreisen hat er sich so den Spitznamen „Spähhofer“ verdient, vgl. etwa https://twitter.com/hashtag/Sp%C3%A4hhofer.

7 Siehe hierzu auch https://freakattack.com/.

8 Mit Ausnahme von wenigen Sonderfällen, wie z. B. gesonderte Identitäten für verdeckte Ermittler der Polizei, gibt es kaum sinnvolle Nutzungsszenarien.

9 Siehe dazu u. a. *Deusch/Eggendorfer*, K&R 2022, 404 ff. oder auch 6. Hamburger IT-Sicherheitsrechtstag 2023, Policing Crime Chat Networks, Lessons from the EncroChat Operation (Tagungsband voraussichtlich im Januar 2024).

10 European Academics, Offener Brief zu eIDAS 2.0, abrufbar unter https://nce.mpi-sp.org/index.php/s/cG88cptFdaDNyRr; https://www.heise.de/news/Hunderte-Wissenschaftler-warnen-vor-staatlichen-Root-Zertifikaten-9355165.html; https://netzpolitik.org/2023/eidas-trilog-hunderte-wissenschaftlerinnen-und-dutzende-ngos-warnen-vor-massenueberwachung/.

11 https://www.european-signature-dialog.eu/ESD_experts_support_trilogue_Art. 45_results-6nov2023.pdf.

12 https://www.bitkom.org/sites/main/files/2022-05/20220320_Bitkom_Position_QWACs.pdf.

II. Technische Grundlagen

1. Zertifikate

Zertifikate dienen primär der Identifikation des Kommunikationspartners im Internet, in aller Regel der des Servers. Damit verhindern sie Angriffsszenarien, in denen der Täter einen gefälschten Server betreibt. Solche Fälschungen sind relativ einfach zu realisieren.

2. Domain-Name-System – Angriffe auf das Adressbuch

Eine mögliche Angriffsstrategie wären modifizierte Einträge im Domain-Name-System (DNS), die Nutzer anstelle des Zielsystems auf das System des Angreifers umleiten. Das DNS fungiert quasi als Internet-Telefonbuch, indem es Rechnernamen wie www.example.org in IP-Adressen wie 192.0.2.15 übersetzt. Früher war das ähnlich wie heutzutage in Handys organisiert: Die Nutzer legten sich ein lokales Adressbuch an, das Name und Rufnummer bzw. hier Rechnername und IP-Adressen enthält. Dieses lokale Adressbuch existiert auch heute noch auf modernen Rechnern, beispielsweise in /etc/hosts bei Unix-artigen Systemen und in C:/Windows/System32/Drivers/etc/hosts auf Windows-Rechnern. Aus diversen Gründen lesen Betriebssysteme diese Datei zuerst, wenn sie einen Namen auflösen möchten – analog einem Handy-Nutzer, der auch aus dem Adressbuch wählt, bevor er jedes Mal die Auskunft anruft.[13]

Ein Angreifer könnte nun z. B. durch Schadsoftware einen Eintrag in der /etc/hosts anlegen, der anstelle der Original-IP z. B. von www.bank.de auf eine IP eines vom Angreifer betriebenen Servers verweist. Ruft der Nutzer die Seite auf, landet er auf der Seite des Angreifers.

Doch auch das Äquivalent der Telefonauskunft, das DNS, erlaubt eine Manipulation: Steht die Namensauflösung nicht im lokalen Adressbuch, erfolgt eine Abfrage beim DNS-Server des eigenen Internetproviders.[14] Hat dieser die Auflösung nicht zwischengespeichert, kann er sich durch ein hierarchisches System von DNS-Servern die zugehörige IP-Adresse erfragen. Da das Abfragen über die Hierarchie Zeit und Bandbreite kostet, speichern DNS-Server in einem Zwischenspeicher (Cache) die Ergebnisse von solchen Abfragen für eine bestimmte Zeit (TTL, Time-To-Live) zwischen. Hier lassen sich diverse Angriffe konstruieren, ein einfacher ist z. B. eine unsolicited DNS-Reply, bei der der Angreifer unaufgefordert Namensauflösungen scheinbar als Antworten auf DNS-Abfragen verschickt, natürlich mit modifizierten Daten. Mit etwas Glück landen diese Antworten trotzdem im Cache des DNS.

Doch gerade mit dem Instrumentarium eines Staats sind Modifikationen des DNS noch wesentlich einfacher, so könnte der Provider eines zu überwachenden Nutzers z. B. durch richterliche Anordnung gezwungen werden, eine falsche DNS-Antwort zurückzuliefern, die auf ein von der Regierung kontrolliertes System verweist, statt auf die Original-IP.[15]

3. Man-in-the-Middle

In der Praxis fälschen dabei Angreifer nicht die Original-Seite, sondern nehmen die Anfragen an ihrer statt entgegen, lesen sie aus, modifizieren sie soweit nötig und stellen dann ihrerseits diese Anfrage an den echten Server. Dessen Antwort wiederum werten sie aus, modifizieren sie wiederum soweit nötig, und schicken das an den Client. Da sich der Angreifer in die Mitte der Kommunikation einklinkt, spricht man von einem Man-in-the-Middle-Angriff.

4. Vertrauen in Zertifikate

Um derartige Angriffe zumindest zu erkennen und die Kommunikation abzubrechen, sieht beispielsweise HTTPS, das Protokoll für den sicheren Aufruf von Webseiten, vor, dass sich der Server mit einem Zertifikat „ausweist“. Dieses Zertifikat beinhaltet den oder die Namen des Servers, die der Client mit dem aufgerufenen Namen abgleicht. Stimmen sie nicht überein, warnt der Client und verhindert zunächst weitere Kommunikation.

Ähnlich wie bei einem Personalausweis basiert das Vertrauen in das Zertifikat sowohl auf dem Vertrauen in den Aussteller als auch auf dem Nachweis der Authentizität.

Während bei einem Personalausweis Merkmale wie Hologramme und spezielle Druckmuster Fälschungen erschweren, ist dies bei einem virtuellen Zertifikat nicht möglich. Daher wird hier zur Authentifizierung eine digitale Signatur verwendet.

a) Digitale Signatur

Die digitale Signatur nutzt dabei Verfahren aus der asymmetrischen Verschlüsselung. Die asymmetrische Verschlüsselung hat zwei Schlüssel, den private und den public key, die mathematisch miteinander zusammenhängen. Bei der Verschlüsselung verwendet der Absender zum Verschlüsseln den public key des Empfängers. Der Empfänger (und nur er) kann dann mit seinem private key entschlüsseln.

Den public key kann der Empfänger, wie der Name andeutet, veröffentlichen, z. B. auf seiner Homepage oder einem Key-Server. Den private key dagegen muss er geheim halten und so schützen, dass nur er darauf Zugriff hat.

Die digitale Signatur nutzt diese Schlüsseleigenschaften: Zum Signieren verschlüsselt der Unterzeichnende mit seinem private key. Jeder kann dann mittels seines public keys entschlüsseln. Würde das Entschlüsseln scheitern, würden private und public key nicht zusammenpassen – das wäre ein Hinweis darauf, dass die digitale Signatur nicht authentisch ist.

In dem Fall erzeugt also die Verschlüsselung keine Vertraulichkeit, sondern schafft das digitale Äquivalent einer händischen Unterschrift zusammen mit einer hinterlegten Unterschriftsprobe.

b) Kryptographische Hash-Verfahren

Um möglichst effizient signieren zu können und die Datenmenge überschaubar zu halten, verschlüsselt die digitale Signatur nicht die Daten selbst, sondern deren kryptographisch sicheren Hashwert.[16] Ein Hash ist dabei eine nicht umkehrbare Abbildung auf eine begrenzte Menge an Werten, eine Einwegfunktion. Beispiele von Hashwerten wären im Fall von Teilnehmern einer Konferenz etwa die Anfangsbuchstaben ihrer Vor- und Nachnamen. Dieses Beispiel zeigt, dass es hierbei zu Kollisionen kommen kann: Max Muster und Mara Muster wären beide MM.

Je nachdem, wie wahrscheinlich eine solche Kollision ist, ist das Hashverfahren kryptographisch sicher – nämlich dann, wenn

13 Siehe hierzu u. a. *Tannenbaum*, Computernetzwerke, 5. Aufl. 2012, Kapitel 7.1.

14 Die Darstellung ist etwas vereinfacht, es könnte auch ein DNS-Server eines DNS-Providers konfiguriert sein, bekannt und relativ verbreitet sind die von Google (IPs 8.8.8.8, 8.8.4.4), Cloudflare (IP 1.1.1.1) und Quad9 (IP 9.9.9.9). Doch für die folgende Betrachtung ist das nicht relevant.

15 Die Idee ist gar nicht so neu, *von der Leyen* hat sie seinerzeit 2009, als sie noch Familienministerin war, als Internet-Stopp-Schild vorgeschlagen, vgl. https://www.computerwoche.de/a/rotes-stopp-schild-statt-kinderpornos-im-internet,1884229.

16 Technischer dazu: https://www.linux-magazin.de/ausgaben/2015/10/hashfunktionen/.

die Wahrscheinlichkeit einer Kollision extrem unwahrscheinlich ist. Für einen Hashwert mit einer Länge von 256 Bit muss die Wahrscheinlichkeit einer Kollision kleiner als 2^{-128} sein.[17] Allgemein gilt: Für eine Hashlänge von n Bit muss die Wahrscheinlichkeit kleiner $2^{-n/2}$ sein.

Zudem sollten sich kryptographisch sichere Hashwerte stark unterscheiden, selbst wenn sich der Ursprungswert nur minimal ändert, und eine Umkehrung sollte möglichst aufwendig sein, um nicht aus dem Hashwert auf die Nachricht zu schließen.[18]

c) Prüfung der Signatur

Die digitale Signatur bestätigt also die Echtheit des Zertifikates. Es stellt sich jedoch die Frage, wie der Client die Echtheit der Signatur verifizieren kann und wo die Ursprungskette beginnt.

Zertifikate werden von sogenannten Zertifizierungsstellen (Certificate Authorities, CAs) signiert. Diese Zertifizierungsstellen verfügen ihrerseits wiederum über verifizierte Zertifikate. Am Ende dieser Kette aus Zertifikaten stehen Root-Certificate-Authorities (Root-CA), die Wurzelzertifikate.[19] Der Client vertraut diesen, da er sie kennt: Sie sind zum Beispiel im Betriebssystem oder Browser hinterlegt. Ist also ein Zertifikat letztendlich von einer Root-CA signiert, dann gilt es als authentisch.

d) Der Ansatz von eIDAS 2.0

eIDAS 2.0 baut auf der Prämisse auf, dass Root-Zertifikate der EU in jedem System implementiert werden. Dies ermöglicht es der EU oder ihren Mitgliedstaaten theoretisch, Man-in-the-Middle-Angriffe zu realisieren. Denn nun könnte eine Behörde für den „Man-in-the-Middle“ ein gültiges Zertifikat ausstellen, es würde sich also korrekt ausweisen können.

e) Technisches Zwischenfazit

Dass es staatliche Versuche gab, Zertifikate zu kompromittieren, listet u. a. eine Gegeninitiative[20] zu eIDAS 2.0 auf und benennt Fälle im EU-Mitgliedsland Frankreich, dem EU-Beitrittsinteressenten Türkei sowie China und Kasachstan.

Für die technische Bewertung ist es dabei unerheblich, ob eine Regierung sich aktuell verpflichtet, sich an selbst gesetzte Grenzen zu halten, oder ob sie bereits suspekt ist: Allein die technische Möglichkeit eines Missbrauchs ist das entscheidende Kriterium. Denn die Geschichte zeigt, dass auch auf vertrauenswürdige Regierungen weniger vertrauenswürdige folgen können, die dann sich ihnen bietende Möglichkeiten ausnutzen, notfalls unter Anpassung der sie beschränkenden Regularien. Aus technischer Sicht ist daher eine schon technologisch sichere Lösung, die auf einen regulatorischen Überbau verzichtet, noch dazu auf einen, den ein einziger Akteur verändern kann, zu bevorzugen.

5. Auswirkungen auf die Verschlüsselungen

Die Verschlüsselung der Kommunikation basiert auf der sicheren Authentifizierung des Servers: Beim hier vorliegenden Verfahren TLS[21] baut der Client die Verbindung zum Server auf, sendet sein ClientHello und eine Liste möglicher Verschlüsselungsverfahren, nach absteigender Präferenz sortiert.[22]

Der Server antwortet mit seinem Key, seinem Zertifikat und dem von ihm präferierten Verschlüsselungsverfahren – dabei sollte er das erste aus der Liste des Clients nehmen, das er auch beherrscht.[23]

Vertraut der Client nun dem Zertifikat des Servers, etabliert er die Verschlüsselung mit dem Server, mit den von ihm gesandten Parametern, wie Verfahren und zugehörigen Schlüssel. Damit kontrolliert der Server letztlich die Verschlüsselung. Und kann damit von Man-in-the-Middle bis zur Impersonisation eines Servers alle Angriffe durchführen.

III. Rechtliche Bewertung

Unabhängig von den andernorts bereits adressierten Bedenken[24] gegen eIDAS 2.0 wird nachfolgend eine rechtliche Prüfung durchgeführt.

1. eIDAS 2.0 im Rechtsrahmen von EU und Mitgliedstaaten

eIDAS 2.0 ist eine Verordnung gem. Art. 288 Abs. 2 AEUV, die in allen Teilen verbindlich ist und unmittelbar, d. h. ohne nationalen Umsetzungsakt, in jedem Mitgliedstaat gilt. Bei einer Verordnung und generell den in Art. 288 AEUV genannten Rechtsakten handelt es sich um Sekundärrecht, beim EUV, dem AEUV oder den anderen Gründungsverträgen sowie den – etwa in Art. 6 Abs. 3 EUV erwähnten – allgemeinen Rechtsgrundsätzen handelt es sich um Primärrecht.[25] Im Verhältnis von Primärrecht und Sekundärrecht gilt, wie bereits aus Art. 12 Abs. 2 EUV folgt, das Gebot der primärrechtskonformen Auslegung des Sekundärrechts.[26] Nach herrschender Auffassung stellt das EU-Recht, wie etwa die eIDAS 2.0, eine im Vergleich zu den Mitgliedstaaten autonome Rechtsordnung dar, weswegen zwischen EU-Recht und dem Recht der Mitgliedstaaten ein Normendualismus besteht.[27] EU-Recht stellt supranationales Recht dar, das sich vom Völkerrecht dadurch unterscheidet, dass es unmittelbar anwendbar und gegenüber dem mitgliedstaatlichen Recht vorrangig ist.[28] Diesen Normenvorrang hat auch das BVerfG anerkannt, obgleich sich das BVerfG vorbehält, Unionsrechtsakte im Hinblick auf das GG in bestimmten Fällen zu prüfen (vgl. dazu weiter unten bei Überprüfbarkeit der Verletzung des GG durch Unionsrecht).

Eine Verordnung, wie etwa eIDAS 2.0, kann im Wege der Nichtigkeitsklage angefochten werden mit der Folge, dass der EuGH dann diese Verordnung gem. Art. 264 AEUV ex tunc für nichtig erklärt.[29] Ebenso ist eine inzidente Normenkontrolle

17 Für einen negativen Exponent gilt: $2^{-n} = 1/2^n$. 2^{128} ist 3,4 * 10^{38}, also 340 Sextillionen. Die Wahrscheinlichkeit beträgt dann 1 zu 340 Sextillionen. Zum Vergleich: Die Chance für einen Lotto-Jackpot ist um Größenordnungen (etwa den Faktor 10^{30}) größer, sie liegt bei 1:140 Millionen.

18 Für die Umkehrung gibt es bei anderen, nicht kryptographisch sicheren Hash-Verfahren, in der Praxis tatsächlich Angriffe, ein Beispiel diskutieren die Autoren in *Eggendorfer/Schmidt-Wudy*, ZD 2021, 679.

19 Siehe u. a. *Stallings/Brown*, in: Computer Security: Principles and Practice, 2017, Kapitel 22.3, 22.4, 23.2.

20 https://last-chance-for-eidas.org/art45interception.html.

21 TLS (Transport Layer Security) und der Vorläufer SSL (Secure Socket Layer) sind die Verfahren, die zur Verschlüsselung von dem hier vorrangig betroffenen HTTPS, SMTP mit TLS, IMAPS etc. zum Einsatz kommen. Also Protokolle zum sicheren Aufruf von Webseiten, dem sicheren Versand von Mails und dem sicheren Empfang von Mails. Siehe auch Fn. 19.

22 Dazu wesentlich detaillierter, als für diesen Artikel nötig: https://tls13.xargs.org/.

23 Hier gab es in der Vergangenheit Fehler, so hat z. B. beim FREAK-Angriff (https://freakattack.com/) der Server ein vom Client zwar unterstütztes, aber nicht angebotenes Protokoll zurückgesandt, das eine schwache RSA-Verschlüsselung nutzte. Dies war ein auf eine lächerliche Schlüssellänge von 40-Bit (statt üblichen 1024 - 8192 Bit) reduziertes RSA und Resultat staatlicher Intervention in Verschlüsselung, um mitlesen zu können.

24 Siehe oben Fn. 10.

25 Dazu umfassend *Nettesheim*, in: Grabitz/Hilf/Nettesheim, 79. EL Mai 2023, AEUV Art. 288 Rn. 27 ff.

26 EuGH, 13. 12. 1983 – C-218/82, Rn. 15 – Kommission/Rat; *Ruffert*, in: Calliess/Ruffert, EUV AEUV, 6. Aufl. 2022, AEUV Art. 288 Rn. 10 m. w. N.

27 Zu den anderen Auffassungen, die EU-Recht etwa lediglich als durch den Anwendungsbefehl in den jeweiligen Mitgliedstaaten geschaffenes nationales Recht sehen, vgl. *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 35 ff.

28 *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 38.

29 *Dörr*, in: Grabitz/Hilf/Nettesheim (Fn. 25), AEUV, Art. 263 Rn. 197.

von Verordnungen gem. Art. 277 AEUV denkbar.[30] Dabei beschränkt sich der Prüfungsumfang des EuGH ausschließlich auf die Verletzung von Unionsrecht, nicht mitgliedstaatlichem Recht.[31] Eine Klagebefugnis haben gem. Art. 263 Abs. 2 AEUV stets das Europäische Parlament, der Rat, die Kommission und die Mitgliedstaaten. Der Rechnungshof, die Europäische Zentralbank sowie der Ausschuss der Regionen sind nach Art. 263 Abs. 3 AEUV teilprivilegiert und können eine Nichtigkeitsklage anstrengen, wenn der angegriffene Akt in die spezifischen Rechte und Befugnisse dieser Institutionen eingreift.

Natürlichen und juristischen Personen steht eine Klagebefugnis nur im Umfang des Art. 264 Abs. 4 AEUV zu: Hiernach können Verordnungen, wie die eIDAS 2.0, von Privaten angegriffen werden, sofern solche Kläger direkte Adressaten des angegriffenen Rechtsakts sind oder unmittelbar und individuell betroffen sind.[32] In Bezug auf eIDAS 2.0 und die in Art. 45 sowie 45a genannten Themen ist eine Klagebefugnis sowohl in Bezug auf die Browserhersteller als auch – nach hier vertretener Ansicht – in Bezug auf alle Privatpersonen, die QWACs nutzen oder zwangsweise nutzen müssen,[33] denkbar.

2. Mögliche Verletzung von Art. 7, 8 und 11 EU-Grundrechtecharta (GRCh) sowie Art. 16 AEUV

eIDAS 2.0 könnte gegen Art. 7, 8 und 11 GRCh sowie Art. 16 AEUV verstoßen. Art. 7 GRCh schützt das Grundrecht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, was gemäß der Rechtsprechung des EuGH auch das Recht auf vertrauliche Kommunikation umfasst.[34] Art. 8 GRCh schützt ebenso wie Art. 16 AEUV die auf eine Person bezogenen Daten. Art. 11 GRCh schützt ergänzend dazu die Meinungsäußerung und Informationsfreiheit, wozu die Beschaffung, der Empfang und der Zugang zu Informationen zählt.[35]

Die eIDAS-Verordnung, die die Möglichkeit von Man-in-the-Middle-Angriffen beinhaltet, könnte potenziell in die Schutzbereiche dieser Grundrechte eingreifen, indem sie die Vertraulichkeit elektronischer Kommunikation (Art. 7 GRCh) gefährdet, den Einzelnen von der Ausübung der ihm zustehenden Freiheit der Meinungsäußerung (Art. 11 GRCh) abhält und schließlich auch Zugriffe auf dessen personenbezogene Daten vermittelt.[36] Allerdings ist fraglich, ob in Bezug auf Art. 16 AEUV sowie Art. 8 GRCh ohne tatsächlich erfolgten Tausch von QWACs durch Behörden ein Eingriff in personenbezogene Daten erfolgt, was im Ergebnis eher zu verneinen ist. Demgegenüber bedarf es nach hier vertretener Auffassung keines tatsächlichen Tauschs eines QWACs durch Behörden für Eingriffe in Art. 7, 11 GRCh, da alleine eine Möglichkeit eines solchen Zertifikats-Tauschs mit der Folge von Man-in-the-Middle-Eingriffen für den Einzelnen sich faktisch so auswirken wird, dass er davon absehen wird, seine Meinungsfreiheit auszuüben, weil er um die Vertraulichkeit der elektronischen Kommunikation fürchten muss. So greifen die QWACs doch in die Grundrechte ein.[37]

Ein Eingriff in die Schutzbereiche dieser Grundrechte ist zwar, wie Art. 52 Abs. 1 GRCh (bezogen auf Art. 7, 8, 11 GRCh) sowie Art. 16 Abs. 2 AEUV i. V. m. DSGVO zeigen, nicht grundsätzlich unzulässig, er muss jedoch gesetzlich vorgesehen sein und den Wesensgehalt dieser Grundrechte wahren. Wie der EuGH in seinem Urteil zur Vorratsdatenspeicherung zuletzt klargestellt hat,[38] ist erforderlich, dass ein Eingriff in das Grundrecht – bezogen auf die durch die angegriffene Rechtsnorm verfolgten Ziele – geeignet, erforderlich und verhältnismäßig ist sowie wirksame Garantien gegen Missbrauch enthält.[39]

Bei eIDAS 2.0 sind jedoch erhebliche Zweifel angebracht, ob diese Voraussetzungen erfüllt sind.

a) Mangel an effektiven Kontroll- und Missbrauchsschutzmechanismen

eIDAS 2.0 verpflichtet Webbrowserherstellern zur Nutzung von QWACs. Effektive Missbrauchskontrollmöglichkeiten sind in eIDAS 2.0 weder für Webbrowserhersteller noch für betroffene Personen, die auf die Legitimität von QWACs vertrauen und ihre Daten übertragen, vorgesehen. Betroffene Personen, die gem. Art. 13, 14 DSGVO bei der Verarbeitung von personenbezogenen Daten von der verantwortlichen Stelle proaktiv zu informieren sind, erfahren bei derartiger Manipulation von QWACs durch staatliche Stellen nichts hiervon und können demzufolge auch keine Rechtsschutzmöglichkeiten initiieren. Bereits deswegen ist eIDAS 2.0 rechtlich höchst bedenklich, da diese Verordnung die vom EuGH[40] verlangten klaren und präzisen Regelungen für die Tragweite von Maßnahmen, um Betroffenen für einen wirksamen Schutz vor Missbrauch zu vermitteln, nicht enthält.

Erschwerend kommt hinzu, dass die aktuellen eIDAS-2.0-Regelungen es erlauben würden, dass einzelne Mitgliedstaaten nicht nur ihre eigenen Bürger, sondern auch diejenigen der anderen Mitgliedstaaten bewusst ausspähen.[41] Gerade dieser Aspekt der gegenseitigen Ausspähung dürfte auch dem EuGH missfallen, da er jüngst[42] entschieden hat, dass abstrakt generelle Maßnahmen, die ein Mitgliedstaat gegen andere Mitgliedstaaten erlassen dürfte, das gegenseitige Vertrauen der Mitgliedstaaten untereinander untergraben könnte und daher Regelungen so auszulegen sind, dass sie derartige abstrakt generelle Maßnahmen nicht ermöglichen.

Zertifikatsmanipulationen wirken dabei auch technisch nicht gegen nur einen Tatverdächtigen, sondern gegen alle Nutzer, die auf durch QWAC „geschützte“ Seiten zugreifen wollen. Damit entsteht ein erheblicher Streuverlust und Kollateralschaden, anders als bei gezielteren Operationen wie im Fall EncroChat.

b) Geeignetheit, erforderlich, verhältnismäßig?

Des Weiteren ist fraglich, ob Art. 45, 45a eIDAS 2.0 geeignet sind, um die angestrebten Ziele zu erreichen. Ausweislich des Erwägungsgrunds 4 des ursprünglichen Entwurfs sind Ziele eine Binnenmarktstärkung durch ein harmonisiertes Herangehen an eine digitale Identifizierung sowie eine sichere Art und Weise eines Zugangs zu Dokumenten. Diese Ziele können zweifelsohne durch Teile von eIDAS 2.0 erreicht werden. Für diese Ziele sind aber die Missbrauchsmöglichkeiten in Art. 45,

30 EuGH, 14. 12. 1962 – C-31/62 – Wöhrmann und Lütticke/Kommission; allg. auch *Stoll/Rigod*, in: Grabitz/Hilf/Nettesheim (Fn. 25), AEUV, Art. 277 Rn. 1 - 3.
31 *Dörr*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 160.
32 *Dörr*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 57 ff.
33 Da Browser- und andere Softwareanbieter gem. Art. 45 Abs. 2 eIDAS 2.0 verpflichtet werden, die Zertifikate anzuerkennen, kann ein Nutzer, der sie nicht nutzen möchte, sich nicht entziehen. Die Nutzung erfolgt damit zwangsweise.
34 EuGH, 20. 9. 2022 – C-793/19, C-794/19, K&R 2022, 832 ff.; weiterführend *Jarass*, EU-Grundrechte-Charta, 4. Aufl. 2021, Art. 7 Rn. 25 f.; *Kingreen*, in: Calliess/Ruffert, EU-Grundrechte-Charta, 6. Aufl. 2022, Art. 7 Rn. 10.
35 *Jarass*, EU-Grundrechte-Charta (Fn. 34), Art. 11 Rn. 15.
36 So EuGH, 20. 9. 2022 – C-793/19, C-794/19, K&R 2022, 832 ff.
37 Ähnlich *Jarass*, EU-Grundrechte-Charta (Fn. 34), Art. 11 Rn. 20, Art. 7 Rn. 31; In diese Richtung auch EuGH, 20. 9. 2022 – C-793/19, C-794/19, K&R 2022, 832 ff., der annimmt, dass eine Vorratsdatenspeicherung in die Rechte gem. Art. 7 und 11 GRCh eingreift, da sie Nutzer von der Meinungsäußerung abhalten kann und dies unabhängig davon gilt, ob die gespeicherten Daten in der Folge verwendet werden.
38 EuGH, 20. 9. 2022 – C-793/19, C-794/19, K&R 2022, 832 ff.
39 EuGH, 20. 9. 2022 – C-793/19, C-794/19, K&R 2022, 832 ff.
40 EuGH, 8. 4. 2014 – C-293/12, C-594/12.
41 Vgl. https://nce.mpi-sp.org/index.php/s/cG88cptFdaDNyRr.
42 EuGH, 9. 11. 2023 – C-376/22, K&R 2023, 788 ff., Rn. 53. Dort ging es um die RL 2000/31.

45a der aktuellen Fassung gänzlich ungeeignet. Bereits deswegen erscheint eiDAS 2.0 ungeeignet.

Hilfsweise ist zu prüfen, ob die von Art. 45, 45a vermittelten Eingriffsmöglichkeiten erforderlich sind, d. h. ob es ein milderes Mittel zur Erreichung der angestrebten Ziele gibt. Nach hier vertretener Auffassung gibt es offensichtlich mildere Mittel als Art. 45, 45a, um die vorstehend genannten Ziele einer Binnenmarktstärkung durch ein gemeinsames Ökosystem der Identifikation zu erfüllen.[43]

Schließlich sind die von eIDAS 2.0 in Art. 45, 45a vorgesehenen Missbrauchsmöglichkeiten auch unverhältnismäßig, da sie – schrankenlos – eine Totalüberwachung mittels einer der am effektivsten Methoden eines Man-in-the-Middle-Angriffs erlauben und damit die abschreckende Dystopie des Big Brother aus George Orwells Roman 1984 wahr werden lassen könnten. Dabei sind sie auch noch unspezifisch in ihrer Wirkung, da sie nicht nur den Tatverdächtigen, sondern auch Dritte umfassend überwachen.

c) Zwischenergebnis

Nach hier vertretener Auffassung verstoßen die Regelungen in Art. 45, 45a eIDAS 2.0 jedenfalls gegen Art. 7, 11 GRCh und bei tatsächlichem Man-in-the-Middle-Angriff ebenso gegen Art. 8 GRCh sowie Art. 16 AEUV. Die hiermit verbundenen unionsrechtlichen Bedenken erfordern eine eingehende Prüfung durch den EuGH.

3. Möglicher Verstoß gegen Art. 2, 10, 23 GG

Wie bereits weiter oben aufgezeigt, ist es nicht ausgeschlossen, dass das BVerfG die Verletzung des GG durch Unionsrecht rügt. Daher sollen im Folgenden mögliche einschlägige Rechtsverletzungen untersucht werden.

a) Möglicher Verstoß gegen Art. 2 GG

Fraglich ist, ob Art. 45, 45a eIDAS 2.0 einen unverhältnismäßigen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darstellen, ein Recht, das in der richtungsweisenden Entscheidung des BVerfG zu Online-Durchsuchungen von diesem entwickelt wurde.[44]

Die juristische Fachliteratur interpretiert dieses Grundrecht unterschiedlich. Einige Autoren sehen es als ein neues, eigenständiges IT-Grundrecht,[45] während andere es als eine Fortentwicklung des Rechts auf informationelle Selbstbestimmung sehen.[46] Unabhängig von der dogmatischen Einordnung umfasst der Schutzbereich dieses Grundrechts das Interesse des Nutzers an der Vertraulichkeit von Daten, die von informationstechnischen Systemen erzeugt, verarbeitet und gespeichert werden.[47]

eIDAS 2.0 greift in diesen Schutzbereich ein, indem anlasslos und ohne Kontrollmöglichkeit Man-in-the-Middle-Angriffe durch Zertifikatstausch ermöglicht werden. Fraglich ist, ob dieser Eingriff verfassungsrechtlich gerechtfertigt sein könnte. Hierzu müsste er zur Erreichung eines legitimen Gemeinwohlziels geeignet, erforderlich und verhältnismäßig sein.[48] Bereits die Geeignetheit ist zweifelhaft, denn die von Art. 45, 45a eIDAS 2.0 vermittelten Überwachungsmöglichkeiten sind unbegrenzt und daher zur Erreichung des von eIDAS 2.0 grundsätzlich verfolgten Ziels der Binnenmarktstärkung ungeeignet. Selbst wenn man dies anders sehen würde, wäre die Erforderlichkeit zweifelhaft, da mildere Mittel als eine Totalüberwachung existieren, z. B. spezifisch definierte, eng begrenzte und richterlich überprüfbare Kontrollmaßnahmen. Hieraus folgt, dass auch die Verhältnismäßigkeit im engeren Sinn durch eIDAS 2.0 nicht gewahrt wird.

Im Ergebnis verstoßen Art. 45, 45a eIDAS 2.0 nach hier vertretener Auffassung gegen Art. 2 GG.

b) Möglicher Verstoß gegen Art. 10 GG

Der Schutzbereich von Art. 10 GG umfasst u. a. die Vertraulichkeit nicht-öffentlicher Kommunikation.[49] Bereits deswegen wird offensichtlich, dass die von Art. 45, 45a eIDAS 2.0 ausgehenden Möglichkeit von Behörden oder Mitgliedstaaten, die Kommunikation zu überwachen, einen Eingriff in Art. 10 GG darstellt.[50] Zur verfassungsrechtlichen Rechtfertigung kann auf Art. 2 GG verwiesen werden mit dem Ergebnis, dass auch dieser Eingriff weder geeignet, noch erforderlich und schon gar nicht verhältnismäßig im Sinne von angemessen ist.

c) Möglicher Verstoß gegen Art. 23 GG durch einen Ultra-vires-Akt

Denkbar ist des Weiteren, dass die von Art. 45, 45a eIDAS 2.0 vermittelte anlasslose Überwachung ohne Kontrollmöglichkeiten einen offensichtlich „ausbrechenden Rechtsakt“ darstellt, der gemäß der Ultra-vires-Doktrin des BVerfG zu einem Verstoß gegen Art. 23 GG führt.[51] Zwar beschränkt das BVerfG die Ultra-vires-Doktrin auf Extremfälle, die so offensichtlich sind, dass sich die Verstöße geradezu aufdrängen.[52] Nach hier vertretener Auffassung ist dies – gerade angesichts der erheblichen Bedenken aus Wissenschaft und Praxis[53] – aber durchaus vertretbar.

d) Zwischenergebnis

Nach hier vertretener Auffassung lässt es sich vertreten, zu argumentieren, dass die Regelungen in Art. 45, 45a eIDAS 2.0 jedenfalls auch gegen Art. 2, 10, 23 GG verstoßen.

e) Überprüfbarkeit der Verletzung des GG durch Unionsrecht

Fraglich ist jedoch, ob und wie das BVerfG eine Verletzung des GG rügen würde. Grundsätzlich überprüft das BVerfG in bestimmten Fällen EU-Sekundärrecht, wie eIDAS 2.0, im Hinblick auf ihre Vereinbarkeit mit dem deutschen Grundgesetz. Allerdings ist diese Möglichkeit begrenzt und unterliegt spezifischen Bedingungen: Bezüglich einer Überprüfung von EU-Recht im Hinblick auf das GG hat das BVerfG in der Vergangenheit im „Solange II-Beschluss“[54] festgestellt, dass es auf die Überprüfung der Anwendbarkeit von abgeleitetem Unionsrecht, wie EU-Verordnungen, verzichtet, solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des EuGH, einen wirksamen Schutz der Grundrechte gewährleisten, der dem vom Grundgesetz geforderten Grundrechtsschutz im Wesentlichen

43 Aus technischer Sicht sind die Art. 45, 45a eIDAS 2.0 gar nicht erforderlich, um ein sicheres Identifikations-Ökosystem zu schaffen. Vielmehr würde es ausreichen, würde die EU für Identifikationszwecke mit der Idee eines ID-Wallets zusätzliche Zertifikate herausgeben, die ausschließlich zur Identifikation von natürlichen und juristischen Personen dienen, aber eben gerade nicht zur Identifikation von Systemen. Dann wäre ein Äquivalent eines digitalen Ausweises ohne die Überwachungsoption gegeben.

44 BVerfG, 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07 – Online-Durchsuchung.

45 Vgl. *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, Werkstand: 37. EL Mai 2022, 50.1 Rn. 368 ff.

46 *Barcak*, in: Dreier, GG, 4. Aufl. 2023, Art. 2 Abs. 1 Rn. 97.

47 BVerfG, 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07 – Online-Durchsuchung, Rn. 204.

48 *Rixen*, in: Sachs, GG, 9. Aufl. 2021, Art. 2 Rn. 21.

49 Vgl. *Pagenkopf*, in: Sachs (Fn. 48), Art. 10 Rn. 14 ff.; *Martini*, in: v. Münch/Kunig, 7. Aufl. 2021, Art. 10 Rn. 69.

50 So auch *Martini*, in: v. Münch/Kunig (Fn. 49), Rn. 105 für das „Anzapfen“ von Kommunikationsvorgänge durch den Staat.

51 Zum Ganzen: *Scholz*, in: Dürig/Herzog/Scholz, 101. EL Mai 2023, Art. 23 Rn. 40a.

52 BVerfG, 6. 7. 2010 – 2 BvR 2661/06 – Honeywell.

53 Fn. 10 und 43.

54 BVerfG, 22. 10. 1986 – 2 BvR 197/83 – Solange II.

gleichzusetzen ist. Später hat das BVerfG im sog. „Bananenmarkt-Beschluss“[55] entschieden, dass ein deckungsgleicher Schutz zwischen dem GG und dem Unionsrecht nicht gefordert sei, da der gegenwärtig auf Unionsebene bestehende Schutz im Wesentlichen mit dem GG vergleichbar sei. Wenn es um die Überprüfung sekundären EU-Rechts auf mögliche Grundrechtsverstöße laut dem deutschen Grundgesetz geht, hat das BVerfG festgelegt, dass Klagen oder Anträge von Gerichten als unzulässig betrachtet werden, es sei denn, es wird in der Beschwerde oder im Antrag konkret und fundiert dargelegt, dass der allgemein erforderliche und unerlässliche Schutz der Grundrechte grundsätzlich nicht sichergestellt wird.[56] Hierdurch wird zu Recht gefolgert, dass das BVerfG die Messlatte für eine Überprüfung von Unionsrecht im Hinblick auf die Einhaltung der Grundrechte des GG extrem hoch legt.[57] Angewendet auf den vorliegenden Fall dürfte es daher praktisch ausgeschlossen sein, das BVerfG zu einer Überprüfung von eIDAS 2.0 anhand der Grundrechte des GG zu bewegen.

Eine weitere Möglichkeit, um Unionsrecht zu überprüfen, behält sich das BVerfG allerdings im „Honeywell-Beschluss“ vor, basierend auf Art. 23 GG im Hinblick auf die Frage, ob ein Unionrechtsakt das im unionsrechtlichen Primärrecht vorgesehene Prinzip der begrenzten Einzelermächtigung[58] überschreitet und somit einen „Ultra-vires“-Akt darstellt.[59] Nach Ansicht des BVerfG erfordert ein derartiger Ultra-vires-Akt jedoch einen Kompetenzverstoß, der offensichtlich ist und erheblich ins Gewicht fällt.[60] Und selbst dann verlangt das BVerfG, dass zunächst dem EuGH über eine Vorlage Gelegenheit gegeben wird, den ausbrechenden Rechtsakt zu korrigieren. Inhaltlich werden diese Voraussetzungen nur dann erfüllt, wenn nachgewiesen werden kann, dass der betreffende Rechtsakt, selbst unter Berücksichtigung der Argumente, die sich aus der spezifischen Auslegung des primären EU-Verfassungsrechts ergeben, die ihm zugewiesenen Kompetenzen übersteigt.[61] Kommt man nach hier vertretener Auffassung zum Ergebnis, dass eine Verletzung des Art. 23 GG durch Art. 45, 45a eIDAS 2.0 vorliegt, dann wird man konsequenterweise auch zum Ergebnis kommen, dass das BVerfG – nach erfolgloser Vorlage an den EuGH – entsprechend die Verfassungswidrigkeit von Art. 45, 45a eIDAS 2.0 feststellen muss.

IV. Fazit

Die Regelungen Art. 45, 45a eIDAS 2.0 greifen durch die Ermöglichung von Man-in-the-Middle-Angriffen, welche zahlreiche Internetnutzer und nicht ausschließlich gezielt Tatverdächtige betreffen können, unverhältnismäßig in Rechtspositionen ein, die sowohl nach Unionsrecht als auch nach dem deutschen GG geschützt sind. Zudem sind die Art. 45, 45a auch für eine technische Umsetzung einer Identifikation von natürlichen und juristischen Personen nicht erforderlich. Insgesamt wirft die eIDAS 2.0-Novelle gewichtige rechtliche Bedenken auf, die eine Prüfung durch den EuGH unumgänglich machen.

Tobias Eggendorfer

Professor für IT-Sicherheit an der TH Ingolstadt. Davor an der Cyberagentur zuständig für anwendungsbezogene Forschung & Innovation im Bereich „Sichere Systeme“, davor Professor für IT-Sicherheit in Ravensburg und IT-Forensik in Hamburg. Zusätzlich freiberuflich IT-Berater mit Schwerpunkten IT-Sicherheit, IT-Forensik und Datenschutz.

Florian Schmidt-Wudy

Rechtsanwalt, Syndikusrechtsanwalt und kaufmännische Geschäftsleitung eines Softwareunternehmens, Gründer von Start-Ups. Davor langjährig Geschäftsleitung eines führenden Medienunternehmens im Gesundheitsbereich. Publiziert im Beck’schen Onlinekommentar zum Datenschutz- und Datenrecht (Wolff/Brink). IAPP-zertifiziert als CIPP/E/US.

55 BVerfG, 7. 6. 2000 – 2 BvL 1/97 – Bananenmarktordnung.
56 *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 61.
57 Laut *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 61 ist eine solche Überprüfung „nahezu ausgeschlossen“.
58 Art. 4 EUV, Art. 5 Abs. 1 EUV, vgl. *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 62.
59 BVerfG, 6. 7. 2010 – 2 BvR 2661/06 – Honeywell; dazu auch *Ludwigs*, NVwZ 2015, 537 ff.
60 BVerfG, 6. 7. 2010 – 2 BvR 2661/06 – Honeywell.
61 *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Fn. 25), Rn. 63.

RA Alexander Devlin und wiss. Mitarbeiter Jan-Henning Steeneck*

Keine generell-abstrakten Ausnahmen vom Herkunftslandprinzip

Zugleich Kommentar zu EuGH, Urteil vom 9. 11. 2023 – C-376/22, K&R 2023, 788 ff. (Heft 12/2023)

Kurz und Knapp

Dieser Beitrag befasst sich mit dem bereits in Heft 12/2023 abgedruckten Urteil des EuGH vom 9. 11. 2023 – C-376/22 (Google Ireland Limited, Meta Platforms Ireland Limited, Tik Tok Technology Limited gegen Kommunikationsbehörde Austria (KommAustria))[1] und stellt die voraussichtlichen Auswirkungen auf die nationale Gesetzeslage und Praxis dar. Der Schwerpunkt liegt auf dem in der E-Commerce-Richtlinie (RL 2000/31/EG, nachfolgend „ECRL“) statuierten Herkunftslandprinzip und darauf, inwiefern der Regelungsspielraum deutscher Gesetzgeber dadurch eingeschränkt wird.

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 12. 12. 2023.
1 EuGH, 9. 11. 2023 – C-376/22, K&R 2023, 788 – KommAustria.