

# Datenschutz Nachrichten

48. Jahrgang  
ISSN 0137-7767  
16,00 Euro

Deutsche Vereinigung für Datenschutz e.V.  
[www.datenschutzverein.de](http://www.datenschutzverein.de)



## Digitalzwang

■ Digitalzwang und unsere Grundrechte ■ Digitalzwang – ein Bericht aus dem Maschinenraum ■ BigBrotherAward 2023 – Deutsche Post DHL Group ■ BigBrotherAward 2024 in der Kategorie „Mobilität“: Der Preis geht an die Deutsche Bahn AG ■ Die E-Rechnung – eine aufgedrängte Bereicherung oder Zwang? ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

# Inhalt

Thilo Weichert <b>Digitalzwang und unsere Grundrechte</b>	4	DVD-Presseerklärung vom 11.12.2024 <b>Offener Brief mit der Forderung, dass die EU-Agenda für digitale Sicherheit die Grundrechte fördert und ein sicheres digitales Ökosystem unterstützt</b>	28
Nils Büschke <b>Digitalzwang – ein Bericht aus dem Maschinenraum</b>	14	<b>Offener Brief an die polnische Ratspräsidentschaft in der EU: Übernehmen Sie eine Vorreiterrolle bei der Bekämpfung von Spyware-Missbrauch in der EU</b>	29
Rena Tangens <b>BigBrotherAward 2023 – Deutsche Post DHL Group</b>	16	<b>Aktuelles aus der DVD</b>	30
padeluum <b>BigBrotherAward 2024 in der Kategorie „Mobilität“: Der Preis geht an die Deutsche Bahn AG</b>	19	<b>Datenschutznachrichten</b>	
Hans-Hermann Schild <b>Die E-Rechnung – eine aufgedrängte Bereicherung oder Zwang?</b>	21	Deutschland	31
<b>Nachrichten zum Digitalzwang</b>	24	Ausland	39
DVD-Presseerklärung vom 06.12.2024 <b>Aufruf der Zivilgesellschaft an die neue europäische Führung</b>	26	<b>Technik-Nachrichten</b>	47
		<b>Rechtsprechung</b>	47
		<b>Buchbesprechungen</b>	52

# Termine

Donnerstag, 01.05.2025

**Redaktionsschluss DANA 2/2025**  
„Social Media“

Dienstag-Donnerstag, 06.-08.05.2025  
**LEARNTEC – Fachmesse für digitale Bildung**  
Karlsruhe

Dienstag-Donnerstag, 20.-22.05.2025  
**Datenschutztag**  
FFD, Frankfurt/M. oder virtuell

Montag-Mittwoch, 26.-28.05.2025  
**re:publica 25**  
STATION Berlin

Dienstag/Mittwoch, 27./28.05.2025  
**BvD-Verbandstage**  
Berlin

Montag/Dienstag, 02./03.06.2025  
**DuD 2025 – Datenschutzkongress**  
Computas, Potsdam

Mittwoch, 02.07.2025  
**4. Datenschutztag Hessen & Rheinland-Pfalz**  
BvD, Frankfurt/M.

Weitere Veranstaltungshinweise finden Sie regelmäßig im jeweils aktuellen Blog-Beitrag unter  
<https://www.datenschutzverein.de/kategorie/blog/>

Foto: Pixabay.com

## DANA

### Datenschutz Nachrichten

ISSN 0137-7767

48. Jahrgang, Heft 1

#### Herausgeber

Deutsche Vereinigung für  
Datenschutz e.V. (DVD)

DVD-Geschäftsstelle:

Reuterstraße 157, 53113 Bonn

Tel. 0228-222498

IBAN: DE94 3705 0198 0019 0021 87

Sparkasse KölnBonn

E-Mail: [dvd@datenschutzverein.de](mailto:dvd@datenschutzverein.de)

[www.datenschutzverein.de](http://www.datenschutzverein.de)

#### Redaktion (ViSDP)

Thilo Weichert

c/o Deutsche Vereinigung für  
Datenschutz e.V. (DVD)

Reuterstraße 157, 53113 Bonn

[dvd@datenschutzverein.de](mailto:dvd@datenschutzverein.de)

Den Inhalt namentlich gekennzeichnete Artikel verantworten die jeweiligen Autorinnen und Autoren.

#### Layout und Satz

Frans Jozef Valenta, 53119 Bonn

[valenta@datenschutzverein.de](mailto:valenta@datenschutzverein.de)

#### Druck

Onlineprinters GmbH

Dr.-Mack-Straße 83

90762 Fürth

[www.onlineprinters.de](http://www.onlineprinters.de)

Tel. +49 (0) 9161 6209800

Fax +49 (0) 9161 8989 2000

#### Bezugspreis

Einzelheft 16 Euro (zzgl. Porto). Jahresabonnement 54 Euro (inkl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

#### Copyright

Die Urheber- und Vervielfältigungsrechte liegen bei den Autorinnen und Autoren.

Der Nachdruck ist nach Genehmigung durch die Redaktion bei Zusendung von zwei Belegexemplaren nicht nur gestattet, sondern durchaus erwünscht, wenn auf die DANA als Quelle hingewiesen wird. Die DANA wird indiziert bei EBSCO.

#### Leserbriefe

Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

#### Abbildungen, Fotos

Pixabay, iStock,

Frans Jozef Valenta

Titel: iStock – Tijana87

## Editorial

### Digitalisierung um jeden Preis?

Unter dieser Frage fand am 25.01.2025 die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder – kurz Datenschutzkonferenz – organisierte Tagung zum Europäischen Datenschutztag statt. Es referierten Heribert Prantl (Süddeutsche Zeitung), Jutta Gurkmann (Verbraucherzentrale Bundesverband), Alexander Roßnagel (Hessischer Beauftragter für Datenschutz und Informationsfreiheit), Rena Tangens (Digitalcourage e. V.), Steffen Augsburg (Universität Gießen) und Nico Lüdemann (Bundesverband der mittelständischen Wirtschaft). Damit gelangte das Thema „Digitalzwang“ erstmals in den offiziellen öffentlichen Diskurs und wurde aus ökonomischer, sozialer, technisch-praktischer und rechtlicher Sicht beleuchtet. Das Thema steht in der Zivilgesellschaft schon lange auf der Agenda, wird aber von einer digitalisierungsbetrunkenen Politik bisher ignoriert.

Seitdem Trump und Digitalkonzerne in den USA die Macht übernommen haben, sind digitalpolitische Bedenken nicht nur dort, sondern auch in Europa nochmals weniger hoffähig und nochmals wichtiger, da es um Grundrechte und unsere soziale Demokratie geht. Tatsächlich sind die Segnungen der Digitalisierung unserer Gesellschaft allgegenwärtig. Doch mindestens ebenso gegenwärtig ist die hässliche Seite der Medaille, zu der auch der Digitalzwang gehört. Gibt es für bestimmte Angebote keine analoge Alternativen, so diskriminiert dies möglicherweise nicht nur alte, arme oder behinderte Menschen, sondern zwingt uns alle zur Datenpreisgabe, die wir nicht wollen und oft nicht mehr kontrollieren können.

Digitalzwang ist also auch ein Datenschutzthema. Dass es das ist, verdanken wir insbesondere dem Verein Digitalcourage, der hierzu im Jahr 2021 eine Kampagne gestartet hat. In diesem Rahmen wurde ein Digitalzwangsmelder eingerichtet, erfolgten zwei prominente Auszeichnungen mit dem BigBrotherAward (BBA) und läuft eine Petition mit dem Ziel unsere Grundrechte zu ergänzen. Unterstützend hierzu erstellte das Netzwerk Datenschutzexpertise ein Gutachten. Die Deutsche Vereinigung für Datenschutz beschloss sich dieser Kampagne anzuschließen. Ein Ergebnis dieser Unterstützung ist das vorliegende Heft, in dem Nils Büschke die Erkenntnisse von Digitalcourage präsentiert, die beiden BBA-Laudationen zur Deutschen Post und zur Deutschen Bahn von Rena Tangens und padeluun abgedruckt werden, eine verfassungsrechtliche Verortung von Thilo Weichert erfolgt und von Hans-Hermann Schild die Pflicht zur eRechnung vorgestellt wird.

Da Datenschutz derzeit zwar nicht „en vogue“ ist und stark unter Beschuss, gibt es hierzu wieder viele Meldungen und Stellungnahmen, aus denen klar hervorgeht, dass Datenschutz angesichts politischer und ökonomischer Bestrebungen keinesfalls an Bedeutung einbüßt und wir diesen brauchen wie die Luft zum Atmen.

Die Redaktion

### Autorinnen und Autoren dieser Ausgabe:

#### Nils Büschke

Mitarbeiter bei Digitalcourage e. V., Bielefeld, [nils.bueschke@digitalcourage.de](mailto:nils.bueschke@digitalcourage.de)

#### padeluun

Künstlerischer Leiter von Digitalcourage e. V., Bielefeld, [padeluun@digitalcourage.de](mailto:padeluun@digitalcourage.de)

#### Hans-Hermann Schild

Vorstandsmitglied der DVD, Kassel, [schild@datenschutzverein.de](mailto:schild@datenschutzverein.de)

#### Rena Tangens

Geschäftsführerin von Digitalcourage e. V., Bielefeld, [rena.tangens@digitalcourage.de](mailto:rena.tangens@digitalcourage.de)

#### Dr. Thilo Weichert

Vorstandsmitglied der DVD, Netzwerk Datenschutzexpertise, Kiel, [weichert@datenschutzverein.de](mailto:weichert@datenschutzverein.de)

Thilo Weichert

## Digitalzwang und unsere Grundrechte

*Immer mehr Lebensbereiche werden digitalisiert. Dies führt dazu, dass Menschen, die sich hieran nicht beteiligen können oder wollen, ausgeschlossen sind. Im Folgenden wird – insbesondere aus verfassungsrechtlicher Sicht – untersucht, ob und unter welchen Voraussetzungen „Digitalzwang“ gerechtfertigt ist, wann nicht und wann analoge Alternativen bereitzustellen sind.*

### 1. Einleitung

„Digital first – Bedenken second“ – das war der Werbeslogan der FDP bei der Bundestagswahl 2017. Die Klagen über rückständige Digitalisierung in vielen Lebensbereichen sind leider immer noch oft berechtigt. Dies führt zu unnötigen Kosten und Aufwand, ineffizientem Handeln, unzureichender Kommunikation und Bürger- bzw. Kundenunfreundlichkeit. Mit Hilfe digitaler Prozesse lassen sich staatliche wie unternehmerische Leistungen oft kostengünstiger, wirksamer und schneller erbringen. Sie erleichtern die Inanspruchnahme durch die Menschen unaufwändig von zu Hause.<sup>1</sup>

Digitalisierung kann aber auch Probleme hervorbringen. Machtkonzentration, Intransparenz, Datenmissbrauch, Cyberkriminalität, soziale Vereinsamung durch Konsum digitaler Medien, Hate-speech und Fakenews im Internet sind im öffentlichen Bewusstsein angekommen und werden politisch adressiert.

Bisher wenig adressiert wird, dass die Digitalisierung von Lebensbereichen zu einer Freiheitseinschränkung für viele Menschen führen kann, wenn sie die digitalen Dienste und Angebote nicht nutzen können oder wollen. Wird aus „digital first“ „digital only“, so kann dies Menschen ausschließen. Ob es sich dabei um eine Diskriminierung im rechtlichen Sinn handelt, hängt von vielen Umständen ab. Digitalzwang finden wir zunehmend im Alltag der Menschen. Digitalzwang bedeutet, dass es keine analoge oder datenschutzfreundliche

Alternative zu einem Produkt oder Service gibt, obwohl sie realisierbar wäre.<sup>2</sup>

Diskriminierungen wegen Digitalzwang sind heute oft anerkannt rechtswidrig; in vielen Fällen aber ist die Rechtslage unklar oder streitig. Einfachgesetzliche Regulierungen enthalten teilweise klare Regeln. Angesichts der zunehmenden Verbreitung des unregulierten Digitalzwangs muss aber zunehmend auf Verfassungsrecht zurückgegriffen werden bei der Prüfung, ob ausschließliche digitale Angebote gerechtfertigt sind und ob sich hieraus Diskriminierungswirkungen ergeben.

Im Raum steht letztlich die Frage, ob ein Grundrecht auf eine analoge Alternative ausdrücklich verfassungsrechtlich verankert werden sollte. Die Forderung nach einem solchen Grundrecht wird immer wieder erhoben.<sup>3</sup> Es gibt Widerstand dagegen, dass Menschen gezwungen sind sich digitaler Mittel im Alltag zu bedienen. Ziel ist dabei oft die Normierung eines entsprechenden Grundrechts, zumindest aber ein einfachgesetzlicher Schutz vor Digitalzwang.

Ein solches Grundrecht auf eine analoge Alternative kann nicht voraussetzungslos und unbeschränkt gelten und muss sich in die gesamte Verfassungsordnung einfügen. Digitalisierung dient in vielen Bereichen der Grundrechtsverwirklichung und ist aus Betroffenen-sicht oft unproblematisch. Letztlich stellt sich die Frage, ob ein explizit eingeräumtes Grundrecht dazu beiträgt eine sinnvolle menschenorientierte Digitalisierung unserer Gesellschaft zu fördern.

### 2. Praktische Fälle und Rahmenbedingungen des Digitalzwangs

Rund 6% der 16- bis 74-Jährigen waren 2022 nach Angaben des Statistischen Bundesamts „Offliner“. Über 3 Millionen Menschen in Deutschland waren noch nie im Internet. Am größten war der Anteil in der Altersgruppe von 65 bis 74 Jahren. Immer noch nutzen mehr als die

Hälfte der über 65-Jährigen kein Smartphone. Bei den über 80-Jährigen haben zwei Drittel keinen Zugang zum Netz. Manche Senioren hatten trotz bestehenden Interesses keine Gelegenheit die digitale Welt zu erlernen und fühlen sich dadurch „analphabetisiert“. Gemäß dem E-Government-Monitor sprachen sich 44% der Befragten für analoge Alternativen neben digitalen Angeboten aus; 20% monierten, es werde zu viel digitalisiert. Viele entscheiden sich bewusst für die Nutzung analoger Wege, obwohl ihnen die Online-Alternativen bekannt sind und deren Nutzung möglich wäre.<sup>5</sup>

Das Statistikamt destatis teilte 2023 mit: „Ob digitales Deutschlandticket, Terminbuchungen oder Überweisungen – viele Dienstleistungen werden (fast) nur noch online angeboten. Für Menschen ohne Internet ist der Alltag zunehmend schwerer zu bewältigen.“<sup>6</sup>

Es gibt Gründe, weshalb Menschen digitale Dienste nicht nutzen können. Es gibt aber auch legitime Gründe, aus denen selbst Menschen mit der theoretischen und praktischen Möglichkeit zur Nutzung digitaler Dienste diese bewusst meiden bzw. verweigern.

#### 2.1 Unmöglichkeit der Inanspruchnahme digitaler Dienste

Insbesondere ältere Menschen haben es in ihrem Leben nicht gelernt mit digitalen Medien umzugehen. Sie fühlen sich von der digitalen Welt überfordert.<sup>7</sup> Anderen ist die Finanzierung eines Internetanschlusses und die Anschaffung eines technischen Endgeräts, etwa eines Smartphones, Tablets oder Laptops nicht möglich. Menschen mit verringerter Sehkraft, mit Schwerhörigkeit oder mit anderen Einschränkungen fällt es oft schwer oder ihnen ist es gar unmöglich digitale Endgeräte zu nutzen. Alter, Armut und persönliche Beeinträchtigungen können so zum Ausschluss vom gesellschaftlichen Leben und von der Befriedigung wesentlicher Bedürfnisse führen.<sup>8</sup>

Die Nutzung eines digitalen Dienstes ist oft trotz Vorliegen der technischen und finanziellen Voraussetzungen aus zeitlichen, instrumentellen und kognitiven Gründen nicht möglich oder zumutbar wegen der konkreten Gestaltung des Dienstes. So müssen u. U. mehrere nicht verfügbare Endgeräte gemeinsam genutzt werden, die Nutzerführung leitet fehl oder die zugelassene Eingabezeit ist zu kurz bemessen.

Die digitale Einbindung der Nutzer entlastet die Diensteanbieter. Entstehen Probleme, so wird Nutzenden oft nicht der nötige Service angeboten, mit dem in zumutbarer Zeit eine angemessene Hilfe zur Problemlösung geliefert wird. Derzeit gibt es keine rechtlichen oder organisatorischen Instrumente, mit denen die notwendige Anwendungsfreundlichkeit und der nötige Service für Digitalnutzungen gewährleistet werden.

Werden bestimmte Menschen bei der Nutzung digitaler Medien ausgeschlossen, so ist eine mögliche Folge, dass sie sich von der Gesellschaft abgehängt und ausgegrenzt fühlen. Diese „psychologische Obsoleszenz“ trägt zu Einsamkeit und Technikskepsis bei.<sup>9</sup>

Im Laufe der Zeit mögen die Probleme unzureichender Medienkompetenz, mangelnder Medienverfügbarkeit und schlechten Services und Anwendungsfreundlichkeit abnehmen. Die Zahl derjenigen, die sich erst im Alter digitale Fähigkeiten mühsam aneignen konnten, wird geringer. Auch mögen Digitalgeräte preisgünstiger werden. Es werden digitale Geräte entwickelt, mit denen zunächst ausgeschlossene Menschen in die Lage gesetzt werden am digitalen Leben teilzuhaben. Auch bei Veränderungen der äußeren Rahmenbedingungen wird sich grundsätzlich nichts daran ändern, dass ein Teil der Menschen in unserer Gesellschaft durch ausschließliche Digitalangebote ausgegrenzt ist. Die weit verbreitete Ansicht, durch Zeitablauf und technische Entwicklung werde sich das Problem des Digitalzwangs von alleine erledigen<sup>10</sup>, ist irrig.

## 2.2 Gründe für eine Verweigerung digitaler Dienste

Das Verweigern der Nutzung des Internets kann gute Gründe haben. Viele potenzielle Nutzer befürchten die Ab-

hängigkeit von einem unkontrollierbaren Medium, den Missbrauch ihrer Daten und Verstöße gegen ihr Grundrecht auf Datenschutz. Derartige Verstöße sind an der Tagesordnung.

Digitale Dienste unterscheiden sich von analogen dadurch, dass regelmäßig mehr Daten erhoben werden als für die vergleichbare analoge Dienstleistung erforderlich sind und dass mehr Stellen hierbei beteiligt sind. Dies ergibt sich schon allein durch Anforderungen an die Sicherheit digitaler Dienste. Es besteht eine Tendenz zur Vorratsdatenspeicherung („wenn man schon mal dabei ist“). Mit vermeintlichem Komfortgewinn wird häufig die Erhebung offensichtlich nicht erforderlicher Daten gerechtfertigt. Die anfallenden Informationen werden für andere Zwecke weitergenutzt. Spätestens seit 2013 und den Enthüllungen von Edward Snowden ist zudem bekannt, dass selbst westliche Geheimdienste in großem Umfang auch private Internetnutzungsdaten missbräuchlich erheben, auswerten und nutzen. Dienstleister haben ihren (Haupt-)Sitz oft außerhalb des Europäischen Wirtschaftsraums und versuchen so sich der Anwendung des europäischen Datenschutzrechts zu entziehen. Unternehmen verfolgen Geschäftsmodelle, die strukturell gegen geltende Datenschutznormen verstoßen. Dies trifft insbesondere auf große Unternehmen mit Monopolcharakter zu, die sich dabei durch gezielte Vorkehrungen von ihren Kunden und deren Wünschen und Beschwerden abschotten.

Die Nutzung vieler Dienstleistungen setzt eine bestimmte Art, Leistungsfähigkeit oder Aktualität des Endgeräts, etwa des Smartphones, voraus. Der Markt internetfähiger moderner Mobilgeräte beschränkt sich hinsichtlich der eingesetzten Betriebssysteme, mit Ausnahme zahlenmäßig kaum relevanter alternativer Vorkommen, auf Android von Google und iOS von Apple. Die für eine Dienstleistung nötigen Apps sind oft nur in den App-Stores dieser beiden Unternehmen verfügbar. Diese beschränkte Wahlmöglichkeit führt zu einer Abhängigkeit von einem dieser beiden Unternehmen.

Digitale Dienste sind von der Verfügbarkeit von Elektrizität, Software und Netzabdeckung abhängig. Ein leerer

Akku eines Smartphones oder fehlende Verfügbarkeit des Kommunikationsnetzes machen die Nutzung unmöglich. Im Mai 2022 konnte wegen massiver technischer Probleme bei Kartenzahlungen wochenlang in einer Reihe von Geschäften nicht mit EC-Karten bezahlt werden.<sup>11</sup>

In vielen Staaten nimmt die Nutzung von anonymem Bargeld beim Konsum und der Nutzung von Dienstleistungen ab. In Deutschland besteht weiterhin – mit abnehmender Tendenz – ein starkes Bedürfnis nach Nutzung von (analogem) Bargeld. Gemäß einer Umfrage des Verbraucherzentrale Bundesverbands gaben 75% der Befragten an, dass sie wählen möchten, ob sie bargeldlos oder mit Bargeld zahlen wollen.<sup>12</sup> Die Bargeldnutzung ermöglicht den Betroffenen eine bessere Kontrolle über ihre Finanzen und gewährleistet, dass sie gegenüber ihren Vertragspartnern bzw. Dienstleistern sowie Dritten unerkannt bleiben können.<sup>13</sup>

## 3. Einfachgesetzliche Vorgaben

Einfachgesetzliche Regeln sehen obligatorische digitale Nutzungen vor, erlauben aber zugleich Ausnahmen hiervon. Gemäß § 23 Abs. 1 S. 2 ZensusG 2022 muss die Auskunftserteilung bei der Volkszählung grds. elektronisch erfolgen. Zur Vermeidung unbilliger Härten kann die zuständige Stelle eine Ausnahme von der elektronischen Nutzung zulassen, so dass ein Papierformular ausgefüllt werden kann (§ 23 Abs. 1 S. 3 ZensusG i. V. m. § 11a Abs. 2 S. 2 BStatG).

Gemäß § 25 Abs. 4 S. 1 EStG (i. V. m. §§ 2 Abs. 1 S. 1 Nr. 1-3, 46 Abs. 2 Nr. 1-8 EStG) sind Einkommenssteuererklärungen elektronisch zu übermitteln, wenn Gewinneinkünfte aus Land- und Forstwirtschaft, aus Gewerbebetrieb oder aus selbstständiger Arbeit in Höhe von über 410 Euro vorliegen. Die Regelung gilt für Gewerbetreibende, nicht für Rentner, Arbeitnehmer, Auszubildende oder Studierende. § 25 Abs. 4 S. 2 EStG regelt, dass das Finanzamt zur Vermeidung unbilliger Härten auf eine elektronische Übermittlung verzichten kann. § 228 Abs. 6 BewG verpflichtet zur elektronischen Erklärung bei der Feststellung des Grundsteuerwerts an das Finanzamt.

Das Finanzamt kann zur Vermeidung unbilliger Härten eine analoge Datenübermittlung ermöglichen.

Ist eine elektronische Abgabe der Steuererklärung für einen Steuerpflichtigen wirtschaftlich oder persönlich unzumutbar, so hat dieser eine Freistellungsmöglichkeit (§ 150 Abs. 8 AO). Dies ist anzunehmen, wenn die Schaffung der technischen Möglichkeiten für eine elektronische Datenübermittlung nur mit einem nicht unerheblichen finanziellen Aufwand verbunden wäre oder wenn der Steuerpflichtige nach seinen individuellen Kenntnissen und Fähigkeiten nicht oder nur eingeschränkt in der Lage ist diese zu nutzen. Es besteht bzgl. der Befreiung von der elektronischen Übermittlungspflicht kein Ermessensspielraum. Bei Bestehen der Voraussetzungen muss ausnahmsweise eine Befreiung erfolgen.<sup>14</sup>

Allgemeine Sicherheitsbedenken Steuerpflichtiger gegen die Abgabe der Steuererklärung über das Internet sollen nicht für die Annahme einer unbilligen Härte genügen.<sup>15</sup> Ein Urteil des Finanzgerichts Berlin-Brandenburg bejahte eine persönliche Unzumutbarkeit bezüglich der elektronischen Übermittlung eines Steuerpflichtigen, wenn diesem die Medienkompetenz hierfür fehlt. Er sei nicht verpflichtet auf medienkompetente Familienangehörige zurückzugreifen.<sup>16</sup>

§ 4 Abs. 1 S. 1 Onlinezugangsgesetz (OZG) erlaubt der Bundesregierung für die elektronische Abwicklung von Verwaltungsverfahren, die der Durchführung unmittelbar geltender Rechtsakte der Europäischen Union oder der Ausführung von Bundesgesetzen dienen, im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung ohne Zustimmung des Bundesrates die Verwendung bestimmter IT-Komponenten nach § 2 Abs. 6 OZG verbindlich vorzugeben. Das OZG zielt auf „digital only“ ab, also darauf Digitalpflichten einzuführen. Am 24.02.2024 beschloss der Bundestag eine Novellierung des OZG.<sup>17</sup> Im Interesse der Verhältnismäßigkeit wird in § 1a OZG-E eine Ausnahme von der Digitalpflicht geregelt: „Davon kann bei berechtigtem Interesse des Nutzers abgewichen werden.“

Bestimmte Absendergruppen, z. B. Rechtsanwälte, sind verpflichtet ihre Schriftsätze an Gerichte grundsätzlich

elektronisch zu übermitteln (z. B. § 55d VwGO). Diese Pflicht gilt nicht für Menschen generell.

Gemäß § 6 Schuldnerverzeichnisführungsverordnung erfolgt die Einsicht in das Schuldnerverzeichnis über „ein zentrales und länderübergreifendes elektronisches Informations- und Kommunikationssystem der Länder im Internet.“ Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, „dass registrierte Nutzer in jedem Amtsgericht Einsicht in das elektronische Schuldnerverzeichnis nehmen können (§ 11 Abs. 1 SchFV). Die Einsichtsberechtigten können verlangen, dass ihnen ein Ausdruck ihrer Datenabfrage überlassen wird.“<sup>18</sup>

Auch landesrechtlich gibt es entsprechende Vorgaben. So besteht in Bayern ein Recht auf digitale Kommunikation mit der Verwaltung, das aber nicht exklusiv ist: „Die Möglichkeit, Verwaltungsverfahren auch nichtdigital zu erledigen, bleibt unberührt“ (Art. 12 Abs. 1 S. 1 BayDiG). Art. 14 Abs. 2 der Landesverfassung Schleswig-Holstein besagt: „Das Land sichert im Rahmen seiner Kompetenzen einen persönlichen, schriftlichen und elektronischen Zugang zu seinen Behörden und Gerichten. Niemand darf wegen der Art des Zugangs benachteiligt werden.“<sup>19</sup>

Während die Kommunikation des Staates mit seinen Bürgern einfachgesetzlich konkretisiert wird, fehlt es an entsprechenden Regelungen im Verhältnis zwischen Verbrauchern und privaten Unternehmen. § 307 Abs. 1 BGB verbietet aber in Allgemeinen Geschäftsbedingungen (AGB) unangemessene Benachteiligungen von Verbrauchern, die gegen Treu und Glauben verstoßen. Eine AGB-Regelung, wonach Kundenkontakte ausschließlich elektronisch zu erfolgen haben und Kosten für die Kommunikation mit Briefpost „verursachungsgerecht in Rechnung gestellt“ werden, können gegen Treu und Glauben verstoßen.<sup>20</sup>

#### 4. Verfassungs- und Europarecht

Grundrechte haben zumeist eine doppelte Ausrichtung. Sie enthalten Eingriffsverbote und können Leistungsansprüche sowie ein Recht auf Teilhabe begründen. Die Grundrechte gewähr-

leisten, dass die Rechtsordnung Bedingungen schafft und bewahrt, unter denen der Einzelne am gesellschaftlichen Leben teilhaben, sich in seiner Persönlichkeit entfalten und seine Grundrechte in Anspruch nehmen kann. Dem Staat kommt insofern eine Schutzpflicht zu.<sup>21</sup> Der Anspruch auf Teilhabe erstreckt sich auf alle grundrechtlich geschützten Handlungsweisen, auf die Pflege zwischenmenschlicher Beziehungen, auf Teilhabe am gesellschaftlichen und kulturellen Leben generell wie am politischen Leben speziell.<sup>22</sup>

##### 4.1 Adressaten

Grundrechte begründen in erster Linie Rechte gegenüber dem Staat. Öffentlichen Stellen kommt i. d. R. keine Grundrechtsträgerschaft zu. Die meisten öffentlichen Einrichtungen erfüllen aber eine gesetzlich begründete, verfassungsrechtlich legitimierte Funktion für das Gemeinwesen.

Grundrechte können auch private Unternehmen binden, die selbst ein Recht auf Wahrung ihrer Grundrechte haben. Die Grundrechte entfalten im Privatrechtsverkehr Wirkkraft als verfassungsrechtliche Wertentscheidungen, die durch Gesetze konkretisiert werden. Hierbei ist es regelmäßig notwendig Grundrechtspositionen zueinander in ein Verhältnis zu setzen und diese zu einer praktischen Konkordanz zu bringen.<sup>23</sup>

Verträge sind das maßgebliche Instrument für das freie und eigenverantwortliche Handeln zwischen Privatpersonen, auch solchen mit Privatunternehmen. Kommt in einem Vertragsverhältnis einem Vertragspartner ein solches Gewicht bei, dass er den Vertragsinhalt einseitig bestimmen kann, ist es Aufgabe des Rechts auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt. Eine solche einseitige Bestimmungsmacht eines Vertragspartners kann sich daraus ergeben, dass die vom überlegenen Vertragspartner angebotene Leistung für den anderen Partner zur Sicherung seiner persönlichen Lebensverhältnisse von so erheblicher Bedeutung ist, dass die denkbaren Ver-

haltungsalternativen ihn dazu veranlassen von einem Vertragsabschluss ganz abzusehen, da ihm dieser nicht zumutbar ist. In solchen Fällen gebietet die staatliche Schutzpflicht dem unterlegenen Teil eine zumutbare Alternative zu eröffnen.<sup>24</sup>

#### 4.2 Menschenwürde und Handlungsfreiheit

Mit der Unantastbarkeit der Würde des Menschen und der staatlichen Verpflichtung, diese zu schützen (Art. 1 Abs. 1 GG, Art. 1 GRCh), wird die Rechtssubjektivität aller Menschen anerkannt. Der Mensch genießt Schutz um seiner selbst willen und dieser Schutz darf nicht zugunsten vermeintlich höherer Zwecke geopfert werden. Der Mensch soll sein Leben in Freiheit selbst bestimmen und eigenverantwortlich gestalten können. „Mit der Subjektqualität des Menschen ist ein sozialer Wert- und Achtungsanspruch verbunden, der es verbietet den Menschen zum ‚bloßen Objekt‘ staatlichen Handelns zu degradieren“.<sup>25</sup>

Mit der digitalen Erfassung und Behandlung von Menschen erfolgt deren Objektivierung durch eine Reduzierung auf digital erfassbare und erfasste Merkmale. Hierin liegt kein Würdeverstoß, wenn bei dieser Erfassung und Behandlung dem Menschen dienliche Zwecke verfolgt werden. Werden nicht nur Einzelelemente des Menschen digitalisiert und erfolgt eine totale Digitalisierung des Alltags, so wird die Schwelle des Würdeverstoßes überschritten. Der Mensch darf nicht zum ausschließlichen Objekt der Technik werden:<sup>26</sup> „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert wird, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.“<sup>27</sup>

Soziale Beziehungen zwischen Menschen erfordern ihrem Wesen nach direkte Interaktion. Das menschliche Zusammenleben setzt Empathie voraus und die Fähigkeit einander zu verstehen. Die Unbeschwertheit sozialer Beziehungen kann dadurch beeinträchtigt sein, dass Dritte diese beobachten und manipulieren können. Dies gilt für die zwischenmenschliche Kommunikation, hat aber auch Relevanz für die Bezie-

hung der Menschen zu Behörden und Unternehmen. Digitale Instrumente müssen sich darauf beschränken Hilfsmittel für die Bewältigung der analogen menschlichen Aktivitäten zu sein.<sup>28</sup>

Die allgemeine Handlungsfreiheit garantiert jedem das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und gegen die verfassungsmäßige Ordnung verstößt (Art. 2 Abs. 1 GG). Dazu gehört die Freiheit die benutzten Medien selbst zu wählen („Recht auf mediale Selbstbestimmung“).<sup>29</sup> Sie schützt vor unverhältnismäßigen staatlichen Vorgaben in Bezug auf die Art der Kommunikation mit Dritten.<sup>30</sup>

Wird Alltagshandeln digital erfasst und besteht keine Möglichkeit sich dem zu entziehen, so liegt hierin ein Eingriff in die Handlungsfreiheit. Dadurch werden Einblicke in das soziale Umfeld und in die individuellen Aktivitäten und das Erstellen von Persönlichkeitsprofilen ermöglicht. Der Schutz hiervoor stößt auf strukturelle Grenzen. Verstärkt wird dies in Fällen, in denen die Datenverwaltung ein hohes Maß an Technikbeherrschung sowie anspruchsvolle Software voraussetzt, womit die Gefahr von Schwachstellen und das Risiko von Manipulationen durch interessierte Dritte verbunden ist, insbesondere wenn nicht sichergestellt ist, dass die Betroffenen diese Risiken bemerken.<sup>31</sup>

#### 4.3 Wahlfreiheit fürs Digitale

Es besteht zunehmend darüber Einigkeit, dass den Menschen ein subjektives Zugangsrecht zum Internet zusteht.<sup>32</sup> Der Zugang und der Datentransport müssen diskriminierungsfrei sein.<sup>33</sup> Allerdings ist bis heute die Bereitstellung der Internet-Infrastruktur hierfür noch nicht überall gesichert; diskutiert wird schon über ein Recht auf schnelles Internet.<sup>34</sup>

Grundrechte haben eine digitale Dimension. Kommunikation erfolgt heute nicht mehr nur per Briefpost; digitale Kommunikation wird durch das Telekommunikationsgeheimnis (Art. 10 GG, Art. 7 GRCh) besonders geschützt. Zur unternehmerischen Freiheit (Art. 16 GRCh) gehört das Recht zur Digitalisierung, ohne die es oft nicht mehr möglich ist im Wettbewerb zu bestehen. Für

die Meinungs- und Informationsfreiheit (Art. 5 GG, Art. 11 GRCh) eröffnen digitale Medien völlig neue Chancen. Die Wahrnehmung vieler Grundrechte ist in einer modernen Gesellschaft ohne digitale Medien nicht mehr vorstellbar. Die digitale Dimension der Grundrechte bleibt aber ein Teilaspekt der objektiven Grundrechtsfunktion. Sie kann die räumlich-gegenständliche Grundrechtsdimension nicht verdrängen, die Bestand behält.<sup>35</sup> Lediglich der Schwerpunkt hat sich verlagert: Die Freiheit zur Internetnutzung wird zunehmend gewährleistet; nötig wird in gleichem Maße und zunehmend eine Freiheit vor dem Zwang zum Internet. Die Garantie von Grundrechten erstreckt sich sowohl auf deren Ausübung mit analogen als auch mit digitalen Mitteln. Der Staat darf prinzipiell nicht vorgeben, welche digitalen oder sonstigen Mittel ein Mensch zu seiner Persönlichkeitsentfaltung wählt.<sup>36</sup>

Staatliche Stellen können für sich grds. keine Grundrechte für ihre Digitalisierung in Anspruch nehmen, um diese einem möglichen Recht auf Analoges entgegenzusetzen. Wohl aber findet deren digitale Aufgabenerledigung in der Verfassung eine Grundlage: Dem Staat muss es möglich sein seine Verwaltung effektiv und wirtschaftlich zu organisieren, um ihre Funktionstüchtigkeit angesichts der Ressourcenbegrenztheit zu wahren.

Digitale Kommunikation ermöglicht einer Stelle von den Bürgern stammende Daten unmittelbar und ohne Medienbruch weiterzuverarbeiten. Neben der Verwaltungsvereinfachung und der administrativen Kostenersparnis verbessert die elektronische Übermittlung die Überprüfungs- und Auswertungsmöglichkeiten und beschleunigt damit die Bearbeitung. Gut durchdachte Digitalisierung, die schlecht beherrschbare Verarbeitungen vermeidet, geht regelmäßig mit einer Erhöhung der Datensicherheit einher. Die Gewährleistung einer effektiven, möglichst wirtschaftlichen und einfachen Verwaltung ist ein gewichtiger öffentlicher Belang (Art. 20 Abs. 3 GG).<sup>37</sup> Damit kann angesichts begrenzter Ressourcen eine in Art. 3 GG geforderte Gleichbehandlung der Kommunikationspartner erleichtert werden. Der Staat ist nicht gehindert durch An-

reize seines Angebotes die Menschen dazu zu veranlassen digitale Medien zu nutzen.<sup>38</sup>

Es gibt aber keine legitimen Gründe dafür ausschließlich auf Digitalisierung zu setzen. Ein sinnvolles Nebeneinander von Digitalisierung und analogen Alternativenangeboten ist weder fortschritts-hemmend noch unzumutbar. Auch mit analogen Diensten können die grundlegenden Kommunikations- und Konsumbedürfnisse befriedigt werden. In Frankreich hat die Nationalversammlung am 30.11.2023 ein Gesetz über öffentliche Dienste verabschiedet, in dem es in Art. L. 111-4 heißt: „Niemand darf gezwungen werden, in seinen Beziehungen mit der Verwaltung auf entmaterialisierte Verfahren zurückzugreifen.“ Dies bedeutet, dass jeder mit einem Menschen interagieren können muss, um seine Rechte ausüben zu können.<sup>39</sup>

#### 4.4 Allgemeines Persönlichkeitsrecht

Das BVerfG hat aus der Handlungsfreiheit (Art. 2 Abs. 1 GG) und der Würdegarantie (Art. 1 Abs. 1 GG) in richterlicher Rechtsfortbildung eine Vielzahl inhaltlicher Ausprägungen des allgemeinen Persönlichkeitsrechts abgeleitet. Zur freien Entfaltung der Persönlichkeit gehört die Freiheit etwas nicht tun zu müssen (negative Handlungsfreiheit) und so auch auf die Nutzung des Internets zu verzichten.<sup>40</sup> Eine frühe Ausprägung des allgemeinen Persönlichkeitsrechts, die insbesondere in den USA entwickelt wurde, ist das „Recht auf Privatheit“ in Form des „Rechts, in Ruhe gelassen zu werden“.<sup>41</sup>

Angesichts der Digitalisierung und insbesondere der Nutzungsdatenerfassung im Internet wurde über ein „Recht auf Anonymität“ diskutiert, soweit die Internetnutzung nicht in die Rechte Dritter eingreift.<sup>42</sup> Dieses begründet aber kein Recht auf analoge Teilhabe. Auch bei analogem Handeln, etwa dem Ausfüllen von Papierformularen, entstehen persönliche Daten, die von den Datenempfängern digitalisiert werden können.

Ein Recht auf analoge Teilhabe bewahrt den Betroffenen aber davor selbst zur Digitalisierung beizutragen. Es macht dabei dem Betroffenen in stärkerem Maße bewusst, welche seiner Daten

durch wen erfasst und möglicherweise weiterverarbeitet werden. Der Aufwand bei der Digitalisierung analog erfasster Daten erhöht bei den Verantwortlichen zudem die Hemmschwelle für einen digitalen Missbrauch der Daten.

Eine spezifische Ausgestaltung des allgemeinen Persönlichkeitsrechts ist das Recht auf informationelle Selbstbestimmung, das als Grundrecht auf Datenschutz in Art. 8 GRCh europaweit anerkannt ist. Es begründet die Befugnis grundsätzlich selbst zu bestimmen, wer was wann und bei welcher Gelegenheit über einen weiß. Wer unsicher ist, ob seine Verhaltensweisen notiert und als Information dauerhaft gespeichert, verwendet und weitergegeben werden, kann in seiner Freiheit beeinträchtigt sein.<sup>43</sup>

Die Wahrnehmung des Rechts auf informationelle Selbstbestimmung setzt voraus, dass Betroffene hinsichtlich der sie betreffenden Datenverarbeitung hinreichend informiert sind (Art. 5 Abs. 1 lit. a DSGVO). Dies gilt für den Fall der Verarbeitung nach Einholung einer Einwilligung (Art. 7 Abs. 2 DSGVO), aber auch, wenn keine Zustimmung eingeholt wird (Art. 13 f. DSGVO). In der Praxis wird das Transparenzgebot gerade bei digitalen Angeboten missachtet.<sup>44</sup>

Bei einer Nutzung des Internets fallen zumeist zusätzliche Daten an, die bei einer analogen Inanspruchnahme eines Dienstes nicht entstehen. Solche Metadaten, z. B. durch Cookies ausgelöste Speicherungen bei Drittunternehmen, geben Auskunft über Ort, Zeit und Kontext einer digitalen Aktivität, über Art und Identität des genutzten Geräts. Für das Erbringen der Dienstleistung selbst sind zumindest einige dieser Daten nicht erforderlich.<sup>45</sup> Bei einer digitalen Dienstleistung können sie zur Gewährleistung der IT-Sicherheit nötig sein. Jenseits der Sicherheitszwecke steht die Nutzung zusätzlich entstehender Daten aber oft im Widerspruch zum Datenminimierungsgebot (Art. 5 Abs. 1 lit. c DSGVO).<sup>46</sup>

Die anfallenden Meta-Daten werden oft zweckwidrig genutzt, z. B. für Werbezwecke oder gar missbräuchlich für cyberkriminelle Angriffe. Öffentliche wie nichtöffentliche Stellen nehmen bei ihren Bürger- und Kundenkontakten regelmäßig Dienste großer IT-Kon-

zerne mit Hauptsitz in den USA – wie Microsoft, Google, Apple, Meta oder Amazon – in Anspruch. Von diesen Unternehmen werden zumeist in den USA die personenbezogenen Daten in eigener Verantwortung verarbeitet, so dass selbst die direkten Leistungserbringer hierüber keine weitere Kontrolle mehr haben. Wie oben bereits erwähnt, ist seit den Enthüllungen durch Edward Snowden zudem bekannt, dass auch westliche Geheimdienste das gesamte Kommunikationsverhalten im Internet kontrollieren können und dies auch tun.<sup>47</sup> Die Risiken, die von ausländischen Geheimdiensten und von Kriminellen ausgehen, nehmen in den letzten Jahren zu. Die von staatlicher Seite dagegen ergriffenen Schutzmaßnahmen sind nur bedingt erfolgreich.<sup>48</sup> So ist es Datenschutzaufsichtsbehörden bisher de facto nicht möglich bei großen Internet-Plattformen die in Art. 25 DSGVO normierten Grundsätze des „Privacy by Default“ und „Privacy by Design“ auch nur ansatzweise effektiv durchzusetzen.<sup>49</sup>

Die rechtskonforme Gestaltung ist bei digitalen Medien häufig nicht gewährleistet. Aufgrund nicht ausreichender Schutzvorkehrungen sind sie in hohem Maße verletzlich. Werden Menschen gezwungen diese Medien zu nutzen, so sind diejenigen, von denen der Zwang ausgeht, verpflichtet alle möglichen Maßnahmen zum Schutz vor Verletzungen zu ergreifen, die durch die Nutzung entstehen. Die digitalen Angebote dürfen nicht im Verdacht stehen gegen den Datenschutz zu verstoßen oder keine Datensicherheit zu gewährleisten. Es bedarf der Bestätigung der Datenschutzkonformität und angemessener Sicherheit durch eine vertrauenswürdige, qualifizierte unabhängige Stelle, so wie dies in Art. 42 DSGVO vorgesehen ist. Solange diesen grundlegenden Anforderungen bei digitalen Angeboten nicht genügt wird – so wie dies derzeit durchgängig der Fall ist – ist Digitalzwang eine unverhältnismäßige Beeinträchtigung aller Betroffenen hinsichtlich ihrer informationellen Selbstbestimmung.<sup>50</sup>

Medienkompetenz der Handelnden sowie objektiv gegebene Schutzmöglichkeiten sind nötig, damit Nutzende private Vorkehrungen zum Schutz ih-

rer Daten ergreifen können. Digitaler Selbstschutz ist in der Regel nicht ohne Aufwand und Kosten machbar. Angesichts der Beschränktheit staatlicher Schutzmöglichkeiten haben die Menschen bei der Nutzung digitaler Medien ein Recht auf Selbstschutz. Staatliche Stellen trifft die Pflicht die rechtlichen und tatsächlichen Voraussetzungen zu schaffen, so dass Menschen wirkungsvollen informationellen Selbstschutz praktizieren können.<sup>51</sup> Dieser Selbstschutz kann in der Nutzung analoger Alternativen zu einem digitalen Angebot liegen.<sup>52</sup>

Viele Menschen versuchen ihre Internetnutzung auf ein Minimum zu reduzieren, um dadurch entstehende Risiken zu vermeiden, insbesondere wenn aufgrund des jeweiligen Dienstes besonders sensitive Daten anfallen, wie z. B. beim Online-Banking. Informationelle Selbstbestimmung impliziert, dass Betroffene grundsätzlich die freie Wahl ihres Instruments der Datenverarbeitung haben und ihnen die Möglichkeit, so über die Form des Schutzes vor digitalen Angriffen selbst mitzubestimmen, zusteht.<sup>53</sup> Es genügt nicht eine hinreichend präzise bereichsspezifische gesetzliche Regelung zu etablieren, um einen Eingriff ins Recht auf informationelle Selbstbestimmung durch Digitalzwang zu rechtfertigen;<sup>54</sup> dieser Eingriff muss auch geeignet, erforderlich und verhältnismäßig im engeren Sinne sein.

#### 4.5 Gleichheitsgebot und Diskriminierungsverbot

Art. 3 GG, Art. 20 GRCh sowie Art. 14 EMRK garantieren ein Recht auf Gleichbehandlung. Für die Rechtfertigung einer Ungleichbehandlung bedarf es eines sachlichen Grundes. Der Anspruch auf Gleichbehandlung richtet sich vorrangig an hoheitliche Einrichtungen. Er begründet auch ein Recht auf gleiche Teilhabe in Bezug auf staatliche oder existenzielle Leistungen. Werden diese digital erbracht, so kann sich hieraus ein Recht auf alternative Leistungserbringung auf analogem Wege ergeben, wenn es keinen sachlichen Grund gibt eine solche Leistungserbringung auszuschließen.<sup>55</sup> Der Diskriminierungsschutz erfordert zumindest, dass für

Personen, für die eine Internetnutzung nicht möglich ist, „Auffanglösungen“ gefunden werden.<sup>56</sup> Werden Menschen, die digitale Dienste nicht in Anspruch nehmen können, ausgeschlossen, so liegt hierin eine unzulässige Diskriminierung.<sup>57</sup>

Dies gilt insbesondere für die Verletzung spezifischer Diskriminierungsverbote. Art. 21 Abs. 1 GRCh verbietet Diskriminierungen wegen des Vermögens, einer Behinderung oder des Alters. Zwar werden Menschen bei ausschließlich digitalen Angeboten zumeist nicht direkt wegen ihrer Armut, einer Behinderung oder dem hohen Alter ausgeschlossen; rechtlich relevante mittelbare Diskriminierungen<sup>58</sup> sind aber in der Praxis weit verbreitet.<sup>59</sup> Die Nutzung digitaler Dienste setzt die Investition in ein digitales Endgerät sowie die Zahlung von Anschlusskosten voraus. Eine Diskriminierung kann vermieden werden, wenn der Staat als Leistungserbringer die benötigten technischen Einrichtungen bereitstellt, etwa Tablets für Schüler oder Leseterminale für die elektronische Gesundheitskarte für gesetzliche Krankenversicherte. Digitale Dienste sind oft nicht barrierefrei. Blinde, Gehörlose oder Personen mit einer körperlichen Einschränkung sind bei der Nutzung von üblichen Digitalgeräten faktisch ganz oder teilweise ausgeschlossen. Das Alter kann dazu führen, dass Menschen nicht mehr in der Lage sind die komplexen Anforderungen bei der Nutzung digitaler Dienste zu erfüllen (s. u. 4.7).

#### 4.6 Pflicht zur Daseinsvorsorge

Art. 36 GRCh anerkennt und achtet den „Zugang zu Dienstleistungen von allgemeinem wirtschaftlichen Interesse“. Es ist streitig, inwieweit aus dieser Regelung ein subjektives Recht abzuleiten ist, ebenso, ob sich die Regelung nur an die Europäische Union richtet oder auch an die einzelnen Mitgliedsstaaten.<sup>60</sup> Die Konkretisierung der Zugangsmöglichkeit erfolgt durch „Rechtsvorschriften und Gepflogenheiten“. Diese dürfen keinen ausschließenden Charakter haben. Art. 36 GRCh begründet als Grundrecht zumindest für äußerst wichtige Dienste einen subjektiven Zugangsanspruch.<sup>61</sup> Erfasst sind Dienstleistungen der Infrastrukturwirt-

schaft wie Telekommunikation, Energieversorgung, Postwesen, Wasser, Abfall- und Abwasserversorgung, öffentliche Verkehrsmittel, Arbeitsvermittlung und Rundfunkdienste.

Das BVerfG hat aus dem Sozialstaatsprinzip des Art. 20 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein Grundrecht auf Gewährleistung eines menschenwürdigen Existenzminimums abgeleitet, das jedem Hilfebedürftigen diejenigen materiellen Voraussetzungen zusichert, die für seine physische Existenz und für ein Mindestmaß an Teilhabe am gesellschaftlichen, kulturellen und politischen Leben unerlässlich sind, und die Möglichkeit zur Pflege zwischenmenschlicher Beziehungen sichert.<sup>62</sup> Erfasst werden die sozialen Existenzbedingungen, also die Bedingungen, die das Leben der Menschen in der aktuellen Gesellschaft bestimmen. Es geht darum die infrastrukturellen Voraussetzungen einer zeitgemäßen, der Zivilisation entsprechenden Persönlichkeitsentfaltung sicherzustellen.

Der Gesetzgeber ist angehalten die soziale Wirklichkeit zeit- und realitätsgerecht im Hinblick auf die Gewährleistung des Existenzminimums zu erfassen. Die Erhebung der Bedürfnisse bedarf der stetigen Aktualisierung. Hierfür muss der Gesetzgeber regelmäßig Entwicklungsstand und Lebensbedingungen prüfen.<sup>63</sup> Gerade im Hinblick auf die sich dynamisch entwickelnden Informations- und Kommunikationstechnologien muss diese Prüfung regelmäßig stattfinden. Mittlerweile gehört die Möglichkeit der Nutzung moderner Medien zum Mindestmaß sozio-kultureller Teilhabe.<sup>64</sup>

Aus dem Sozialstaatsprinzip und der Garantie der kommunalen Selbstverwaltung wird die staatliche Pflicht zur Daseinsvorsorge abgeleitet. Es ist staatliche Aufgabe Güter und Leistungen bereitzustellen, die für ein menschliches Dasein notwendig sind. Dies umfasst nach bisherigem Verständnis Energie- und Wasserversorgung, Verkehrsleistungen, Telekommunikation, Rundfunk, Abwasser- und Müllentsorgung, die Bereitstellung von Bildungs- und Kultureinrichtungen, Krankenhäusern, Friedhöfen, Schwimmbädern, Feuerwehr und vieles mehr. Inzwischen ist anerkannt, dass auch der Zugang zum

Internet neben einem Strom- und einem Telefonanschluss zur elektronischen Daseinsvorsorge gehört.<sup>65</sup>

Kann der Staat aus ökonomischen Gründen Bedürftigen für ihre Teilhabe nicht die nötige Technologie bereitstellen, besteht die Notwendigkeit nicht-digitaler Alternativen. Es gibt zudem sozio-kulturelle Teilhaben, bei denen den Betroffenen Wahlmöglichkeiten eingeräumt bleiben müssen. In einigen existenziellen Lebensbereichen kann bisher unter keinen Umständen auf eine analoge Erbringung verzichtet werden, etwa bei der Bildung, in der Pflege oder in der Gesundheitsversorgung.

2017 wurde auf EU-Ebene als Grundsatz 20 der „Europäischen Säulen sozialer Rechte“ das Recht auf Grundversorgungsleistungen im Europäischen Referenzrahmen für Sozialrechte wie folgt beschrieben: „Jede Person hat das Recht auf den Zugang zu essenziellen Dienstleistungen wie Wasser-, Sanitär- und Energieversorgung, Verkehr, Finanzdienste und digitale Kommunikation. Hilfsbedürftigen wird Unterstützung für den Zugang zu diesen Dienstleistungen gewährt.“<sup>66</sup> Diese Dienste tragen zur Deckung der Grundbedürfnisse bei und sind von zentraler Bedeutung für das Wohlergehen und die soziale Inklusion, v. a. für benachteiligte Gruppen.<sup>67</sup> Der Grundsatz konkretisiert Grundrechtsnormen der Grundrechtecharta und gemeinsame Werte der EU-Mitgliedstaaten. Der darin zum Ausdruck kommende Versorgungsanspruch ist voraussetzungslos formuliert und gilt auch für Personen, für die eine digitale Inanspruchnahme aus objektiv nachvollziehbaren Gründen nicht in Frage kommt. In diesem Sinne verfasste die parlamentarische Versammlung des Europarats 2023 eine Resolution gegen die gesellschaftliche „digitale Spaltung“.<sup>68</sup>

Zur Realisierung des sich hieraus ergebenden Gestaltungsauftrags an den Gesetzgeber<sup>69</sup> kann der Staat ein eigenes Angebot bereitstellen. Die nötigen Dienste können auch durch Private und auf dem Markt erbracht werden. Voraussetzung bleibt, dass diese kostenlos oder zumindest erschwinglich und diskriminierungsfrei bereitgestellt werden. Der Bedarf an staatlicher Intervention, sei dies über eigene Leistungen, Schutzvorkehrungen oder Schaffung objekti-

ver Rahmenbedingungen, steigt in dem Maße, wie Angebote sozio-kultureller Teilhabe und der Daseinsvorsorge kommerzialisiert sind.<sup>70</sup>

#### 4.7 Anspruch auf Barrierefreiheit

Gemäß Art. 3 Abs. 3 S. 2 GG und Art. 21 Abs. 1 GRCh darf niemand wegen seiner Behinderung benachteiligt werden. Art. 26 GRCh begründet einen „Anspruch von Menschen mit Behinderung auf Maßnahmen zur Gewährleistung ihrer Eigenständigkeit, ihrer sozialen und beruflichen Eingliederung und ihrer Teilhabe am Leben der Gemeinschaft“. Die Regelung geht auf Vorgaben des internationalen Rechts zurück.<sup>71</sup> Als Behinderte sind die Personen anzusehen, die von einer nicht nur vorübergehenden Funktionsbeeinträchtigung betroffen sind, die auf einem vom typischen Zustand abweichenden körperlichen, geistigen oder seelischen Zustand beruht.<sup>72</sup> In Umsetzung dieses Anspruchs regelt die EU-Richtlinie 2016/2102, dass „die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zu den Barrierefreiheitsanforderungen für die Websites und mobilen Anwendungen öffentlicher Stellen (anzugleichen sind), damit diese Websites und mobilen Anwendungen für die Nutzer, insbesondere für Menschen mit Behinderungen, besser zugänglich gestaltet werden“.<sup>73</sup> Ende 2021 prangerten Verbände an, dass 95% der Webseiten den rechtlichen Anforderungen an diese Barrierefreiheit nicht genügen und „Behördengänge für Menschen mit Behinderungen extrem kompliziert und sogar unmöglich“ seien.<sup>74</sup>

Der in Art. 26 GRCh begründete Anspruch ist im Hinblick auf digitale Dienste zunächst darauf ausgerichtet Behinderten die Teilhabe durch entsprechende technische, personale oder soziale Angebote zu ermöglichen.<sup>75</sup> Sind die Behinderung kompensierende technische Maßnahmen nicht möglich, so kann sich ein Teilhabeanspruch auf Angebote in analoger Form ergeben.

Einen entsprechenden Teilhabeanspruch „auf ein würdiges und unabhängiges Leben und auf Teilnahme am sozialen und kulturellen Leben“ anerkennt Art. 25 GRCh für ältere Menschen. Dem zur Seite steht das Diskri-

minierungsverbot wegen des Alters (Art. 21 Abs. 1 GRCh).

#### 4.8 Meinungs- und Informationsfreiheit

Das Recht auf freie Meinungsäußerung und Informationsfreiheit (Art. 5 Abs. 1 S. 1 GG, Art. 11 Abs. 1 GRCh, Art. 10 EMRK) schließt das Recht, die Wege der Kommunikation zu wählen, ein. Ein zentrales Medium ist insofern das Internet. Ein Recht auf Internet darf aber nicht zur alternativlosen Pflicht bei der Grundrechtsverwirklichung werden; den Menschen müssen weitere Mittel in Bezug auf spezifische Meinungsäußerungen und als Informationsquelle zur Verfügung stehen.<sup>76</sup>

#### 4.9 Einhaltung des Rechtsstaatsgrundsatzes

Das in Art. 20 Abs. 3 GG normierte Rechtsstaatsprinzip garantiert, dass Menschen einen Anspruch auf einen effektiven Zugang zur staatlichen Verwaltung haben. Art. 41 GRCh sichert den Menschen ein Recht zu, dass ihre Angelegenheiten hinsichtlich der Unionsverwaltung unparteiisch und gerecht behandelt werden, dass sie gehört werden und Zugang zu den sie betreffenden Akten erhalten. Art. 13 EMRK gewährt ein Recht auf einen wirksamen Rechtsbehelf. Daraus ergibt sich kein Anspruch darauf sich über ein bestimmtes Medium mit der Verwaltung auszutauschen. Wohl aber muss der Zugang zur Verwaltung fair und diskriminierungsfrei eingeräumt werden. Wolfgang Hoffmann-Riem mahnte bereits zur Jahrtausendwende, dass „die Verwaltung neue Kommunikationsmöglichkeiten nicht einsetzen (dürfe), wenn solche Zugangshürden zu Barrieren bei der Interaktion mit der Verwaltung“ führen.<sup>77</sup> Die Möglichkeit zum analogen Austausch haben faktisch fast alle Menschen, was für den digitalen Austausch nicht gilt. Eine Pflicht zur ausschließlich digitalen Kommunikation mit der Verwaltung kann daher nur in gut begründeten Fällen gesetzlich statuiert werden, wobei der Verhältnismäßigkeitsgrundsatz zu beachten ist.<sup>78</sup> Umgekehrt kann es geboten sein für Menschen, die für den Zugang zur staatlichen Verwaltung technische Hilfen benötigen, diese

– auch in digitaler Form – zur Verfügung zu stellen.

#### 4.10 Öffentlichkeitsgrundsatz

Das BVerfG urteilte am 03.03.2009, dass der Einsatz von digitalen Wahlgeräten mit dem verfassungsrechtlichen Grundsatz der Öffentlichkeit der Wahl und der hierbei nötigen Kontrolle (Art. 38 i. V. m. Art. 20 Abs. 1, 2 GG) nicht vereinbar ist. Ausschlaggebend war, dass sich Entscheidungsprozesse in den Wahlgeräten abspielen, deren Richtigkeit im Nachhinein nicht verlässlich verifiziert werden kann. Es ist bei wichtigen Vorgängen wie demokratischen Wahlen unabdingbar, dass der zugrundeliegende Prozess vertrauenswürdig ist und nicht durch Manipulationen oder Fehlfunktionen beeinträchtigt werden kann. Die wesentlichen Schritte bei der Ergebnisermittlung müssen öffentlich nachvollzogen werden können.<sup>79</sup>

Der Aspekt der öffentlichen wie auch der individuellen Kontrolle und Kontrollierbarkeit hat keine direkte Relevanz für die Bewertung der von ausschließlich digitalen Angeboten ausgelösten Zwangssituationen. Er ist jedoch für die Bewertung der Güte digitaler Prozesse und damit für die Berechtigung ihrer Ablehnung durch Betroffene wichtig. Die Undurchsichtigkeit des Digitalen macht es oft schwierig Fehler zu erkennen, die auf die Entscheidungsfindung in einem Prozess Einfluss haben.

Grundsätzlich können digitale Prozesse ähnlich gestaltet, dokumentiert und kontrolliert werden wie analoge Prozesse, wenngleich sich dies als technisch aufwändig erweisen kann. Art. 5 Abs. 1 lit. a DSGVO erklärt Transparenz zu einem Grundprinzip des Umgangs mit personenbezogenen Daten generell. Besonders relevant wird die Frage individueller wie demokratischer Kontrollierbarkeit, wenn bei verpflichtenden digitalen Angeboten komplexe Verfahren mit vielen Beteiligten, etwa unter Verwendung von Methoden der Künstlichen Intelligenz (sog. KI), zum Einsatz kommen, bei denen sich Transparenz und Kontrollierbarkeit schnell verflüchtigen,<sup>80</sup> oder wenn Dienste großer Plattformbetreiber in Anspruch genommen werden, die das Funktionieren ihrer Dienste nicht mehr offenlegen.<sup>81</sup>

#### 4.11 Gemeinwohlerwägungen

Das BVerfG hat in der Volkszählungsentscheidung dargelegt, dass informationelle Selbstbestimmung nicht nur der individuellen Entfaltung dient, sondern zugleich dem Gemeinwohl, da diese „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist“.<sup>82</sup> Dies gilt nicht nur für die Wahrung informationeller Selbstbestimmung generell, sondern auch für die Bereitstellung analoger Alternativen speziell.

Der Ausfall digitaler Dienste nach Cyberangriffen, auf Grund von Unfällen oder (Natur-)Katastrophen zeigt, welche Verletzlichkeit unseres Gemeinwesens mit der zunehmenden Digitalisierung einhergeht. Dem muss mit Resilienzmaßnahmen entgegengewirkt werden. In der Praxis erweist sich, dass hierbei auf analoge Redundanzen nicht verzichtet werden kann. Das Vorhalten analoger Alternativen zu digitalen Diensten kann in Krisensituationen hilfreich sein, um diese zu überwinden.

#### 4.12 Verfassungsrechtliche Schlussfolgerungen

Für die verfassungs- und europarechtliche Bewertung von Technik ist typisch, dass eine Vielzahl von Regeln und vor allem Grundrechte tangiert sind und eine Gesamtschau erfolgen muss. So lassen sich Wertungslücken hinsichtlich spezifischer Verfassungsregelungen schließen. Letztlich bestehen keine rechtsfreien Räume; wohl aber sind im Hinblick auf technische Entwicklungen Regeln konkretisierungsbedürftig.<sup>83</sup>

Ein Recht auf analoge Teilhabe bzw. auf Schutz vor Digitalzwang lässt sich schon heute aus den Grundrechten ableiten. Der Anspruch auf eine analoge Alternative zu einem digitalen Angebot kann sowohl gegenüber der öffentlichen Hand als auch in vielen Fällen gegenüber privaten Anbietern geltend gemacht werden. Dieser Anspruch begründet sich aus dem allgemeinen Persönlichkeitsrecht, dem Gleichheitsanspruch und dem Diskriminierungsverbot, aus der Sozial- und der Rechtsstaatlichkeit sowie aus dem Demokratieprinzip. Die-

ses Recht besteht nicht umfassend und voraussetzungslos, sondern ist von der jeweiligen Fallgestaltung abhängig. Folgende Aspekte sind relevant:

- Handelt es sich um ein Angebot, das für die Bevölkerung generell oder für jeden Einzelnen von existenzieller Bedeutung oder für die Teilhabe am ökonomischen, sozialen, kulturellen und politischen Leben grundlegend ist?
- Gibt es in der Person des Anspruchstellenden oder aus generellen Erwägungen Gründe, weshalb die digitale Inanspruchnahme des Angebots nicht zumutbar ist?
- Ist eine analoge Alternative zum digitalen Angebot erforderlich und geeignet, um die Funktion für die betroffene Person zu erfüllen?

Letztlich kommt es in jedem Fall auf eine Abwägung zwischen den individuellen Belangen des Betroffenen und den Interessen des Staates oder der privaten Stelle an einer ausschließlichen digitalen Bereitstellung eines Angebots oder Dienstes an.

Öffentliche Stellen haben grundsätzlich die Pflicht zur zumindest ausnahmsweisen Bereitstellung einer analogen Alternative. Eine generelle gesetzlich normierte Verpflichtung zum Digitalen setzt voraus, dass die technischen, infrastrukturellen und sonstigen Voraussetzungen für die digitale Nutzung flächendeckend oder jedenfalls im erfassten Teilbereich vorliegen.<sup>84</sup> Wird die analoge Alternative nur ausnahmsweise bereitgestellt, nachdem der Betroffene hierfür eine Berechtigung nachgewiesen hat, so bedarf es hierfür wegen des Gesetzesvorbehalts beim Grundrechtseingriff einer gesetzlichen Grundlage, in der die Bedingungen für die ausnahmsweise analoge Inanspruchnahme hinreichend konkretisiert wurden (Art. 52 Abs. 1 GRCh).<sup>85</sup>

Ein Anspruch auf eine analoge Alternative gegenüber Privaten hängt davon ab, inwieweit auf dem Markt für die grundlegende Bedürfnisbefriedigung eine bezahlbare Alternative besteht. Bei monopolartigen Angeboten kann ein Anspruch auf Analoges eher vermutet werden als bei einem pluralen funktionierenden Markt. Besteht kein hinreichendes Angebot durch private Anbie-

ter, so kann der Staat aus Gründen der Daseinsvorsorge verfassungsrechtlich verpflichtet sein selbst für ein Angebot zu sorgen.

Bei der Bereitstellung einer analogen Alternative für einen digitalen Dienst dürfen die dadurch entstehenden zusätzlichen Kosten für die analoge Dienstleistung nicht voll den Nutzenden auferlegt werden. Ist ein Dienst oder ein Angebot von existenzieller Bedeutung, so dürfen sich die Kosten der digitalen und der analogen Nutzung grundsätzlich nicht unterscheiden.<sup>86</sup> In keinem Fall dürfen die zusätzlichen Kosten die Wahlfreiheit der Nutzenden derart beschränken, dass für sie nur die digitale Variante in Betracht kommt.

## 5. Vorschläge für eine verfassungsrechtliche Weiterentwicklung

Die Initiativen zur Etablierung eines Rechtes auf analoge Alternativen stehen vor einem politischen Dilemma, das Jonas Botta vom Forschungsinstitut für öffentliche Verwaltung in Speyer beschreibt: „Ein ‚Recht auf Analog‘ schwindet in dem Maße, wie die Verbreitung von IT-Kompetenz und technischem Zugang zunimmt.“ Vor 20 Jahren war es für Verfassungsrechtler selbstverständlich, dass aufgrund der damals bestehenden Zugangshürden zu den neuen Kommunikationstechnologien ein Recht auf analoge Verwaltung bestand. Inzwischen gibt es nur noch eine Minderheit in Deutschland, die am digitalen Leben nicht teilhaben kann. Für diese muss sich der Staat verantwortlich fühlen und Wege sichern, um in wesentlichen Lebenslagen kommunizieren zu können.<sup>87</sup>

Bedarf es hierfür – ergänzend zum bestehenden Recht – eines „Grundrechts auf eine analoge Alternative“? Ein explizites Grundrecht hätte zur Folge, dass ein Anspruch von Menschen einfacher eingeklagt werden kann digitale Medien nicht nutzen zu müssen. Wie alle Grundrechte wäre ein solches Grundrecht nicht voraussetzungslos und könnte nicht ausnahmslos gelten. Durch ein Grundrecht würden aber öffentliche Stellen explizit und grundsätzlich zu einer analogen Alternative verpflichtet. Der Zwang zum Digitalen

würde einem Gesetzesvorbehalt unterliegen. Für Einschränkungen des Grundrechts bedürfte es also eines Gesetzes, das die Voraussetzungen des Digitalzwangs benennt und sicherstellt, dass dadurch nicht unverhältnismäßig und diskriminierend in Freiheitsrechte eingegriffen wird.

Vorschläge für eine europäische digitale Grundrechte-Charta haben bisher keine offiziellen Gesetzgebungsinitiativen ausgelöst.<sup>88</sup> Dort wird in einem Art. 3 unter der Überschrift „Gleichheit“ folgende Regelung vorgeschlagen: „(1) Jeder Mensch hat das Recht auf eine gleichberechtigte Teilhabe in der digitalen Sphäre. Es gilt das in der Europäischen Grundrechte-Charta formulierte Diskriminierungs-Verbot. (2) Die Verwendung von automatisierten Verfahren darf nicht dazu führen, dass Menschen vom Zugang zu Gütern, Dienstleistungen oder von der Teilhabe am gesellschaftlichen Leben ausgeschlossen werden. Dies gilt insbesondere im Bereich Gesundheit, Schutz vor elementaren Lebensrisiken, Recht auf Arbeit, Recht auf Wohnen, Recht auf Bewegungsfreiheit und bei Justiz und Polizei.“ Gemäß einem anderen Vorschlag soll Art. 3 Abs. 3 des Grundgesetzes um einen Satz ergänzt werden: „Die Grund- und Daseinsvorsorge für einen Menschen darf nicht davon abhängig gemacht werden, dass er digitale Angebote nutzt.“<sup>89</sup>

## 6. Fazit

Die Diskussion über ein Recht auf analoge Teilhabe hat begonnen. Es ist wichtig die einzelnen relevanten Sachverhalte konkret zu erörtern. Heute besteht eine Vielzahl von Lebenssituationen, bei denen Digitalzwang herrscht. Menschen, die digitale Medien nicht nutzen können und wollen, werden diskriminiert. Dies kann durch einfachgesetzliche Regulierung eingeholt werden. Angesichts der immer weiter zunehmenden Digitalisierung aller gesellschaftlichen Lebensbereiche und der damit einhergehenden zunehmenden Diskriminierung durch Digitalzwang ist es darüber hinausgehend geboten ein umfassendes und übergeordnetes „Recht auf analoge Teilhabe“ normativ festzuschreiben.

- 1 Degrave, Justice sociale et Services publics numériques: Pour le Droit fondamental d'utiliser – ou non – internet, *Revue belge de Droit constitutionnel* 2023, 214 ff.
- 2 So Digitalcourage, [https://digitalcourage.de/digitalzwang#was mit plastischen Beispielen](https://digitalcourage.de/digitalzwang#was-mit-plastischen-Beispielen).
- 3 Z. B. Lorenz, Das Recht auf ein analoges Leben, *MMR* 2022, 935 ff; Prantl, Raus bist Du, *Süddeutsche Zeitung (SZ)* 06./07.05.2023, 5; Digitalcourage, *Faltblatt, Digitalzwang Für ein Recht auf analoges Leben*, 2024.
- 4 Prantl, Raus bist Du, *SZ* 06./07.05.2023, 5.
- 5 Krempel, Recht auf analog? 3,4 Millionen Deutsche sind noch immer offline, 11.04.2023, <https://heise.de/-8935324>; D21-Digital-Index 2022/2023, <https://initiatived21.de/publikationen/d21-digital-index/2022-2023>.
- 6 destatis, Knapp 6 % der Bevölkerung im Alter von 16 bis 74 Jahren in Deutschland sind offline, 11.04.2023, <https://www.destatis.de>.
- 7 Lorenz, Das Recht auf ein analoges Leben, *MMR* 2022, 936.
- 8 Schulz, Der elektronische Zugang zur Verwaltung, *RDi* 2021, 382.
- 9 Lang in BAGSO, Leben ohne Internet – geht's noch? <https://www.bagso.de/themen/digitalisierung/aktion-leben-ohne-internet/>.
- 10 Z. B. Heckmann, Grundrecht auf IT-Abwehr, *MMR* 2006, 7.
- 11 Zahlung mit EC-Karte nicht möglich: Störung hält weiter an, <https://www.om-online.de> 27.05.2022.
- 12 vzbv, Verbraucher:innen wollen mit Bargeld bezahlen, <https://www.vzbv.de>, 27.12.2021.
- 13 Lorenz *MMR* 2022, 938.
- 14 Lorenz *MMR* 2022, 937 f.
- 15 BFH 14.02.2017 – VIII B 43/16 Rn. 16-19, vgl. BFH 14.03.2012 – XI R 33/09 Rn. 28 ff.
- 16 FG Berlin-Brandenburg 14.02.2018 – 3 K 3249/17, EFG 2018, 705; FG Münster 28.01.2021 – 5 K 436/20 AO, BeckRS 2021, 2757.
- 17 BT-Drs. 20/8093 v. 23.08.2023; dazu Schulz, „Digital only“ und „digital first“ im Onlinezugangsgesetz, *RDi* 2023, 519 f.
- 18 BayObLG 18.11.2020 – 101 VA 124/20, DGVZ 2021, 45; zustimmend Schulz *RDi* 2021, 381.
- 19 Dazu Botta, „Digital First“ und „Digital Only“ in der öffentlichen Verwaltung, *NVwZ* 2022, 1251; Schulz *RDi* 2021, 383;

- Hoffmann/Schulz, Schleswig-Holsteins digitale Verfassung, NordÖR 2016, 389 ff.
- 20 LG Hamburg 29.04.2021 – 312 O 94/20.
- 21 BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 33, DVBl 2007, 111; BVerfG 17.07.2013 – 1 BvR 3167/08, Rn. 17 f., NJW 2013, 3086.
- 22 Schulz, Das Grundrecht auf Achtung und Gewährung eines menschenwürdigen Existenzminimums, in Schliesky/Ernst/Schulz, Die Freiheit des Menschen in Kommune, Staat und Europa, Festschrift für Edzard Schmidt-Jortzig, 2011, S. 34 ff.
- 23 BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 29, JZ 2007, 576.
- 24 BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 35 f.; Hornung in Schoch/Schneider, Verwaltungsrecht, Stand Nov. 2023, Vorb. § 3a Rn. 22 m. w. N.
- 25 Statt vieler BVerfG 17.01.2017 – 2 BvF 1/15, Rn. 539, NVwZ 2018, 1703.
- 26 Botta, NVwZ 2022, 1250; Geminn in Hentschel/Hornung/Jandt, Mensch-Technik-Umwelt: Verantwortung für eine sozialverträgliche Zukunft, Festschrift für Alexander Roßnagel zum 70. Geburtstag, 2020, S. 75 f.; vgl. Heckmann K&R 2011, 1 ff.
- 27 BVerfG 02.03.2010 – 1 BvR 256/08 u. a., Rn. 218, NJW 2010, 839; dazu Roßnagel NJW 2010.
- 28 Schulz in Schliesky/Ernst/Schulz, Festschrift für Schmidt-Jortzig (En. 22), S. 30, 35 f.
- 29 Schulz, Der elektronische Zugang zur Verwaltung, RD i 2021, 379.
- 30 Hornung in Schoch/Schneider, Verwaltungsrecht, Stand Nov. 2023, Vorb. § 3a Rn. 20.
- 31 BVerfG 02.03.2010 – 1 BvR 256/08 u. a., Rn. 210-212, NJW 2010, 838 f.
- 32 Z. B. schon Mecklenburg, ZUM 1997, 525 ff. m. w. N., abrufbar unter <http://www.wmecklenburg.de/plugins/files/796483/internetfreiheit-sx.pdf>; Hoffmann/Luch/Schulz/Borchers, Die digitale Dimension der Grundrechte, 2015, S. 100 ff.
- 33 Degrave, Revue belge des Droit constitutionnel 2023, 232 ff.
- 34 Was bringt das Recht auf schnelles Internet?, <https://www.tagesschau.de/wirtschaft/digitales/internet-rechtsanspruch-verbraucher-100.html>, 03.07.2024; Internet-Mindestversorgung: Ausschuss folgt BNetzA-Empfehlung, <https://www.bundestag.de/presse/hib/kurzmeldungen-1011896> 03.07.2024.
- 35 Hoffmann u. a. (FEn. 32), S. 186 f.
- 36 Hoffmann u. a. (En. 32), S. 101 f.
- 37 BFH 14.03.2012 – XI R 33/09, Rn. 30 ff.
- 38 Botta, „Digital First“ und „Digital only“ in der öffentlichen Verwaltung, NVwZ 2022, 1248.
- 39 Degrave, Revue belge des Droit constitutionnel 2023, 236 ff. mit weiteren Beispielen zu Belgien; Kloza, It's all about choice: the right not to use the internet 29.11.2021, <https://biblio.ugent.be/publication/8738527>.
- 40 Lorenz MMR 2022, 936.
- 41 Warren/Brandeis, Das Recht auf Privatheit – The Right to Privacy, DuD 2012, 755; dazu Weichert DuD 2012, 753 f.
- 42 Dazu ausführlich Bäumler in Bäumler, Anonymität im Internet, 2003, 1 ff.; Brunst, Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, 2009, S. 196 ff.
- 43 BVerfG 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 422.
- 44 Degrave, Revue belge des Droit constitutionnel 2023, 226 f. mit dem Beispiel der in Belgien eingeführten „eBox“.
- 45 Degrave, Revue belge des Droit constitutionnel 2023, 225 f.
- 46 Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 3. Aufl. 2024, Art. 5 Rn. 48 f.
- 47 Statt vieler Snowden, Permanent Record, 2019.
- 48 Degrave, Revue belge des Droit constitutionnel 2023, 227 ff.
- 49 Hansen in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 25, Rn. 6-9; Dix in Hentschel/Hornung/Jandt (En. 26), S. 261 f.
- 50 Siehe hierzu etwa die Vorwürfe Rechtswidrigkeit gegenüber den Angeboten der Deutschen Bahn Conrad, Rechtswidriges Tracking in der App DB Navigator?, 03.11.2022, <https://www.datenschutz-notizen.de/rechtswidriges-tracking-in-der-app-db-navigator-3238891/>.
- 51 BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 33, JZ 2007, 578.
- 52 Dies übersieht Botta NVwZ 2022, 1250.
- 53 Degrave, Revue belge des Droit constitutionnel 2023, 226 f.
- 54 So aber Schulz RD i 2023, 520 f.
- 55 Lorenz MMR 2022, 936; a. A. Botta NVwZ 2022, 1251.
- 56 Schulz RD i 2023, 521.
- 57 Hornung in Schoch/Schneider, Verwaltungsrecht, Stand Nov. 2023, Vorb. § 3a Rn. 20.
- 58 Graser/Reiter in Schwarze (Hrsg.: Becker/Hatje/Schoo/Schwarze), EU-Kommentar, 4. Aufl. 2019, GRC Artikel 21, Rn. 12, 14.
- 59 Degrave, Revue belge des Droit constitutionnel 2023, 221 ff. mit Verweis darauf, dass das Belgische Verfassungsgericht 2004 Regelungen für nichtig erklärte, die vorsahen, dass die praktisch nur-digitale Bereitstellung des Belgischen Staatsblatts über das Internet eine unverhältnismäßige Diskriminierung bestimmter Personengruppen zur Folge hätte.
- 60 Rohleder in Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019, Art. 36 Rn. 15, m. w. N.
- 61 Lorenz MMR 2022, 936 f.
- 62 BVerfG 09.02.2010 – 1 BvL 1/09, 1 BvL 3/09, 1 BvL 4/09 Rn. 135., NJW 2010, 505; Schulz, Informations- und Kommunikationstechnologie als Grundversorgung, DuD 2010, 700; Schulz in Schliesky/Ernst/Schulz (En. 22), S. 17 ff.
- 63 BVerfG 09.02.2010 – 1 BvL 1, 3, 4/09, Rn. 133 ff., NJW 2010, 507 f.
- 64 Hoffmann u. a. (En. 32), S. 98; Schulz in Schliesky/Ernst/Schulz, (En. 22) S. 43.
- 65 Wissenschaftliche Dienste Deutscher Bundestag, Internet als Teil der staatlichen Daseinsvorsorge, 03.02.2012, WD 10 – 3000/115-11 m. w. N.
- 66 European Commission, The European Pillar of Social Rights in 20 principles, [https://www.ogbl.lu/wp-content/uploads/2024/07/Dossier\\_Aktuell\\_2403\\_DE.pdf](https://www.ogbl.lu/wp-content/uploads/2024/07/Dossier_Aktuell_2403_DE.pdf).
- 67 <https://ec.europa.eu/social/main.jsp?catId=1592&langId=de>.
- 68 Closing the digital divide: promoting equal access to digital technologies, Resolution 2510 (2023), 23.06.2023, <https://pace.coe.int/en/files/33001/html>.
- 69 Schulz DuD 2010, 701 f.
- 70 Hoffmann u. a. (En. 32), S. 100 m. w. N.
- 71 Art. 15 bzw. Art. 23 der revidierten Europäischen Sozialcharta, Nr. 26 Gemeinschaftscharta der sozialen Grundrechte der Arbeitnehmer; Teil II Art. 2 ff. Übereinkommen Nr. 159 der Internationalen Arbeitsorganisation, UN-Behindertenrechtskonvention; Hölscheidt in Meyer/Hölscheidt (En. 60), Art. 26 Rn. 1.
- 72 Hölscheidt in Meyer/Hölscheidt (En. 60), Art. 26 Rn. 19; Heckmann MMR 2006, 6.
- 73 RL (EU) 2016/2102 v. 26.10.2016 über den barrierefreien Zugang zu den Websites und mobilen Anwendungen öffentlicher Stellen, ABl. EU v. 02.12.2016, L 327/1.

- 74 Degrave, Revue belge des Droit constitutionnel 2023, 230.
- 75 Martin-Jung, Sprich mit mir, Süddeutsche Zeitung (SZ) 18.03.2024, 16.
- 76 Degrave, Revue belge des Droit constitutionnel 2023, 241.
- 77 Hoffmann-Riem in Schmidt-Aßmann/Hoffmann-Riem, Verwaltungsrecht in der Informationsgesellschaft, 2000, S. 9, 49 f.; ähnlich Heckmann MMR 2006, 6.
- 78 Hornung in Schoch/Schneider, Verwaltungsrecht, Stand Nov. 2023, Vorb. § 3a Rn. 20-22; vgl. Botta NVwZ 2022, 1251.
- 79 BVerfG 03.03.2009 – 2 BvC 3/07, 2 BvC 4/07, Rn. 118, 156, NJW 2009, 2195.
- 80 Vgl. Art. 13, 50 Gesetz über künstliche Intelligenz, Europäisches Parlament v. 13.03.2024 (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
- 81 Dix in Hentschel/Hornung/Jandt (En. 26), S. 261 f.
- 82 BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 422.
- 83 Jandt, in Hentschel/Hornung/Jandt (En. 26), S. 88 f.
- 84 Schulz RDi 2023, 521.
- 85 Hornung in Schoch/Schneider, Verwaltungsrecht, Stand Nov. 2023, Vorb. § 3a Rn. 23.
- 86 Weitergehend Lorenz MMR 2022, 939, der generell keine zusätzlichen Kosten akzeptiert.
- 87 Kein Recht auf analog, 14.10.2022, [https://www.kommune21.de/meldung\\_39673\\_Kein+Recht+auf+analog.html](https://www.kommune21.de/meldung_39673_Kein+Recht+auf+analog.html).
- 88 Wir fordern digitale Grundrechte, 2. Fassung 2018, <https://digitalcharta.eu/>.
- 89 Prantl, Digitalzwang ist Diskriminierung, Interview mit Nellissen, <https://www.bagso.de/themen/digitalisierung/aktion-leben-ohne-internet/aktuelle-meldungen/interview-mit-heribert-prantl/>.

Nils Büschke

## Digitalzwang – ein Bericht aus dem Maschinenraum

Wir wollen den Anspruch auf ein Leben ohne Digitalzwang im Grundgesetz verankern. Dazu hat Digitalcourage eine Petition gestartet: „Für das Recht auf ein Leben ohne Digitalzwang ins Grundgesetz“ (<https://digitalcourage.de/recht-auf-leben-ohne-digitalzwang>). Die Petition wurde inzwischen von rund 40.000 Menschen unterschrieben. Die vielen emotionalen Rückmeldungen und eigentlich ausschließlich positiven Reaktionen überraschen uns bis heute immer wieder und geben uns Kraft weiter hartnäckig am Thema zu arbeiten.

### • Digitalzwangsmelder

Unsere Auseinandersetzung mit Digitalzwang reicht weit zurück und wurzelt in der jahrelangen Arbeit zu einzelnen Aspekten des Themas: Datensparsamkeit, die Ablehnung von Konto- oder Account-Zwang oder der Kampf gegen die großen geschlossenen Plattformen von Apple oder Google. Bereits im Jahr 2021 haben wir unseren Digitalzwangsmelder online gestellt (<https://digitalzwangsmelder.de/>), über den Menschen seitdem Fälle von Digitalzwang an uns melden können. Die Auseinandersetzung mit diesen Meldungen ließ uns irgendwann bewusst werden, dass

es hier ein größeres Problem gibt, das wir angehen wollen. Die Reaktionen auf den BigBrotherAward an die Deutsche Post DHL Group im Jahr 2023 (<https://bigbrotherawards.de/2023/deutsche-post-dhl>, s. S. 16) haben uns weiter darin bestärkt.

Seitdem wir im Mai letzten Jahres an die Öffentlichkeit gegangen sind, hat sich die Zahl der Digitalzwangsmeldungen an uns vervielfacht. Vieles geht über den online erreichbaren Digitalzwangsmelder oder per Mail ein – doch auch unser Postbote scherzte zwischenzeitlich, ob wir ein Gewinnspiel veranstalten würden, so viel Post wie er täglich bei uns abliefern würde. Und die Zahl der Meldungen ist bis heute auf einem hohen Niveau geblieben. Um diese Meldungen, die häufig zugleich herzerwärmend und sehr deprimierend zu lesen sind, soll es hier gehen.

Was bei der Sichtung der Meldungen als erstes ins Auge fällt: Privatwirtschaftliche Angebote der Freizeitgestaltung nehmen nur einen verschwindend geringen Anteil ein. Ob die Kurse im neuen Fitnessstudio ausschließlich über eine App gebucht werden können oder die Getränkekarte der Bar nur über einen QR-Code zu erreichen ist, löst bei den meisten Menschen wohl nur ein leichtes Kopfschütteln aus – und befördert die

Entscheidung beim nächsten Mal ein anderes Lokal zu besuchen.

Ganz anders sieht es abseits von Freizeitangeboten aus – bei Dingen, an denen es häufig kein Vorbei gibt: Bankgeschäfte, Versicherungen und Krankenkassen, Arztbesuche, der öffentliche Personen-Nahverkehr, die Deutsche Bahn, Telekommunikationsunternehmen oder Carsharing-Anbieter. Nicht zu vergessen Post und DHL. Neben dem Bereich der öffentlichen Verwaltung kommt in diesen Bereichen die Mehrzahl aller Meldungen rein. Zudem ist die Emotionalität dieser Meldungen eine ganz andere als im Bereich der Freizeitangebote – häufig bestimmt von einem Gefühl der Hilflosigkeit und der Ausgrenzung. Oft schreiben Menschen explizit, dass sie sehr dankbar sind, dass Digitalcourage das Problem in den Fokus der breiteren Öffentlichkeit bringt.

### • Schwerpunkt: eine digitalbürokratische „Verwaltung“

Der Bereich mit den meisten Meldungen ist die öffentliche Verwaltung. Das erklärt sich zum einen sicherlich dadurch, dass jede und jeder irgendwann mit ihr Kontakt kommt und es hier meist keine Alternativen und kein „dran vorbei mogeln“ gibt. Meinen

neuen Ausweis gibt es nur im Rathaus, den Führerschein nur bei der Fahrerlaubnisbehörde. Das am häufigsten gemeldete Digitalzwang-Beispiel aus dem Bereich der Verwaltung betrifft zudem meist alle Angelegenheiten, die im Rathaus zu erledigen sind: die Online-Terminvergabe. In viele deutsche Rathäuser und Bürgerbüros kommt nämlich inzwischen nur noch, wer vorher online einen Termin ausgemacht hat. Dass es Menschen gibt, die dazu nicht in der Lage sind, etwa weil eine körperliche Einschränkung sie daran hindert, scheint mancherorts jedoch ausgeblendet zu werden.

Was dabei immer wieder irritiert, ist die Kälte, mit der diese Regeln durchgezogen werden. Das gilt nicht nur für unsere öffentliche Verwaltung, sondern auch für die Bürokratie bei Banken, Krankenkassen oder Telekommunikationsunternehmen. Das Klima ist gefühlt ungnädiger geworden. Das System gibt vor, was erlaubt ist und wie ein Prozess zu laufen hat – ohne Raum für Abweichung und viel zu oft ohne Rücksicht auf Verluste. Wir haben unzählige Mitteilungen von Menschen, die – aus welchen Gründen auch immer – nicht in der Lage sind dieses oder jenes System zu nutzen. Häufig versuchen sie dann die Angelegenheit (also beispielsweise einen Termin im Rathaus zu buchen) im Gespräch am Telefon zu klären – doch rennen sie meist gegen eine Wand aus Ignoranz und Unverständnis. „Dann müssen Sie sich halt Hilfe holen!“ ist ein Satz, den ich in den Nachrichten an uns sehr häufig gelesen habe. Dabei wäre es oft möglich mit etwas Kreativität und Toleranz eine unbürokratische Lösung anzubieten.

#### • Privatwirtschaft

Doch auch abseits der öffentlichen Verwaltung gibt es genug Beispiele, die Menschen hilflos zurücklassen – gerne verbunden mit dem völlig unangebrachten erhobenen Zeigefinger sich dieser Entwicklung nicht verschließen zu können.

Bankgeschäfte beispielsweise werden immer schwieriger ohne Zugriff auf Computer und Internet oder Smartphone und App. Es mag sie noch geben, die lokal verwurzelten Banken, die für ihre Kund:innen ansprechbar und erreichbar

sind. Aber gemessen an den Einsendungen, die wir bekommen, werden sie weniger. Bargeld- oder gar Überweisungsautomaten im Eingangsbereich? Werden zunehmend abgebaut. Überweisungsträger? Nicht mehr vorgesehen oder so teuer, dass es einer Strafzahlung gleichkommt. Mitarbeiter am Schalter? Verweisen nur allzu gerne auf die ausschließlich zu nutzenden digitalen Prozesse. Und selbst wenn der Kunde gerne Online-Banking am eigenen Rechner nutzen möchte, stellen manche Banken ihre Autorisierungsprozesse (TAN-Generierung, etc.) inzwischen auf einen App-Only-Ansatz um.

Dieses Szenario wird uns häufig gemeldet: Als erstes wurden nach und nach alle Kontaktmöglichkeiten abgeschafft, die ohne IT-Technik funktionierten und am Ende läuft dann alles über eine App – inklusive gratis Überwachungstechnik und erzwungenem Vertragsverhältnis mit den App-Stores von Google oder Apple.

Gerne bemänteln Firmen ihre Digitalzwang-Schikanen als Maßnahmen zum Wohle der Umwelt und im Namen der Nachhaltigkeit. Das prominenteste Beispiel hierfür ist sicherlich die Deutsche Bahn und die Abschaffung der Plastik-Bahncard – was, als einzelner Vorfall betrachtet, einer der am häufigsten gemeldeten Sachverhalte war. Wobei Menschen zur Anschaffung eines stets aktuellen Smartphones oder anderer Hardware zu zwingen keineswegs nachhaltig ist.

Ein anderes aktuelles Beispiel aus dem Bereich der Krankenkassen: Der

Widerspruch gegen die elektronische Patientenakte. Bei vielen Krankenkassen scheint ein Widerspruch nur digital möglich zu sein. Selbst wenn der Kunde oder die Kundin zur Geschäftsstelle geht und freundlich darum bittet vor Ort Widerspruch einlegen zu dürfen, lautet die Antwort oft: Leider nicht vorgesehen. Nichts zu machen.

Diese Beispiele ließen sich nun endlos weiterführen – seien es Semestertickets an Universitäten oder der Besuch der Olympischen Spiele, der Wunsch ein Fahrrad zu leihen oder an Judo-Wettbewerben teilzunehmen (in diesen Fällen: alles nur mit Smartphone möglich). Doch der Kern der Meldungen ähnelt sich: Firmen und Organisationen verstecken sich immer häufiger nur allzu gerne hinter ihren digitalen Systemen – um jede Abweichung, sei sie noch so gut begründet, abzuschmettern – mit der simplen Begründung: Die Maschine sagt nein.

#### • Widerstand wirkt

Und daher sind wir überzeugter denn je: Der Kampf gegen Digitalzwang lohnt sich. Es geht um so viel mehr als irgendeinen Stand der Technik zu nutzen oder nicht. Es geht um Teilhabe und um Respekt. Und es geht um Rücksicht. Darum, möglichst vielen Menschen ein selbstbestimmtes Leben zu ermöglichen – ohne auf Hilfe anderer angewiesen zu sein. Dabei kann Technik durchaus helfen. Aber Technik, die „alternativlos“ ist oder uns gängelt, brauchen wir nicht.

**Wir fordern den Bundestag auf, ein  
Recht auf Leben ohne Digitalzwang ins  
Grundgesetz aufzunehmen!  
Forderung jetzt unterschreiben:**

<https://digitalcourage.de/recht-auf-leben-ohne-digitalzwang>

Rena Tangens

## BigBrotherAward 2023 – Deutsche Post DHL Group

Die Deutsche Post DHL Group erhält den BigBrotherAward 2023 in der Kategorie Verbraucherschutz für praktizierten Digitalzwang. Sie will die Kund:innen durch die Umstellung (der Funktionsweise) ihrer Packstationen dazu zwingen ein Smartphone und ihre „Post & DHL“-App zu nutzen. Die „Post & DHL“-App sendet ungefragt Daten an Tracking-Firmen. Dieser Digitalzwang gehört besonders gerügt, denn hier schließt ein ehemaliges Staatsunternehmen Bürgerinnen und Bürger von einer wichtigen Grundversorgung aus.

Lieber Preisträger,

„Leider haben wir Sie nicht angetroffen.“ Deshalb gibt es jetzt eine öffentliche Zustellung:

Der BigBrotherAward in der Kategorie Verbraucherschutz geht an die Deutsche Post DHL Group,

1. weil sie die Technik ihrer Packstationen so umgestellt haben, dass man dort kein Paket mehr abholen kann ohne Smartphone und die Nutzung der „Post & DHL“-App.
2. weil die „Post & DHL“-App sofort nach dem Start ungefragt munter Daten an Trackingfirmen sendet. Das ist illegal.
3. für den Versuch, sich den Pflichten der Grundversorgung bei der Briefzustellung zu entziehen, u.a. durch den Plan Postfilialen durch Automaten – sogenannte „Poststationen“ – zu ersetzen.

Erinnern Sie sich an die Zeiten, als Kinder noch unbeaufsichtigt draußen spielen durften? Manchmal haben die Streiche gespielt: Sie haben irgendwo an einer Haustür geklingelt – und sind dann schnell weggelaufen. Diese Kinder sind jetzt erwachsen und arbeiten heute bei DHL<sup>1</sup>.

Manchmal klingeln sie auch vorsichtshalber gar nicht erst, sondern werfen direkt eine Karte in Ihren Briefkasten, die Ihnen mitteilt, dass Sie nicht ange-

troffen wurden. Dann gibt es mehrere Möglichkeiten: Das Paket wurde einem freundlichen Nachbarn übergeben. Oder: Das Paket geht an ein Postamt, wo Sie es zu den vorgegebenen Öffnungszeiten („heute jedoch nicht“) abholen müssen. Oder es landet in einer DHL-Packstation. Wenn Sie Glück haben, in der Packstation beim Supermarkt um die Ecke. Wenn Sie Pech haben, bei irgendeiner am anderen Ende der Stadt.

Keine Frage, so eine Packstation kann praktisch sein. Man muss sich dafür anmelden. Bisher bekam man dann eine DHL-Kundenkarte. Mit der Kundenkarte und einer PIN für das Paket konnte man dann zu jeder Tages- und Nachtzeit das Paket abholen.

Nicht so nett ist die Überraschung, wenn Sie sich gar nicht bei der Packstation angemeldet haben, aber Ihr Paket trotzdem dorthin umgeleitet wurde.

Ganz besonders, wenn es sich bei der Packstation um das neue Modell handelt – die sogenannte „lean“ (also: schlanke) Packstation. Eine solche „schlanke“ Packstation hat kein Display mehr zur Bedienung. Nun stehen Sie ratlos davor und fragen sich, wie Sie denn jetzt an Ihr Paket kommen.

### Der Zwang zum Smartphone – Digitalzwang!

„Lean“ heißt, dass DHL nicht nur das Display eingespart hat, sondern auch das Kartenlesegerät und die Netzanbindung. Technisch gesehen bedeutet das: Ihr Smartphone muss eine Verbindung zur Packstation via Bluetooth Low Energy aufmachen. Und über die „Post & DHL“-App muss es eine Mobilfunk-Verbindung zum zentralen Rechenzentrum der Post herstellen. Ohne diese Verbindung zum Rechenzentrum ist so eine neue Packstation dumm wie Brot und weiß nicht mehr, was für wen in welchem Fach liegt. Die Post spart die eigenständige Netzanbindung der Packstationen ein – und nutzt jetzt für die Datenübertragung zwischen Pack-

station und Post-Server kackfroh das Smartphone der Kundinnen und Kunden.

Wenn die Packstation nun in einer Gegend mit schlechtem Mobilfunkempfang steht? Pech gehabt.<sup>2</sup> Wenn das Guthaben für Mobildaten auf Ihrem Gerät verbraucht ist? Pech gehabt. Und wenn Sie gar kein Smartphone haben? Dann können Sie das mit der Abholung komplett vergessen. Ist Ihnen schon klar, oder? Ohne Smartphone haben Sie eigentlich gar keine Lebensberechtigung mehr.

Dabei gibt es gute Gründe, kein Smartphone zu haben: Es gibt Menschen, die schlicht kein Geld dafür übrig haben. Andere sind vielleicht zu alt, um sich noch mit der Technik auseinanderzusetzen zu wollen. (Aber trotzdem gerne Pakete empfangen!). Und schließlich gibt es sehr Technik-affine Menschen, die gerade weil sie sich gut auskennen, nicht dauernd mit einem solchen Taschen-Spion herumlaufen wollen.

Nein, liebe Post & DHL: Es ist überhaupt nicht ok einfach vorauszusetzen, dass jede und jeder ein Smartphone haben muss.

### Die „Post & DHL“-App – erst senden, dann fragen

Selbst wenn Sie ein Smartphone besitzen, gibt es gute Gründe, die „Post & DHL“-App nicht darauf installieren zu wollen. So fängt die „Post & DHL“-App nach dem Start sofort munter an Daten an externe Stellen zu übertragen.

Der IT-Sicherheitsexperte Mike Kuetz hat das Verhalten der App gründlich geprüft und dabei Folgendes herausgefunden: Die App macht Verbindungen auf u.a. zu Google Firebase (USA), Adobe Inc. (USA), u.a. der Adobe Experience Cloud<sup>3</sup> und zu Google Firebase Remote Config (USA). Weiterhin zu Sentry<sup>4</sup>, und schließlich zum „Google Firebase Analytics“ Tracker.

Wohlgemerkt: Das passiert alles für Sie unsichtbar, noch bevor Sie irgendwie mit der App interagiert haben. Dann

erscheint – Sie haben es befürchtet – ein Cookie-Consent-Banner. Hier passiert das Übliche: Durch manipulatives Design versucht man Sie dazu zu verlocken auf den roten Button mit „Alle akzeptieren“ zu klicken.

Doch auch wer geschafft hat „Nur Auswahl bestätigen“ anzuklicken, ist damit keinesfalls vor weiteren Trackern gefeit. Sogleich wird eine weitere Verbindung zu Adobe aufgemacht und weitere Dateien zur Verhaltensmessung nachgeladen.

### Rechtliche Bewertung der App

Rechtsanwalt Peter Hense hat die „Post & DHL“-App juristisch geprüft. Sein Fazit: Sowohl die europäische Datenschutz-Grundverordnung (DSGVO) wie auch das TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz) werden sträflich missachtet. Denn die Übermittlung von Daten an Google und Adobe, beide in den USA ansässig, ist einwilligungspflichtig.<sup>5</sup> Die „Post & DHL“-App überträgt die Daten aber schon, bevor die Nutzer:innen das Cookie-Consent-Banner angezeigt bekommen. Einfach auf „Alle akzeptieren“ klicken reicht übrigens nicht für eine informierte Einwilligung. Denn dafür müsste vorher verständlich informiert werden, welche persönlichen wirtschaftlichen Konsequenzen es haben kann, wenn man einer Datennutzung durch Tracking zustimmt. Was die Post nicht tut. Also liegt keine gültige Einwilligung vor – und damit ist jede Datenverarbeitung auf dieser Basis schlicht rechtswidrig. Für solche Verstöße gegen geltendes Recht sieht die DSGVO übrigens deutliche Bußgelder vor: 4 % vom globalen Umsatz der Deutschen Post DHL (94 Milliarden Euro im Jahr 2022) sind eine Größenordnung, wo eigentlich auch das Management anfangen sollte, sich für Datenschutz zu interessieren...<sup>6</sup>

Mike Kuketz hat die Deutsche Post AG DHL über die technische und juristische Analyse der „Post & DHL“-App informiert. Die Antwort der Deutschen Post AG ist komplett uneinsichtig. In Kurzform: „Es ist alles in Ordnung, hier gibt es nichts zu sehen, bitte gehen Sie weiter.“

Dieser ehemalige Staatskonzern meint als Aktiengesellschaft geltendes Recht einfach missachten zu dürfen –

und hält sich offenbar für völlig unangreifbar.

Dabei wäre es durchaus möglich die Paketabholung datenschutz- und verbraucherfreundlich zu programmieren. Wir fragen uns, ob die mangelhafte Gestaltung von Packstationen und App durch böartige Absicht oder durch pure Unfähigkeit zustande kommt. Die Frage stellt sich nochmal neu, wenn man weiß, dass die Post / DHL gerade die Hälfte der zuständigen IT-Abteilung entlässt ... DHL macht sich einen schlanken Fuß bei der IT und will uns dann zwingen ihre schrottnige Software zu installieren.

### Das Greenwashing des Gilb

Der Zwang zur Nutzung von Smartphone und „Post & DHL“-App an den Packstationen und dazu die unberechtigte Datenübermittlung an Tracking-Firmen allein wären schon eines Big-BrotherAwards würdig. Oben drauf aber gebührt der Deutschen Post DHL auch noch ein Sonderpreis in der Kategorie „Heuchelei“.

Die neuen „lean“ Packstationen werden allen Ernstes mit Nachhaltigkeit, Umwelt- und Klimaschutz begründet. Ja, Mann – coole Idee, da oben Solarpanel draufzupacken. Auch die Paketzustellung an Packstationen wird als Klimaschutz verkauft, denn wenn die DHL-Fahrzeuge die Pakete gesammelt in den Packstationen ablaichen statt sie zuzustellen, spart DHL natürlich CO<sub>2</sub> ein. Das allerdings verbrauchen dann die Kundinnen und Kunden, die einzeln zur Packstation fahren müssen, um ihr Paket abzuholen.<sup>7</sup> In der Gesamtbilanz für das Klima wahrscheinlich kein Gewinn. Gewinn ist es aber für die Deutsche Post DHL.

Bei diesem BigBrotherAward geht es um die Tendenz, den schleichenden Druck auf alle Menschen sich auf Überwachungsstrukturen einzulassen: An einer Stelle wird zwingend ein Login verlangt, an einer anderen wird Bargeld nicht mehr akzeptiert, hier wird die Installation einer App gefordert, dort bekomme ich ohne Smartphone keine Informationen zum Service mehr – oder überhaupt keinen Service. Wer sich nicht fügt, dessen Alltag wird immer schwerer gemacht.

Das nennen wir „Digitalzwang“.<sup>8,9</sup> Warum geben wir jetzt ausgerechnet der Deutschen Post AG DHL einen Big-BrotherAward für Digitalzwang?

### Der Abbau der Grundversorgung

Dafür etwas Kontext: Die Post AG hat am 1. Januar 1995 den bis dahin staatlichen Briefdienst übernommen und damit auch die damit einhergehenden Verpflichtungen. Also: Grundversorgung für alle, Zuverlässigkeit, Zustellung auch auf die letzte Hallig.

Tatsächlich war der Briefdienst jahrelang die Cashcow der Post AG, sie hat fettes Plus gemacht. Trotzdem wurde das Porto immer weiter erhöht. Die Vermutung liegt nahe, dass damit die Paketpost quersubventioniert wurde, um mit billigen Paketpreisen die Wettbewerber vom Markt zu verdrängen.<sup>10,11</sup> Mittlerweile ist die Deutsche Post DHL Group zum weltweit führenden Logistikanbieter gewachsen.

Jetzt, wo der Paketdienst boomt und Briefe vielfach durch E-Mail ersetzt werden, ist der Briefdienst nicht mehr so ertragreich. Als die Post Anfang 2023 bestreikt wurde, drohte die Deutsche Post AG den Streikenden prompt damit die Briefzustellung noch in diesem Jahr einfach abzustoßen. Und bei Neuverhandlungen dann nur noch mit billigen Subunternehmen zu arbeiten. Eine Post, die keine Briefe mehr zustellt?!

Die Pflichten der Post AG sind im Postgesetz und in der Post-Universaldienstleistungsverordnung festgehalten. Doch diese Pflichten erfüllt die Post AG schon seit Jahren nicht mehr korrekt. Wegen langer Laufzeiten und schlechter Qualität der Briefzustellung und der mangelnden Versorgung mit Postfilialen, speziell auf dem Land, gibt es eine ständig steigende Zahl von Beschwerden bei der Bundesnetzagentur.<sup>12</sup>

Die Deutsche Post AG DHL bemüht sich nun keineswegs diese Mängel zu beheben. Sondern sie will die Mängel weg-definieren und sich der Pflichten entledigen: Sie verlangt Änderungen im Postgesetz und in der Post-Universaldienstleistungsverordnung. Ziel: Die verlängerte Laufzeit für Briefe wird einfach legalisiert. Wenn die Briefe doch am nächsten Tag ankommen sollen, sollen wir in Zukunft erhöhtes Porto

zahlen. Die Aufgaben der Postfilialen sollen zukünftig durch weitere Automaten, sogenannte „Poststationen“ erfüllt werden können – das sind aufgemotzte Packstationen, die dann auch Briefdienste anbieten.

Diese „Poststationen“ sind nicht barrierefrei<sup>13</sup>: Die Fächer sind für Kinder, Rollstuhlfahrer:innen und Kleinwüchsige nicht erreichbar, die Bedienung ist für Blinde schwierig. Für alle, die Hilfe oder Beratung brauchen, gibt es anders als in den Filialen keinen Menschen mehr vor Ort. Und schließlich werden die Poststation-Automaten kein Bargeld mehr annehmen. Also können Sie in Zukunft ohne elektronische Spuren zu hinterlassen keine Briefmarke mehr kaufen. Ein weiterer Fall von Digitalzwang.

Der derzeit regierenden Ampelkoalition hat die Post AG die Idee für die Postgesetz-Änderungen jeweils passend schmackhaft gemacht. Der SPD irgendwie mit Modernisierung, der FDP mit Förderung des Wettbewerbs und den Grünen mit dem Klimaschutz. Es steht zu befürchten, dass das Postgesetz noch 2023 im Sinne der Gewinnvermehrung der Deutschen Post DHL Group geändert wird.

Warnung an die Bundestagsabgeordneten, Bundesnetzagentur und die Klima-Engagierten im Wirtschaftsministerium: Lassen Sie sich nicht einwickeln! Und stoppen Sie den Umbau der Packstationen zu solchen mit Smartphone- und App-Zwang. Bisher gibt es erst etwa 2.000 neue, aber noch rund 10.000 alte Packstationen, die weiterhin mit Kundenkarte und PIN funktionieren könnten, wenn die Post es denn zuließe. Es ist also nicht zu spät.

Es geht nicht um einen einzelnen Tracker. Sondern es geht um ein ganzes Universum von Dauerüberwachung. Es geht hier auch nicht um irgendeinen Spielkram, den es nur per Smartphone gäbe. Sondern es geht um etwas so Grundlegendes wie an ein Paket zu kommen, das an mich geschickt wurde. Es geht nicht um die Kosten einer einzelnen Briefmarke. Sondern um die rücksichtslose Haltung Gewinne zu privatisieren und die Verpflichtungen auf die Allgemeinheit abzuwälzen. Und schließlich geht es um die Tendenz Menschen bei jeder alltäglichen Handlung der Überall-und-

nebenbei-Überwachung auszuliefern.

Liebe Deutsche Post AG DHL – die Benachrichtigung über Ihren BigBrother-Award ist Ihnen zugegangen. Nein, der BigBrotherAward wird Ihnen nicht zugestellt – Sie müssen ihn sich schon abholen. Das geht auch ohne App.

Herzlichen Glückwunsch!

(Die Preisverleihung mit der obigen Laudatio erfolgte am 28.04.2023)

- 1 Dank für diese Erkenntnis an Ingo Borchers und seinen „Satirischen Jahresrückblick“ im Dezember 2022 im Theater am Alten Markt in Bielefeld.
- 2 Ja, das gibt es tatsächlich!
- 3 Der Analytics-Server heißt „smetrics.dhl.de“ und tut damit so, als ob er bei DHL läge. Doch dann verweist er weiter auf „dhl.de.ssl.sc.omtrdc.net“. Anders als auf den ersten Blick vermutet, findet die Erfassung/Verarbeitung der Analyse-Daten also nicht bei der Deutschen Post statt, sondern in Adobes Experience Cloud. Die Domain „\*.omtrdc.net“ gehört nämlich zu Adobe.
- 4 Sentry: Der Tracker Google Analytics wurde durch Sentry (<https://sentry.io/>) ersetzt, das von DHL unter der Domain „quality.dpdl.com“ selbst gehostet wird. Wie der Name „quality“ schon sagt, ist das Tracking und damit zur reinen Funktionserbringung der App nicht erforderlich.
- 5 Die gesetzlichen Vorgaben für eine gültige Einwilligung sind in § 25 TTDSG geregelt. Vgl. (EuGH, Urt. v. 30.04.2014 – C-26/13, Rn. 71 – Kásler/OTP Jelzálogbank Zrt. <https://curia.europa.eu/juris/liste.jsf?language=de&num=C-26/13>).
- 6 Für die im Gesetz unter Art. 83 Abs. 5 DSGVO aufgelisteten, besonders gravierenden Verstöße beträgt der Bußgeldrahmen bis zu 20 Millionen Euro oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen

Geschäftsjahr, je nachdem, welcher Wert der höhere ist.

- 7 Ja, in der Stadt ist die Packstation-Dichte hoch genug, so dass Menschen auch zu Fuß oder per Fahrrad abholen können. Aber auf dem Land wird das Auto die Regel sein.
- 8 „Digitalzwang“-Grundlagenartikel <https://digitalcourage.de/digitalzwang>.
- 9 Für Digitalzwang gibt es viele Beispiele. Digitalcourage sammelt Meldungen dazu im „Digitalzwangmelder“: <https://civi.digitalcourage.de/digitalzwangmelder>. Ja, Digitalcourage nimmt auch Meldungen per Brief an :).
- 10 Das sagt der Wettbewerbsrechtler Prof. Haucap. Welt.de, 22.02.2023, Birger Nicolai: Interview mit Prof. Justus Haucap. <https://www.welt.de/wirtschaft/plus243900307/Deutsche-Post-Ich-koennte-auf-den-Montag-als-Zustelltag-verzichten.html>.
- 11 Siehe Gutachten Justus Haucap und Christiane Kehler, 1/2016 für BIEK: Unfairer Wettbewerb im Postmarkt. Deutsche Post AG/DHL: Quersubventionierung in den Paketmarkt, Marktherrschaft und unzureichende Regulierung <https://www.biek.de/download.html?getFile=148>.
- 12 Golem.de, 16.12.2022: Bundeswirtschaftsministerium: Briefzustellung an Packstationen könnte möglich werden. <https://www.golem.de/news/bundeswirtschaftsministerium-briefzustellung-an-packstationen-koennte-moeglich-werden-2212-170560.html>; Zitat: „In diesem Jahr zählte die Bundesnetzagentur schon mehr als 37.000 Beschwerden über die Brief- und Paketdienste, mehr als doppelt so viele wie im Vorjahr. Ein Großteil der Reklamationen bezieht sich auf die Briefzustellung der Post.“
- 13 Die fehlende Barrierefreiheit kritisiert auch der Sozialverband VdK. Siehe Logistik-Watchblog.de, 03.02.2023: Nicht barrierefrei: Sozialverband kritisiert Postautomaten. <https://www.logistik-watchblog.de/neuheiten/3830-barrierefrei-sozialverband-kritisiert-postautomaten.html>.



Foto: Deutsch Post DHL Group (Screenshot aus einem YouTube-Video)

padeluum

## BigBrotherAward 2024 in der Kategorie „Mobilität“: Der Preis geht an die Deutsche Bahn AG

Die Deutsche Bahn AG wird ausgezeichnet, weil sie Digitalisierung dafür einsetzt, um anonymes Reisen nach und nach komplett unmöglich zu machen.

Kaum ein Unternehmen hat in den vergangenen Jahren seine Kundinnen und Kunden so massiv gegen sich aufgebracht wie die Deutsche Bahn. Es geht hier nicht um Verspätungen, geschlossene Bahn-Bistros oder sonstige scheinbare Lässlichkeiten. Es geht um Digitalzwang, es geht um die Missachtung von Datenschutzprinzipien wie Datensparsamkeit – und für viele Reisende geht es um existentielle Dinge:

1. Die Bahncards 50 und 25, die seit Mitte 2024 nicht mehr als Karte, sondern nur noch zum Vorzeigen auf dem Smartphone herausgegeben werden.
2. Sparpreis- und Supersparpreis-Tickets werden mittlerweile nicht mehr am Automaten verkauft. Beim Kauf im Reisezentrum muss jetzt zwingend eine Mobilfunknummer oder eine Mailadresse angegeben werden.
3. Das Deutschland-Ticket wird von der DB ausschließlich als elektronisches Ticket auf dem Smartphone angeboten.
4. Dazu kommt, dass das Fahrkarten-Kaufen am Automaten immer mehr erschwert wird: Automaten werden abgebaut oder umgerüstet und akzeptieren dann kein Bargeld mehr. Die Automaten, die Bargeld nehmen, ziert oft ein Schild „defekt“.

Bei Betrachtung jeder einzelnen Maßnahme könnten wir immer noch denken, dass da die Folgen nicht bedacht wurden, dass es einfach schlecht gemachte Digitalisierung ist. Aber wenn wir einen Schritt zurücktreten, erkennen wir ein Muster – Steinchen für Steinchen eines Überwachungs-Mosaiks. Die Deutsche Bahn setzt offenbar alles daran, um anonymes Bahnreisen unmöglich zu machen.

Schauen wir da einmal genauer hin:

### Der erste Stein: Die Bahncards 50 und 25

Die Bahncards 50 und 25 gibt's nicht mehr als Karte. Die Begründung ist, dass jetzt sowieso alles digital wird – da kann man halt nichts machen. Ihr werdet alle digitalisiert – Widerstand ist zwecklos. Besonders scheinheilig aber ist die Behauptung der Bahn-PR, dass die DB mit dieser Maßnahme 30 Tonnen Plastikmüll pro Jahr einsparen und damit besonders umweltbewusst handeln würde. Das müssen wir jetzt gerade mal auseinanderpflücken: Nein, es ist nicht umweltfreundlich Reisende zur Anschaffung eines modernen Smartphones zu nötigen. Smartphone-Nutzung ist keineswegs per se nachhaltig, denn die Elektronikproduktion und der Betrieb der Rechenzentren verbraucht viele Ressourcen.

Im Übrigen bräuchte es auch gar kein Plastik für eine Bahncard. Es gibt längst andere innovative Lösungen. Die GLS-Bank macht es vor: Sie produziert ihre Bankkarte auf Holzbasis. Damit hat die GLS sogar auf beleuchteten Werbetafeln in ICEs geworben. Und beim Bestellen könnte die Bahn einfach abfragen, ob man als Kunde auf eine physische Karte verzichten möchte.

Aber seien wir ehrlich – es geht der Bahn überhaupt nicht um Plastik. Es geht um den Zwang zur App – und ums Datensammeln.

Den Aufschrei aus der Bevölkerung, der auf die Ankündigung folgte, die Bahncard ab Mitte 2024 nur noch elektronisch auf Smartphone auszugeben, dürfte man bis in die Vorstandsetage gehört haben. Es gab massenweise Protestschreiben, E-Mails und Bahncard-Kündigungen, die Digitalcourage in Kopie erreicht haben.

Wir haben erschütternde Briefe bekommen. „Ich kann meine Enkel nicht

mehr so oft besuchen, weil das ohne Bahncard 50 zu teuer ist und mit der Bahncard auf dem Smartphone komme ich nicht zurecht.“

Wegen der massenhaften Proteste rüdete die DB ein bisschen zurück und gestattet nun, dass die Bahncard beim Bestellen im Reisezentrum als PDF-Ersatzdokument ausgedruckt wird. Das ist aber nur eine vorübergehende Maßnahme, um den Protest gegen den Digitalzwang abzufedern. Die DB schreibt das auch in diversen Antworten an Bahncard-Kund:innen: Das ist nur eine Übergangslösung. Ihr werdet alle digitalisiert.

### Ein weiterer Stein: Sparpreis- und Supersparpreistickets

Diese günstigen Tickets, von denen sowieso immer viel zu wenige verfügbar sind, gibt es nun nicht mehr am Automaten zu kaufen. Denn seit ein paar Monaten müssen Reisende beim Kauf eines Sparpreis- oder Supersparpreis-Tickets zwingend persönliche Daten angeben, nämlich eine Mailadresse. Oder eine Mobilfunknummer. Und das geht nicht am Automaten, nur im Reisezentrum. Oder online natürlich. Schwups, und schon haben wir eine Personalisierung des Tickets. Jeder Kauf, jeder Klick wird zum Stein im Mosaik. Und das ist ein Problem für Menschen, die kein Smartphone besitzen. Auch hier liefert die DB wieder ein vorgeschobenes Argument: Die Telefonnummer oder ersatzweise die Mailadresse würde gebraucht, um mit den Reisenden Kontakt aufzunehmen, falls sich ihr Zug verspäten oder früher fahren würde. Da lachen ja die Hühner. Inzwischen hat auch Alexander Roßnagel, der Hessische Landesdatenschutzbeauftragte, der für den DB-Konzern zuständig ist, klargestellt: Der Zwang, Handynummer oder E-Mail-Adresse anzugeben, ist datenschutzrechtlich unzulässig.<sup>1</sup>

## Deutschlandticket

Auch die Politik und Verbände legen Mosaiksteinchen um Mosaiksteinchen dazu: Deutschlandticket? Semestertickets? Beides soll es bei der Bahn ausschließlich in der Digitalzwang-Edition geben. Die Grundlage dazu steht im Regionalisierungsgesetz<sup>2</sup>: „[Das Deutschlandticket] soll in digitaler Form erhältlich sein.“ Mein Kleinhirn sagt mir: da steht „soll“, nicht „muss“.<sup>3</sup> Von Ausschließlichkeit ist keine Rede. Aber die Bahn besteht darauf.

So haben wir derzeit auf der einen Seite Menschen, die kein Smartphone besitzen – oder die zwar eins haben, aber denen das Bedienen von Technik zu komplex ist, die sich unter Druck gesetzt fühlen und ihre Bahncard kündigen, weil sie denken, dass sie diese gar nicht mehr nutzen können. Auf der diametral entgegengesetzten Seite sind die technisch versierten Menschen, die ein freies Betriebssystem auf ihrem Gerät haben und deswegen nicht an die App-Stores von Google oder Apple rankommen. Denn ausschließlich dort bekommt man (anders als bei vielen Fahrplan-Apps) die zur Nutzung zwingend notwendige App „DB Navigator“. Diese Menschen haben viel Ahnung von Datenverarbeitung – genau deshalb achten sie auf ihre informationelle Selbstbestimmung und wollen nicht alenthalben eine Datenschleimspur hinterlassen.

Der Verbraucherzentrale Bundesverband (vzbv) hat in seiner repräsentativen Umfrage<sup>4</sup> mit dem Titel „Wahlfreiheit in der Mobilität“ untersucht, wie die Bevölkerung zu digitalen Tickets und ausschließlich digitalen Tickets steht. Ein Ergebnis der Studie: Obwohl ein Großteil der Bahnfahrer:innen ihre Tickets online kauft, finden trotzdem 81 % der Befragten, dass Verkehrsunternehmen wie die Bahn in der Verantwortung stehen auch Menschen ohne Smartphone oder Internetzugang den Fahrkartenkauf zu ermöglichen.

## Fahrkartenautomaten

Die Frage, wer, wie, wann und wohin fährt, ist für die Bahn offenbar von großem Interesse. Fahrkartenautomaten werden systematisch verknappert oder

stehen – da, wo die Deutsche Bahn noch Regionalstrecken bedienen darf – unrepräsentiert an trostlosen Haltepunkten. Und Bargeld wird meist nicht angenommen – auch hier ist er, der Zwang zum Digitalen; zum unbaren Zahlen mit Geldkarte.<sup>5</sup>

Und, fast vergessen: Anders als früher werden in Zügen der Deutschen Bahn keine Fahrkarten mehr im Zug verkauft.

## „DB Navigator“

Das nächste Überwachungs mosaiksteinchen: die App „DB Navigator“. Eine App, die nicht nur Tickets verkauft und Fahrpläne anzeigt, sondern auch still und heimlich die digitalen Fäden spinnt, mit denen wir kontrolliert werden. Tracker.

Die Deutsche Bahn drängt darauf, dass alle die App „DB Navigator“ nutzen. Die schnüffelt ihre Nutzer:innen allerdings aus und gibt eine Menge Daten über sie weiter. Der Trick: Die Bahn deklariert alle Tracker, die sie unbedingt haben will, einfach als „erforderlich“. Bei der neuen Version der App sind es insgesamt sechs Unternehmen – unter anderem Adobe und Google –, deren Mitwirkung laut Bahn angeblich zwingend erforderlich ist und an die deshalb Daten abfließen. Ohne dass die Bahn ihren Kund:innen eine Möglichkeit einräumt das abzuschalten. Technisch sind diese Tracker aber kein bisschen „notwendig“.

Vor zwei Jahren – 2022 – hat Digitalcourage die Deutsche Bahn wegen dieser nicht abwählbaren Tracker verklagt. Sie haben sicher davon gehört. Zusammen mit dem Blogger und Sicherheitsexperten Mike Kuketz und mit Unterstützung des Rechtsanwalts Peter Hense warten wir seit nunmehr zwei Jahren auf einen Termin für eine Verhandlung.

Wir haben jetzt einige Mosaiksteinchen zusammgelegt. Da sind noch viele Lücken, die den Rahmen dieser Laudatio sprengen würden. Aber wir können im Mosaik bereits ein Muster erkennen.

Diejenigen, deren Zug tatsächlich fährt, werden von freundlichen Zugbegleiter:innen kontrolliert. Diese haben ein Smartphone, mit dem sie die Ticketkontrolle durchführen. Installiert ist darauf eine App, die eine Kontrollhistorie anlegt – wodurch der Reiseweg jedes Fahrgastes nachverfolgbar wird.

Der Name dieser App ist übrigens: Mosaik.

Wir würden diesem Mosaik gerne ein eigenes Muster geben: Umweltfreundlich, datenschutzfreundlich. Eine Bahn, die die Bedürfnisse und das Wohlgefühl der Reisenden ernst nimmt. Zu diesem „datenschutzfreundlich“ und „Wohlgefühl“ gehört auch anonym und unüberwacht mit der Bahn reisen zu können.

Warum die Möglichkeit, sich unerkannt in unserem Land frei bewegen zu können, wichtig ist? Weil wir als Bürger:innen und Bürger an allererster Stelle der Souverän dieses Staates sind und nicht Mobilitätsverschiebemasse, Verdachtsfall oder Marketingobjekt. Deshalb wollen wir uns frei bewegen können. Auch mit und gerade mit der Bahn.

Herzlichen Glückwunsch, Deutsche Bahn AG, zum BigBrotherAward 2024!

(Diese Laudatio wurde anlässlich der Preisverleihung am 11.10.2024 vorgelesen)

- 1 tagesschau.de, 02.10.2024: Ausschluss von Kunden Datenschützer kritisieren Regeln für Sparpreistickets. <https://www.tagesschau.de/wirtschaft/verbraucher/bahn-sparpreis-ticket-datenschutz-100.html>.
- 2 <https://www.gesetze-im-internet.de/regg/RegG.pdf>.
- 3 In einem Gesetzestext bedeutet das Wort „soll“ in der Regel „muss, wenn es geht“. Es drückt eine Verpflichtung aus, aber keine Ausschließlichkeit. Es unterscheidet sich vom Wort „muss“, das eine absolute Verpflichtung darstellt. Das bedeutet, dass der Verpflichtete der Soll-Vorschrift nachkommen muss, es sei denn, es liegen triftige Gründe vor, die eine Ausnahme rechtfertigen.
- 4 [https://www.vzbv.de/sites/default/files/2024-09/Charts\\_Wahlfreiheit-Mobilit%C3%A4t.pdf](https://www.vzbv.de/sites/default/files/2024-09/Charts_Wahlfreiheit-Mobilit%C3%A4t.pdf).
- 5 <https://web.archive.org/web/20241008165411/https://www.deutschernahverkehrstag.de/umfrage-zum-vertrieb-der-zukunft/>.

Hans-Hermann Schild

## Die E-Rechnung – eine aufgedrängte Bereicherung oder Zwang?

Durch das Wachstumschancengesetz vom 27.03.2024<sup>1</sup> wurde mit Artikel 23 „Weitere Änderung des Umsatzsteuergesetzes“ so ganz nebenbei § 14 UStG dahin geändert, dass die E-Rechnung im Bereich B2B ab dem 01.01.2025 zwingend eingeführt worden ist.<sup>2</sup> Der Bereich B2B bezieht sich auf jede Person, die dem Umsatzsteuerrecht unterliegen. Wichtig ist nur, dass sie den Unternehmerbegriff erfüllt. Dies ist, wer eine gewerbliche oder berufliche Tätigkeit selbstständig ausübt, unabhängig davon, ob er nach anderen Vorschriften rechtsfähig ist (§ 2 UStG), es sei denn, die Person ist ein Kleinunternehmer. Dies ist jemand, dessen Gesamtumsatz im vorangegangenen Kalenderjahr 25.000 Euro nicht überschritten hat (dazu § 19 UStG). Fahrausweise und Rechnungen über Kleinbeträge bis 250 Euro sind von der E-Rechnung ausgenommen.

### Baustein der Digitalisierung

Nach dem Erlass über die Ausstellung von Rechnungen nach § 14 UStG (Einführung der obligatorischen elektronischen Rechnung bei Umsätzen zwischen inländischen Unternehmen ab dem 1. Januar 2025)<sup>3</sup> stellt die E-Rechnung einen wesentlichen Baustein zur Digitalisierung des Geschäftsverkehrs dar. Ab dem 01.01.2025 wird durch § 14 Abs. 1 UStG der Begriff der elektronischen Rechnung neu definiert. Zukünftig liegt eine elektronische Rechnung (also E-Rechnung) nur dann vor, wenn die Rechnung in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird und eine elektronische Verarbeitung ermöglicht (§ 14 Abs. 1 S. 3 UStG). Das strukturierte elektronische Format einer elektronischen Rechnung muss entweder der europäischen Norm für die elektronische Rechnungsstellung und der Liste der entsprechenden Syntaxen gemäß der Richtlinie 2014/55/EU des Europäi-

schen Parlaments und des Rates vom 16. April 2014 über die elektronische Rechnungsstellung bei öffentlichen Aufträgen<sup>4</sup> entsprechen (§ 14 Abs. 1 Satz 6 Nummer 1 UStG)<sup>5</sup> oder aber kann zwischen Rechnungsaussteller und Rechnungsempfänger vereinbart werden. Voraussetzung für eine solche Vereinbarung ist, dass das verwendete Format die richtige und vollständige Extraktion der nach dem UStG erforderlichen Angaben aus der E-Rechnung in ein Format ermöglicht, das der EN 16931 entspricht oder mit dieser interoperabel ist (vgl. § 14 Abs. 1 Satz 6 Nummer 2 UStG).<sup>6</sup>

Sollte der geneigte Leser wissen wollen, was sich unter EN 16931 verbirgt, so findet man diese Norm nicht so richtig. Man findet die kostenpflichtige „DIN EN 16931-1 – Elektronische Rechnungsstellung – Teil 1: Semantisches Datenmodell der Kernelemente einer elektronischen Rechnung; Deutsche Fassung EN 16931-1:2017+A1:2019 + AC:2020“ beim Deutschen Institut für Normung e. V.<sup>7</sup> Eine DIN EN 16931-8 gibt es im Entwurfsstadium. Dies scheint schon ein „ernsthafter“ Beitrag zur Normenklarheit bei der Finanzverwaltung zu sein. Denn eine EN 16931 als solche gibt es beim Deutschen Institut für Normung e. V. nicht. Daher spricht der Erlass des Bundesfinanzministeriums wohl bewusst von einer „Normenreihe EN 16931“. Ganz einfach ausgedrückt: Die E-Rechnung basiert auf einem XML-Format, das in erster Linie der maschinellen Verarbeitung dient und sich nicht für eine Sichtprüfung eignet. Durch den Einsatz von Visualisierungsprogrammen kann der XML-Datensatz allerdings auch für den Menschen lesbar dargestellt werden.

### E-Rechnung für die Wirtschaft

Demgegenüber kennt das BSI die CEN 16931, eine europäische Norm für ein einheitliches Austauschformat von Rechnungen im öffentlichen Bereich. Dies bezieht sich wiederum auf E-Rech-

nungen, die nach Erfüllung von öffentlichen Aufträgen und Aufträgen sowie zu Konzessionen von Stellen im Sinne von § 159 Abs. 1 Nummer 1 bis 4 des Gesetzes gegen Wettbewerbsbeschränkungen ausgestellt wurden (§ 4a Abs. 1 E-Government-Gesetz, EGovG). Diese Regelung beruht wiederum auf der RiLi 2014/55/EU über die elektronische Rechnungsstellung bei öffentlichen Aufträgen<sup>8</sup>, welche sich ausschließlich auf die Rechnungslegung bei öffentlichen Aufträgen und gerade nicht auf alle Rechnungen im B2B-Bereich bezieht. In diesem Bereich ist auch ein sicherer Datenaustausch der Rechnungen gegeben.<sup>9</sup> Der vom Rechnungssteller präferierte Übertragungsweg ist in diesem Fall vor dem Rechnungsversand auszuwählen und – ja, leider auch kompliziert – zu eröffnen. Dazu gibt es noch eine Verordnung über die elektronische Rechnungsstellung im öffentlichen Auftragswesen des Bundes vom 13. Oktober 2017<sup>10</sup>, die durch Art. 76 der Verordnung vom 19. Juni 2020<sup>11</sup> geändert worden ist. Dies alles gilt aber für die „normale“ neu geschaffene E-Rechnung gerade nicht.

Vorliegend hat der nationale Gesetzgeber EU-Recht einfach auf alle Bereiche des Wirtschaftsverkehrs ausgeschüttet. Nach der amtlichen Begründung zu Art. 23<sup>12</sup> wird darauf hingewiesen, dass „der Rat .... die Bundesrepublik Deutschland auf Grundlage von Artikel 395 der Richtlinie 2006/112/EG ermächtigt (habe) die Verwendung elektronischer Rechnungen, die von im Hoheitsgebiet Deutschlands ansässigen Steuerpflichtigen ausgestellt wurden, nicht von einer Zustimmung des im deutschen Hoheitsgebiet ansässigen Rechnungsempfängers abhängig zu machen (ABL. L 188 vom 27.07.2023, S. 42). Auf dieser Grundlage kann eine obligatorische eRechnung für inländische Umsätze im zwischenunternehmerischen Bereich eingeführt werden. In Umsetzung dieser Ermächtigung werden im Inland ansässige Unternehmer

*für ihre steuerbaren und steuerpflichtigen Umsätze zur Ausstellung einer eRechnung verpflichtet, wenn diese Umsätze an andere im Inland ansässige Unternehmer für deren Unternehmen erbracht werden. Umsätze an Unternehmer in anderen Mitgliedstaaten und an Endverbraucher sind von dieser Verpflichtung nicht betroffen.“*

Die Regelungen zur verpflichtenden Verwendung von E-Rechnungen gelten genauso für die Rechnungsausstellung in Form einer Gutschrift (§ 14 Abs. 2 Satz 5 UStG) sowie für Rechnungen

- über Umsätze, für die der Leistungsempfänger die Steuer schuldet (§ 13b UStG), wenn sowohl Leistender als auch Leistungsempfänger im Inland ansässig sind,
- die von Kleinunternehmern (§ 19 UStG) ausgestellt werden,
- über Umsätze, die der Durchschnittsatzbesteuerung für land- und forstwirtschaftliche Betriebe unterliegen (§ 24 UStG),
- über Reiseleistungen (§ 25 UStG) und
- über Umsätze, für welche die Differenzbesteuerung (§ 25a UStG) angewendet wird.

Sie gelten auch, wenn der Rechnungsempfänger ein Unternehmer ist, der Kleinunternehmer bzw. Land- und Forstwirt ist oder ausschließlich steuerfreie Umsätze (z. B. Vermieter einer Wohnung) ausführt. Ebenso gelten die Regelungen, wenn nur Teile der abgerechneten Leistungen der Pflicht zur Verwendung einer E-Rechnung unterliegen (z. B. bei teilweise steuerpflichtigen, teilweise nach § 4 Nummer 8 bis 29 UStG steuerfreien Umsätzen).

Die E-Rechnung gilt auch für Ärzte. Erstellt ein Arzt z. B. ein Gutachten für eine Krankenversicherung, so ist dieses umsatzsteuerpflichtig und der Arzt muss seine Leistung in der Form der E-Rechnung abrechnen. Zwar sind Versorgungsleistungen im Bereich der Gesundheit von Ärzten in der Regel umsatzsteuerbefreit, dies gilt allerdings nicht bei Gutachten und ähnlichen Tätigkeiten. Hier sind Ärzte Unternehmer i. S. d. Umsatzsteuergesetzes und es fällt Umsatzsteuer an. Dies mit der Folge, dass ggf. der Patient und die Diagnose auf der Rechnung mit aufzunehmen sind.

## Datenschutz bei E-Rechnung?

Doch wie wird diese E-Rechnung von dem Arzt an die Versicherung übersandt? In einen Briefumschlag passt sie nicht. Dies ist nicht weiter geklärt. Der Erlass über die Ausstellung von Rechnungen des Bundesfinanzministeriums sagt dazu lapidar, auf „*welchen zulässigen Übermittlungsweg sich die Vertragsparteien einigen, ist zivilrechtlich zwischen ihnen zu klären. Für die Übermittlung von E-Rechnungen kommen beispielsweise der Versand per E-Mail, die Bereitstellung der Daten mittels einer elektronischen Schnittstelle, der gemeinsame Zugriff auf einen zentralen Speicherort innerhalb eines Konzernverbundes oder die Möglichkeit des Downloads über ein Internetportal in Betracht.*“

Dies bedeutet letztendlich die Übermittlung von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO über eine E-Rechnung kraft gesetzlichen Zwangs.<sup>13</sup> Die Ausnahmeregelung des Art. 9 Abs. 2 lit. g) DSGVO dürfte da wohl schwer Anwendung finden. Denn dass das Recht des Mitgliedstaats – hier das Umsatzsteuerrecht – bezüglich der E-Rechnung als Datenverarbeitung in einem angemessenen Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, und aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist, ist nicht ersichtlich.

Schnittstellen und zentrale Speicherorte kommen vielleicht bei großen Unternehmen in Betracht. Der Regelfall wird mit hoher Wahrscheinlichkeit die E-Mail werden. Eine solche kann unterwegs abgefangen und geändert werden und damit auch die E-Rechnung.<sup>14</sup>

Nach Auffassung des OLG Schleswig ist die Transportverschlüsselung, beim Versand der Mail in der Form von SMTP über TLS, unzureichend und nicht zum Schutz der Daten „geeignet“ im Sinne der DSGVO. Gerade bei sensiblen oder persönlichen Inhalten komme nur eine Ende-zu-Ende-Verschlüsselung in Betracht, wenn durch Verfälschung der angehängten Rechnung für den Kunden ein hohes finanzielles Risiko besteht.<sup>15</sup>

Natürlich steht es dem Unternehmer frei sich zur Erstellung und/oder Übermittlung von E-Rechnungen externer Dienstleister zu bedienen. „In diesem Fall hat der leistende Unternehmer sicherzustellen, dass der externe Dienstleister die Einhaltung der sich aus den §§ 14, 14a UStG ergebenden formalen Voraussetzungen gewährleistet.“<sup>16</sup> Also besteht die Möglichkeit der Auftragsverarbeitung nach Art. 28 DSGVO. Hier bedarf es eines Auftragsverarbeiters, der hinreichende Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und er den Schutz der Rechte der betroffenen Person gewährleistet. Mithin eines Vertrages über die Auftragsverarbeitung mit allem, was Art. 28 DSGVO da so vorsieht. Eine erhebliche Verwaltungsvereinfachung und Entbürokratisierung scheint dies gerade nicht zu sein.

Auf jeden Fall weist der Erlass darauf hin, dass ab dem 1. Januar 2025 für inländische Unternehmer die Notwendigkeit besteht eine E-Rechnung empfangen zu können. Hierfür reiche es aus, wenn der Rechnungsempfänger ein E-Mail-Postfach zur Verfügung stelle.<sup>17</sup> Entspricht ein übersandter Datensatz nicht den Anforderungen an eine E-Rechnung, könne der zivilrechtliche Anspruch auf Erteilung einer Rechnung vor den ordentlichen Gerichten geltend gemacht werden.<sup>18</sup>

Auch ist das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO anzupassen, ebendies gilt für die Informationspflichten nach Art. 12 ff. DSGVO. Die RiLi 2014/55/EU hatte hingegen erkannt, dass E-Rechnungen personenbezogene Daten enthalten können. Insoweit wird in ErwG 20 RiLi 2014/55/EU ausgeführt, dass die Kommission ebenfalls vorschreiben solle, dass eine europäische Norm für die elektronische Rechnungsstellung den Schutz personenbezogener Daten gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates und die Grundsätze des Datenschutzes durch Technik („data protection by design“), der Verhältnismäßigkeit sowie der Datenminimierung berücksichtigten soll. Insoweit sieht auch Art. 3 Abs. 1 S. 2

3. Spiegelstrich RiLi 2014/55/EU vor, dass die Kommission bei der Erarbeitung der Normierung der E-Rechnung den notwendigen Schutz personenbezogener Daten im Sinne der Richtlinie 95/46/EG (also nun der DSGVO), das Konzept des Datenschutzes durch Technik sowie die Grundsätze der Verhältnismäßigkeit, der Datenminimierung und der Zweckbegrenzung berücksichtigt. Ferner gibt es noch einen Art. 8 RiLi 2014/55/EU zum Datenschutz, wonach die Richtlinie das geltende Unionsrecht zum Datenschutz nicht berühre. Es findet mithin auf die E-Rechnung also die DSGVO vollständig Anwendung.<sup>19</sup> Hierzu schweigt der nationale Gesetzgeber ganz einfach. Es wird noch nicht einmal ersichtlich, dass der Gesetzgeber überhaupt einen Gedanken an diese Problematik in den Raum geworfen hat.

### Kleine und mittlere Unternehmen

Auch ging der Richtliniengeber der RiLi 2014/55/EU davon aus, dass den Unternehmen, einschließlich Kleinstunternehmen sowie kleinen und mittleren Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission<sup>20</sup>, keine zusätzlichen Kosten oder Belastungen auferlegt werden sollen. Darüber hinaus sollten sich die Kommission und die Mitgliedstaaten nach Kräften bemühen, die Kosten der europäischen Norm für die elektronische Rechnungsstellung für ihre Nutzer, insbesondere für Kleinstunternehmen sowie kleine und mittlere Unternehmen, zu minimieren, um ihre Verbreitung in der gesamten Europäischen Union zu erleichtern. Auch hiervon merkt man beim nationalen Gesetzgeber schier gar nichts. Softwareanbieter und Auftragsverarbeiter sehen vielmehr neue Einnahmequellen und werben entsprechend für die E-Rechnung freudig unter Hinweis auf die Pflicht zur Nutzung der E-Rechnung.<sup>21</sup>

Ein entsprechendes Programm zur Erstellung und zum Lesen der E-Rechnung wird für kleine und mittlere Unternehmen von dem Bundesfinanzministerium nicht angeboten. Auch gibt es kein Angebot für einen sicheren Übertragungsweg. Damit ist die nun geschaffene Regelung eine zusätzliche Belastung für kleine und mittlere Unternehmen. Versteht die Politik dies als Entlastung?

Denn besteht eine Verpflichtung zur Ausstellung einer E-Rechnung und wird stattdessen eine sonstige Rechnung im Sinne von § 14 Abs. 1 S. 4 UStG ausgestellt, handelt es sich nicht um eine ordnungsmäßige Rechnung im Sinne von §§ 14, 14a UStG. Folglich ist die ausgestellte Rechnung auch nicht zum Vorsteuerabzug nach § 15 Abs. 1 S. 1 Nr. 1 UStG berechtigt. Es entsteht dann ein wirtschaftlicher Schaden. Könnte man hierin einen Aufruf des Gesetzgebers, nicht mehr wirtschaftlich tätig zu werden, sehen?

### Aufbewahrung

Der strukturierte Teil einer E-Rechnung ist so aufzubewahren, dass dieser in seiner ursprünglichen Form vorliegt und die Anforderungen an die Unveränderbarkeit erfüllt werden. Eine maschinelle Auswertbarkeit seitens der Finanzverwaltung muss sichergestellt sein. Sofern in einem zusätzlich übersandten Dokument (z. B. Bildteil einer hybriden Rechnung) Aufzeichnungen enthalten sind, die für die Besteuerung von Bedeutung sind, z. B. Buchungsvermerke, sind diese ebenfalls so aufzubewahren, dass sie in ihrer ursprünglichen Form vorliegen und die Anforderungen an die Unveränderbarkeit erfüllt werden.<sup>22</sup> Mithin bedarf es entsprechender elektronischer Speicherungen, welche sicher sein müssen.

### Übergangsregelungen

§ 27 Nr. 38 UStG enthält jedoch freundlicherweise noch Übergangsvorschriften. Hiernach kann bis zum Ablauf des Kalenderjahres 2026 eine Rechnung für einen bis dahin ausgeführten Umsatz auch als sonstige Rechnung ausgestellt und übermittelt werden. Die Ausstellung und Übermittlung einer Papierrechnung ist bis dahin umsatzsteuerlich immer zulässig. Jedoch bedarf es dazu der Zustimmung des Empfängers der Rechnung. Diese Zustimmung zu der Rechnungserteilung in einem anderen elektronischen Format bedarf allerdings keiner besonderen Form und kann stillschweigend erfolgen. Der Betroffene ist damit von dem Empfänger abhängig.

Hat der Gesamtumsatz des rechnungsausstellenden Unternehmers im

vorangegangenen Kalenderjahr nicht mehr als 800.000 Euro betragen, kann eine Rechnung für einen nach dem 31. Dezember 2026 ausgeführten Umsatz bis zum Ablauf des Kalenderjahres 2027 ebenfalls noch als sonstige Rechnung ausgestellt und übermittelt werden. Allerdings ist dies auch von der Zustimmung des Empfängers abhängig.

### Fazit

Damit wird die E-Rechnung zwanghaft allen wirtschaftlich Tätigen aufgebürdet, ohne dass die Sicherungen und Erleichterungen, welche gerade für Kleinunternehmer nach der RiLi 2014/55/EU enthalten sind, auch nur im Ansatz von dem deutschen Gesetzgeber und der Finanzverwaltung berücksichtigt wurden. Ob dies europarechtskonform ist, kann bezweifelt werden. Die Finanzgerichtsbarkeit dürfte sich an diese Fragen, gerade auch bezüglich des Datenschutzes, wohl eher nicht heranwagen, auch wenn sich hier ein ganzer Strauß an Vorlagefragen eröffnen dürfte. Es sei denn, das Bundesverfassungsgericht (BVerfG) würde den Bundesfinanzhof (BFH) hierzu zwingen. Denn der BFH ist der Auffassung, dass das BVerfG im Rahmen einer Verfassungsbeschwerde bei willkürlicher Nichtbeachtung der Vorlagepflicht an den EuGH durch den BFH dafür zuständig ist, dass letztendlich eine Vorlage an den EuGH erfolgt.<sup>23</sup> Insoweit düstere Aussichten für die „Zwangsverpflichteten“.<sup>24</sup>

Es wäre sehr wünschenswert, wenn die neue Bundesregierung bei allen Gesetzgebungsvorhaben zukünftig europäisches Recht stärker beachten und sich bei der Digitalisierung nicht auf den Zwang beschränken würde. Denn Digitalisierung ist kein Selbstzweck und sollte das Leben erleichtern und nicht erschweren. So stellt die europäische Erklärung zu den digitalen Rechten und Grundsätzen<sup>25</sup> klar, dass die in der Erklärung genannten Rechte allen Menschen in der EU garantiert werden und zwar online wie offline.<sup>26</sup> Offline bedeutet aber auch, dass Unternehmen – zumindest kleine und mittlere Unternehmen – ein Wahlrecht haben müssen, ob sie die E-Rechnung einsetzen, es sei denn, der Staat sorgt für die entsprechenden Rahmenbedingungen.

- 1 BGBl. 2024 I Nr. 108 vom 27.03.2024.
- 2 Siehe Art. 33 Abs. 6 Wachstumschancengesetz.
- 3 BStBl. 2024 I S. 1320; GZ III C 2 – S 7287-a/23/10001 :007 DOK 2024/0883282.
- 4 ABL. L 133 vom 6. Mai 2014, S. 1.
- 5 Siehe auch Ausführungen im Erlass über die Ausstellung von Rechnungen, Rn. 28 zur EN 16931.
- 6 Siehe auch Ausführungen im Erlass über die Ausstellung von Rechnungen, Rn. 33 und 34.
- 7 <https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:327729047>, Stand Januar 2025).
- 8 ABL. EU L 133 vom 06.05.2014, S. 1.
- 9 Siehe nur die E-Rechnung im BSI, [https://www.bsi.bund.de/DE/Service-Navi/Die-E-Rechnung-im-BSI/die-e-rechnung-im-bsi\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Die-E-Rechnung-im-BSI/die-e-rechnung-im-bsi_node.html), Stand Januar 2025.
- 10 BGBl. I S. 3555.
- 11 BGBl. I S. 1328.
- 12 Dort noch Art. 29, BT-Dr. 20/8628, S. 204 f.
- 13 Zum geplanten European Health Data Space (EHDS) und zur E-Rechnung siehe auch Raji, Datenräume in der Europäischen Datenstrategie am Beispiel des European Health Data Space, ZD 2023, 3 ff.
- 14 Siehe auch Schild: Die E-Rechnung – und wo bleibt der Datenschutz? ZD-Aktuell 2024, 01804.
- 15 OLG Schleswig, Urteil vom 18.12.2024 – 12 U 9/24.
- 16 Ausführungen im Erlass über die Ausstellung von Rechnungen, Nr. 37.
- 17 Ausführungen im Erlass über die Ausstellung von Rechnungen, Nr. 40.
- 18 Ausführungen im Erlass über die Ausstellung von Rechnungen, Nr. 43 - vgl. hierzu Abschnitt 14.1 Absatz 5 UStAE Umsatzsteuer-Anwendungserlass vom 1. Oktober 2010, BStBl I S. 846 – (aktueller Stand 15. Januar 2025), [https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF\\_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/Umsatzsteuer-Anwendungserlass-aktuell.pdf?\\_\\_blob=publicationFile&v=22](https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/Umsatzsteuer-Anwendungserlass-aktuell.pdf?__blob=publicationFile&v=22).
- 19 Siehe zur Übergangsregelung Beck-OK DatenschutzR/Schild, 50. Ed. 01.11.2024, DSGVO Art. 94 Rn. 6-11.
- 20 Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABL. L 124 vom 20.05.2003, S. 36).
- 21 So wirbt ein Buchhaltungsprogrammhersteller mit seinem Buchhaltungsprogramm täglich im Hessischen Rundfunk damit, dass die E-Rechnung für Selbstständige seit dem 01.01.2025 Pflicht sei und alles am besten in der Cloud und online.
- 22 Erlass Ausstellung von Rechnungen nach § 14 UStG, Rn. 69. Wegen der Einzelheiten hierzu siehe BMF-Schreiben vom 28. November 2019, BStBl I S. 1269, Rn. 131 und 133.
- 23 BFH, Urteil vom 10.10.2023 – IX K 1/21 –, BFHE 281, 503, BStBl. II 2024, 182, Rn. 17.
- 24 Zum Digitalzwang siehe Weichert, Gegen Digitalzwang – ein Recht auf eine analoge Alternative, NJOZ 2024, 1537 ff.
- 25 GEMEINSAME ERKLÄRUNGEN des EUROPÄISCHES PARLAMENT RAT EUROPÄISCHE KOMMISSION, Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade (2023/C 23/01), ABL. EU C 23 vom 23.01.2023, S. 1.
- 26 [https://ec.europa.eu/commission/presscorner/detail/de/ip\\_22\\_7683](https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7683), Stand Januar 2025.

## Nachrichten zum Digitalzwang

### DB: Analoge Ankunftsangaben bleiben verfügbar

Eigentlich sollten die weißen Pläne mit den Ankunftszeiten der Züge zum Fahrplanwechsel Mitte Dezember 2024 aus den Bahnhöfen verschwinden. Nach Kritik erklärte die Deutsche Bahn (DB), dass sie die gedruckten weißen Ankunftspläne an den Bahnhöfen nun doch hängen lässt.

Erst wenige Tage zuvor hatte die Bahn Ende November 2024 mitgeteilt, dass die Aushänge der Ankunftspläne in den Bahnhöfen ab 15.12.2024 wegfallen sollen. Der Schritt wurde damit begründet, dass Reisende Informationen in Echtzeit benötigten. Die Ankunftszeit und das Ankunftsgleis erfahre man am Bahnhof am zuverlässigsten über die Monitore, die Live-Ankunftstafeln oder

die dynamischen Anzeiger direkt am Bahnsteig. Die Papieraushänge würden von den Reisenden kaum genutzt; sie verursachten in der Datenpflege und im Druck jedoch hohen Aufwand. Die gedruckten gelben Abfahrtspläne sollten von den Plänen nicht betroffen sein.

Von Sozial- und Fahrgastverbänden hatte es daraufhin deutliche Kritik gegeben. So meinte Verena Bentele, Präsidentin des Sozialverbands VdK: „Die geplante Abschaffung von analogen Aushängen, auch wenn es bisher nur die Ankunftspläne betrifft, verschärft das Gefühl des Abgehängtseins.“ Dies betreffe insbesondere Menschen, die nicht durchgängig digital unterwegs seien – Seniorinnen und Senioren, Menschen mit Behinderungen oder arme Menschen: „Ohne Not werden Menschen von wichtigen Informationen ausgeschlossen.“

Der Vorsitzende des Fahrgastverbands Pro Bahn, Detlef Neuß, erklärte: „Wir sind der Meinung, die gedruckten Fahrpläne könnten ruhig noch weiter aushängen.“ Viele Leute orientierten sich lieber in Ruhe an den Plänen, anstatt die digitalen Anzeigen zu nutzen (Bahn-Ankunftspläne auf Papier bleiben doch hängen, <https://www.tagesschau.de> 29.11.2024).

### Kein Digitalzwang mehr bei DB-Sparpreistickets

Nach Kritik an den Regeln zum Kauf von Sparpreistickets hat die Deutsche Bahn (DB) reagiert. Vom Fahrplanwechsel am 15.12.2024 an müssen Bahnreisende nicht mehr eine E-Mail-Adresse oder Handynummer nennen, um diese

vergünstigten Fahrscheine zu erhalten. Sie können am Bahnschalter auch einen Ausdruck des Sparpreistickets ohne diese Angaben bekommen. Der hessische Landesdatenschutzbeauftragte Alexander Roßnagel erklärte: „Wir begrüßen, dass der Datenschutzkonflikt auf konstruktive Weise gelöst werden konnte.“ Hintergrund ist ein Aufsichtsverfahren, das er aufgrund einer Vielzahl von Beschwerden nach Änderungen bei den Sparpreisen im Herbst 2023 angestoßen hatte. Bahnreisende ohne Internetanschluss oder Smartphone seien vom Erwerb ausgeschlossen worden. Auch Verbraucher, die besonders auf Datenschutz achten, würden ausgegrenzt.

Eine Bahnsprecherin bestätigte: „Wir werden unseren Verkaufsprozess für Sparpreistickets im Reisezentrum und DB Agenturen zum Fahrplanwechsel am 15. Dezember ändern. Wir haben uns hier das Kundenfeedback in den Verkaufsstellen genau angeschaut. Auch wenn es nur sehr wenige Menschen gibt, die keine Mailadresse haben, möchten wir diesen weiterhin die Möglichkeit geben Sparpreistickets zu buchen.“ Die Bahn empfehle jedoch allen Reisenden, bei der Buchung eine E-Mail-Adresse anzugeben. Dies ermögliche eine bessere Information etwa bei Gleiswechseln oder Verspätungen (Bahn ändert Regeln zum Kauf von Sparpreistickets, <https://www.nw.de> 07.12.2024).

## DB-Bordbistros testen Abschaffung der Bargeldzahlung

Im Februar 2025 startet ein „Pilotprojekt“ der Deutsche Bahn (DB) zur bargeldlosen Zahlung in den Bordbistros des Fernverkehrs. Zwischen Anfang Februar und Anfang Mai werden Fahrgäste auf bis zu sechs ICE-Strecken täglich nur noch mit Karte und nicht mehr bar bezahlen können. Auf der Website der Bahn sowie in der App DB Navigator werde vorab auf die bargeldlosen Züge hingewiesen. Die Bahn begründet ihren Schritt damit, dass bargeldlose Zahlungen die Prozesse an Bord vereinfachten und für die Fahrgäste „zu kürzeren Wartezeiten“ führten. Bereits bisher zahle die Hälfte der Bahnfahrer ohnehin bargeldlos.

Eine flächendeckende Abschaffung des Bargelds in Bordbistro und Bordrestaurant soll es aber nicht zwingend geben: Die Ausweitung auf weitere Verbindungen hänge, so die DB, von den Ergebnissen des Tests ab: „Diese werten wir ganz genau aus.“ Zeitgleich wird im Bordbistro gezapftes Bier vollständig abgeschafft. Stattdessen kündigt das Unternehmen eine größere Auswahl bei Flaschenbier an (Bald kein gezapftes Bier mehr im Bordbistro, <https://www.tagesschau.de> 12.12.2024).

## Aus für Telekom-Telefon- auskunft

Am 30.11.2024 war die Telefonauskunft der Deutschen Telekom zum letzten Mal erreichbar. Das Unternehmen hatte dies bereits im Mai 2024 angekündigt. Das damals sogenannte „Fräulein vom Amt“ war seit dem Beginn der Telefonie Ende des 19. Jahrhunderts eine Instanz. Auch, weil die Verbindungen in den Ortsvermittlungsstellen durch von Hand gesteckte Kabel hergestellt werden mussten. Man landete als Anrufer oder Angerufener immer bei einer Telefonistin, Direktwahl setzte sich erst später durch.

Wegen der Bedeutung eines Auskunftsdienstes war die frühere Rufnummer 118 auch neben den Notrufen 110 und 112 eine der dreistelligen Kurzwahlnummern. Mit der Privatisierung des Telefoniemarktes in den 1990er Jahren wurde 118XX als der Rufnummernraum festgelegt, mit dem Auskunftsdienste aller Art angeboten werden konnten. Die Telekom erhielt dabei die bis jetzt genutzte 11833 und machte kräftig Werbung dafür, unter anderem mit Fernsehspots, ebenso wie die privaten Anbieter. „Da werden Sie geholfen“ lautete der Slogan des größten privaten Anbieters mit der Nummer 11880, vorgetragen von Verona Feldbusch. Mitte der 1990er Jahre kam es zur höchsten Nachfrage. Laut Telekom gab es 1995 den Rekord mit 550 Millionen Anrufen bei der Auskunft, seitdem ging die Nachfrage jährlich um 20% zurück. Im Jahr 2023 soll es dennoch rund 2 Millionen Anrufe gegeben haben. Der Dienst sei damit nicht mehr kostendeckend. Zuletzt wurde der Ser-

vice vorwiegend über ein Callcenter im mecklenburg-vorpommerschen Ort Paesewalk abgewickelt. Die meisten Mitarbeiterinnen und Mitarbeiter sollen nun in den Ruhestand gehen.

Zuletzt arbeiteten noch 40 Beschäftigte bei der Telefonauskunft der Telekom, in der Spitze waren es rund 5.000. Wälzte man dort anfangs noch Telefonbücher, so kamen später Mikrofilme und schließlich Computer hinzu. Ebenso wie die Auskunft selbst waren in den 1990er-Jahren Telefonbuch-CDs für zahlreiche Anbieter ein gutes Geschäft, das weitgehend durch das Internet verdrängt wurde. Inzwischen meinte auch die Telekom, der Dienst sei „aus der Zeit gefallen“. Schon bei der Ankündigung zum Ende der Telekom-Auskunft gab es Kritik, unter anderem vom Sozialverband VdK. Ältere und arme Menschen könnten nicht mit einem Smartphone umgehen oder sich eines leisten, und somit auch nicht ohne Weiteres auf Internetsuchmaschinen zur Nummernsuche zurückgreifen. Die Auskunft der Telekom ist jedoch nicht der einzige Dienst: Die Bundesnetzagentur verzeichnet in ihrer aktuellen Liste der Anbieter noch einige Dutzend andere Auskunftsdienste.

Wer zuletzt die 11833 anrief, musste je Anruf aus dem Festnetz 1,99 Euro zahlen, per Mobilfunk in der Regel mehr. Als die Bundespost in den 1980er-Jahren noch das Telefonmonopol hatte, war das eine Gebühreneinheit, die über lange Zeit 20 Pfennige kostete. Mit der Inlandsauskunft unter 11833 wurden auch die Auslandsauskunft (früher 11834) und der Weckdienst eingestellt, welcher auch unter der 11833 erreichbar war. Da rief dann schon seit vielen Jahren auch keine freundliche Dame, sondern eine aufgezeichnete männliche Stimme an (Ernst, Telekom stellt Auskunft ein: Kein Anschluss mehr unter 11833, <https://www.heise.de> 30.11.2024, Kurzlink: <https://heise.de/-10183762>).

## Doctolib nutzt ungefragt Gesundheitsdaten für KI

Der IT-Gesundheitsdienstleister Doctolib hat angekündigt, dass er Daten seiner Nutzenden für das Trainieren von

KI-Modellen verwendet. In den aktualisierten Datenschutzhinweisen des Anbieters, die ab dem 22.02.2025 wirksam werden, beruft sich Doctolib auf sein berechtigtes Interesse bei Daten wie Geschlecht, Geburtsmonat und -jahr oder Antworten auf freiwillige Umfragen. Das Unternehmen unterstellt dabei fälschlich, dass es sich hierbei nicht um Gesundheitsdaten handeln würde, die nach den Vorgaben der DSGVO nur nach erteilter Einwilligung verwendet werden dürfen.

Laut einer E-Mail, die an Account-Inhaber verschickt wurde, entwickle Doctolib „fortlaufend neue daten- und KI-gestützte Produkte“. Als Beispiele nennt das Unternehmen „Erinnerungen an erforderliche Rezepterneuerungen und neue Funktionen bei den Patientennachrichten“. Nutzende sollen zeitnah weitere Informationen in ihren Accounts angezeigt bekommen. „Dort haben Sie auch die Möglichkeit, Ihre Einwilligung zu erteilen. Selbstverständlich entscheiden Sie frei, ob Sie uns Ihre Einwilligung geben möchten. Diese können Sie jederzeit in Ihren Einstellungen anpassen.“

In den Datenschutzhinweisen wird dargestellt, welche Art von Gesundheitsdaten zusätzlich per Einwilligung für das KI-Training genutzt werden sollen: „Suchdaten, Terminhistorie, Dokumente, medizinische Notizen, vom Nutzer auf der Plattform eingegebene medizinische Informationen“. Auch Informationen, die von den Praxen erhoben und bei Doctolib eingespeist werden, sollen dazuzählen.

Doctolib hatte 2024 einen immer größeren Fokus auf KI-Entwicklung gelegt. Im Mai verkündete das Unternehmen die Übernahme von Aaron.ai, einem KI-gestützten Telefonassistenten und bietet seitdem eine automatisierte Anrufentgegennahme als Produkt an. Einen Monat später übernahm Doctolib auch Typeless, das auf Spracherkennung im medizinischen Kontext spezialisiert ist. Bis Ende 2024 wollte Doctolib dann eigentlich einen „medizinischen Assistenten“ vorstellen.

Das aus Frankreich stammende Startup Doctolib gilt als sogenanntes „Unicorn“ und ist die am weitesten verbreitete Plattform für Online-Arzttermine in Deutschland. Laut eigener Aussage

nutzen hierzulande 20 Millionen Patienten den Dienst, zudem bediene es über 100.000 Gesundheitsfachkräfte. Doctolib steht seit Jahren in der Kritik. So hatte es laut einer Recherche von mobil sicher.de zeitweise sensible Gesundheitsdaten an Facebook und die Werbeplattform Outbrain übertragen. Auch sammelt es bei der Vermittlung von Arztterminen unnötig viele Daten und nutzt sie für eigene Zwecke (DANA 2/2024, 73 ff.).

Ein weiteres Problem kommt durch die Praxen, die Doctolib nutzen: Immer mehr ermöglichen eine Terminbuchung nur noch über Doctolib, was die Einrichtung eines Accounts voraussetzt. Doctolib profitiert von diesem Digitalzwang und nutzt die anfallenden Daten für sich selbst. Ein Ausstieg bei dem Anbieter durch Löschen des Accounts führt dazu, dass schon gebuchte Termine aufgekündigt werden: „[U]m die Aktion durchzuführen, müssen Sie alle kommenden Termine in Ihrem Konto stornieren“ (Rudl/Biselli, Neue Datenschutzhinweise: Doctolib will KI-Modelle mit Gesundheitsdaten trainieren, <https://netzpolitik.org> 24.01.2025).

DVD-Presseerklärung vom 06.12.2024

## Aufruf der Zivilgesellschaft an die neue europäische Führung

*Am 26. November 2024 haben sich die DVD und 47 weitere europäische Nichtregierungs-Organisationen mit einem Aufruf zur EU-Technologiepolitik und -praxis an die neue europäische Führung gewendet.*

*Nach der Neubesetzung der Europäischen Kommission fordern die unterzeichnenden Organisationen bei der Politikgestaltung mehr Transparenz und Beteiligung der Zivilgesellschaft und präsentieren ihre gemeinsamen Erwartungen an eine dem öffentlichen Interesse dienende EU-Technologiepolitik.*

Besorgt über den vorgeschlagenen neuen Ansatz der EU-Kommission, der sich auf Unternehmens- und Sicher-

heitsinteressen fokussiert, fordern sie gemeinsam einen digitalen Rahmen, der gerecht, sicher, offen, nachhaltig und inklusiv ist. So heißt es im Aufruf: „Wir fordern eine Politikgestaltung, bei der der Mensch im Mittelpunkt steht und die eine sinnvolle Beteiligung der Zivilgesellschaft sowie eine Rechenschaftspflicht und Konsultation der Gruppen, die die Hauptlast des technologischen Schadens innerhalb und außerhalb der EU tragen, vorsieht. Die Auswirkungen der EU-Rechtsvorschriften sowie der Bemühungen der EU um Diplomatie in Digitalangelegenheiten und Handelsabkommen mit anderen Regionen dürfen den Schutz der Menschenrechtsstandards weltweit nicht untergraben.“

Die Organisationen der Zivilgesellschaft, die sich in den Bereichen Menschen-, Digital- und Verbraucherrechte, Sozial- und Umweltgerechtigkeit sowie Rechenschaftspflicht von Unternehmen engagieren, haben acht präzise Punkte an die EU-Kommission aufgelistet, darunter zum Thema Digitalzwang die Forderung „Offline-Alternativen zur allumfassenden Digitalisierung öffentlicher und wesentlicher Dienste zu bewahren und sicherstellen, dass niemand von der digitalen ‚Transformation‘ ausgeschlossen oder zurückgelassen wird“.

Frank Spaeing, Vorsitzender der DVD: „Es ist entscheidend auch der neuen EU-Kommission die Pflicht zum Schutz der in der EU lebenden Menschen vor

überbordenden Datenverarbeitungen und vor Digitalzwang in Erinnerung zu rufen.“

Der Aufruf im Wortlaut:

## **EU-Technologiepolitik und -praxis müssen ein Schwerpunkt des öffentlichen Interesses werden**

Nach der Neubesetzung der EU-Kommission fordern die unten aufgeführten unterzeichnenden Organisationen der Zivilgesellschaft, die sich in den Bereichen Menschen-, Digital- und Verbraucherrechte, Sozial- und Umweltgerechtigkeit sowie Rechenschaftspflicht von Unternehmen engagieren, mehr Transparenz und Beteiligung der Zivilgesellschaft bei der Politikgestaltung. Vorliegend präsentieren wir unsere gemeinsamen Erwartungen an eine dem öffentlichen Interesse dienende EU-Technologiepolitik.

Am 1. Oktober 2024 veranstalteten 41 zivilgesellschaftliche Organisationen den „Tech & Society Summit“, an dem mehr als 350 Vertreterinnen und Vertreter eines breiten Spektrums von Nichtregierungs-Organisationen (NGO), EU-Entscheidungsträgern, Regulierungsbehörden und Journalisten teilnahmen. Die Podiumsdiskussionen, Diskussionsrunden, Kamingsgespräche, Action Desks und informellen Gespräche zeugten von der dringend nötigen Alternative zu den zahlreichen von der Industrie gesponserten Technologie-Veranstaltungen. Die Teilnehmer des Tech & Society Summit forderten dabei vielfach ein klareres Bekenntnis der Entscheidungsträger zur öffentlichen Rechenschaftspflicht bei der Technologie-Regulierung und für die damit verbundenen sozialen, wirtschaftlichen und ökologischen Anwendungen und Auswirkungen.

Die Unterzeichner fordern gemeinsam einen digitalen Rahmen, der gerecht, sicher, offen, nachhaltig und inklusiv ist. Wir sind besorgt über den vorgeschlagenen neuen Ansatz der Europäischen Kommission, der sich auf Unternehmens- und Sicherheitsinteressen fokussiert und von der Annahme ausgeht, dass für die Aufrechterhaltung der europäischen Werte und Lebensweise

Wachstum bei Wahrung des Status Quo notwendig seien. Entscheidungsträger sollten kritisch gegenüber den Narrativen und Argumenten sein, die Interessen von Unternehmensakteuren fördern und unsere Abhängigkeit von diesen verstärken. Sie sollten unbeirrbar Maßnahmen und Praktiken hinterfragen, die die Ausbeutung des Planeten ignorieren, Schäden, Diskriminierung und Ungleichheiten verstärken und die zentralen Funktionen unserer Institutionen bedrohen.

Wir fordern eine Politikgestaltung, bei der der Mensch im Mittelpunkt steht und die eine sinnvolle Beteiligung der Zivilgesellschaft sowie eine Rechenschaftspflicht und Konsultation der Gruppen, die die Hauptlast des technologischen Schadens innerhalb und außerhalb der EU tragen, vorsieht. Die Auswirkungen der EU-Rechtsvorschriften sowie der Bemühungen der EU um Diplomatie in Digitalangelegenheiten und Handelsabkommen mit anderen Regionen dürfen den Schutz der Menschenrechtsstandards weltweit nicht untergraben.

Bei diesem Mandat der Europäischen Kommission ist die Durchsetzung der bestehenden EU-Rechtsvorschriften von entscheidender Bedeutung. Die Gesetzgebungsorgane müssen die Berichte der Zivilgesellschaft und der betroffenen Gruppen über die Durchsetzung vor Ort zur Kenntnis nehmen und darauf reagieren. Wir müssen zudem die regulatorischen Lücken schließen – vor allem, um den durch Big Tech verursachten tiefgreifenden Wandel unserer Volkswirtschaften und Institutionen, die schädliche Gestaltung digitaler Produkte und Dienstleistungen, den Einsatz von Massenüberwachungstechnologien im öffentlichen Raum und an Grenzen sowie die Umweltschäden durch Technologie einzudämmen.

Es gibt für Europa einen Weg nach vorn mit Technologien, Strategien und Ansätzen, die Menschen, Demokratie und unseren Planeten in den Mittelpunkt stellen. In diesem Sinn wird die neue Europäische Kommission aufgefordert

- Rechte, sozialen Schutz und Sicherheit zu gewähren statt Überwachung, Kontrolle und Ausweitung der Polizeibefugnisse. Dies schafft die Voraus-

setzungen für gesunde und blühende Gemeinschaften;

- mit Vorrang die Umsetzung und Durchsetzung der in den letzten Jahren verabschiedeten digitalen Gesetze und Richtlinien, einschließlich der DSGVO, des DSA, des DMA und des EU-KI-Gesetzes, zu betreiben;
- die Sicherheit von Online-Plattformen, -Produkten und -Dienstleistungen für alle in den Mittelpunkt zu stellen und von Rechtsvorschriften abzusehen, die Massenüberwachungsmaßnahmen einführen oder den Schutz der Cybersicherheit untergraben;
- den Technosolutionismus zur Bewältigung komplexer sozialer oder ökologischer Probleme zurückzuweisen, der Marginalisierung und die Überwachung und Zensur abweichender Meinungen verstärkt und der schutzbedürftigen Gruppen wie Journalisten und Menschenrechtsverteidigern, Frauen, LGBTI-Personen sowie ethnischen oder sonstigen ausgegrenzten Minderheiten schadet;
- die Digitalisierung nach dem Motto „Wachstum um jeden Preis“ zu überwinden, wodurch Ressourcen und Arbeitskräfte ausgebeutet werden, und eine Politik der Nachhaltigkeit festzuschreiben. Stattdessen sollten Strategien zur digitalen Suffizienz, Kreislaufwirtschaft, Materialnutzung und Abfallreduzierung gefördert werden, die sich auf Wiederverwendung, Aufarbeitung und Reparatur konzentrieren;
- Offline-Alternativen zur allumfassenden Digitalisierung öffentlicher und wesentlicher Dienste zu bewahren und sicherstellen, dass niemand von der digitalen „Transformation“ ausgeschlossen oder zurückgelassen wird;
- eine offene, inklusive Vision von Europa voranzubringen, die auf Menschenrechten, Gleichheit und Rechtsstaatlichkeit ausgerichtet ist und die Menschenrechte von Migranten und Menschen auf der Flucht schützt;
- gleiche Wettbewerbsbedingungen durch Investitionen in echte alternative Technologien und Wirtschaftsmodelle zu schaffen, die keine ausbeuterischen Geschäftsmodelle produzieren oder die Macht der Technologieunternehmen nicht weiter festigen.

**Unterzeichnende Organisationen:**

1. Access Now, 2. AlgorithmWatch, 3. AlgorithmWatch CH, 4. Alternatif Bilişim, 5. Amnesty International, 6. ARTICLE 19, 7. Aspiration Tech, 8. BEUC – The European Consumer Organisation, 9. Bits of Freedom, 10. Center for Technology and Democracy Europe, 11. Citizen D / Državljan D, 12. Civil Liberties Union for Europe, 13. Communia, 14. Corporate Observatory Europe, 15. D3 – Defesa dos Direitos Digitais, 16. Danes je nov dan, 17. **Deutsche Vereinigung**

**für Datenschutz e.V. (DVD)**, 18. Digital Action, 19. ECOS, 20. Electronic Frontier Foundation (EFF), 21. Electronic Frontier Norway (EFN), 22. EPIC, 23. Equinox – Initiative for racial Justice, 24. European Anti Poverty Network, 25. European Center for Non-Profit Law (ECNL), 26. European Digital Rights (EDRi), 27. European Environmental Bureau, 28. European Sex Workers Alliance (ESWA), 29. Friends of the Earth Europe, 30. Global Health Advocates, 31. Gong, 32. Health Action International, 33. Homo Digitalis, 34. IT-Pol, 35. LobbyControl,

36. Mnemonic, 37. Open Markets Institute, 38. Oxfam, 39. PICUM, 40. Politiscope, 41. Privacy International, 42. PublicSpaces, 43. SHARE Foundation, 44. SOMO, 45. SUPERRR Lab, 46. Transatlantic Consumer Dialogue (TACD), 47. Weaving Liberation, 48. Wikimedia EU

Der englische Originaltext des Aufrufs ist veröffentlicht unter <https://edri.org/our-work/centering-public-interest-in-eu-technology-policies-and-practices-a-civil-society-call-to-the-new-european-leadership/>

DVD-Presseerklärung vom 11.12.2024

## Offener Brief mit der Forderung, dass die EU-Agenda für digitale Sicherheit die Grundrechte fördert und ein sicheres digitales Ökosystem unterstützt

Die „Going Dark“-Expertengruppe hat ihren Abschlussbericht vorgelegt und empfiehlt den maximalen Zugang zu personenbezogenen Daten für Strafverfolgungsbehörden in Europa.

Die Deutsche Vereinigung für Datenschutz warnt in einem von EDRi initiierten und von einem breiten Bündnis von NGO mitgezeichneten offenen Brief vor den Gefahren für die digitale Sicherheit und die Privatsphäre, wenn der im Abschlussbericht beschriebenen Agenda gefolgt wird.

Die „Going Dark“-Expertengruppe schlägt Maßnahmen vor, die bisher von Experten und Gerichten gleichermaßen abgelehnt wurden. Drei Hauptpunkte sind besonders besorgniserregend:

- Der so genannte „lawful access by design“ beschreibt einen neuen Versuch Hintertüren (Backdoors) flächendeckend in Technologien einzubauen. Dieses würde die Sicherheit und Vertraulichkeit der gesamten elektronischen Kommunikation und Daten gefährden. Außerdem würde dies einen schwerwiegenden Eingriff in die Grundrechte der Menschen in der EU darstellen.
- Vorratsdatenspeicherung: Die „Going Dark“-Expertengruppe schlägt

vor die Vorratsdatenspeicherung auf praktisch alle Internetdienste auszuweiten, mit EU-weit harmonisierten Regeln, einschließlich der Vorratsdatenspeicherung für das Internet der Dinge.

- Die Verschlüsselung soll mit rechtlichen und technischen Mitteln ausgehebelt werden, damit die Strafverfolgungsbehörden auf verschlüsselte Daten zugreifen können. Die „Going Dark“-Expertengruppe schlägt vor den Diensteanbietern die unmögliche Aufgabe, Zugang zu verschlüsselten Daten im Klartext zu gewähren ohne die Sicherheit zu gefährden, zu stellen. Dies würde die Verschlüsselung und die Cybersicherheit untergraben und die Verantwortung auf die Diensteanbieter abwälzen.

Der Abschlussbericht folgt auf einen früheren Vorschlag mit 42 Empfehlungen der „Going Dark“-Expertengruppe, der von Experten – u.a. aus dem EDRi-Netzwerk – heftig kritisiert wurde. Der Europäische Datenschutzausschuss warnte, dass die Forderungen der „Going Dark“-Expertengruppe an die Diensteanbieter widersprüchlich seien, da es nicht möglich sei Zugang zu Über-

wachungszwecken zu gewähren und gleichzeitig die Sicherheit der digitalen Systeme zu schützen.

Dazu Frank Spaeing, Vorsitzender der DVD: „Anstelle auf diese Überwachungsphantasien sollte der Fokus auf die Stärkung eines digitalen Ökosystems diversifizierter, sicherer und vertrauenswürdiger Lösungen gesetzt werden, damit die Menschen in der EU durch die Technologie gestärkt werden können, anstatt sie zu gefährden. Es besteht real keine technische Möglichkeit das Versprechen der Ende-zu-Ende-Verschlüsselung zu brechen ohne die Sicherheit der Kommunikationssysteme zu schwächen.“

DVD-Vorstandsmitglied Thilo Weichert ergänzt: „Eine Analyse des Forschungsdienstes des Europäischen Parlaments zeigte keine messbaren Auswirkungen der Vorratsdatenspeicherung auf die Kriminalitätsrate oder die Aufklärungsquote in EU-Mitgliedstaaten, die die Vorratsdatenspeicherung nutzen. Die Vorratsdatenspeicherung ist grundsätzlich abzulehnen.“

Der offene Brief ist in der deutschen Übersetzung unter der URL <https://www.datenschutzverein.de/wp->

content/uploads/2024/12/Offener-Brief-GoingDark.pdf sowie im englischen Original unter der URL <https://www.datenschutzverein.de/wp->

content/uploads/2024/12/Open\_Letter\_on\_HLG\_Access\_to\_Data\_for\_Effective\_Law\_Enforcement\_Recommendations.pdf abrufbar, die

Themenseite von EDRI findet sich unter der URL <https://edri.org/our-work/shedding-light-we-address-the-flawed-going-dark-report>.

## Offener Brief an die polnische Ratspräsidentschaft in der EU: Übernehmen Sie eine Vorreiterrolle bei der Bekämpfung von Spyware-Missbrauch in der EU

H.E. Agnieszka Bartol  
Amtierende ständige Vertreterin der Republik Polen bei der Europäischen Union  
Rue Stevin 139, 1000 Brussels, Belgium  
Brüssel, den 13.12.2024

Sehr geehrte Frau Botschafterin Bartol,

im Namen der Spyware Coordination Group, einer Koalition aus zivilgesellschaftlichen und journalistischen Organisationen, die sich für Transparenz, Rechenschaftspflicht und die Achtung der Grundrechte im Zusammenhang mit Spyware-Technologien einsetzen, fordern wir die polnische EU-Ratspräsidentschaft auf während ihrer Amtszeit entschlossen gegen den Missbrauch von Spyware-Technologien vorzugehen.

Spionageprogramme sind eine ernste Bedrohung für die Grundrechte und demokratischen Grundsätze in der EU. Gemäß der Feststellung des ehemaligen UN-Sonderberichterstatters für Terrorismusbekämpfung im Jahr 2023 hat sich „(i)ntrusive verdeckte Technologie zur Überwachung des Inhalts der digitalen Kommunikation von Einzelpersonen (...) – gemeinhin als ‚Spyware‘ bekannt – international unkontrolliert ausgebreitet und stellt eine erhebliche Gefahr für die Förderung und den Schutz der Menschenrechte dar“. Für internationale Organisationen wie die UNO und einzelne Länder ist die Verbreitung kommerzieller Spähsoftware eine Bedrohung ihrer eigenen nationalen Sicherheit, ihrer außenpolitischen Interessen und der Grundrechte ihrer Bürger.

Der Europäische Datenschutzbeauftragte und das Europäische Parlament

haben in der EU den weit verbreiteten Missbrauch von Spähsoftware durch EU-Regierungen angeprangert und dringende EU-weite Maßnahmen gefordert, wie z. B. eine strengere Regulierung des Exports und der Verwendung von Spähsoftware sowie verbesserte Schutzmaßnahmen für Einzelpersonen und demokratische Institutionen. Trotz dieser Forderungen haben die EU-Institutionen noch keine wirksamen Lösungen oder ein umfassendes Konzept vorgelegt, um den zahlreichen berichteten Missständen und dem Machtmissbrauch durch die Mitgliedstaaten in der vergangenen Legislaturperiode zu begegnen. Dieser Mangel an entschlossenem Handeln steht in krassem Gegensatz zu Ländern wie den Vereinigten Staaten, die relevante Maßnahmen ergriffen haben, u.a. das Verbot der Verwendung kommerzieller Spionagesoftware durch alle nationalen Behörden, die Verhängung von Sanktionen gegen Anbieter und die Durchsetzung von Visabeschränkungen.

Frankreich und Großbritannien stehen zudem an der Spitze des Pall-Mall-Prozesses, einer internationalen Initiative weiterer Staaten, den Privatsektor und die Zivilgesellschaft zusammenzubringen, um gegen die weltweite Verbreitung und den rücksichtslosen Einsatz kommerzieller Spionageprogramme vorzugehen. Der Pall-Mall-Prozess basiert auf einem wachsenden Konsens zwischen wichtigen Nationen, darunter Polen und die Mehrheit der EU-Mitgliedstaaten, dass für demokratische Staaten angesichts der eskalierenden Risiken für die nationale Sicherheit und die Rechtsstaatlichkeit, die sich aus dem Missbrauch von Spionageprogrammen

ergeben, Untätigkeit nicht länger akzeptabel ist.

Wir anerkennen die Maßnahmen der polnischen Regierung zur Untersuchung des Missbrauchs von Spähsoftware auf nationaler Ebene und zur Gewährleistung der Rechenschaftspflicht und Opfer-Wiedergutmachung. Da Polen den rotierenden Ratsvorsitz übernimmt, ermutigen wir die polnische Regierung diese Verpflichtungen auf die EU-Ebene auszuweiten. Polen hat zusammen mit zehn anderen EU-Mitgliedsstaaten die Gemeinsame Erklärung über Bemühungen zur Bekämpfung der Verbreitung und des Missbrauchs kommerzieller Spähsoftware unterzeichnet. Angesichts der ernststen Bedrohung, die kommerzielle Spähsoftware für die nationale Sicherheit und die Grundrechte darstellt, haben sich die unterzeichnenden Regierungen dazu verpflichtet „innerhalb [ihrer] jeweiligen Systeme robuste Leitplanken und Verfahren einzurichten, um sicherzustellen, dass jegliche Nutzung kommerzieller Spähsoftware durch [ihre] Regierungen mit der Achtung der allgemeinen Menschenrechte, der Rechtsstaatlichkeit sowie der Bürgerrechte und bürgerlichen Freiheiten vereinbar ist“, und eng mit zivilgesellschaftlichen Gruppen zusammenzuarbeiten, „um [ihren] Ansatz zu informieren, zur Sensibilisierung beizutragen und angemessene Standards festzulegen“.

Um diese Ziele zu fördern, hat die Spyware-Koordinierungsgruppe Anfang des Jahres eine gemeinsame Erklärung zum Einsatz von Überwachungsspähsoftware in der EU und darüber hinaus verabschiedet, in der wichtige Empfeh-

lungen für die neuen EU-Institutionen formuliert sind. Wir empfehlen der polnischen Ratspräsidentschaft nachdrücklich dieses Dokument als Leitfaden für ihren Ansatz zur Bekämpfung der Verbreitung und des Missbrauchs von Spionagetechnologien zu nutzen.

Die Europäische Union kann sich durch ein umfassendes und koordiniertes Konzept als weltweit führend im Kampf gegen den Missbrauch von Spionageprogrammen positionieren. Die Verwirklichung dieses bedeutenden Potenzials erfordert jedoch eine starke politische und institutionelle Führung, um die Kluft zwischen Absicht und Handeln zu überbrücken. Die polnische EU-Ratspräsidentschaft trägt mit ihrer neuen Rolle entscheidende Verantwortung für eine Priorisierung und ein Vorantreiben dieser wichtigen Reformen.

Zwecks Unterstützung Ihrer Bemühungen würden wir es begrüßen mit Vertretern des polnischen Ratsvorsitzes zusammenzutreffen, um unsere Empfehlungen vorzustellen und zu erörtern, wie wir dazu beitragen können Maßnahmen zur Bekämpfung des Missbrauchs von Spähsoftware voranzubringen. Wir glauben, dass ein solcher Dialog von unschätzbarem Wert für die Umsetzung von Verpflichtungen in wirksame Strategien und Maßnahmen wäre.

Wir vertrauen darauf, dass die EU unter Ihrer Führung den Ehrgeiz und die Entschlossenheit an den Tag legen wird, die für den Schutz der Grundrechte, die Stärkung der demokratischen Institutionen und die wirksame Bekämpfung des Spionagemissbrauchs erforderlich sind.

Mit freundlichen Grüßen

Access Now, Amnesty International ARTICLE 19, Centre for Democracy and Technology Europe (CDT Europe), Civil Liberties Union for Europe (Liberties), Committee to Protect Journalists (CPJ), Data Rights, **Deutsche Vereinigung für Datenschutz e.V. (DVD)**, European Digital Rights (EDRi), Electronic Privacy Information Center (EPIC), Epicenter. works – for digital rights European Federation of Journalists (EFJ), Hungarian Civil Liberties Union (HCLU), Panoptikon Foundation

Der englischsprachige Originaltext findet sich im Internet unter <https://www.article19.org/resources/poland-take-the-lead-in-combatting-spyware-abuse-in-the-eu/>

## Aktuelles aus der DVD



Bild: Björn Staschen

### Save Social

Aus der Zivilgesellschaft wird der Ruf nach wirksamer Kontrolle digitaler Plattformen immer lauter. Die DVD ist deswegen als Unterstützerin einer Initiative und durch das Unterzeichnen eines offenen Briefes im ersten Quartal 2025 aktiv geworden.

Die Initiative, bei der wir als Unterstützer auftreten, ist „Save Social“ mit dem Ziel „Soziale Netzwerke als demokratische Kraft retten“, der offene Brief, den wir mitgezeichnet haben, wurde von Germanwatch.de mit der Forderung „Demokratische Diskursräume auch im Digitalen“ erstellt.

Save Social stellt zehn Punkte vor, in denen unter anderem gefordert wird, dass Alternativen zu den chinesischen und amerikanischen Plattformen gestärkt, gemeinwohlorientierte

Angebote ermöglicht und Medienbildung verbessert werden soll. Es wurde ein Manifest ([http://savesocial.eu/wp-content/uploads/2025/02/SAVESOCIAL\\_DE\\_eg\\_FINAL.pdf](http://savesocial.eu/wp-content/uploads/2025/02/SAVESOCIAL_DE_eg_FINAL.pdf)) veröffentlicht. Ein Unterzeichnen des Aufrufs ist unter <https://savesocial.eu> möglich. Zur Drucklegung dieser DANA hatten bereits ca. 250.000 Menschen den Aufruf der Initiative unterzeichnet.

### Act Now!

Mit einem von mehr als 75 Organisationen und Bündnissen unterzeichneten offenen Brief wendet sich Germanwatch zu den Sondierungsgesprächen an die Spitzen von Union und SPD und stellt fest: Die problematische Vermischung von politischer, medialer und ökonomischer Macht und die derzeitige Abhängigkeit von Tech-Unternehmen aus den USA und China sind ein Risiko für Europas digitale Souveränität, Wohlstand und Demokratie. Die nächste Bundesregierung muss klare Schritte einleiten:

1. Die bestehenden Digitalregeln wie der Digital Services Act und Digital Markets Act sowie das Wettbewerbsrecht müssen konsequent angewendet werden.

2. Regulierung muss zielgerichtet ergänzt werden, etwa bei der Transparenz von Algorithmen, bei Tracking-basierter Werbung und suchtförderndem Design sowie Interoperabilitätsverpflichtungen.
3. Der Aufbau demokratisch kontrollierter, gemeinwohlorientierter und souveräner digitale Infrastrukturen muss unterstützt werden.



Wir berichten über alle aktuellen Aktivitäten auf [www.datenschutzverein.de](http://www.datenschutzverein.de) oder tröten es unter <https://eupolicy.social/@datenschutzverein>.

# Datenschutznachrichten

## Datenschutznachrichten aus Deutschland

### Bund

#### Weiterhin großes Interesse an Stasi-Akten

35 Jahre nach dem Fall der Mauer ist das Interesse an Stasi-Akten gemäß Medienberichten nur leicht zurückgegangen. Im Jahr 2024 stellten demgemäß 28.571 Bürgerinnen und Bürger Anträge zur Stasi-Akteneinsicht. 2023 waren es knapp 30.700 Anträge gewesen, 2022 rund 29.000. Im Jahr vor der Corona-Pandemie, 2019, waren es laut Bundesarchiv noch etwa 56.500 Anträge auf Akteneinsicht. Der Präsident des Bundesarchivs, Michael Hollmann, bezeichnete die Einsicht in Stasi-Unterlagen als „gesamtgesellschaftliche Erfolgsgeschichte“. Insgesamt seien seit Ende 1990 mehr als 7,5 Millionen Anträge zu Stasi-Unterlagen eingegangen, davon allein mehr als 3,4 Millionen Bürgeranträge: „Wir müssen immer wieder an das von den Machthabern der SED-Diktatur und der DDR-Geheimpolizei begangene Unrecht erinnern, gerade in dieser Phase wachsender Verklärung der DDR.“ Auf Grundlage des 1991 in Kraft getretenen Stasi-Unterlagen-Gesetzes können Bürger Einsicht in die Akten beantragen, die das Ministerium für Staatssicherheit (Stasi) der ehemaligen DDR über sie anlegte. Die Verantwortung für die Stasi-Unterlagen hat 2021 das Bundesarchiv übernommen (Weiterhin Interesse an Stasi-Akteneinsicht, <https://www.sueddeutsche.de> 08.01.2025).

### Bund

#### Videoüberwachung auf Bahnhöfen hilft angeblich bei Straftatenbekämpfung

Die Deutsche Bahn AG (DB) und das Bundesministerium des Innern und für Heimat teilten mit, dass alle großen Bahnhöfe in Deutschland inzwischen

über moderne Videotechnik verfügen. Insgesamt 11.000 Kameras sind an rund 750 Bahnhöfen im Einsatz. Bundesinnenministerin Nancy Faeser (SPD) erklärte: „Mit dem starken Ausbau der Videoüberwachung haben wir mehr Sicherheit an unseren Bahnhöfen geschaffen.“ Der Bund habe dafür rund 180 Millionen Euro investiert. Die Bahn gebe jährlich mehr als 200 Millionen Euro für die Sicherheit der Fahrgäste aus. Die Zahl der aufgeklärten Kriminalitätsfälle habe sich mithilfe der Technik im Vergleich zum Jahr 2019 verdreifacht. DB-Infrastrukturvorstand Berthold Huber begründet das Engagement: „Die modernen Kameras ermöglichen einen Überblick auf die Stationen aus über 30.000 verschiedenen Blickwinkeln und unterstützen die Bundespolizei effektiv bei der Kriminalitätsbekämpfung.“ Nach früheren Angaben der Bundespolizei wurden vor dem Projektstart vor etwa vier Jahren rund 3.500 Straftaten jährlich mithilfe von Videotechnik aufgeklärt, 2023 waren es demnach mehr als 8.000 gewesen. Im September 2024 lag die Zahl bereits bei 7.000 Straftaten, bei deren Verhinderung bzw. Überführung die neue Technik zum Einsatz kam (Bahn: Moderne Videotechnik an allen großen Bahnhöfen, <https://www.heise.de> 29.12.2024, Kurzlink: <https://heise.de/-10221672>).

### Bundesweit

#### Großes Datenleck bei VW-Tochter

Das Tochterunternehmen des Volkswagen-Konzerns Cariad hat teils extrem detaillierte Bewegungsdaten von 800.000 Elektroautos so in der Amazon-Cloud abgelegt, dass Nachrichtendienste, Konkurrenten, Kriminelle oder „gelangweilte Teenager“ ohne große Schwierigkeiten darauf hätten zugreifen können. Eine Recherche des Spie-

gels in Zusammenarbeit mit dem Chaos Computer Club (CCC), die auf einen anonymen Hinweisgeber zurückgeht, stellte fest, dass die Daten teilweise eindeutig zuordenbar sind, etwa zu der niedersächsischen Landtagsabgeordneten Nadja Weippert von den Grünen oder zum Bundestagsabgeordneten Markus Grübel von der CDU. Betroffen sind den Spiegel-Recherchen zufolge weitere Politiker, Wirtschaftsbosse, auch die Hamburger Polizei mit ihren rund 35 elektronischen Streifenwagen sowie mutmaßliche Nachrichtendienstmitarbeiter.

Die VW-Tochter Cariad ist für die Softwareentwicklung des Autokonzerns zuständig. Wegen einer „Fehlkonfiguration“ seien die Daten nicht ausreichend gesichert worden. Es handelt sich um mehrere Terabyte an Standortdaten von Fahrzeugen der Marken VW, Seat, Audi und Skoda. Gesammelt hatte diese Daten die Volkswagen-App, über die sich verschiedene Informationen zum Zustand der Fahrzeuge abrufen lassen. Zu 460.000 Fahrzeugen sind die entdeckten Daten so präzise, dass sie Rückschlüsse auf das Leben der Menschen hinter dem Steuer zulassen. Ca. 300.000 der betroffenen Fahrzeuge sind in Deutschland zugelassen. Die Geodaten bei VW- und Seat-Modellen sind auf zehn Zentimeter genau.

Laut der Recherche konnten die Daten teilweise mit persönlichen Profilen von Fahrzeughaltern und -halterinnen verknüpft werden. Die detaillierten Bewegungsdaten konnten teilweise mit Adressen und Handynummern zusammengeführt werden. CCC-Sprecher Linus Neumann spricht von einem „riesigen Schlüsselbund, der unter einer viel zu kleinen Fußmatte lag“. Cariad habe erklärt, dass die Daten gesammelt worden seien, „um Batterien und die dazugehörige Software zu verbessern“. Die beschriebene Zusammenführung sei niemals so vorgenommen worden, „dass ein Rückschluss auf einzelne Personen möglich ist oder Bewegungsprofile erstellt werden“.

Nachdem der CCC auf die zugängliche Datensammlung aufmerksam gemacht worden war, wurden Cariad und die VW-Konzernzentrale informiert. Die Konzerntochter reagiert binnen weniger Stunden und versuchte erst gar nicht das Ausmaß des Vorfalls kleinzureden. Mittlerweile wurde die Lücke gestopft, auf die Daten können Unbefugte nicht mehr zugreifen. Bei der „Fehlkonfiguration“ handelte es sich um die Kopie des jeweils aktuellen Speicherauszugs einer Anwendung von Cariad. Darin lagen die Zugangsdaten zum Cloudspeicher bei Amazon, wo sich die Bewegungsdaten befanden.

Mit den Daten hätten, so der Spiegel, Unbefugte beispielsweise ermitteln können, welche Fahrzeuge regelmäßig vor Gebäuden des Geheimdiensts oder des US-Militärs parken und wem die gehören. Auch hätte man damit herausfinden können, welche Autos etwa regelmäßig vor einem Bordell, einem Gefängnis oder Suchtkliniken halten, und damit Erpressungsversuche in die Wege leiten können. Auch für Stalking wären die Daten enorm hilfreich gewesen. Die grüne Nadja Weippert wies darauf hin, dass sie als Landes- und Kommunalpolitikerin Anfeindungen und Drohungen ausgesetzt ist: „Es kann nicht sein, dass meine Daten unverschlüsselt in der Amazon-Cloud gespeichert und dann nicht einmal ausreichend geschützt werden. Ich erwarte, dass VW das abstellt, insgesamt weniger Daten erhebt und diese auf jeden Fall anonymisiert.“ Der betroffene CDU-MdB Markus Grübel findet die Datenpanne „ärgerlich und peinlich“: „Besonders mit Blick aufs autonome Fahren und mögliche manipulierende Hackingangriffe darauf muss die IT-Kompetenz der Hersteller offenbar noch deutlich zulegen.“

Laut Cariad gibt es nach aktuellem Kenntnisstand keine Hinweise darauf, dass außer dem CCC und dem Spiegel Dritte auf die Daten Zugriff hatten. Für die Kunden bestehe „keinerlei Handlungsbedarf, da keine sensiblen Informationen wie Passwörter oder Zahlungsdaten betroffen sind“ (Beuth/Flüpke/Hoppenstedt/Kreil/Rosenbach/Wilkin, Wir wissen, wo dein Auto steht, Der Spiegel Nr. 1 28.12.2024, S. 60-62; Holland, 38C3: Terabyte an Bewegungsdaten von VW-Elektroautos in

der Cloud gefunden, <https://www.heise.de> 27.12.2024, Kurzlink: <https://heise.de/-10220623>).

## Bundesweit

### Datenbroker beschaffen hochsensible Standortdaten

Recherchen von Netzpolitik, Bayerischem Rundfunk (BR) und dem US-amerikanischen Online-Medium Wired zeigen auf, wie Datenhändler Daten von Millionen Smartphones – auch in Deutschland – verkaufen. Davon erfasst sind auch Standortdaten von Menschen mit Zugang zu militärischen Arealen. Die Recherche stützt sich auf 3,6 Milliarden Standortdaten, die ein US-Datenhändler gratis zur Verfügung gestellt hat; laut Netzpolitik als Kostprobe für ein Abonnement. Darin enthalten sind Standortdaten von Geräte-IDs, die an US- und Nato-Stützpunkten in Deutschland erfasst wurden.

Im Juli 2024 hatten Recherchen von Netzpolitik und BR anhand eines Samples aufgezeigt, dass Datenhändler Standortdaten milliardenfach zum Verkauf anbieten. Erfasst werden solche Daten zu Werbezwecken, sie lassen sich aber auch zu Spionagezwecken nutzen. Gekauft werden sie entsprechend nicht nur von Werbetreibenden, sondern auch von Geheimdiensten. Die Datenbroker prüfen laut Netzpolitik nicht besonders genau, wer die Daten zu welchen Zwecken kaufen möchte.

Einmal gekauft, lassen die Daten gemäß Netzpolitik detaillierte Rückschlüsse auf die Aktivitäten einzelner Personen zu: „Die Wege einzelner Personen mit Zugang zu sicherheitsrelevanten Bereichen lassen sich nachverfolgen, von Baracken bis hin zu Privatadressen, bis zum Supermarkt und teils sogar bis in Bordelle“. Mit solchen Informationen könne man Einzelpersonen unter Umständen erpressen. Oder man könne zum Beispiel gezielt versuchen Handwerker mit Zutritt zu sensiblen Bereichen anzuwerben.

Das Problem beschäftigt Geheimdienste und Militär aus Deutschland und den USA bis in die höchsten Ebenen. Die Gefahren sogenannter Adver-

tising-based-Intelligence, kurz ADINT, sind seit Jahren bekannt: So warnte etwa das Nato-Forschungszentrum Stratcom schon 2021 in einem Bericht davor, dass sich militärisches Personal anhand von Standortdaten identifizieren lässt. Trotzdem bekommen Verantwortliche das Problem nicht in den Griff. Laut Netzpolitik setzen deutsche und US-Behörden vor allem darauf ihre Beschäftigten für die Problematik zu sensibilisieren. Dass das nicht besonders gut klappt, zeigt die aktuelle Recherche.

Es gibt zwar offenbar Ideen, um das Problem anzugehen, die aber bislang nicht umgesetzt wurden. Der Ansatz einer besseren Regulierung des Datenhandels wurde bisher nicht näher verfolgt. Der Vorsitzende des Parlamentarischen Kontrollgremiums, Konstantin von Notz (Bündnis 90/Die Grünen), sagte dazu, dass es zwar gut sei, dass die Problematik nach den Recherchen von BR und Netzpolitik im Sommer ernster genommen werde, die Konsequenzen seien aber unklar. Das Bundesinnenministerium hält nichts davon deutschen Geheimdiensten den Kauf solcher Datensätze zu untersagen, um den Markt nicht weiter zu stützen. Die Bundesdatenschutzbeauftragte hatte vorgeschlagen die Datenhändler stärker in die Verantwortung zu nehmen.

Verbraucherschützer und Politiker blicken deshalb offenbar auf die EU. Die Präsidentin des Bundesverbands der Verbraucherzentralen, Ramona Pop, forderte im Sommer 2024 ein EU-weites Verbot von Profilbildung und Tracking zu Werbezwecken. Der stellvertretende Vorsitzende des Parlamentarischen Kontrollgremiums, der CDU-Abgeordnete Roderich Kiesewetter, sagte, er halte eine Regulierung dieser Praxis durchaus für denkbar. Es könnte „beispielsweise beschlossen werden, dass Internetdienste nicht mehr Daten erheben dürfen als für deren Funktionsfähigkeit notwendig“. Der liberale EU-Abgeordnete Moritz Körner meinte hingegen, dass die DSGVO bereits klar regelt, „dass das nicht geht“. Die Durchsetzung funktioniere nur nicht (Stoll, Medienrecherche: Standortdaten lassen sich zu Spionagezwecken nutzen. <https://www.heise.de> 21.11.2024, Kurzlink: <https://heise.de/-10081732>; Anyone Can Buy Data Tracking US Soldiers and Spies to

Nuclear Vaults and Brothels in Germany, <https://www.wired.com> 19.11.2024; Meineck/Dackwitz, Firma verschleudert 3,6 Milliarden Standorte von Menschen in Deutschland, <https://netzpolitik.org> 16.07.2024).

## Bundesweit

### Schadenersatzkampagne von Privacy ReClaim und vzbv wegen Android-Datensammlung

Das Münchener Unternehmen Privacy ReClaim kündigte Ende November 2024 an Google wegen massenhaften Sammelns von Nutzerdaten zu verklagen – und bietet Android-Nutzern 40 Euro, wenn diese ihre Ansprüche gegen Google an das Unternehmen abtreten bzw. verkaufen. Klagegrund ist das massenhafte Sammeln von Nutzerdaten, die der Konzern ohne Rechtsgrundlage verarbeitet. Google anonymisiere einen Großteil der gesammelten Daten von Anwendungen wie Dating- oder Schwangerschaft-Apps und Standorten nicht, sondern verknüpfe sie mit den Nutzern. Dadurch würden Einzelpersonen identifizierbar, weshalb ihnen Schadenersatz zustehen. Um klagen zu können, will Privacy ReClaim vielen Android-Nutzern diese potenziellen Ansprüche abkaufen. Insgesamt möchte das Unternehmen so die Rechte von 100.000 Nutzenden einsammeln, um eine gewisse Schlagkraft gegenüber Google entfalten zu können. Drei von vier Handybesitzern haben hierzulande ein Android-Gerät, nutzen also das mobile Betriebssystem von Google. All diese Menschen könnten die 40 Euro in Anspruch nehmen und ihre Rechte abtreten.

Alex Petrasincu, Anwalt und Partner einer Rechtsanwaltskanzlei, die Privacy ReClaim vertritt, sagt: „Google greift bei der Nutzung von Android-Handys deutlich mehr Daten ab, als allgemein bekannt ist.“ Abhängig von den individuellen Datenschutzeinstellungen der Nutzenden wisse Google zum Teil, ob jemand regelmäßig ins Gebäude eines Arztes gehe oder eine Kirche, Moschee oder Synagoge besuche. „Was Google mit den Daten macht, weiß ich nicht. Aus unserer Sicht verstößt die Daten-

verarbeitung der persönlichen Daten von Android-Nutzern in dem aktuellen Umfang aber gegen die Datenschutz-Grundverordnung.“ Das Gutachten, auf das sich Petrasincu bezieht, hat Privacy ReClaim selbst beauftragt.

Das Unternehmen erwartet Schadenersatzzahlungen in vierstelliger Höhe je Betroffenen. Das Angebot sei dennoch wirtschaftlich für die Betroffenen sinnvoll: „Für einen eigenen Anwalt muss man rund 500 zahlen, dazu kommen in der ersten Instanz Gerichtskosten von 300 Euro – und wenn man verliert, hat man noch das Kostenrisiko für die Gegenseite von erneut rund 500 Euro.“ Da sei es doch besser, die 40 Euro zu nehmen, als gar nichts zu bekommen.

Nach Angaben des Unternehmens haben bereits mehrere Tausend Verbraucher ihre Ansprüche verkauft und 40 Euro bekommen. Im Jahr 2025 will Privacy ReClaim dann die Klage vor einem deutschen Landgericht einreichen.

Am 09.12.2024 kündigte dann die Verbraucherzentrale Bundesverband (vzbv) an wegen des Facebook-Datenlecks eine Sammelklage als Musterfeststellungsklage beim Hanseatischen Oberlandesgericht Hamburg einzureichen, um Verbrauchern Schadenersatzansprüche zukommen zu lassen. Das Bundesamt für Justiz muss hierfür ein Klageregister öffnen, in das sich Klagegwillige eintragen können. Durch die Sammelklage wird die Verjährung der Ansprüche, die ansonsten Ende 2024 eingetreten wäre, verhindert. Die Betroffenen konnten anhand einer Webseite prüfen, ob sie betroffen sein könnten, und sich melden, um informiert zu werden, wenn sie sich in das Klageregister eintragen können, was Anfang 2025 der Fall sein soll.

Der Fall des Facebook-Datenlecks, über den der Bundesgerichtshof (BGH) am 18.11.2024 entschieden hat (Az. VI ZR 10/24, s. u. S. 50), zeigt, dass es möglich ist, derart gegen Datenschutzverstöße vorzugehen: Unbekannte hatten auf der Plattform 2021 eine Funktion zur Freunde-Suche ausgenutzt und damit Daten von Hunderten Millionen Nutzern abgegriffen, darunter Namen und Telefonnummern. Ein Betroffener hatte deshalb mithilfe einer Kanzlei gegen den Facebook-Mutterkonzern Meta wegen Datendiebstahls geklagt.

Der BGH setzte mit seiner Entscheidung vergleichsweise niedrige Hürden für einen Schadenersatzanspruch. Klagende müssen nur nachweisen, dass sie Opfer des Vorfalls waren. Allerdings ist auch der Geldbetrag, den Betroffene laut BGH in dem Fall erwarten können, mit ca. 100 Euro eher niedrig. Der BGH machte deutlich, dass der Schadenersatz beim bloßen Kontrollverlust nicht allzu hoch ausfallen könne.

Christoph Herrmann, Rechtsexperte der Stiftung Warentest, kommentiert: „Grundsätzlich ist gegen den Verkauf der Forderung nichts einzuwenden. Verbraucher-Inkasso kann ein absolut faires Geschäft sein“. Ein Problem sei natürlich der Kaufpreis und wie viel Arbeit es mache beim Ankäufer seine Daten einzugeben. Zudem sollten Verbraucher ihre Rechte nur abtreten, wenn sie ein Standardfall seien und der Schaden nicht wirklich wehgetan habe. Ist ansonsten viel mehr als 100 Euro Schadenersatz fällig, wäre es besser sich selbst einen Anwalt zu nehmen.

Neben dem Anspruchsverkauf gibt es auch die Verbandsklage: Verbraucherschutzverbände können Schadenersatz für Betroffene gesammelt einklagen, so Herrmann: „Das passt für die großen spektakulären Fälle, bei denen die Verbraucherverbände die nötigen Kapazitäten mobilisieren können.“ Aber es sei illusorisch zu glauben, dass sie gegen einen nennenswerten Anteil aller möglichen Fälle vorgehen können.

Ein Sprecher von Google erklärte: „Privacy ReClaim mangelt es an technischem Wissen und verzerrt weithin dokumentierte Fakten über die Funktionsweise moderner Smartphones.“ Google arbeite in voller Übereinstimmung mit den geltenden Datenschutzgesetzen und stelle Nutzerinnen und Nutzern Datenschutz-Tools zur Verfügung, mit denen sie die Kontrolle über ihre Daten behalten. Der Google-Fall wird wohl durch mehrere Instanzen gehen, bis es zu einer höchstgerichtlichen Entscheidung kommt. Wie hoch, wenn überhaupt, dann der Schadenersatz für Betroffene ausfällt, ist unklar (Hauck, 40 Euro für Android-Nutzer, SZ 25.11.2024, 13; Nach BGH-Urteil zu Facebook-Datenleck: vzbv reicht Sammelklage ein, <https://www.verbraucherzentrale.de> 09.12.2024).

## Bundesweit

## Schufas Transparenzinitiative mit Bonify

Mietvertrag, Autokauf, Onlineshopping oder Mobilfunkvertrag – nichts geht ohne Schufa. Die Wirtschaftsauskunftei gibt über ihren Schufa-Score an, wie zahlungskräftig und kreditwürdig Kundinnen und Kunden sind. Daten von rund 68 Millionen Menschen liegen auf den Servern des Unternehmens. Bei Käufen oder Verträgen erhält der Kunde den sogenannten Schufa-Hinweis und das Schufa-Informationsblatt, in dem erklärt wird, dass und wie die Schufa Daten verarbeitet. Ein Algorithmus ermittelt aus diesen und aus anderen persönlichen Daten den so genannten Schufa-Score.

Die Schufa stellt seit dem 26.11.2024 Verbrauchern über die Finanzplattform Bonify, die von der Wirtschaftsauskunftei Ende 2022 übernommen worden war, nahezu alle ihre individuellen bonitätsrelevanten Daten digital zur Verfügung. Nutzer können über die App der Schufa-Tochter auch gratis einsehen, welche Unternehmen in den vergangenen 12 Monaten Daten über sie abgefragt haben und welche Vertragsinformationen gespeichert sind. Dazu zählen bestehende Kreditkarten, Girokonten sowie laufende Raten- und Immobilienkredite. Bisher war dies nur über die kostenlose und per Post versandte „Datenkopie“ oder für tagesaktuelle Informationen über die Schufa-Abo-Produkte möglich, die mit monatlichen Kosten von 4,95 Euro für die Bonitätsauskunft inklusive tagesaktuellem Score starten und beim Premiumtarif für 9,99 Euro enden. Eine einmalige Bonitätsauskunft bietet die Schufa für knapp 30 Euro an.

Andreas Bermig, Gründer und Chef von Bonify, erklärte, bei den nun einsehbaren Vertragsdaten und Benachrichtigungen über Zugriffe auf die eigene Bonität handle es sich um das „finale Puzzlestück“. Neun Jahre habe das Startup daran gearbeitet Nutzern dabei zu helfen ihre Bonität zu verbessern. Schritt für Schritt seien – auch dank der laufenden Transparenzinitiative der Schufa – mehr Informationen dazugekommen und nun „sämtliche

Schufa-Daten“ digital über die App verfügbar. Stoße der Nutzer auf „Unstimmigkeiten“ etwa bei den sich neutral bis positiv auswirkenden Vertragsdaten, gelange er „mit einem Klick“ auf den Button „Fehler melden“ zur Schufa und könne dort über das Hilfeportal einen „Korrekturvorgang anstoßen“.

Für die allgemeine Inanspruchnahme der Bonify-App ist eine Registrierung mit dem Personalausweis per Identverfahren oder über ein eigenes Bankkonto erforderlich. Im zweiten Fall müssen Verbraucher zunächst einwilligen, dass der Anbieter „den Kontosaldo sowie die Kontoumsatzdaten von bis zu vierundzwanzig Monaten abrufen“.

In einem zweiten Schritt steht es Nutzern frei ihre Transaktionshistorie mit Bonify zu teilen, wenn sie etwa einen zusätzlich angebotenen Score für „finanzielle Fitness“ angezeigt bekommen wollen. Bermig versichert, dass in diesem Fall die Daten aber nicht an die Schufa oder andere Dritte gehen. Die Verbraucherzentrale Bayern warnte, dieses Angebot zur Bonitätsverbesserung könnte „viele Nutzer dazu verleiten leichtfertig einen Einblick in die Kontodaten zu gewähren“. Die Bürgerbewegung Finanzwende hatte sogar eine Online-Petition gegen die App ins Leben gerufen. Michael Möller, Referent für Verbraucherschutz bei Finanzwende, meinte: „Daten wie Gehalt oder Kontostand sind sensibel und gehen die Schufa nichts an, finden wir.“

Bestehende Bonify-Nutzer müssen für die Einsicht von Vertragsinformationen ein Update durchführen. In der App erscheint dann die entsprechende weitere Kachel. Wer diesen Service in Anspruch nehmen will, muss sich zusätzlich mit dem elektronischen Identitätsnachweis (eID) des Personalausweises identifizieren. Dabei geht es, so die Schufa, darum „eine eindeutige Zuordnung der Daten sicherzustellen“. Alle nach 2017 ausgestellten Personalausweise verfügten über die einschlägige Möglichkeit. Es werde dazu die persönliche PIN und ein Mobilgerät benötigt, das NFC-fähig ist beziehungsweise eine Kontaktlosfunktion hat.

Bereits seit Mitte 2023 können Bonify-Nutzer Einblick in ihren individuellen Basis-Score der Schufa nehmen. Im Bereich der Bonitätswerte arbeitet

die Auskunftei parallel an einer Vereinfachung. Seit Ende Januar 2024 sind dort ebenfalls Negativeinträge einsehbar – sofern vorhanden. Im Juni 2024 startete ein Benachrichtigungsservice, über den sich Nutzer über Bonify digital und kostenlos informieren lassen können, wenn erstmalig ein Negativeintrag gespeichert wird oder jemand erneut in den Negativbereich rutscht. Größter Unterschied jenseits des Preises: Bei der Tochter werden die Daten quartalsweise aktualisiert, beim Online-Abo der Schufa tagesaktuell. Zudem gibt es über Letzteres Hinweise auf jede Veränderung bei Negativeinträgen.

Bonify hat Bermig zufolge aktuell knapp über 2 Millionen Nutzer, 70.000 bis 80.000 neue kämen pro Monat dazu: „Wir wollen auf 10 Millionen Nutzer wachsen bis 2030.“ Die hinter Bonify stehende Berliner Firma Forteil habe eine eigene Lizenz für Kreditvermittlung, die sie eventuell über ihren Marktplatz später wieder forcieren werde. Aktuell stehe aber die Bonitätsdarstellung im Fokus neben Diensten wie einem Darknet-Monitoring über Partner („Ident Protect“). Skurrilerweise waren über die App sogar „Schufa-freie“ Digitalkredite im Angebot.

Das Bundesministerium für Verbraucherschutz drängt seit Langem auf mehr Transparenz bei der Schufa. Es kritisierte zudem im Jahr 2023 die über Bonify ermöglichten Kontoeinblicke: Der Anbieter – und möglicherweise könnten so vertrauliche Finanzdaten einsehen, auf die sie bislang keinen Zugriff hätten. Sicherheitslücken, wie sie die IT-Sicherheitsforscherin Lilith Wittmann auch bei der Bonify-App bereits aufgedeckt hatte, dürften sich nicht wiederholen: Für einen kurzen Zeitraum war es ihr zufolge über eine unsichere Schnittstelle möglich beliebige Daten, wie die Bonität des CDU-Politikers Jens Spahn, aus dem Dienst abzurufen (Eberl, Schufa-Dienst „bonify“ Die Tücken des Bonitäts-Checks per App, <https://www.tagesschau.de/06.11.2024>; Krempel, Schufa: Alle bonitätsrelevanten Daten jetzt digital einsehbar, <https://www.heise.de/26.11.2024>).

## Bundesweit/NRW

### CDU-ler und Polizisten fordern Zugriff auf Daten psychisch Kranker

Der Anschlag auf den Weihnachtsmarkt in Magdeburg am 20.12.2024 hat die Diskussion um die Prävention von Gewalttaten und die Früherkennung von potenziellen Tätern erneut entfacht. CDU-Generalsekretär Carsten Linnemann forderte zuletzt ein Register psychisch erkrankter Gewalttäter. Ermittler wünschen sich in solchen Fällen eine Auflockerung der ärztlichen Schweigepflicht.

In Nordrhein-Westfalen (NRW) gibt es bereits einen Ansatz, um potenzielle Attentäter frühzeitig zu erkennen. Das Programm heißt „PeRisikoP“ (Personen mit Risikopotenzial). Der Fokus liegt auf Menschen mit psychischer Erkrankung. In jeder Polizeibehörde gibt es Beamte, die dafür eng mit Gesundheitsämtern und Kliniken zusammenarbeiten. Der 38-Jährige Iraner, der im Oktober 2024 versucht hat einen Brandsatz in einem Krefelder Kino zu zünden, war hier registriert. Es ist nicht die erste Tat eines Menschen, der durch PeRisikoP beobachtet wird. Deshalb gibt es Zweifel an der Effektivität des Programms. Ermittler kritisieren, dass ihre Möglichkeiten bei PeRisikoP zu eingeschränkt sind.

Mehr als 5.000 Menschen wurden 2024 von PeRisikoP überprüft, 362 von ihnen werden als gefährlich eingestuft und überwacht. Trotzdem kommt es immer wieder zu Anschlägen solcher Risikopersonen. Beispiele gibt es mittlerweile einige. Der Syrer, der im Herbst 2024 zwei Häuser in Essen angezündet hatte, stand unter Beobachtung von PeRisikoP. Auch beim versuchten Amoklauf an einem Bielefelder Berufskolleg 2022 und bei einem Messerangriff auf zwei Duisburger Grundschüler in Duisburg 2024 handelte es sich um Täter, die bei PeRisikoP gelistet waren.

Oliver Huth vom Bund Deutscher Kriminalbeamter sieht durch solche Beispiele das Vertrauen der Bürger in die Arbeit der Sicherheitsbehörden gefährdet. PeRisikoP sei ein guter und wichtiger Ansatz, doch wenn die Ermittler eine Person im Fokus haben, sei man darauf angewiesen, dass die Person selbst die behandelnden Ärzte von der Schwei-

gepflicht entbindet: „Ich würde mir tatsächlich wünschen, dass die Polizei direkten Zugriff auf Gesundheitsdaten bekommen kann.“ Man könne durch einen Verhaltenskodex verhindern, dass die Daten innerhalb der gesamten Polizei kursieren. Dies sei in anderen Deliktsfeldern, wie bei sexuellem Missbrauch an Kindern, auch gelungen.

Die Forderung, die Schweigepflicht zu lockern, sehen Mediziner kritisch. Mazda Adli, Psychiater am Berliner Fliedner Klinikum, warnt vor den Folgen: „Wir können davon ausgehen, dass Menschen sich erst dann öffnen, wenn sie einen Schutzraum vorfinden, bei dem garantiert ist, dass das, worüber sie sprechen, nicht weitergetragen wird.“ Adli sieht in den derzeitigen Debatten die Gefahr einer pauschalen Stigmatisierung. Im schlimmsten Fall würden Menschen mit psychischer Erkrankungen sich überhaupt keine Hilfe mehr holen, weil sie befürchten als Sicherheitsrisiko zu gelten.

Die SPD nennt die Vorschläge für ein Register psychisch kranker Gewalttäter oder zur Lockerung der Schweigepflicht populistisch. Es brauche keine neuen Gesetze, sondern konsequentere Verfolgung von Warnsignalen, so Lisa Kapteinat, stellvertretende Fraktionsvorsitzende der SPD im NRW-Landtag: „Bei dem Täter von Magdeburg hat es ja nicht an Hinweisen gemangelt, sondern eher daran, dass niemand die so umgesetzt hat, wie es offensichtlich angemessen gewesen wäre.“ Auch die FDP warnt, dass es keine einfachen Lösungen gibt. Es brauche interdisziplinäre Teams aus Psychologen, Sozialarbeitern und Sicherheitskräften, die auffällige Personen engmaschig betreuen und potenzielle Gefährdungssituationen entschärfen, so Marc Lürbke, innenpolitischer Sprecher der FDP-Landtagsfraktion.

Auch NRW-Innenminister Herbert Reul hält von einer Lockerung der ärztlichen Schweigepflicht wenig: „Patientenschutz ist extrem wichtig.“ Eine Lockerung in diesem Bereich sei mit ihm nicht zu machen. „Deshalb lebe ich mit dem Risiko und auch mit der Erklärungsnot, die ich dann geben muss.“ Den Fällen aus Krefeld, Duisburg oder Essen hält Reul entgegen, das 90 Prozent der beobachteten Menschen bei PeRisikoP nicht straffällig werden. Eine hundertprozentige Sicherheit gebe es nun mal nicht, aber man könne das Risiko reduzieren.

Dies ist nach Ansicht Reuls zumindest in NRW in den vergangenen Jahren gelungen (Köksalan/Sprenghart, Ermittler fordern weniger Datenschutz im Kampf gegen Attentate, <https://www1.wdr.de> 12.01.2025).

## Baden-Württemberg/Bayern

### Datenlecks bei Auskunftsdiensten „it’s my data“ und Infoscore Consumer Data

Auskunfteien wie die Schufa oder Infoscore geben Einschätzungen über die Kreditwürdigkeit möglicher Vertragspartner ab. Nicht nur Banken und Unternehmen, sondern auch Vermieter fordern diese Informationen routinemäßig an. Das Münchener Start-up „it’s my data“ macht aus diesem Umstand gleich mehrere Produkte wie einen „Bonitätspass“ und eine „Mietermappe“ zur Vorlage beim Vermieter. Die „it’s my data“-Produkte seien von Maklern empfohlen, 100 Prozent DSGVO-konform und zertifiziert für digitale Transparenz, so die Eigenwerbung des Unternehmens.

Doch Hackerin Lilith Wittmann stellte mehr Transparenz her als vom Anbieter beabsichtigt. Nachdem sie ein Konto bei „it’s my data“ angelegt hatte, konnte sie mithilfe eines ungeschützten API-Calls ihre eigenen Daten wie Name und Meldeadresse ändern und durch die einer fremden Person ersetzen. Deren Bonitätsauskunft erhielt sie dann im praktischen PDF-Format. Laut Wittmann ließ sich dieses Vorgehen mehrfach wiederholen.

Fast zeitgleich fand Lilith Wittmann eine Schwachstelle bei der Absicherung der Datenbank von Infoscore Consumer Data (ICD). Über eine von ihr programmierte Webseite ließen sich Bonitätsdaten von mutmaßlich allen bei Infoscore gelisteten Personen finden. Infoscore hat seinen Sitz in Baden-Baden. Gemäß eigenen Angaben hat das Unternehmen Negativdaten wie Privatinsolvenzen oder erfolglose Mahnverfahren von 8 Mio. Menschen gespeichert. Sie alle waren von dem Datenleck potenziell betroffen. Infoscore reagierte umgehend. Man sei über einen mutmaßlichen IT-Sicherheitsvorfall bei zwei Partnerunternehmen unterrichtet worden: „Wir haben sofort Maßnahmen ergriffen, um

den Zugriff der betroffenen Unternehmen auf Daten der Infoscore Consumer Data zu unterbinden.“

Derlei Lücken sind für die Berlinerin Wittmann nichts Neues: Bereits vor gut einem Jahr hatte sie sich die App „Bonify“, eine Schufa-Tochter, vorgenommen und ebenfalls Bonitätsdaten eines Prominenten abgerufen (s.o. S. 34). Die Kreditwürdigkeit des Ex-CDU-Gesundheitsministers habe sich immerhin ein wenig verbessert, bemerkte Wittmann belustigt in den sozialen Netzwerken (Heck, Großes Datenleck bei wichtiger Auskunft, SZ 19.11.2024, 14; Kunz, Datenleck bei Online-Auskunft: Hackerin kann beliebige Bonitätsdaten einsehen, <https://www.heise.de> 14.11.2024, Kurzlink: <https://heise.de/-10034774>).

## Bayern/weltweit

### BayLDA geht gegen World-Iris-Identifikation vor

Das vom KI-Unternehmer Sam Altman (ChatGPT) mitgegründete World (ehemals Worldcoin) will mit Hilfe von Augen-Scans dafür sorgen, dass sich Menschen im Internet identifizieren können. Diese Technologie verspricht die Sicherheit und Anonymität der Nutzer durch dezentral gespeicherte Daten zu erhöhen. Dabei werden einige Daten verschlüsselt und aufgeteilt auf verschiedene Anbieter gespeichert. Aus Sicht von World ist damit eine Anonymisierung gewährleistet. Bei dem Dienst legen Menschen mit einem Scan der Iris ein Profil – die „World ID“ – an. Damit soll man sich im Internet zum Beispiel von KI-Fakes unterscheiden können. Die Profile werden nicht bei World gespeichert, sondern auf die Geräte der Nutzer übertragen.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) kam jedoch zu dem Schluss, dass dieses nicht reicht und weitere Anpassungen wie die Umsetzung des Rechts auf Löschung notwendig sind. Es hat am 19.12.2024 eine entsprechende Verfügung erlassen. Zuvor hatte es eine Abstimmung mit sämtlichen betroffenen europäischen Datenschutzbehörden gegeben. Über die Verhängung eines Bußgeldes

könnte gesondert entschieden werden. Das BayLDA ordnete auch an, dass World für einige Schritte bei der Verarbeitung eine ausdrückliche Erlaubnis einholen müsse. Mit der Entscheidung, die europaweit zu befolgen ist, wurde ein im April 2023 eingeleitetes Prüfverfahren abgeschlossen. World kündigte an gegen die Entscheidung rechtlich vorzugehen. Das Unternehmen will vor Gericht vor allem Standards für eine Anonymisierung von Daten in Europa klären lassen. Die Frage dabei ist, ab welchem Punkt man davon ausgehen kann, dass Informationen nicht mehr mit Nutzern in Verbindung gebracht werden können.

World sieht ein Problem in dem Recht auf Löschung der Daten. Eine Grundidee des Projekts sei, dass Menschen nur ein Profil angelegen können, um sich damit eindeutig identifizieren zu können. Im aktuellen System wird deshalb anhand der anonymisierten und abgewandelten Daten erkannt, wenn ein Nutzer sich nicht zum ersten Mal registriert. Bei einer Löschung der Daten wären aber mehrere Anmeldungen möglich.

World setzt darauf, dass die Entscheidung mit dem Widerspruch bis zur Klärung ausgesetzt wird. Die Diskussion um die Anonymisierung von Daten und das Recht auf Datenlöschung könnte weitreichende Auswirkungen auf die europäische Datenschutzlandschaft haben. Experten sind sich uneinig darüber, ab wann Daten tatsächlich nicht mehr einem einzelnen Nutzer zugeordnet werden können. Diese Frage wird künftig weiter diskutiert werden, der Fall World könnte als Präzedenzfall für zukünftige Entscheidungen dienen (BayLDA PM v. 19.12.2024, Erste Ergebnisse der Worldcoin-Untersuchung; Streit um Augen-Scans könnte Daten-Anonymisierung klären, <https://www.flz.de> 19.12.2024; Worlds Datenanonymisierung: Ein Streit um Datenschutz in der EU, <https://www.it-boltwise.de> 19.12.2024).

## Berlin

### Rechte Presse wird mit polizeilichen Internamunitioniert

Die Berliner Polizei ermittelt wegen eines Verstoßes gegen den Datenschutz in

den eigenen Reihen. Ein Beamter hatte demnach eine Liste mit Vornamen der Verdächtigen in der Silvesternacht an das rechte Portal „Nius“ des ehemaligen „Bild“-Chefredakteurs Julian Reichelt durchgestochen. Der Sprecher der Berliner Polizei, Florian Nath, bezeichnete dies als inakzeptabel: „Die Herausgabe persönlicher Daten ohne jede rechtliche Grundlage“ werde von der Polizei Berlin immer verfolgt. Gegen den oder die Beamten, die die Namensliste möglicherweise aus „geschützten, internen Polizeisystemen rechtswidrig extrahiert und herausgegeben haben“, ermittle das Dezernat für Polizei- und Korruptionsdelikte beim Landeskriminalamt. Die Herausgabe dieser Unterlagen sei nicht nur ein Verstoß gegen den Datenschutz, sondern „befeuert nebenher einen unverhältnismäßigen und diskriminierenden Erklärungsansatz für individuelle, strafrechtliche Verhaltensweisen“.

Das rechte Portal „Nius“ wollte nach eigenen Angaben mit der polizeiinternen Liste belegen, dass unter den vielen deutschen Verdächtigen der Silvesternacht ein Großteil einen Migrationshintergrund hat. Die Polizei darf den Migrationshintergrund von Verdächtigen nicht erfassen. Also wird versucht, aus den Vornamen Rückschlüsse auf eine vermeintliche Migrationsbiografie zu ziehen.

Der innenpolitische Sprecher der Linken, Niklas Schrader, hält den Vorgang für einen „handfesten Skandal“: „Jemand in der Berliner Polizei meint personenbezogene Daten an ein rechtes Portal geben zu können, um eine rechte Debatte anzufeuern.“ Dabei wisse jeder Polizist, dass Vornamen kriminologisch keine empirische Grundlage darstellen. „Die Namensdebatte führt zu nichts und ist kontraproduktiv“. Bei der Suche nach Ursachen der Gewalt und nach strategischen Lösungen sei dies nicht zielführend. Schrader kündigte an den Vorfall im Innenausschuss zu besprechen. „Ich erwarte von der Innensenatorin eine Übersicht, wer überhaupt auf diese Daten Zugriff hat.“ Die Verantwortlichen müssten disziplinarrechtlich und möglicherweise auch strafrechtlich sanktioniert werden. Die Senatsinnenverwaltung wollte sich nicht zum Vorfall äußern.

Kritik kommt von Berlins Datenschutzbeauftragter Meike Kamp: „Die Herausgabe personenbezogener Daten aus poli-

zeitlichen IT-Systemen für private Zwecke stellt einen schweren Verstoß gegen die Datenschutzgesetze dar.“ Kamp begrüßt die internen Ermittlungen: „Wer so eine Liste unbefugt erstellt oder herausgibt, muss mindestens mit einem Bußgeld rechnen.“

Es ist nicht das erste Mal, dass im Zusammenhang mit der Silvesternacht die Vornamen von Tatverdächtigen ins Spiel gebracht werden. Nach den Krawallen in der Silvesternacht 2022 hatte die CDU 2023 im Innenausschuss des Abgeordnetenhauses nach den Vornamen von Tatverdächtigen mit deutscher Staatsangehörigkeit gefragt. Dies sorgte für große Empörung und Rassismus-Vorwürfe. Auch die AfD-Fraktion hatte unmittelbar nach dem jüngsten Jahreswechsel eine parlamentarische Anfrage an den Senat zu den Vornamen der Verdächtigen angekündigt. Vor zwei Jahren war die rechts-extreme Partei bereits damit, den Senat per Gericht dazu zu verpflichten über die Staatsangehörigkeiten von Verdächtigen hinaus auch deren Vornamen mitzuteilen, gescheitert.

Nach aktuellen Zahlen der Berliner Polizei zu Vorfällen in der Silvesternacht wurden 1.453 für Silvester typische Straftaten registriert. 58 Polizisten und Polizistinnen sowie ein Mitarbeiter eines Rettungsdienstes wurden demnach angegriffen. Verletzt wurden dabei 17 Polizisten, 8 davon durch Pyrotechnik.

Die Polizei erfasste nach eigenen Angaben insgesamt 670 Verdächtige. 406 davon besitzen nach den Angaben eine deutsche Staatsangehörigkeit, 264 eine andere. 40 der Verdächtigen sollen Einsatzkräfte angegriffen haben. Dabei handele es sich laut Polizei um 16 Erwachsene, 12 Heranwachsende und 11 Jugendliche sowie ein Kind (Frank, Polizei ermittelt gegen Beamten – Vornamen Silvester-Verdächtiger nach rechts durchgestochen, <https://taz.de/Polizei-ermittelt-gegen-Beamten!/6061142/> 09.01.2025).

## Brandenburg

### Hochvertraulicher Polizeirechner ungeschützt am Netz

Ein Server der Staatsschutzabteilung des Landeskriminalamts (LKA) Brandenburg war offenbar lange Zeit öffentlich zugänglich, auf dem u. a. Geheimpapiere, Ermittlungsergebnisse und Passwörter lagen. Ein Bürger entdeckte das Leck bei der Nutzung eines öffentlichen Hinweisportals der Polizei im Internet für Zeugen eines tödlichen Brandes. Mit einem weiteren Klick gelangte er an einen eigentlich geheimen Netzwerkspeicher des Staatsschutzes, an den das Hinweisportal angebunden war. Der IT-affine Entdecker gab seine Erkenntnisse daraufhin an die Behörden weiter.

Die Brandenburger Polizei meldete die Sicherheitslücke am 20.09.2024 der Landesdatenschutzbeauftragten Dagmar Hartge und dem Innenministerium, welches mitteilte: „Der Vorfall wird derzeit als schwerwiegender Verstoß gegen datenschutzrechtliche Vorgaben und technisch-organisatorische Maßnahmen zum Schutz personenbezogener Daten gewertet.“ Es zeichnete sich ab, dass der mit dem Hinweisportal verbundene Server jahrelang vom polizeilichen Staatsschutz betrieben wurde. Der Server soll von der internen Security-Abteilung weder überprüft noch freigegeben worden sein. Es ist fraglich, ob das System Sicherheits-Updates erhalten hatte. Der Rechner war offenbar ohne Firewall ans Internet angebunden.

Das WLAN und ein Netzwerkspeicher mit Passwörtern für Verbindungen zu einem Server des Bundeskriminalamts (BKA) waren gemäß Presseberichten kaum geschützt. Das BKA kappte demnach nach der Entdeckung den Datenaustausch mit dem Staatsschutz des LKAs aus Sorge, Informationen könnten abgefischt werden. Unbefugten wäre es wohl leichtgefallen die Zugangsseite zum Datennetz

des Staatsschutzes zu finden und sich darüber Zugriff auf weitere Rechner zu verschaffen. Es gab zunächst keine Kenntnis über Anhaltspunkte dafür, dass Daten abgeflossen oder missbräuchlich verwendet worden sind (Krempel, Staatsschutz-Server offen: Gravierendes Datenleck bei Brandenburger Polizei, <https://www.heise.de> 04.12.2024, Kurzlink: <https://heise.de/-10188509>).

## Hessen

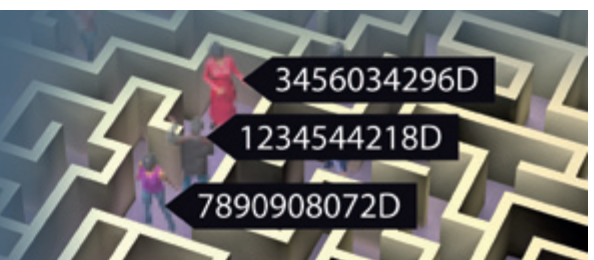
### Neues Polizeirecht erlaubt KI-Echtzeit-Einsatz bei Videoüberwachung

Der hessische Landtag hat am 12.12.2024 ein von der schwarz-roten Landesregierung vorgeschlagenes „Gesetz zur Stärkung der Inneren Sicherheit“ verabschiedet, das den polizeilichen Einsatz von KI voranbringen soll. Das Gesetz sieht vor, dass bei der Videoüberwachung öffentlicher Plätze die Daten mithilfe einer intelligenten Bildanalyse-Software ausgewertet werden. Deuten Bewegungsmuster auf eine bevorstehende Straftat mit erheblicher Bedeutung hin oder besteht der Verdacht auf Waffen, dann soll die Polizei unter bestimmten Bedingungen eine verdächtige Person in dem Bildmaterial markieren dürfen.

Drohen erhebliche Gefahren für das Leben oder die körperliche Unversehrtheit von Menschen, dann soll eine biometrische Echtzeit-Fernidentifizierung möglich sein. Mithilfe der Aufnahmen wird so gezielt nach dem möglichen Gefährder in den Datenbanken der Polizei gesucht. Der biometrischen Echtzeit-Fernidentifizierung wird die Prüfung durch einen Polizeibeamten oder eine Polizeibeamtin vorgeschaltet. Auch die Suche nach Vermissten, Opfern von Entführung, Menschenhandel oder sexual-

Jetzt in den Presseverteiler eintragen:  
**[www.datenschutzverein.de](http://www.datenschutzverein.de)**

Folgen Sie uns auf Mastodon:  
<https://eupolicy.social/@datenschutzverein>



ler Ausbeutung soll unter bestimmten Voraussetzungen möglich werden.

Brennpunkt-Bereiche wie beispielsweise das Frankfurter Bahnhofsgelände stehen bereits unter besonderer Videoüberwachung der Polizei, so die Gesetzesbegründung: „Eine vollständige und ausreichend schnelle Auswertung des gesicherten Bildmaterials ist jedoch aufgrund des erheblichen personellen und zeitlichen Aufwandes nicht möglich.“ Durch den Einsatz von entsprechender Bildanalyse-Software auf Grundlage künstlicher Intelligenz solle eine bessere Kontrolle von Brennpunkten möglich werden, um Straftaten zu verhindern und Opfer zu schützen.

Hessens Innenminister Roman Poseck (CDU) zeigte sich zufrieden: „Mit der intelligenten Videoüberwachung erhalten unsere Sicherheitsbehörden ein wichtiges präventives Instrument, um auf die steigenden Herausforderungen angemessen reagieren zu können.“ Die Polizei werde entlastet und zugleich werde die Effizienz gesteigert: „KI ist eine wertvolle Unterstützung, die Entscheidung trifft am Ende aber immer ein Mensch.“

Schon jetzt kommt KI bei den Sicherheitsbehörden an verschiedenen Stellen zum Einsatz. So beschleunigt KI im Kampf gegen sexuellen Missbrauch von Kindern und Jugendlichen die zielgerichtete Auswertung von Bild- und Videodateien. Zudem hat sich nach Ansicht der Regierung bei der Protokollierung von Vernehmungen die automatische Spracherkennung bewährt. In einer Antwort des Innenministeriums auf eine parlamentarische Anfrage der FDP-Landtagsfraktion heißt es: „Für eine effektive Ermittlungsarbeit bedarf es regelmäßig einer schnellen und automatisierten Auswertung großer Datenmengen.“ Der bayerische Landtag hat bereits im Juli 2024 dem Einsatz der umstrittenen Polizeisoftware VeRA von Palantir zugestimmt.

Das Gesetz sieht weitere polizeiliche Befugnisse vor: eine Erweiterung der Videoüberwachung an besonders gefährdeten Orten und der Einsatz der polizeilichen Body-Cams auch in Wohnungen. Die Beamten sollen mehr Spielraum bekommen, um Menschen in Gewahrsam zu nehmen, indem die Präventivhaftzeiten verlängert werden. Vorgesehen

sind zudem erweiterte Einsatzmöglichkeiten für elektronische Fußfesseln, etwa, um Frauen vor gewalttätigen Männern zu schützen (KI soll Hessens Polizei bei Auswertung von Videobildern unterstützen, <https://www.heise.de> 08.12.2024, Kurzlink: <https://heise.de/-10191815>; Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz, Gesetz zur Modernisierung des Polizeirechts beschlossen, <https://hessen.de> 12.12.2024).

## Niedersachsen

### SPD-Fraktion thematisiert Andersdenkende in Hannovers Verwaltung

Die SPD-Ratsfraktion in Hannover sammelte als kritisch bewertete Äußerungen von städtischen Mitarbeitenden in einem Dossier. Erst nach öffentlicher Kritik wurde ihr klar, dass das nicht in Ordnung ist. Erfasst wurde z. B. eine Verwaltungsmitarbeiterin, die sich ehrenamtlich in einem Verein engagiert, der zu den Vereinen gehört, denen auf Betreiben der informellen „Deutschland-Koalition“ aus SPD, CDU und FDP die städtischen Zuschüsse gekürzt werden sollen, weil sie auf ihrem privaten Facebook-Account einen Aufruf zur Demo gegen diese Kürzungen teilte. Sie ahnte nicht, dass sich kurze Zeit später die Geschäftsordnungskommission und der Verwaltungsvorstand im hannoverschen Rathaus über diesen Beitrag beugen würden.

Die Geschäftsordnungskommission ist das Gremium, in dem sich die Fraktionsspitzen und die Verwaltung über grundsätzliche Verfahrensfragen – üblicherweise in vertraulicher Sitzung – austauschen. Die SPD-Ratsfraktion hatte das Thema auf die Tagesordnung gesetzt und mindestens fünf solcher Beiträge zu einem kleinen Dossier zusammengestellt: Aufrufe zu Demonstrationen, die auf Facebook geteilt wurden; jemand, der im Netzwerk LinkedIn einen kritischen Beitrag zur Rolle rückwärts in der Verkehrspolitik geteilt und kommentiert hatte; Leserbriefe von Verwaltungsmitarbeitern an die Hannoversche Allgemeine Zeitung. Die SPD-Ratsfraktion forderte den Oberbürger-

meister und seine Verwaltungsspitze auf zu prüfen, ob hier das Neutralitäts- und Mäßigungsgebot verletzt wurde. Schließlich sei der Rat Haushaltssouverän und Dienstherr, da dürfe man doch etwas Zurückhaltung erwarten.

Die Verwaltung prüfte die Vorwürfe und wies sie in einem Gutachten zurück. Alle Äußerungen waren von privaten und nicht von dienstlichen Accounts getätigt worden. Teilweise war erkennbar, dass es sich um Mitarbeitende der Stadt handelte, z. B. weil das im Profil steht. In keinem Fall hatten die betreffenden Personen ihre politischen Äußerungen ausdrücklich mit ihrer dienstlichen Funktion in Verbindung gebracht oder suggeriert, dass sie im Namen einer Behörde sprachen.

Thomas Schremmer, Vorsitzender des Gesamtpersonalrats, bestätigte, dass der Vorgang Unruhe verursachte. „Natürlich spricht sich so etwas im Betrieb herum.“ Besonders entsetzt seien er und die Mitglieder seines Vorstands darüber gewesen, dass es hier offenbar durchgehend um einfache Angestellte ging. „Beim Spitzenpersonal, bei Wahlbeamten wie den Dezernenten, da guckt man da ja anders drauf als bei der Sachbearbeiterebene. Ich habe den Eindruck, dass hier Wahlkampf auf dem Rücken der Beschäftigten gemacht wird. Das geht gar nicht.“ Die rund 12.000 Beschäftigten der Stadt seien in erster Linie auch Bürger der Stadt, für die nun einmal die Meinungsfreiheit gelte. Besonders ärgerlich für den Personalrat war, dass am Tag des Bekanntwerdens die Stadt eine neue Kampagne zur Gewinnung von Personal wegen des Fachkräftemangels vorstellte, weil 750 Stellen unbesetzt waren. Mit der Kampagne „Für alle & dich“ möchte sich die Stadt als moderner, offener Arbeitgeber in Szene setzen.

Oberbürgermeister Belit Onay (Grüne) stellte sich mit einem Statement deutlich vor seine Mitarbeitenden und bezeichnete das Kontrollieren und Sammeln privater Äußerungen als Grenzüberschreitung, die er nicht akzeptiere, da sie Angst und Unsicherheit schüre. Er habe im Übrigen volles Vertrauen, dass die Mitarbeitenden der Stadtverwaltung ihren Aufgaben und Pflichten nachkommen – unabhängig davon, welche persönliche Meinung sie vertreten.

Die SPD gab sich angesichts der massiven Kritik kleinlaut. Nach Veröffentlichung des Vorgangs in der Hannoverischen Allgemeinen Zeitung distanzierte sich der Stadtverband. Man sei enttäuscht über das Bild, das nun entstanden sei, und bitte die Mitarbeitenden um Entschuldigung. Man wolle die Vorgänge aufarbeiten und entsprechende Schlüsse ziehen. Beim Vorsitzenden der Ratsfraktion, Lars Kelich, den viele für die treibende Kraft hinter der Aktion halten, klang die Entschuldigung gewundener: Man habe das Ganze wohlbedacht in einem vertraulich tagenden Gremium zur Debatte gestellt. Die Sammlung habe man doch überhaupt erst angelegt, als die Verwaltung um konkrete Beispiele gebeten habe. Dass daraus ein falscher Eindruck entstanden sei, bedaure er sehr. Später erklärte er, er übernehme die Verantwortung und trete sowohl als Fraktionsvorsitzender als auch als Ratsmitglied zurück.

In einem ersten Statement war noch die Rede davon gewesen, „die Fraktionen“ hätten diese Frage bloß einmal grundsätzlich klären lassen wollen, weil sie eine entsprechende Verunsicherung in Teilen der Belegschaft wahrgenommen hätten. CDU und FDP machten jedoch schnell klar, dass dies ein SPD-Thema gewesen sei. Er sei einigermaßen fassungslos über diese Sammlung gewesen, aus der die SPD dann auch noch genüsslich vorgelesen habe, sagte der FDP-Fraktionsvorsitzende Wilfried Engelke. „Ich habe mich auch schon über viele Social-Media-Äußerungen geärgert, vor allem wenn wir in die Nähe zur AfD gerückt werden. Aber so lange es den Regeln entspricht, muss man das als Mandatsträger eben auch mal abkönnen. Da sind die Genossen im Moment einfach zu empfindlich.“ Auch sein CDU-Kollege habe sich an den Kopf gefasst (Conti, Hannovers SPD spielt Stasi, taz nord, 10.12.2024, 25).

nachgekommen sei. Angesichts des Umfangs der Eingabe und der Komplexität der damit verbundenen Verarbeitungsvorgänge müsse diese Analyse „innerhalb eines angemessenen Zeitrahmens gründlich durchgeführt“ werden. Zugleich kündigte Wiewiórowski an keine weiteren Kommentare zu dem Fall abzugeben, da die EU-Kommission seine Entscheidung angefochten habe und die entsprechenden Verfahren vor dem Gericht der EU laufen (Az.: T-262/24 und T-265/24).

Schon 2020 hatte Wiewiórowski die EU-Kommission aufgefordert, sich nach Alternativen zu MS 365 umzuschauen, die „höhere Datenschutzstandards erlauben“. Die Regierungsinstitution unternahm in diese Richtung bislang aber wenig, so ein internes Kommissionsdokument: „Es gibt keine bekannten glaubwürdigen Angebote von europäischen Anbietern.“ Französische Behörden haben demnach aber besondere Sorgen über die potenziellen Risiken geäußert, „die mit der Nutzung von Lösungen mit Sitz in den USA verbunden sind“. Ein Bericht der Generaldirektion für digitale Dienste thematisierte zudem die „übermäßige Macht einiger weniger außereuropäischer Unternehmen, Risiken im Zusammenhang mit einem einzigen Anbieter (Preiserhöhungen, Migrationsschwierigkeiten) und den potenziellen Verlust interner Kompetenzen“.

Die Generaldirektion lobt zwar Initiativen der Mitgliedsstaaten zur Entwicklung offener und souveräner Alternativen zu Microsoft im Streben nach digitaler Souveränität. Sie bewertet dies intern aber nur als „mögliche Ergänzung“ für kleine IT-Vorhaben mit „sehr begrenztem Umfang“. In Deutschland verwiesen Wirtschaftsprüfer 2019 in einer Studie fürs Innenministerium auf „Schmerzpunkte bei der Bundesverwaltung“, die die seit Jahren monierte Abhängigkeit von Microsoft-Produkten verursache. Das Zentrum für digitale Souveränität (ZenDiS) fördert mittlerweile die Windows-Alternative Open-Desk. Schleswig-Holstein will sich ganz von Microsoft lösen.

Wie die Auseinandersetzung weitergeht, dürfte auch mit davon abhängen, ob Wiewiórowski nach dem offiziellen Ende seiner Amtszeit im Dezember wie-

## Datenschutznachrichten aus dem Ausland

### EU

#### Microsoft 365: Konflikt zwischen EDSB und Kommission geht weiter

Im Streit um die Anwendung von Microsoft 365 (MS 365) bei der EU-Kommission und ihr unterstellten Behörden hatte der EU-Datenschutzbeauftragte Wojciech Wiewiórowski im März 2024 festgestellt, dass die Brüsseler Regierungsinstitution das Cloud-basierte Office-Paket im Lichte des „Schrems-II-Urteils“ des Europäischen Gerichtshofs (EuGH) rechtswidrig nutzt. Er wies die EU-Kommission an spätestens bis zum 09.12.2024 alle Datenströme auszusetzen, die sich aus der Nutzung von MS 365 an Microsoft und an seine verbundenen Unternehmen und Unterauftragsverarbeiter in Ländern außerhalb der EU beziehungsweise des Europäischen Wirtschaftsraums (EWR) ergeben. Doch ein Kommissionssprecher erklärte, man sehe keinen Grund für einen Verzicht auf MS 365.

Wiewiórowski betonte nach Ablauf der von ihm gesetzten Frist, dass seine Entscheidung vom März 2024 „voll anwendbar bleibt“, was von der EU-Kommission negiert wird. Sie meint, ihr Einsatz von MS 365 entspreche den gesetzlichen Anforderungen; dies sei während der Untersuchung des EU-Datenschutzbeauftragten „ausreichend nachgewiesen“ worden: „Das Engagement der Kommission für den Schutz der Datenschutzvorschriften bleibt unerschütterlich und sie wird weiterhin die höchsten Standards bei der Einhaltung dieser Vorschriften aufrechterhalten.“ Am 06.12.2024 hatte die EU-Kommission Wiewiórowski den angeforderten Konformitätsbericht nebst zugehöriger Unterlagen vorgelegt.

Der EU-Datenschutzbeauftragte bestätigte den Eingang der Dokumente, sieht die EU-Kommission aber weiter verpflichtet auf MS 365 zumindest vorläufig zu verzichten. Seine Stelle überprüfe derzeit die bereitgestellten Informationen, um zu beurteilen, ob die EU-Kommission der Entscheidung vom März

dergewählt wird. Den Posten streitig machen ihm Bruno Gencarelli von der Generaldirektion Justiz und Verbraucher, der der EU-Kommission weniger kritisch gegenüberstehen könnte, François Pellegrini, Ex-Vizepräsident der französischen Datenschutzbehörde CNIL, und Anna Poulidou, Datenschutzbeauftragte der EU-Organisation für Kernforschung (CERN) (Kreml, EU-Datenschützer und Kommission im Clinch über Einsatz von Microsoft 365, <https://www.heise.de/13.01.2025>, Kurzlink: <https://heise.de/-10241029>).

## EU

### Wettbewerbsstrafe gegen Meta wegen unzulässiger Verknüpfung

Die EU-Kommission hat dem Facebook-Mutterkonzern Meta eine Strafe von 797,72 Millionen Euro wegen Wettbewerbsverstößen auferlegt. Die noch zuständige EU-Kommissarin Margrethe Vestager erklärte: „Meta hat seinen Online-Kleinanzeigendienst Facebook Marketplace mit seinem persönlichen sozialen Netzwerk Facebook verknüpft und anderen Anbietern von Online-Kleinanzeigendiensten unfaire Handelsbedingungen auferlegt.“ So habe Meta seinem eigenen Dienst Facebook Marketplace Vorteile verschaffen wollen, die andere Anbieter von Online-Kleinanzeigendiensten nicht ausgleichen könnten. Die EU-Kommission hatte bereits im Juni 2021 ein förmliches Verfahren wegen möglicher Verstöße gegen europäische Kartellvorschriften durch wettbewerbswidrige Verhaltensweisen von Facebook eingeleitet.

Meta kündigte umgehend an gegen die Entscheidung vorzugehen: „Wir werden die Entscheidung anfechten. Diese Entscheidung missachtet die Realität auf dem florierenden europäischen Markt für Onlinekleinanzeigen.“ Bis zu einem Gerichtsurteil werde Meta aber den Anweisungen der EU-Kommission folgen.

Die EU-Kommission kritisiert, dass durch die Verknüpfung des Online-Kleinanzeigendienstes Facebook Marketplace mit dem sozialen Netzwerk Facebook alle Nutzenden der Plattform automatisch Zugang zum Marketplace hätten und

dies – ob sie es wünschten oder nicht – auch regelmäßig angezeigt werde. Das schließt andere Wettbewerber laut EU-Kommission vom Markt aus. Auf dem Facebook-Marktplatz können Nutzende gebrauchte Gegenstände direkt an andere Verbraucher weiterverkaufen. Dafür müssen sie sich in ihrem Facebook-Profil anmelden und können von dort aus direkt auf den Dienst zugreifen.

Nach Angaben der EU-Kommission wurde bei der Höhe der Geldbuße berücksichtigt, wie lange und wie schwer Meta gegen EU-Recht verstoßen habe. Zudem sei der Umsatz von Facebook Marketplace in die Berechnung eingeflossen: „Die Kommission hat auch den Gesamtumsatz von Meta berücksichtigt, um eine ausreichende Abschreckungswirkung auf ein Unternehmen zu erzielen, das über so große Ressourcen wie Meta verfügt.“

Die EU-Wettbewerbschüter nehmen schon seit Jahren amerikanische Technologie-Konzerne unter die Lupe. Im März 2024 hatte die EU-Kommission bereits eine Wettbewerbsstrafe von 1,8 Milliarden Euro gegen den Techgiganten Apple verhängt. Dem US-Unternehmen wurde vorgeworfen seine marktbeherrschende Stellung für den Vertrieb von Musik-Streaming-Apps an iPhone- und iPad-Nutzer über seinen App Store zu missbrauchen. Auch gegen Google sind Bußgelder in Milliardenhöhe verhängt worden (Meta: EU-Kommission verhängt fast 800 Millionen Euro Strafe – Verstoß gegen Kartellvorschriften, <https://www.spiegel.de> 14.11.2024; Fast 800 Millionen Euro Bußgeld gegen Meta, <https://www.lto.de> 14.11.2024).

## EU

### EU-Strafverfolger fordern Zugriff auf OTT-Daten

Die Hocharangige Gruppe der EU zum Datenzugang für eine wirksame Strafverfolgung (HLG) legt in ihrem Abschlussbericht einen Schwerpunkt darauf, dass Strafverfolger einen „rechtmäßigen“ Zugang zu Daten von Messenger-Diensten wie WhatsApp, Signal, Telegram oder Threema erhalten. Sie bekräftigen damit eine Forderung eines separaten Empfehlungspapiers. Die

„Over the Top“-Anbieter (OTT), die Nutzern Dienste etwa für die Kommunikation direkt übers Internet anbieten, stellen dem Bericht zufolge „für Strafverfolgungsbehörden zusätzliche Herausforderungen dar“. Sowohl auf nationaler als auch auf EU-Ebene seien sie „häufig der Ansicht, dass sie nicht an dieselben Verpflichtungen gebunden sind wie herkömmliche Kommunikationsanbieter“.

OTT-Anbieter fallen zwar in den Anwendungsbereich des Europäischen Kodex für die elektronische Kommunikation, schreibt die auch als „Going Dark“-Arbeitsgruppe bekannte HLG. Doch sie seien häufig außerhalb der EU ansässig und unterlägen so keinen allgemeinen Sanktionen. Dies führe zu Unsicherheit hinsichtlich ihrer Auflagen zur Speicherung von Daten. Während herkömmliche Kommunikationsanbieter in den meisten Fällen einige Informationen wie IP-Adressen mit Portnummer für Geschäftszwecke speicherten, die die Identifizierung von Benutzern ermöglichen, sei dies bei OTT-Anbietern nicht der Fall.

Gleichzeitig trägt den EU-Strafverfolgern zufolge das zunehmende Volumen der bei den Anbietern eingehenden Anfragen dazu bei, dass diese verzögert oder abgelehnt würden. Eine Ursache dafür seien „spezifische Geschäftsmodellentscheidungen“ der Betreiber, etwa bewusst datensparsam zu agieren. Die spärliche Kooperation liege aber auch an der begrenzten Anzahl von Mechanismen für die Zusammenarbeit zwischen Strafverfolgungsbehörden und den privaten Unternehmen. Zudem generierten und verarbeiteten zahlreiche neue Technologie-Anbieter und digitale Akteure wie Autohersteller und KI-Systeme mit großen Sprachmodellen Metadaten. Auch diese könnten Informationen über kriminelle Aktivitäten liefern. Trotz ihrer zunehmenden Bedeutung seien sie derzeit nicht an die Pflicht zur Datenspeicherung gebunden.

In der Praxis haben gemäß der HLG die gängigen OTT-Dienste keine technischen Mechanismen entwickelt, „um auf Anfragen der Behörden der EU-Mitgliedsstaaten zur rechtmäßigen Überwachung zu reagieren“. Im Gegensatz dazu habe Großbritannien mit dem Investigatory Powers Act einen Rahmen für die rechtmäßige Überwachung von OTT-Kommunikation geschaffen, der

dank der Annahme des Datenzugriffsabkommens mit den USA auch für dort ansässige Dienste gelte. Laut den zuständigen britischen Behörden mache dies „einen erheblichen Unterschied bei der Kriminalprävention und -ermittlung“.

Die Gruppe drängt darauf, dass die EU-Mitgliedsstaaten Sanktionen gegen unkooperative Anbieter elektronischer und sonstiger Kommunikationsdienste verhängen können. Instrumente sollten „die Einschränkung ihrer Geschäftsfähigkeit auf dem EU-Markt“ – also etwa eine Sperre auf Netz- oder App-Store-Ebene – genauso sein wie Haftstrafen für die Verantwortlichen. Die von der HLG und den EU-Ländern schon seit längerem verlangte verstärkte Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern werde „die Situation bis zu einem gewissen Grad verbessern“. Diese müsse aber auch gesetzlich verankert werden.

Die EU-Kommission richtete die Arbeitsgruppe 2023 auf Drängen der Mitgliedsstaaten ein. Ausgangspunkt waren die laufenden Crypto Wars und die damit verknüpfte Debatte über das „Going Dark“-Szenario, wonach die zunehmende durchgängige Verschlüsselung Ermittler blind und taub zu machen drohe. Wissenschaftler halten das für einen Mythos, doch Polizei und Justiz wollen das von ihnen ausgemachte „böse Problem“ der Verschlüsselung gelöst wissen. Vertreter von Strafverfolgungs- und Justizbehörden aus den USA forderten so bei einem Treffen mit Abgesandten der EU-Seite 2023 mit dem Grundsatz „Lawful Access by Design“ den Zugang zu unverschlüsselten Kommunikationsdaten direkt in die Technik zu integrieren. Ein großer Cyberangriff auf solche Überwachungsschnittstellen von US-Providern zeigt indes, welche negativen Folgen dieser Ansatz haben kann.

Ziel des Schlussberichts ist es „die von den Experten identifizierten Herausforderungen detailliert zu beschreiben und Optionen für die Fortsetzung der Arbeit und die Operationalisierung der Empfehlungen aufzuzeigen“. Demnach „bedarf es harmonisierter und kohärenter Gesetze zur Vorratsdatenspeicherung“. Die EU soll dazu auch bis 2025 eine Empfehlung zum Echtzeitzugriff auf anlasslos aufbewahrte Verbindungs- und Standortinformationen herausgeben.

Generell sei die „rechtmäßige Überwachung von entscheidender Bedeutung für die wirksame Untersuchung und Verfolgung von organisierter Kriminalität und terroristischen Gruppen“.

Der Bericht meint: „Die standardmäßige Verschlüsselung von Daten auf Geräten ist eine zentrale Herausforderung.“ Ermittlern bleibe oft keine andere Wahl „als Schwachstellen auszunutzen“. Solche Ansätze müssten aber mit dem Ziel, sicherere Hardware und Software zu gewährleisten, in Einklang gebracht werden. Letztlich bleibt es beim Appell Diensteanbieter zu verpflichten Kommunikationsdaten im Klartext herauszugeben. Ein bisschen verschlüsselt gibt es aber genauso wenig wie ein bisschen schwanger. Der EU-Rat sagte im Juli 2024 zu „rechtlich und technisch sichere Lösungen für den Zugriff auf verschlüsselte elektronische Kommunikation im Einzelfall“ vorbehaltlich einer gerichtlichen Anordnung zur Verfolgung schwerer Straftaten zu suchen (Krempel, EU-Strafverfolger fordern: Datensparsame Messenger-Dienste sanktionieren, <https://www.heise.de> 28.11.2024, Kurzlink: <https://heise.de/-10179828>).

## EU-weit

### Datenschützer legen Prüfbericht zum Auskunftsrecht vor

Der Europäische Datenschutzausschuss (EDSA) und der EU-Datenschutzbeauftragte Wojciech Wiewiórowski haben die Ergebnisse einer europaweiten Überprüfungs-Aktion zur Umsetzung des allgemeinen Auskunftsrechts nach Art. 15 Datenschutz-Grundverordnung (DSGVO) vorgelegt. Die Kontrolleure haben demnach einige Probleme ausgemacht, wie Bürger aktuell auf Basis dieses Anspruchs herausfinden können, welche Daten Unternehmen und Behörden über sie gespeichert haben. Als Beispiel nennen sie Hindernisse wie übertriebene formale Anforderungen oder das unbegründete Verlangen Ausweisdokumente vorzulegen.

Die beteiligten 30 Aufsichtsbehörden haben auch inkonsistente und übertriebene Auslegungen der gesetzlich vorge-

sehen Schranken für das Zugangsrecht ausgemacht. Verantwortliche verließen sich teils zu sehr auf bestimmte Ausnahmen, um Anfragen automatisch abzulehnen. Ein weiteres Problem ist dem EDSA-Bericht zufolge, dass interne Verfahren zum Bearbeiten von Auskunftsbegehren nicht dokumentiert werden.

Insgesamt antworteten 1.185 Zuständige aus der Wirtschaft sowie öffentlichen Einrichtungen auf die versandten Fragebögen. Zwei Drittel der teilnehmenden Kontrollinstanzen bewerteten den Grad der Rechtskonformität dieser Verantwortlichen von „durchschnittlich“ bis „hoch“. Ein wichtiger Faktor war dabei das Volumen der bei den Verantwortlichen eingehenden Auskunftsanfragen sowie die Größe der Organisation: Zuständige, die mehr Ersuchen erhielten, genügten den Anforderungen tendenziell eher als kleine Organisationen mit weniger Ressourcen. Positiv bewertet der EDSA die Umsetzung bewährter Verfahren wie nutzerfreundliche Online-Formulare und „Self-Service-Systeme“, mit denen Individuen ihre Daten jederzeit mit wenigen Klicks selbstständig herunterladen können.

Die acht aus Deutschland beteiligten Behörden halten in ihrer Auswertung fest, dass viele der kontaktierten Verantwortlichen angaben, dass sie nur wenige Auskunftsanfragen erhalten hätten. Offenbar sei das wichtige Betroffenenrecht in der Öffentlichkeit nicht ausreichend bekannt. Im privaten Sektor wurzelten die meisten Ersuchen in Rechtsstreitigkeiten.

Viele Verantwortliche haben auch Schwierigkeiten den Umfang des Auskunftsrechts und die Tragweite des Begriffs „personenbezogene Daten“ in der Praxis zu erfassen. Oft würden nur die gängigsten internen Systeme durchsucht, nicht alle Datenbanken. Viele Zuständige wüssten zudem nicht, dass persönliche Informationen auch „in nicht-textuellen Dateien, in Metadaten oder in Sicherungsdaten enthalten sein können“. Teils sei zu hören, dass das Recht auf Erhalt einer Kopie unabhängig vom Recht auf Auskunft sei. So werde eine explizite Anfrage der betroffenen Person zum Bereitstellen von Dokument- oder Datenbankauszügen erwartet.

Der EDSA veröffentlichte schon 2022 Leitlinien zu den Betroffenenrechten, zu

denen der Auskunftsanspruch gehört. Diese will das Gremium nun im Lichte der Resultate aktualisieren. Der Bericht enthält bereits eine Reihe Empfehlungen. Eine konzertierte Prüffaktion 2025 wird die Umsetzung des Rechts auf Löschung in den Fokus nehmen (Krempf, DSGVO-Auskunftsanspruch über gespeicherte Daten hat seine Tücken, <https://www.heise.de> 21.01.2025, Kurzlink: <https://heise.de/-10251146>).

## Dänemark

### Cyberangriff auf Gesundheitsdaten

Anfang Dezember 2024 informierte „Alles Lægehus“, ein Betreiber medizinischer Zentren in Dänemark, dass nach einem Cyberangriff, von dem 130.000 Patienten betroffen sein könnten, persönliche Patientendaten veröffentlicht worden sind. Davon betroffen ist gemäß Medienberichten auch die CPR-Nummer, die im zentralen Personenregister Dänemarks hinterlegt ist und der Identifikation dient. Sie wird im Gesundheitswesen verwendet und ist beispielsweise auf der dänischen Gesundheitskarte vermerkt, wird aber auch in anderen Verwaltungsbereichen genutzt. Weitere Informationen, die in einem geschlossenen Forum veröffentlicht wurden, sind neben der Krankengeschichte auch Informationen über Medikamente.

Die dänische Datenschutzbehörde gab den Ratschlag aus die Betroffenen umgehend zu informieren. Es könne jedoch einige Zeit dauern, bis klar sei, wer alles zu den Betroffenen gehöre. Die Polizei untersucht den Fall zusammen mit dem National Cyber Crime Center und Alles Lægehus. Gemäß Experten ist dies der kritischste Fall von Datenlecks in Dänemark. Laut Berichten waren der Veröffentlichung verschiedener Daten in Untergrundforen dreiwöchige Verhandlungen vorangegangen. Ob Lösegeld für die Nichtveröffentlichung der Daten gezahlt wurde, ist unklar. Die dortige Polizei fordert Bürger auf besonders wachsam zu sein – etwa gegenüber Phishing-Versuchen – und Verdachtsfälle von Datenmissbrauch zu melden.

Immer wieder nutzen Kriminelle Sicherheitslücken im Gesundheitswesen

aus. Gerade Gesundheitsdaten sind wertvoll und werden inzwischen zu höheren Preisen gehandelt als Kreditkartendaten. Anfang 2024 hatten sich Cyberkriminelle über einen ungesicherten Server Zugang bei der UnitedHealth-Tochter „Change Healthcare“ verschafft, einem großen Finanzdienstleister im US-Gesundheitswesen. Anschließend waren die Daten von 300 Millionen US-Bürgern im Darknet veröffentlicht worden, trotz mehrfacher Lösegeldzahlungen. Experten raten davon, Lösegeld zu zahlen, ab, da die Forderungen der Kriminellen dadurch nicht unbedingt zu stoppen sind (Koch, Datenabfluss bei Gesundheitsunternehmen: Dänen bangen um sensible Informationen, <https://www.heise.de> 23.01.2025, Kurzlink: <https://heise.de/-10254683>).

## Spanien

### Widerstand gegen überzogene Hotelmeldepflicht

Seit dem 02.12.2024 bestehen in ganz Spanien neuen Anmeldeeregeln für Gäste. Die Neuregelung verlangt von Hotels und Reiseagenturen, aber auch Pensionen, Ferienwohnungen (Apartments zur touristischen Kurzzeitvermietung), Campingplätzen und Autovermietern die Erfassung von 42 verschiedenen Daten pro Gast und Reisenden. Die Eintragung erfolgt nicht mehr in die bisherigen Polizeiregister „Hospederías“ der Guardia Civil oder „WebPol“ der Policía Nacional, sondern in einer Datenbank direkt beim spanischen Innenministerium. Ausnahmen bilden Katalonien und das Baskenland, wo die bisherigen Datenbanken der Regionalpolizei Mossos d'Esquadra und Ertzaintza aktiv bleiben.

Die neuen Vorschriften des Real Decreto 933/2021 zur Registrierungspflicht für Übernachtungsbetriebe haben für viel Unmut bei den Hoteliers und Vermietern in Spanien gesorgt, nicht nur, da sie mehr Arbeit angesichts immer neuer Touristenrekorde in Spanien bedeuten. Es handelt sich um Daten, die vor Ort nicht auf ihre Richtigkeit überprüft werden können, das Innenministerium möchte aber die Vermieter dafür in Haftung nehmen.

Neben den Angaben, die aus dem jeweiligen Reisedokument hervorgehen und so belegbar sind, kommen für ausländische Reisende wie Spanier hinzu: die Wohnadresse (gewöhnlicher Aufenthaltsort mit Ort, Straße und Hausnummer), Festnetztelefon und Mobilfunknummer, E-Mail-Adresse, Zahl der Reisenden, die genaue Uhrzeit der An- und Abreise. Die Angaben werden von allen Reisenden ab 14 Jahren abgefragt. Außerdem müssen Hotel- und Apartmentgäste in Spanien künftig die Beziehung zu mitreisenden Minderjährigen offenlegen und gegebenenfalls eine Vollmacht der Erziehungsberechtigten vorweisen. Eine Anforderung fällt weg: Das Datum des Ablaufs des Reisepasses oder Personalausweises muss künftig nicht mehr angegeben werden, dafür aber neben der Pass- oder Ausweisnummer auch die Prüfziffer des Dokuments.

Das Innenministerium rechtfertigt die Neuregelung mit Sicherheitsgründen. Die neuen Daten sollen in erster Linie dem Schutz Minderjähriger und dem Kampf gegen den Terrorismus dienen. Der spanische Staat will außerdem die Rechtssicherheit für Schadenersatzfälle bei Beschädigung oder Nichtbezahlung in den Unterkünften sorgen, indem man die Gäste künftig direkt erreichen können soll – sobald für eine Forderung ein Rechtstitel vorliegt. Eine Verwendung der Daten wie Mobilnummer, Anschrift oder E-Mail-Adresse für kommerzielle oder sonstige sachferne Zwecke wird unter Verweis auf den Datenschutz untersagt. Wie bisher werden die persönlichen Daten in den Hotelcomputern zu den bisher gültigen Fristen gelöscht, außer Name und Datum des letzten Aufenthalts. E-Mails dürfen nur gespeichert werden, wenn der Gast dem zustimmte. Das Innenministerium machte keine Angaben dazu, wie lange die Check-in-Daten der Reisenden auf den Servern in Madrid gespeichert bleiben und ob diese auch an andere staatliche Institutionen weitergeleitet werden können.

Die Check-in-Informationen müssen bis spätestens 24 Stunden nach Eintreffen des Reisenden in der Unterkunft bei der betreffenden Datenbank gemeldet sein. Verstöße dagegen werden mit Geldbußen von 100 bis 600 Euro gegen den Gastgeber geahndet. Es ist sogar von möglichen Strafen bis zu 30.000 Euro

die Rede. Fälle von bewussten Falschangaben gelten indes als Straftatbestand und würden auch für Reisende gerichtsanhängig. Die Hoteliers sehen sich in einer rechtlichen Unsicherheit. Handynummern und E-Mail-Adressen können sich ändern, das ist auch nicht verboten, Festnetztelefon haben ohnehin immer weniger Leute. Gäste könnten einfach Falschangaben machen.

Einige spanische Medien nennen das neue Gesetz „gran hermano“ (großer Bruder) und fordern die Hotellerie nicht als Hilfspolizei zu benutzen. Es werden kritische Äußerungen von Touristen zitiert, insbesondere aus Großbritannien, die das Gesetz als Inquisition bezeichneten und erklärten Spanien künftig meiden zu wollen. Als das Gesetz Anfang Dezember 2024 in Kraft trat, war die eigens dafür geschaffene Plattform des Innenministeriums einen Tag lang nicht erreichbar.

Wie die Spanische Vereinigung der Hotels und Tourismusunterkünften (Cehat) mitteilte, habe das Innenministerium bislang nicht auf die Einwände der Hotels reagiert: „Angesichts des Schweigens“ werde man nun die Gerichte bemühen, „um die Rechte der Unternehmen und der Reisenden zu verteidigen“. Das „verwirrende und unangemessene“ Gesetz verstoße gegen europäische Datenschutzbestimmungen.

Auch andere Länder versuchen das Übernachten unter falscher Identität zu verhindern. So will Italien das in kleinen Hotels und Ferienwohnungen gängige Online-Einchecken plus Schlüsselbox abschaffen. Gastgeber müssen künftig ihre Gäste persönlich in Empfang nehmen (Schicker, Hotels in Spanien: Neue Regeln für Registrierung von Gästen - Tourismusbranche zieht vor Gericht, <https://www.costanachrichten.com> 04.12.2024; Illinger, Der gläserne Gast, SZ 05.12.2024, 1; zur deutschen Hotelmeldepflicht DANA 3/2023, 152).

## Spanien

### Privatklage gegen NSO-Verantwortliche wegen Pegasus-Einsatz

In Spanien versucht ein Anwalt, Verantwortliche des Spyware-Herstellers NSO Group persönlich haftbar zu machen,

und verklagte die Gründer und einen Manager der Entwicklerfirma von Pegasus. Ursprünglich richteten sich die Vorwürfe pauschal gegen die NSO-Group mit Sitz in Israel und ihre Tochtergesellschaften in Europa. Der Anwalt und Universitätsprofessor Andreu Van den Eynde war eines von 65 Opfern einer Hacking-Kampagne, die sich vor einigen Jahren gegen Befürworter einer Unabhängigkeit der Region Katalonien richtete. Aufgedeckt wurde die Überwachungsaktion von der Forschungsgruppe Citizen Lab. Der spanische Geheimdienst CNI hatte dazu die Spyware von NSO gekauft und in 18 Fällen mit richterlicher Genehmigung eingesetzt. Dies wurde von einer früheren Chefin des CNI nach anfänglichem Leugnen eingeräumt (DANA 3/2022, 190 f.). Unterstützt wird der Anwalt aus Barcelona von der Menschenrechtsorganisation Iridia.

Gegenstand der Klage ist der Verkauf illegaler Software und die Beteiligung des Herstellers an der illegalen Nutzung der Software. Ferner geht es um die Verletzung der Persönlichkeitsrechte des betroffenen Anwalts und seiner Mandanten durch das Ausspähen. Überdies sollen die NSO-Gründer und -Chefs auch für Überwachungsmaßnahmen ohne strafrechtliches Verfahren oder richterliche Kontrolle in Rechenschaft genommen werden. Angeklagt wurden die Mitgründer Omri Lavie und Shalev Hulio sowie der Manager Yuval Somekh. Als Firmen sind neben der NSO-Group die Luxemburger Tochtergesellschaften Osy Technologies und Q Cyber Technologies genannt worden. Die NSO-Group steht weltweit in der Kritik, auch über gerichtliche Klagen. Unter anderem gehen auch Apple und WhatsApp juristisch gegen NSO vor (Kirchner, Spanien: Klage gegen Verantwortliche der NSO-Group, <https://www.heise.de> 15.11.2024, Kurzlink: <https://heise.de/-10036527>).

## Ungarn

### Oppositionspolitiker Magyar – ausspioniert und diffamiert

Péter Magyar, ehemaliger Regierungsinsider und erfolgreichster Oppositions-

politiker Ungarns, hat sich in einer kurzfristig angesetzten Pressekonferenz am 10.11.2024 an die Öffentlichkeit gewandt und der Regierung von Ministerpräsident Viktor Orbán „Watergate-Methoden“ vorgeworfen. Er sprach von Diffamierung, von Bespitzelung durch Geheimdienste sowie private Sicherheitsdienste, von der Erstellung gefälschter Ton- und Videoclips sowie einer konzertierten Kampagne gegen seine Partei.

Der 43-Jährige Magyar bereitet Orbán schon lange Bauchschmerzen. Seit er im Frühjahr 2024 mit seiner „Partei für Respekt und Freiheit“ (Tisza) die politische Bühne betrat, hat er in Umfragen stetig zugelegt. Zuletzt lag Tisza mit 46 Prozent weit vor Orbáns Fidesz-Partei mit 39 Prozent. Magyar bedroht damit die Position des scheinbar unbesiegbaren Dauerregenten, die sich Orbán mithilfe des Abbaus des ungarischen Rechtsstaats zu sichern versucht. Weil der Herausforderer, der gegen Orbán sehr konkrete Korruptionsvorwürfe erhebt, große Popularität genießt, wird er in Staatsmedien und auf regierungsnahen Webseiten scharf angegriffen.

Nach den Aussagen Magyars recherchieren zahlreiche Medien zu seinen Vorwürfen und finden immer mehr Belege. Deren Kern ist, dass sowohl seine Ex-Frau, die frühere Justizministerin Judit Varga, als auch seine Ex-Freundin Evelin Vogel von einem Orbán-nahen Oligarchen finanziert würden und staatlichen Akteuren zuarbeiteten, die Magyar mit einer Schmutzkampagne überzögen. Erste Andeutungen dazu hatte der Shootingstar der ungarischen Politik bereits im Frühherbst 2024 gemacht. Nun ist er mit einem ganzen Paket von Vorwürfen an die Öffentlichkeit gegangen. Informanten aus Geheimdienst und Staatsapparat, die sich illegalen Aktivitäten verweigerten und Orbáns Methoden ablehnten, hätten ihn auf dem Laufenden gehalten.

Seine Ex-Freundin Evelin Vogel soll, so Magyar, heimlich insgesamt elf Stunden Film- und Audioaufnahmen von ihm erstellt haben, die danach verändert worden seien, teils mit künstlicher Intelligenz. Vogel soll 30 Millionen Forint (knapp 80.000 Euro) gefordert haben, damit sie die Aufnahmen nicht an Fidesz gebe – man sei aber auf die Erpressung nicht eingegangen.

Tatsächlich wurde am 11.11.2024 ein kurzer Videofilm von einer schwer rückverfolgbaren Mailadresse an zahlreiche Medien verschickt. In dem Clip ist Magyar nach einer Wahlkampfveranstaltung vor der EU-Wahl im Juni zu sehen, während er sich abfällig über „stinkende Wähler mit Mundgeruch“ äußert und Vogel Gewalt androht. Magyar war von der Fidesz-Presse schon kurz nach seinem Start als Oppositionspolitiker mit Vorwürfen häuslicher Gewalt überzogen worden. Magyar gibt an, der Clip vom Juni sei bearbeitet und verändert worden, einige Sätze stammten definitiv nicht von ihm. Zahlreiche Online-Blogger melden nachweisen zu können, dass der Clip der Wahlkampfveranstaltung, auf der Magyar Wähler beschimpft haben soll, tatsächlich bearbeitet worden ist.

Ein weiterer Vorwurf Magyars lautet, weitere mit KI bearbeitete und diffamierende Aufnahmen von ihm hätten auf einer neuen Internetseite namens „Objektiv“ präsentiert werden sollen, die einen Tag nach seiner Pressekonferenz gestartet werden sollte. Es gibt diese Website, sie war aber gemäß einer Statusmeldung zum geplanten Zeitpunkt „wegen Wartungsarbeiten nicht erreichbar“.

Auch andere Anschuldigungen Magyars scheinen sich zu bestätigen. So hat der Internet-Unternehmer György Vertán, dessen kleiner Kopiershop in der Orbán-Ära mithilfe staatlicher Milionaufträge zu einem großen Konzern wuchs, auf Nachfragen angegeben, dass die Ex-Frau Magyars tatsächlich neuerdings für ihn arbeite und dessen Ex-Freundin in einer seiner Wohnungen lebe. Er habe ihr aber nie Geld für etwaige parteischädigende Aktivitäten gezahlt. Vogel selbst meldete sich zuletzt nur mit einem kryptischen Post auf Instagram zu Wort: Die Wahrheit werde noch ans Licht kommen. Sie hatte vor einem Monat bereits ein sehr kritisches Interview über ihren früheren Partner auf der regierungsnahen Website Index gegeben. Magyar ist seit Juni EU-Abgeordneter und genießt damit Immunität. Gleichwohl würden er und seine Parteikollegen illegal in Privatwohnungen, Autos und Büros abgehört, sagt der konservative Politiker. Er hat mittlerweile gegen Evelin Vogel Strafantrag wegen Erpressung und Verleumdung gestellt, zudem wurde sie aus seiner Partei

ausgeschlossen. Politikinsider wie der renommierte Journalist Márton Gergely von der Wochenzeitung „HVG“ bestätigen, Peter Magyar stehe wegen seines politischen Erfolgs „unter Dauerfeuer“ von Fidesz. Innerhalb des Apparats gebe es jedoch viele, die Magyar stützten, die „Omertà beginnt zu bröckeln“. Das Büro von Orbáns Stabschef Antal Rogán, der als „Propagandaminister“ der Regierung gilt und dem Magyar vorwirft die Kampagne zu steuern, wird von diversen ungarischen Medien mit der Aussage zitiert, wer sich solche Geschichten einbilde, der solle zum Arzt gehen (Kahlweit, „Watergate-Methoden“, SZ 13.11.2024, 7).

## Großbritannien

### Regierung will sexualisierte Deepfakes unter Strafe stellen

Die britische Labour-Regierung hat angekündigt stärker gegen „sexuell explizite“ Deepfakes vorgehen zu wollen. Das federführende Justizministerium plant die Erstellung und das Verbreiten von hochrealistisch wirkenden, meist mithilfe Künstlicher Intelligenz (KI) generierten Inhalten von Personen mit eindeutig sexuellem Bezug künftig unter Strafe zu stellen. Solche „hyperrealistischen Bilder“ sollen in der Regel als Verbrechen eingestuft werden. Damit werde signalisiert, dass „dieses abscheuliche Verhalten“ nicht geduldet werde. Es gehe auch um eine Verdeutlichung, „dass es keine Entschuldigung dafür gibt einen sexuell eindeutigen Deepfake einer Person ohne deren Zustimmung zu erstellen“.

Prinzipiell ist es in Großbritannien bereits eine Straftat ein intimes Bild ohne Zustimmung zu teilen oder mit der Veröffentlichung zu drohen. Das bezieht sich etwa auf Rache pornos. Die Aufnahme eines entsprechenden Videos oder Fotos ohne Einwilligung ist bislang aber nur unter bestimmten Umständen kriminalisiert, etwa beim sogenannten Upskirting, also dem Fotografieren oder Filmen mit unauffälligen Handy-Kameras heimlich unter den Rock oder das Kleid ihrer Opfer, wenn diese sich etwa auf Treppen befinden.

Mit den geplanten Gesetzesverschärfungen drohen jedem, der ein intimes Bild ohne Zustimmung aufnimmt, bis zu zwei Jahre Haft. Wer Geräte installiert, mit denen er oder jemand anderes intime Aufnahmen ohne Einwilligung erstellen kann, muss ebenfalls mit bis zu zwei Jahren Haft rechnen. Die Initiative, die einen Vorschlag der gescheiterten konservativen Vorgängerregierung vom April 2024 teilweise aufgreift, bezieht sich auf sexuell explizite Deepfakes mit Bildern von Erwachsenen. Einschlägiges Verhalten ist bereits strafbar, wenn das Bild ein Kind oder Jugendlichen unter 18 Jahren abbildet.

Die Female-Rights-Aktivistin Jess Davies, die die Regierung bei dem Vorhaben berät, erklärte: „Der Missbrauch intimer Bilder ist ein nationaler Notfall.“ Frauen und Mädchen würde damit erheblicher, langfristiger Schaden zugefügt, da sie „die Kontrolle über ihren digitalen Fußabdruck völlig verlieren“. Die Opferbeauftragte der Exekutive, Alex Davies-Jones (Labour), betonte: „Es ist inakzeptabel, dass jede dritte Frau Opfer von Online-Missbrauch geworden ist. Diese erniedrigende und abstoßende Form des Chauvinismus darf nicht zur Normalität werden.“

Laut der britischen Racheporno-Hotline hat der bildbasierte Missbrauch durch Deepfakes seit 2017 um mehr als 400 Prozent zugenommen. Zu den über 30 britischen Politikerinnen, die Opfer einer Deepfake-Porno-Webseite wurden, gehört Vizepremierministerin Angela Rayner. Die Strafrechtsverschärfungen sind Teil eines Gesetzesentwurfs der Regierung zu Kriminalität und Polizeiarbeit. Er soll nun zeitnah ins Parlament eingebracht werden (Krempf, KI-Porno: Großbritannien will Deepfakes mit sexuellem Bezug unter Strafe stellen, <https://www.heise.de/10230589>).

## USA

### Musk animiert über X zum Teilen von Gesundheitsdaten zwecks KI-Training

Der Eigentümer von X, Elon Musk, brachte X-Nutzer mit einem Aufruf,

ihre medizinischen Daten an die KI weiterzugeben, am 29.10.2024 dazu, dass diese reihenweise ihre Gesundheitsdaten mit Grok teilten und Röntgenbilder und MRT-Scans posteten. Grok ist der KI-Dienst von Musk. Er schrieb: „Versucht, Röntgen-, PET-, MRT- oder andere medizinische Bilder zur Analyse an Grok zu senden. Dies ist noch ein frühes Stadium, aber es ist bereits ziemlich genau und wird extrem gut werden. Lasst uns wissen, was Grok richtig macht oder wo noch Verbesserungsbedarf besteht.“

Während einige Ärzte die KI mit anonymisierten Computertomografien (CT) testeten und von den guten Ergebnissen positiv überrascht waren, teilten andere Nutzenden ihre persönlichen Aufnahmen und ließen diese auswerten, wobei teilweise fragwürdige Analysen von Grok zurückgegeben wurden. So wurde zum Beispiel die Röntgenaufnahme eines künstlichen Kniegelenks mit der Diagnose zurückgegeben, dass ein Knieersatz nötig ist. Ein Mediziner bemerkte dazu, dass Grok umso bessere Diagnosen erstellt, je mehr Kontext zur Verfügung steht.

Mit dem Zusatz „Sie sind Notarzt, dieser Patient kam mit Atemnot in die Notaufnahme. Kein offensichtliches Trauma. Was ist Ihre Diagnose?“ diagnostizierte Grok auf Grundlage des Röntgenbilds eines Oberkörpers: „Wahrscheinlichste Diagnose: Spannungspneumothorax auf der rechten Seite. Dies ist ein medizinischer Notfall, da er aufgrund des Drucks auf das Herz und die großen Blutgefäße zu lebensbedrohlichen Komplikationen führen kann.“ Auch das weitere Vorgehen, eine Nadeldekompression durchzuführen, um den Druck zu verringern, wurde laut dem Arzt richtig vorgeschlagen.

Der Professor für biomedizinische Informatik an der Vanderbilt University, Bradley Malin, wies darauf hin, dass es sich bei medizinischen Daten um sehr persönliche Informationen handele und man nicht wisse, was Grok damit machen werde. Wenn Technologieunternehmen mit Krankenhäusern zusammenarbeiteten, gäbe es detaillierte Vereinbarungen, welche Daten wie verwendet und gespeichert werden dürfen. Dies sei bei einer privaten Eingabe in

einen KI-Prompt oder einem Social-Media-Beitrag nicht der Fall.

Im Juli 2024 wurde bekannt, dass für das Training von Grok alle auf X verfügbaren Daten verwendet werden. In den Datenschutzrichtlinien von X steht hierzu geschrieben, dass persönliche Daten zwar nicht verkauft, aber „an verbundene Unternehmen“ weitergegeben werden können. In der Richtlinie von Grok heißt es: „Wir beabsichtigen nicht, sensible personenbezogene Daten zu sammeln, und bitten Sie uns keine derartigen Informationen zur Verfügung zu stellen“ (Faust, Künstliche Intelligenz: Musk forderte X-Nutzer auf medizinische Daten zu teilen, <https://www.golem.de> 19.11.2024).

## USA

### FTC schränkt TK-Standortdatenweitergabe ein

Die US-Handels- und Verbraucherschutzbehörde Federal Trade Commission (FTC) verpflichtete gemäß einer Mitteilung vom 04.12.2024 zwei Datenhändler keine Standortdaten im Zusammenhang mit bestimmten Orten mehr weiterzugeben. Den Unternehmen Gravy Analytics und Venntel wird demnach verboten „sensible Standortdaten“ zu verkaufen, offenzulegen oder zu benutzen. Sie sollen jeweils ein Programm einrichten, um den Zugriff auf solche Daten künftig ganz zu unterbinden. Bereits gesammelte Daten sollen gelöscht werden.

Datenhändler sammeln etwa mithilfe normaler Smartphone-Anwendungen oder Internetwerbung Daten über die Aufenthaltsorte der Geräte. Diese Telekommunikations-(TK-)Standortdaten werden dann zusammengefasst und weiterverkauft, unter anderem auch an Behörden. Die Praxis wird schon lange kritisiert, unter anderem, weil US-Geheimdienste und Strafverfolgungsbehörden auf diesem Weg gezielte Überwachung vornehmen können, die ihnen anderweitig untersagt oder stark erschwert wurde.

Der Schritt der FTC wird dem nun aber nicht wirklich Einhalt gebieten. Wie die FTC ausführt, beziehen sich die geplanten Einschränkungen nur auf sensible

Orte wie medizinische Einrichtungen, religiöse Organisationen, Justizvollzugsanstalten, Gewerkschaftsbüros, Schulen oder Kindertagesstätten, Orte zur Unterstützung von Menschen mit unterschiedlichen ethnischen Hintergründen, Stätten der Obdachlosenhilfe und Militäreinrichtungen. Standortdaten zu solchen Einrichtungen dürfen demnach künftig nicht mehr verkauft werden, zumindest nicht von Gravy Analytics und dem Tochterunternehmen Venntel. Der Plan muss noch von einem Gericht abgesegnet werden.

Vor der Bekanntmachung der Vorgaben für Gravy Analytics und Venntel hat die FTC bereits ähnliche Maßnahmen für einen weiteren Datenbroker angekündigt. Mobilewalla soll es demnach verboten werden bestimmte „sensible Standortdaten“ zu verkaufen, darunter solche, die verraten, wo die Betroffenen wohnen. Außerdem soll es der Firma untersagt werden Daten zu verkaufen, die bei Auktionen für Online-Werbeplätze gesammelt wurden, auf denen Mobilewalla gar nicht werben wollte. FTC-Chefin Lina Khan erklärte, damit schütze man die Menschen in Amerika vor „unkontrollierter Überwachung“ (Holland, Sensible Ortungsdaten: FTC setzt zwei Datenhändlern ein paar Grenzen, <https://www.heise.de> 04.12.2024, Kurzlink: <https://heise.de/-10187800>).

## USA

### Apple zahlt 95 Mio. US-Dollar für Siri-Mithören

Eine schon mehrere Jahre laufende Sammelklage gegen Apple wegen unerwünschter Aufzeichnung von Inhalten des Siri-Sprachassistenten ist gegen Zahlung einer Geldauflage beendet worden. Das zuständige Bundesgericht in Oakland, Kalifornien, genehmigte die außergerichtliche Einigung mit einer Auszahlungsumme von insgesamt 95 Millionen US-Dollar (92,38 Millionen Euro). Das Gericht hatte bereits im September 2021 entschieden, dass die Zivilklage Bestand hat. Apple hatte hingegen versucht sie abweisen zu lassen (Lopez et al. v. Apple Inc., U.S. District Court, Northern District of California, No. 19-04577).

Wie üblich bei einer solchen Einigung gibt es kein Schuldeingeständnis der beklagten Partei Apple. Die Summe ist relativ gering. Apple musste im Zusammenhang mit anderen Klagen – etwa wegen Hardware-Fehlern – schon dreistellige Millionenbeträge entrichten. Das Geld geht zudem nicht nur an die Teilnehmer der Klage sowie andere Betroffene, sondern zunächst an die Anwälte, die die Sammelklage vorangetrieben haben. Wie viel pro Person wirklich übrig bleibt, ist bislang unklar.

Die „Class Period“, also die Phase, in der Ansprüche bestehen, reicht vom 17.09.2014 bis zum 31.12.2024. Es ist geplant, dass betroffene Personen, sofern sie ihren Wohnsitz in den USA haben, „bis zu 20 Dollar“ erhalten. Die Summe kann aber schrumpfen. Sie wird pro Siri-fähigem Gerät – etwa iPhone oder Apple Watch – gezahlt. An die Anwälte sollen gemäß Medienberichten bis zu 29,6 Millionen Dollar fließen. 95 Millionen Dollar entsprechen ungefähr neun Stunden Gewinn, die Apple gemäß aktuellen Zahlen erwirtschaftet. Von der Sammelklage abgedeckt wird die gesamte Phase, in der die sogenannte „Hey Siri“-Funktion aktiv war – mit diesem „watch word“ oder „hot word“ wird die Sprachassistentin seitdem aufgerufen. Dabei soll es „routinemäßig“ zu unerwünschten Aufnahmen gekommen sein, die dann – teilweise – zum KI-Training verwendet wurden, inklusive Abhören durch Mitarbeiter des Konzerns. Apple hatte dazu eine eigene Abteilung beschäftigt, die aber später aufgelöst worden war. Im Rahmen der Sammelklage kam sogar der Vorwurf auf, Apple könne die privaten Gespräche auch dritten Parteien wie Werbetreibenden übergeben haben – etwas, das allerdings nicht belegt ist. Einige Nutzer behaupteten, sie hätten zu privaten Gesprächen passende Reklame im Web gesehen.

Die Sammelklage soll sich auf Dutzende Millionen Menschen in den USA beziehen. Der Konzern kommentierte die Entscheidung nicht. 2019 hat der Konzern eine Opt-In-Funktion implementiert, mit der Nutzer auf Wunsch zustimmen können, dass ihre Stimme Siri trainiert – viele Nutzer dürften dies aber nicht tun. Gegen Google läuft eine ähnliche Klage wegen möglicher Lauscheereien des Google Assistant (Schwan, Siri

hört mit: Sammelklage schlägt 95 Millionen US-Dollar bei Apple heraus, <https://www.heise.de> 03.01.2025, Kurzlink: <https://heise.de/-10223724>).

## Australien

### Altersbeschränkung bei Social Media auf 16 Jahre

Das Repräsentantenhaus von Australien hat mit großer Mehrheit einem Gesetzentwurf zugestimmt, der Jugendliche gesetzlich vor zu frühem Social-Media-Konsum schützen will. Plattformen wie etwa Facebook, Instagram und TikTok sollen erst ab 16 Jahren zugänglich sein. Überprüfen sollen das die Tech-Konzerne.

Premier und Labour-Parteichef Anthony Albanese begründete die Initiative: „Ich habe mit Tausenden Eltern, Großeltern, Tanten und Onkeln gesprochen, und sie sind, wie ich, zutiefst besorgt um die Online-Sicherheit unserer Kinder. Ich möchte, dass Eltern sagen können: ‚Tut mir leid, Kumpel, aber das ist gegen das Gesetz.‘“

Nach der Gesetzesverabschiedung soll es ein Jahr dauern, bis die neue Regelung in Kraft tritt. Die Plattformen sollen Zeit bekommen, um die Altersbeschränkung umzusetzen. Albanese betont: „Das ist eine weltweit maßgebende Gesetzgebung, und wir wollen sicherstellen, dass wir alles richtig machen.“ Tatsächlich ist Australien das weltweit erste Land, das ein Mindestalter für den Zugang zu sozialen Medien einführt.

Der Regierungschef hatte die Pläne im September 2024 angekündigt und die Wirkung von Online-Netzwerken wie etwa Facebook, Instagram und TikTok auf Kinder als „Geißel“ bezeichnet. Er wolle, dass Kinder eine Kindheit haben: „Wir wissen, dass soziale Medien sozialen Schaden anrichten und die Kinder von echten Freunden und echten Erfahrungen fernhalten.“ Auch die Opposition unterstützt den Vorstoß. Der für Kommunikation zuständige Sprecher der Liberalen Partei, David Coleman erklärte: „Wir glauben nicht, dass TikTok je für Kinder sicher gemacht werden kann, wir glauben nicht, dass Snapchat jemals für Kinder sicher gemacht werden kann und wir glauben

nicht, dass Instagram für Kinder sicher sein kann.“ Wie der Zugang technisch kontrolliert werden soll, ist noch unklar. Die Pflicht, das Mindestalter der Nutzer zu überprüfen, soll nicht den Eltern, sondern den Tech-Konzernen und Internetplattformen zufallen. Für Nutzer soll es keine Strafen geben. Kritiker warnen, dass das Gesetz Kinder und Jugendliche isolieren könne und sie von den positiven Aspekten sozialer Medien ausschließe.

In Deutschland müssen Social-Media-Plattformen Altersbeschränkungen in ihren Nutzungsbedingungen festlegen. Diese liegen aber fast immer unter 16 Jahren – zumeist bei 13 Jahren. Die Überprüfung ist jedoch sehr schwierig. In Deutschland gibt es kein allgemeines, gesetzlich festgelegtes Mindestalter für User von sozialen Medien. Theoretisch müssten die Eltern von Jugendlichen unter 16 Jahren der Nutzung zustimmen – jedoch wird das nur selten verifiziert, zudem können Geburtsdaten bei der Registrierung leicht gefälscht werden (Australien will Social Media erst ab 16, <https://www.tagesschau.de> 07.11.2024; Soziale Medien erst ab 16 Jahren, SZ 28.11.2024, 8).

## China

### Autonome Ermittlungs-Roboter testweise im öffentlichen Raum im Einsatz

Chinesische Polizeibehörden testen den kugelförmigen Überwachungsroboter RT-G des Robotikunternehmens Logon Technology. Der Roboter besitzt ein einzelnes zentrales Rad, das es ihm ermöglicht sich auf dem Land und im Wasser autonom fortzubewegen. Der Roboter soll mit Künstlicher Intelligenz (KI) selbstständig kriminelle Handlungen und gesuchte Verbrecher identifizieren können. RT-G patrouilliert bereits testweise in der Öffentlichkeit im Verbund mit Polizeibeamten in China.

Der RT-G misst etwa 60 cm im Durchmesser und wiegt 125 kg. Die Fortbewegung erfolgt durch ein rotierendes zentrales Rad, die Richtungssteuerung erfolgt durch Gewichtsverlagerung. Das

einzelne Rad hat mehrere Vorteile: Der Roboter ist so sicherer vor Vandalismus und hält Stößen von bis 4 t stand. Zudem kann er sich robust in unterschiedlichen, auch schwierigen Geländeformationen sowie im Wasser fortbewegen. Im Wasser schwimmt der Roboter an der Oberfläche und wird durch das Rad ähnlich wie ein Schaufelraddampfer fortbewegt. An Land soll er eine Geschwindigkeit von bis zu 35 km/h erreichen.

Der RT-G ist mit einer KI ausgerüstet, die rechtswidrige Handlungen in

der Öffentlichkeit erkennen können soll. Zudem kann der Roboter über seitlich angebrachte Kameras per Gesichtserkennung bereits bekannte und gesuchte Kriminelle erkennen. In solchen Fällen informiert er menschliche Polizeibeamte oder setzt die Verbrecher mit eingebauten Waffen fest oder außer Gefecht. Dazu steht dem Roboter ein ganzes Arsenal nicht-tödlicher Waffen zur Verfügung, u. a. eine Netzpistole, Tränengas, Granaten und Schallwellen-Dispersionsgeräte.

Die chinesischen Sicherheitsbehörden versprechen sich durch den Einsatz des RT-G bekannte Straftäter schneller aufzuspüren, die Strafverfolgung damit zu beschleunigen und durch die Überwachung die öffentliche Sicherheit zu erhöhen (Bunte, Polizeiroboter verfolgt Kriminelle auf einem Rad, <https://www.heise.de> 13.12.2024, Kurzlink: <https://heise.de/-10198109>).

## Technik-Nachrichten

### Europäisches KI-Sprachmodell

Das europäische Forschungsprojekt OpenGPT-X hat ein großes Sprachmodell für Anwendungen künstlicher Intelligenz (KI) veröffentlicht. Das Modell mit dem Namen „Teuken-7B“ wurde auf der Plattform „Hugging Face“ zum Herunterladen bereitgestellt. OpenGPT-X

ist ein europäisches Forschungs- und Entwicklungsprojekt, das Anfang 2022 gestartet wurde. Ziel des Projekts ist die Entwicklung eines großen KI-Sprachmodells, das den Anforderungen europäischer Werte, Datenschutzstandards und sprachlicher Vielfalt gerecht wird. „Teuken-7B“ wurde von Grund auf mit den 24 Amtssprachen der EU trainiert und umfasst sieben Milliarden Parame-

ter. Die USA haben eine Vormachtstellung bei KI-Sprachmodellen. Bislang stammen fast alle relevanten KI-Sprachmodelle der westlichen Welt aus den USA. Dazu gehören GPT-4 von OpenAI, Claude vom KI-Start-up Anthropic, Grok von Elon Musks xAI sowie Llama vom Facebook-Konzern Meta und Gemini von Google (KI-Sprachmodell aus Europa, SZ 27.11.2024, 17).

## Rechtsprechung

### EuGH

#### Geschlechtsangabe für Bahn-Ticket-Erwerb nicht erforderlich

Mit Urteil vom 09.01.2025 entschied der Europäische Gerichtshof (EuGH), dass die Erhebung von Daten hinsichtlich der Anrede der Kunden objektiv nicht unerlässlich ist, insbesondere wenn sie darauf abzielt, die geschäftliche Kommunikation zu personalisieren (Az. C-394/23). Der Verband Mousse hatte sich bei der französischen Datenschutzaufsichtsbehörde, der Commission Nationale de l'Informatique et des Libertés (CNIL), über die Praxis des französischen Eisenbahnunternehmens SNCF Connect, seine Kunden beim On-

lineerwerb von Fahrscheinen systematisch zu verpflichten ihre Anrede („Herr“ oder „Frau“) anzugeben, beschwert. Der DSGVO-Grundsatz der Datenminimierung sei verletzt, da die Anrede, die einer Geschlechtsidentität entspreche, für den Erwerb eines Fahrscheins nicht erforderlich sei. 2021 hatte die CNIL diese Beschwerde zurückgewiesen.

Mousse wandte sich hiergegen an das höchste französische Gericht, den Staatsrat (Conseil d'État), der sich an den EuGH mit der Frage der Erforderlichkeit der Kundenanrede wandte. Der EuGH wies in seiner Entscheidung darauf hin, dass die Ansprache mit „Herr“ oder „Frau“ weder zur Vertragserfüllung noch zur Wahrung eines berechtigten Interesses erforderlich ist. Eine Personalisierung der geschäftlichen Kommunikation, die auf einer anhand der

Anrede des Kunden angenommenen Geschlechtsidentität beruht, ist nicht objektiv unerlässlich, um die ordnungsgemäße Erfüllung eines Schienentransportvertrags zu ermöglichen. Das Eisenbahnunternehmen könnte sich entscheiden, bei seiner Kommunikation allgemeine und inklusive Höflichkeitsformeln zu nutzen, die in keinem Zusammenhang mit der angenommenen Geschlechtsidentität der Kunden stehen. Dies wäre eine praktikable und weniger einschneidende Lösung.

In Bezug auf ein möglicherweise bestehendes berechtigtes Interesse der SNCF stellte der EuGH klar, dass die geschäftliche Kommunikation mit personalisierter Geschlechtsidentität auch insofern nicht erforderlich ist. Dem Kunden müsse bei der Erhebung dieser Daten das verfolgte berechnete Inter-

esse und, dass die Gefahr einer Diskriminierung aufgrund der Geschlechtsidentität entgegenstehen könnte, mitgeteilt werden (EuGH, PM Nr. 2/25 v. 09.01.2025, DSGVO und Schienentransport: Die Geschlechtsidentität des Kunden ist keine für den Erwerb eines Fahrscheins erforderliche Angabe).

## EuG

### EDSA ist gegenüber nationaler Datenschutzaufsicht weisungsbefugt

Das Gericht der Europäischen Union (EuG) urteilte am 29.01.2025, dass der Europäische Datenschutzausschuss (EDSA) als übergeordneter Zusammenschluss der staatlichen europäischen Datenschutzkontrollen der irischen Datenschutzbehörde beim Durchsetzen der Datenschutz-Grundverordnung (DSGVO) verbindliche Vorgaben machen kann (Az. T-70/23, T-84/23, T-111/23). Der Wille des EU-Gesetzgebers gehe dahin „anhaltende Meinungsverschiedenheiten zwischen den betroffenen Aufsichtsbehörden über den Umfang der Analyse eines Falles – sowie gegebenenfalls über den Umfang der diesbezüglich durchgeführten Untersuchung – im Rahmen“ des Koordinationsverfahrens innerhalb des EDSA zu schlichten.

Die Data Protection Commission (DPC) in Dublin ist für „dicke Fische“ wie Google, Meta, Apple, Microsoft, TikTok & Co. zuständig, weil diese ihren europäischen Hauptsitz in Irland haben. Sie gilt als Flaschenhals bei der DSGVO-Durchsetzung. Im Datenschutzausschuss kommt es über Entscheidungsvorlagen der DPC oft zum Streit. Das löst komplizierte und lange Verständigungsverfahren aus, in denen die irische Behörde meist überstimmt wird. Damit wollte sie sich nicht zufriedengeben.

Konkret ging es um EDSA-Beschlüsse vom 05.12.2022. Meta wertete demnach die persönlichen Daten von Nutzern ohne Einwilligung gemäß Artikel 6 DSGVO unrechtmäßig für Werbung aus. Umstritten waren die anzuwendenden Datenschutzbestimmungen, die der US-Konzern bei seinen Töchtern Facebook, Instagram und WhatsApp anwendete. Für die Auswertung des Nutzerverhal-

tens auf fremden Webseiten und Apps bot Meta damals schon einen Opt-out an. Für die Inanspruchnahme ihrer persönlichen Informationen auf Facebook und Instagram selbst zum Zweck personalisierter Reklame hatten Nutzer damals aber keine Wahl.

Meta argumentierte jahrelang, dass eigene Data-Mining sei eine Leistung für die betroffenen Nutzenden. Die DPC versuchte Leitlinien des EDSA für die Auslegung der DSGVO im Sinne des Plattformbetreibers zu beeinflussen. Letztlich wollte sie Facebooks Einwilligungstrick abnicken, womit sie im EDSA aber nicht durchkam. Der entschied zudem, dass die irische Behörde auch die Auswertungen sensibler Daten nach Artikel 9 DSGVO für gezielte Werbung hätte untersuchen müssen. Im November 2023 wies der EDSA die Kollegen in Dublin ferner an das norwegische Verbot verhaltensbasierter Reklame auf ganz Europa auszuweiten.

Die DPC weigerte sich nach einer bereits über vierjährigen Verzögerung des Verfahrens der ersten verbindlichen Entscheidung nachzukommen. Sie beantragte beim EuG die teilweise Nichtigkeitsklärung der EDSA-Beschlüsse, soweit sie ihr auftrug neue Untersuchungen über die mit der Nutzung von Facebook, Instagram oder WhatsApp verbundenen Datenverarbeitungen durchzuführen und auf dieser Basis ergänzende Beschlusssentwürfe auszuarbeiten. Die Richter im Luxemburg wiesen die Klagen nun zurück: Aus der Rechtsauslegung ergebe sich unzweifelhaft, dass der EDSA befugt sei Weisungen wie die angefochtenen zu erlassen.

Das Argument der DPC, dass nur die nationalen Gerichte Einwände im Zusammenhang mit der Untersuchung überprüfen könnten, läuft laut dem EuG ins Leere. Wichtig sei, dass die Stellen, die die Aufsichtsbehörden überwachen, selbst genauso unabhängig sind wie diese selbst. Dies treffe auf den EDSA zu, da er aus Kontrolleuren der Mitgliedsstaaten und dem EU-Datenschutzbeauftragten bestehe. Bei letzterem handele es sich wiederum um eine gegenüber den von ihr überwachten Organen und anderen Behörden der Union unabhängige Instanz. Gegen das noch nicht rechtskräftige Urteil können beide Seiten binnen zwei Monaten und zehn Ta-

gen nach Zustellung beim Europäischen Gerichtshof (EuGH) Berufung einlegen.

Max Schrems, Vorsitzender der österreichischen Bürgerrechtsorganisation noyb, die den Fall mit einer Beschwerde 2018 in Gang brachte, freut sich über die Entscheidung. Sie bedeute aber auch, dass der Fall nach über sechs Jahren „wieder bei null anfängt“. Bis zu einer endgültigen Klärung der Rechtslage werde es voraussichtlich erneut Jahre vor der DPC und vor den irischen Gerichten brauchen. Die irische Aufsicht sei „ein Meister der grotesken Ausweichmanöver und Verfahrenschleifen – mit der Folge, dass ein US-Big-Tech-Unternehmen nie eine Strafe erhält“. Nach vielen Beschwerden versucht auch die EU-Kommission das DPC-Problem zu lösen (Krempel, EU-Gericht stärkt EU-Datenschützern gegenüber Irland den Rücken, <https://www.heise.de> 29.01.2025, Kurzlink: <https://heise.de/-10261219>).

## BVerfG

### Strategische BND-Kommunikationsüberwachung erneut beanstandet

Auf Klage von amnesty international beanstandete das Bundesverfassungsgericht (BVerfG) mit Beschluss vom 08.10.2024 erneut die Regelungen zur strategischen BND-Überwachung der Kommunikation mit dem Ausland (1 BvR 1743/16, 1 BvR 2539/16). Das sogenannte G-10-Gesetz muss bis Ende 2026 nachgebessert werden.

#### • Strategische Telekommunikationsüberwachung

Der deutsche Auslandsgeheimdienst, der Bundesnachrichtendienst (BND), macht strukturell wenig Anderes als das, was Edward Snowden 2013 bzgl. dem US-Geheimdienst NSA und der britischen GCHQ aufdeckte: Massenüberwachung der internationalen Kommunikation. Er überwacht anhand bestimmter Suchbegriffe strategisch die Kommunikation aus Deutschland ins Ausland sowie die Kommunikation zwischen Ausländern im Ausland. Nur die innerdeutsche Kommunikation ist

für den BND tabu. Von strategischer Überwachung spricht man, wenn der BND anlasslos Kommunikationsströme durchkämmt, die Telefonate, SMS und E-Mails enthalten. Der BND greift dabei gewaltige Datenmengen an den internationalen Kabelleitungen und aus dem Satellitenverkehr ab. Mithilfe von Suchbegriffen, sogenannten Selektoren, werden verdächtige Nachrichten automatisch ausgefiltert, um sie näher zu prüfen. Es gibt dabei inhaltliche Suchbegriffe wie zum Beispiel „Panzer“ und formale Suchbegriffe wie Telefonnummern oder E-Mail-Adressen.

Seit 1968 ist die Überwachung der Kommunikation zwischen Deutschland und dem Ausland im sogenannten G-10-Gesetz geregelt. Ursprünglich sollten damit Kriegsvorbereitungen des Ostblocks aufgedeckt werden. Seit 1994 steht der Kampf gegen Terrorismus und illegalen Rüstungshandel im Vordergrund. 2015 wurde die strategische Überwachung auch auf Cyberspionage und Cybersabotage erweitert (§ 5 Abs. 1 Satz 3 Nr. 8 G-10-Gesetz).

Am Ende sind meist nur sehr wenige Kommunikationen so relevant, dass sie von menschlichen BND-Beschäftigten angesehen und geprüft werden. Gemäß dem Bericht zum Jahr 2021 (Bundestags-Drucksache 20/9950) gab es am Ende 45 Treffer zur Rüstungsproliferation, zehn Treffer im Bereich der Schleuserkriminalität, vier Treffer zum internationalen Terrorismus und null Treffer zu Cyberangriffen, weil man seit 2019 gar nicht mehr danach suchte.

#### • Die Klage

Das Bundesverfassungsgericht hatte die strategische Überwachung zwischen Inland und Ausland schon 1999 überprüft und gebilligt (Urt. v. 14.07.1999, Az. 1 BvR 2226/94 u. a.). Aufgrund der enorm gestiegenen Bedeutung der digitalen Kommunikation fällt das Gericht nun aber eine neue Grundsatzentscheidung. Geklagt hatte 2016 die deutsche Sektion von amnesty international (ai) gemeinsam mit fünf Aktivisten in Deutschland und im Ausland. Die ai-Verfassungsbeschwerde war von der Gesellschaft für Freiheitsrechte (GFF) unterstützt worden. Was heute eine Selbstverständlichkeit ist, war damals ein Novum:

Es handelte sich um die erste Verfassungsklage der GFF. Neben ai hatte der Berliner Anwalt Niko Härting eine zweite Verfassungsbeschwerde eingereicht, die nun mitentschieden wurde.

Weil die Verfassungsbeschwerde gegen ein Gesetz nur binnen eines Jahres möglich ist, konnten ai und Härting nur gegen die letzte Erweiterung des § 5 G-10-Gesetz klagen. Zwar ist im Beschluss deshalb viel von Cybergefahren die Rede, doch lassen sich die Ausführungen auf die anderen Felder der strategischen Überwachung wie Terrorismus und Proliferation übertragen.

#### • Der Beschluss

Das Gericht nimmt in der aktuellen Entscheidung oft Bezug auf sein BND-Urteil vom 19.05.2020 (Az.: 1 BvR 2835/17; DANA 3/2020, 202 ff.). Damals hatte das BVerfG die gesetzlichen Regelungen der strategischen Überwachung der Kommunikation von Ausländern mit Ausländern im Ausland (im BND-Gesetz) geprüft und teilweise beanstandet. Zentral ist vor allem die dortige Klarstellung, dass die Grundrechte auch Ausländer gegen das Handeln der deutschen Staatsgewalt im Ausland schützen.

Das Gericht stellte nun fest, dass es sich bei der strategischen Überwachung des Fernmeldeverkehrs um einen „besonders schweren“ Eingriff in die Fernmeldefreiheit gemäß Art. 10 Grundgesetz handelt, da die anlasslose Überwachung potenziell jeden trifft, der mit dem Ausland kommuniziert. Und in E-Mails und SMS gehe es oft auch um (höchst-)persönliche Inhalte, die man nicht gerne mit einer Sicherheitsbehörde teile.

Allerdings sei diese Form der Überwachung grundsätzlich gerechtfertigt, da die Gefahren durch kriminelle, terroristische oder staatliche Cyberangriffe „außerordentlich hoch“ seien und zu einer „Destabilisierung des Gemeinwesens“ führen könnten. Angriffe auf die IT-Infrastruktur bei der Energie-, Wasser oder Gesundheitsversorgung könnten ähnlich schwer wiegen wie ein bewaffneter Angriff.

Das BVerfG erklärte nur die Ausgestaltung der strategischen Überwachung für verfassungswidrig, weil sie an vier Punkten das Prinzip der Verhältnismäßigkeit verletzt. So fehle eine Regelung,

die den BND verpflichtet innerdeutsche Kommunikation – soweit technisch möglich – vorab auszusondern, bevor er die Selektoren anwendet. Nötig ist dies, weil das Internet nicht nach innerdeutschen und grenzüberschreitenden Datenflüssen unterscheidet, im Netz wird vielmehr alles vermischt. Der BND kennt das Problem natürlich auch und hat deshalb Techniken entwickelt, wie er 96 bis 98 Prozent des innerdeutschen Verkehrs vorab aussondern kann. Das Verfassungsgericht stört sich nicht daran, dass der BND keine hundertprozentige Trennung erreicht, wohl fehle es aber an der gesetzlichen Aufforderung hier das technisch Bestmögliche anzustreben.

Das Gericht moniert zudem, dass der BND laut Gesetz nur bei Deutschen auf Suchbegriffe aus dem Kernbereich privater Lebensgestaltung verzichten muss. Das Verfassungsgericht fordert nun die Ausweitung des Kernbereichschutzes auf Ausländer im Ausland. Beispiele für unzulässige Suchbegriffe finden sich in der Entscheidung freilich nicht. So ist unklar, ob z. B. der Ausruf „Gott ist groß“ eine besonders persönliche Aussage oder doch eher ein Indiz für islamistischen Terror ist.

Drittens beanstandeten die Richter, dass Protokolle über das Löschen nicht benötigter Daten nur bis zum Ende des folgenden Jahres aufbewahrt werden müssen. Dies sei viel zu kurz, weil eine Benachrichtigung von Betroffenen (wenn überhaupt) oft erst stattfindet, wenn ein Verdacht sicher ausgeschlossen werden kann, was manchmal Jahre später ist.

Die vierte Kritik bezieht sich auf die Kontrolle der strategischen Überwachung durch die nebenberufliche G-10-Kommission. Der fünfköpfigen Kommission, die vom Bundestag gewählt wird, gehören zum Beispiel Anwälte und ehemalige Abgeordnete an. Vorsitzender ist derzeit der ehemalige SPD-MdB Christian Flisek. Das BVerfG hält eine „fachlich kompetente, professionalisierte gerichtsähnliche Kontrolle“ für erforderlich. Blaupause hierfür dürfte der Unabhängige Kontrollrat (UKR) sein, der seit 2022 die strategische Auslands-Auslands-Überwachung des BND kontrolliert und nach einer entsprechenden Aufforderung des BVerfG aus dem BND-Urteil von 2020

installiert wurde. Vorsitzender ist der ehemalige BGH-Richter Josef Hoch. Es ist gut möglich, dass der sechsköpfige UKR in absehbarer Zeit zusätzliche Arbeit bekommt. Der Bundestag hat Zeit bis zum 31.12.2026, um die Mängel zu beheben. Bis dahin darf der BND weiter die Inland-Ausland-Kommunikation strategisch überwachen (Rath, BND-Überwachung muss neu geregelt werden, <https://www.lto.de> 07.11.2024; Janisch, Das Ohr am Datenstrom, SZ 08.11.2024, 5).

## BVerfG

### Längerfristige Observation nach NRW-Polizeirecht ist verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 14.11.2024 festgestellt, dass die Regelung zur längerfristigen Observation unter gleichzeitigem Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen im Polizeigesetz Nordrhein-Westfalen (PolG NRW) verfassungswidrig ist und deshalb geändert werden muss (1 BvL 3/22). Streitpunkt war die verdeckte Überwachung eines Mannes, von der auch die Freundin betroffen war. Ein Rechtsextremist, der wegen Totschlags und anderen schweren Straftaten zu einer Freiheitsstrafe verurteilt worden war, wurde für längere Zeit von der Polizei in Nordrhein-Westfalen beobachtet. Um ein Abtauchen oder neue Straftaten nach Ende der Haft zu verhindern, wurde der Mann observiert. Davon war aber auch eine unbeteiligte Dritte betroffen, auch von ihr wurden Fotoaufnahmen im Rahmen der Observation erstellt.

Die Frau hielt das für rechtswidrig und klagte bis zum Bundesverwaltungsgericht in Leipzig dagegen. Die Richterinnen und Richter hatten grundsätzliche Zweifel an den Regelungen aus Nordrhein-Westfalen. Sie hielten die Vorschriften zu Observation und Bildaufnahmen für verfassungswidrig. Nach der geltenden Regelung ist eine langfristige Beobachtung für die Polizei nämlich schon dann erlaubt, wenn es Anhaltspunkte dafür gibt, dass eine Person eine schwere Straftat begehen will.

Das Bundesverfassungsgericht stellte in seinem Beschluss fest, dass eine Observation unter Anfertigung von Bildaufnahmen (§ 16a Abs. 1 S. 1 Nr. 2 u. § 17 Abs. 1 S. 1 1. U. 2. Alt. Nr. 2 PolG NRW) einen schweren Eingriff in Grundrechte darstellen kann. Das gelte insbesondere dann, wenn langfristig und dauerhaft heimliche Aufzeichnungen von einer Person erstellt werden. Obwohl es also um schwere Grundrechtseingriffe geht, sei die Schwelle für solche Maßnahmen im Polizeigesetz NRW zu niedrig und könne dadurch zu schnell angeordnet werden. Die Befugnisnormen setzen lediglich voraus, dass Tatsachen die Annahme rechtfertigen, dass Personen bestimmte Straftaten „begehen wollen“. Eine längerfristige Observation mit Erstellung von Bildaufnahmen sei nur erlaubt, wenn es zumindest eine konkrete oder wenigstens eine konkretisierbare Gefahr gibt, dass eine schwere Straftat begangen wird. Ein vager Verdacht reiche nicht aus. Die Polizei müsse Tatsachen vorbringen, die zumindest den Schluss auf ein konkretisiertes und zeitlich absehbares Geschehen zulassen. Nordrhein-Westfalen muss nun bis Ende 2025 sein Polizeigesetz anpassen. Unmittelbar gilt die Entscheidung nur für NRW. Die darin enthaltenen Maßstäbe sind aber auch für die Polizeigesetze der anderen Bundesländer relevant (Lagmüller, NRW-Polizeigesetz teils verfassungswidrig, <https://www.tagesschau.de> 03.01.2025; Längerfristige Observation unter Anfertigung von Bildaufnahmen und Bildaufzeichnungen nach dem PolG NRW mit dem Grundgesetz unvereinbar, BVerfG PM Nr. 1/2025 v. 03.01. 2025).

## BGH

### Schadenersatz für Datendiebstahl bei Facebook

Gemäß einem als Leitentscheidung gefällten Urteil des Bundesgerichtshofs (BGH) ist Facebook nach der Datenschutz-Grundverordnung (DSGVO) schadenersatzpflichtig, wenn Daten der Nutzer entwendet und veröffentlicht werden (Az. VI ZR 10/24). Das Urteil legt niedrige Hürden für Schadenersatzansprüche für immaterielle Schäden nach Art. 82 DSGVO an. Entgegen der

Auffassung von Facebook kann „auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die DSGVO ein immaterieller Schaden im Sinne der Norm sein“. Der Betroffene müsse nicht nachweisen, dass seine Daten missbräuchlich verwendet worden sind. Auch Belege für Angst und Sorge vor einem Missbrauch sind demnach nicht erforderlich.

Im April 2021 hatten Unbekannte eine Funktion zur Freunde-Suche bei Facebook ausgenutzt und Profildaten automatisch abgegriffen („Scraping“). Dabei konnten sie Daten von rund 533 Millionen Nutzern aus 106 Ländern erbeuten, die sie öffentlich im Internet verbreitet haben (DANA 2/2021, 134 f.).

Deswegen gegen Facebook eingereichte Schadenersatzklagen von Nutzern waren vor Gericht bisher zum Großteil ohne Erfolg geblieben. In den Verfahren spielt eine Rolle, ob Facebooks Standardvoreinstellung für die Kontakt-Importfunktion gegen die DSGVO verstößt. Kläger hatten kritisiert, dass die Sicherheitsmaßnahmen zu lasch gewesen seien. Wegen des erlittenen Ärgers und des Kontrollverlusts über die Daten wollten sie Ersatz auch für sogenannte immaterielle Schäden. Facebook-Mutterkonzern Meta lehnte solche Ansprüche ab, weil weder ein Verstoß gegen die DSGVO vorliege, noch den Klägern ein Schaden entstanden sei, der sich unmittelbar aus dem Vorfall ergebe. Eine Meta-Sprecherin hatte betont, dass mehr als 6.000 Klagen von den deutschen Gerichten abgewiesen worden seien, weil die Kläger „keine berechtigten Ansprüche auf Haftung oder Schadenersatz haben“.

Im konkreten Fall waren Kunden-ID, Vor- und Nachname, Arbeitsstätte und Geschlecht eines Facebook-Nutzers „gescraped“ worden. Er machte in seiner Klage am Amtsgericht Bonn geltend, dass Facebook keine ausreichenden Sicherheitsmaßnahmen ergriffen habe, um eine Ausnutzung des Kontakt-Tools zu verhindern. Ihm stehe wegen des erlittenen Ärgers und des Kontrollverlusts über seine Daten Schadenersatz zu. Während seine Klage in erster Instanz teilweise erfolgreich war, scheiterte er in zweiter Instanz am Oberlandesgericht (OLG) Köln.

Der BGH hatte die daraufhin eingereichte Revision zu einem sogenannten „Leitentscheidungsverfahren“ bestimmt. Diese Möglichkeit hat das Gericht, seit am 31.10.2024 das Leitentscheidungsgesetz in Kraft getreten ist: In Fällen, die grundlegende Rechtsfragen betreffen, soll eine Leitentscheidung des BGH als Richtschnur für niedere Instanzen in ähnlichen Fällen dienen. Der BGH urteilt in einem Leitentscheidungsverfahren selbst dann, wenn Prozessparteien ihre Revisionsanträge aus taktischen Gründen zurückziehen. Die BGH-Entscheidung dürfte also großen Einfluss auf tausende offene Verfahren zum selben Sachverhalt haben.

Den konkreten Fall verwies der BGH zur neuen Verhandlung und Entscheidung an das OLG Köln zurück und gab dem Gericht klare Ansagen mit: Die Voreinstellung der Suchbarkeitseinstellung auf „alle“ von Facebook entsprach nach Ansicht des BGH nicht dem DSGVO-Grundsatz der Datenminimierung. Außerdem habe „das Berufungsgericht ergänzend die Frage einer wirksamen Einwilligung des Klägers in die Datenverarbeitung durch die Beklagte zu prüfen“.

In einem Statement reagierte Meta auf das Urteil: „Wir sind der Meinung, dass die Einschätzung des Bundesgerichtshofs in Bezug auf Haftung und Schadenersatz nicht mit der jüngsten Rechtsprechung des Europäischen Gerichtshofs, dem höchsten Gericht in Europa, vereinbar ist.“ Die Systeme von Facebook seien bei diesem Vorfall nicht gehackt worden und es habe keinen Datenschutzverstoß gegeben.

Der BGH gab dem OLG Köln und allen anderen deutschen Zivilgerichten zudem klare Hinweise zur Bemessung des immateriellen Schadens aus Art. 82 Abs. 1 DSGVO: „Unter den Umständen des Streitfalles bestehen von Rechts wegen keine Bedenken dagegen, den Ausgleich für den bloßen Kontrollverlust in einer Größenordnung von 100 Euro zu bemessen.“ Viele Nutzer forderten bisher von Facebook Schadensersatz von 1.000 Euro und mehr.

Um zu prüfen, ob die eigenen Daten von einem Datenklau betroffen sind, können Betroffenen eine Anfrage auf der Webseite „[haveibeenpwned.com](https://haveibeenpwned.com)“ vornehmen. Die Stiftung Warentest hat einen Musterbrief erstellt, der von de-

ren Webseite heruntergeladen werden kann: „Einmal zur Post und höchstens 7,60 Euro Porto für den rechts-sicheren Versand“, heißt es auf der Webseite. Eingesetzt werden müssen weitere Daten; gesendet werden muss der Brief an die Tochtergesellschaft von Meta in Irland. Betroffene können sich auch an Unternehmen wie das Düsseldorfer Start-up Helpcheck wenden. Das LegalTech, das automatisierte juristische Dienstleistungen anbietet, ist im Facebook-Fall aktiv. Wer glaubte, betroffen zu sein, konnte auf der Firmenwebseite per Telefonnummer prüfen, ob dem so ist und dann das Start-up beauftragen. Dieses kassiert im Erfolgsfall 25 Prozent der Zahlung als Provision. Möglich ist auch einen Anwalt mit der Geltendmachung der Ansprüche zu beauftragen, was aber schnell teuer werden kann. Ein Weg ist zuletzt sich seinen Anspruch abkaufen zu lassen: So vermittelte die Anwaltskanzlei WBS Legal, die im Facebook-Fall schon einige Urteile erstritten hat, auf ihrer Webseite betroffene Nutzende an die Firma „Anspruch direkt“. Die zahlt im Facebook-Fall nach eigenen Angaben innerhalb weniger Tage rund 25 Euro aus, Betroffene können dann aber die Ansprüche nicht mehr selbst geltend machen. Die Ansprüche mussten im konkreten Fall bis Ende Dezember 2024 geltend gemacht werden, weil sie danach verjährt sind. Das Urteil hat auf Datenlecks generell Auswirkungen, da nach den BGH-Kriterien Verbraucher mit Klagen mehr Aussicht auf Erfolg haben (siehe auch die Meldung auf S. 33; Hauck, 100 Euro für Facebook-Nutzende, SZ 19.11.2024; Bleich, BGH verpflichtet Facebook zu Schadenersatz bei Datendiebstahl, <https://www.heise.de> 18.11.2024, Kurzlink: <https://heise.de/-10044449>).

## OLG Bremen

### Zwangweise Fingerabdruckentsperrung eines Smartphones ist zulässig

Das Oberlandesgericht Bremen (OLG) entschied mit Beschluss vom 08.01.2025, dass das Entsperrn eines Mobiltelefons durch zwangsweises Auflegen eines Fingers eines Beschuldig-

ten auf den Fingerabdrucksensor des Smartphones auf Grundlage der Strafprozessordnung (StPO) zulässig sei (Az. 1 ORs 26/24). Ähnliche Entscheidungen waren in Deutschland bislang nur von Amts- und Landgerichten bekannt.

Anlass für den Beschluss war eine Hausdurchsuchung, bei der ein Mann sein Mobiltelefon nicht entsperren wollte. Als eine Polizistin des Mannes Hand ergriff, um seinen Finger zwangsweise auf den Sensor zu legen, versuchte der Betroffene sich zu wehren. Er wurde schließlich am Boden fixiert, das Telefon wurde mit seinem Finger entsperrt. Wegen Widerstands gegen Vollstreckungsbeamte setzte es vom Amtsgericht Bremerhaven eine Geldstrafe, die auch vom Landgericht Bremen bestätigt wurde. Hiergegen legte der Bestrafte erfolglos Revision ein: „Die Diensthandlung der einschreitenden Polizeibeamten, mit Anwendung unmittelbaren Zwanges (...) war rechtmäßig. (...) Die Entsperrung eines Mobiltelefons durch Auflegen eines Fingers eines Beschuldigten auf den Fingerabdrucksensor des Telefons kann auf die Ermächtigungsgrundlage des § 81b Absatz 1 StPO gestützt werden.“

Diese Norm gestattet unter anderem die zwangsweise Aufnahme von Lichtbildern und Fingerabdrücken. Die technikoffene Formulierung des Paragraphen erlaube „auch die Vornahme ähnlicher Maßnahmen“. Das Auflegen eines Fingers auf einen Sensor sei so eine ähnliche Maßnahme – ein geringerer Eingriff als die Abnahme eines Fingerabdrucks zur dauerhaften Speicherung durch Ermittlungsbehörden.

Fachjuristen sind dazu geteilter Meinung. Das OLG schlägt sich auf die Seite der Zwangsbefürworter und verweist dazu auf jeweils eine gleichartige Entscheidung des Landgerichts Ravensburg sowie des Amtsgerichts Baden-Baden. Zwar werde in das Grundrecht auf informationelle Selbstbestimmung eingegriffen, aber nur mit geringer Intensität. Dies sei gerechtfertigt. Der Grundsatz, sich in Strafverfahren nicht selbst belasten zu müssen, verbiete nur Zwang zu aktiver Mitwirkung, nicht aber Zwang zur Duldung.

Zudem habe der Staat zwar in das Grundrecht des Bürgers auf Vertraulichkeit und Integrität informations-

technischer Systeme eingegriffen, allerdings verfassungskonform: Für einen heimlichen Zugriff gälten laut Bundesverfassungsgericht und Europäischem Gerichtshof gesteigerte Voraussetzungen, für den offenen Zugriff wie im vorliegenden Fall aber nicht. Im Übrigen sei der allgemeine Grundsatz der Verhältnismäßigkeit anzuwenden, der ebenfalls für die Zwangsmaßnahme spreche. Die Alternative wäre die Anfertigung einer Fingeratruppe gewesen, ein noch tieferer Eingriff in die Rechte des Bürgers.

Getrennt von der Entsperrung sei zu beurteilen, ob die auf dem Telefon gespeicherten oder über das Telefon abrufbaren Daten ausgewertet werden dürfen. Das war allerdings nicht Anlass für die Geldstrafe und daher nicht Kernthema der Entscheidung über das Rechtsmittel. Das OLG verweist kurz auf die Bestimmungen zu Durchsuchung und Beschlagnahme in den Paragraphen 94 und 110 StPO (Sokolov, Polizistin erzwingt Fingerabdruck zu Handy-Entsperrung: OLG findet das OK, <https://www.heise.de> 21.01.2025, Kurzlink: <https://heise.de/-10251294>).

**LG Düsseldorf**

**Entgeltliches selbstauskunft.de wegen Verbrauchertäuschung verurteilt**

Die Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) ist erfolgreich gegen den Betreiber der Seite [www.selbstauskunft.de](http://www.selbstauskunft.de), NLTSGlobalAnalytics s.r.o, vorgegangen und hat beim Landgericht (LG) Düsseldorf am 02.10.2024 ein Anerkenntnisurteil, die Gestaltung der Webseite in dieser Form zu unterlassen, bewirkt (Az. 14c O 70/24). Auf dieser Webseite heißt es: „Wir besorgen Ihre SCHUFA-Auskunft.“ In „unter 1 Minute“ sei der Antrag gestellt. Die Kosten für diese Dienstleistung wurden jedoch nicht deutlich gekennzeichnet. Carolin Semmler, Juristin bei der VZ NRW, ergänzt: „Die Preisangabe war zudem nicht an der richtigen Stelle. Denn laut Gesetz muss der Preis unmittelbar bevor Verbraucher:innen ihre Bestellung abgeben deutlich genannt werden.“ Mittlerweile hat das Unternehmen seine In-

ternetseite angepasst und den Preis für seine Dienstleistung in unmittelbarer Nähe zum Bestellbutton und deutlich hervorgehoben platziert, doch Semmler kritisiert: „Allerdings verlangt die Firma mittlerweile sogar 39,90 € für ihr Angebot.“

Es gibt zahlreiche kommerzielle Anbieter, die mit der kostenpflichtigen Beantragung von Urkunden, Führungszeugnissen oder anderen öffentlichen Leistungen werben, obwohl die direkte Beantragung bei der Behörde in vielen Fällen kostenlos wäre. Auch eine Kopie der bei der Schufa gespeicherten Daten können Verbraucher:innen kostenfrei direkt bei der Schufa beantragen. Die Schufa nennt die kostenlose Auskunft „Daten-Kopie nach Art. 15 DSGVO“. Semmler kritisiert: „Viele Verbraucher:innen stoßen über Suchmaschinen auf diese Anbieter, die durch das Schalten von Werbeanzeigen ganz oben in der Ergebnisliste platziert sind. Manchen Verbraucher:innen ist gar

nicht bewusst, dass sie sich nicht auf der offiziellen Seite für die Antragstellung befinden oder dass es auch einen kostenfreien Weg gibt.“

Wer sich einen Überblick darüber verschaffen möchte, welche Informationen Unternehmen und Auskunftsteien über die eigene Person gespeichert haben, kann eine kostenlose Auskunft verlangen. Insbesondere bei Auskunftsteien lohnt sich ein kontrollierender Blick: Kredite oder der Online-Kauf auf Rechnung scheitern immer wieder an falsch gespeicherten Daten. Daher empfiehlt die VZ NRW Verbraucher:innen regelmäßig eine kostenlose Auskunft nach Art. 15 DSGVO bei Auskunftsteien wie Schufa, CRIF, Creditreform Boniversum, infoscore Consumer Data und anderen einzuholen, um die Richtigkeit der dort gespeicherten Daten zu überprüfen (Verbraucherzentrale NRW, Beantragung kostenfreier Schufa-Auskunft gegen Entgelt, PM v. 27.11.2024).

**Buchbesprechungen**



Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmman, Indra (Hrsg.) **Datenschutzrecht DS-GVO/BDSG** Nomos Verlagsgesellschaft Baden-Baden, 2. Aufl. 2025, 2.679 S., ISBN 978-3-8487-8958-0, 229,00 €

(tw) Spiros Simitis, der Nestor des Datenschutzrechts in Europa, ist am 18.03.2023 gestorben (DANA 2/2023,

95), doch sein Kommentar, der „Simitis“ lebt. Dieser Kommentar hat eine jahrzehntelange Geschichte: Als das deutsche Bundesdatenschutzgesetz (BDSG) 1977 erlassen wurde, erschien auch erstmals die von ihm herausgegebene Erläuterung – damals auf weniger dicht bedruckten immerhin 991 Seiten. Seitdem erschienen insgesamt 8 Auflagen zum mehrfach novellierten BDSG und 2019 die erste Auflage der Kommentierung zur Datenschutz-Grundverordnung (DSGVO). Diese wurde nun – in der Tradition des bisherigen BDSG-Kommentars – gemeinsam mit Indra Spiecker und Gerrit Hornung herausgegeben. Diese Tradition besteht nicht nur im Umfang, sondern auch in seiner wissenschaftlichen Qualität. Es ist also mehr als eine Hommage an Spiros Simitis, dass die zweite Auflage des „Datenschutzrechts“ unter seinem Namen fortgeführt wird, zumal er immer noch in der Einleitung als Mitautor präsent ist.

Während die erste Auflage sich auf die Kommentierung der DSGVO be-

schränkte und in diesem Rahmen das die DSGVO ins deutsche Recht umsetzende BDSG nur cursorisch einbezog, finden wir nun eine umfassende BDSG-Kommentierung, auch der §§ 45 ff, mit denen die Datenschutzrichtlinie Justiz-Inneres umgesetzt werden soll. Zwar gibt es in der Datenschutzliteratur mehr als genug Erläuterungen des allgemeinen Datenschutzrechts, doch hebt sich das Werk heraus. Dies liegt zum einen an den insgesamt 27 Autorinnen und Autoren, die sich im Bereich des Datenschutzes – sei es in der Aufsicht, der Wissenschaft oder der Verwaltung – schon über viele Jahre einen Namen gemacht haben. Dies liegt zudem am Selbstverständnis, das weniger von ökonomischen oder administrativen Interessen, sondern von Grundrechten geleitet wird. Das liegt schließlich in der Durchdringung der Materien: Seit der 1. Auflage ist viel Literatur veröffentlicht worden, wovon die wichtigen Quellen und Meinungen berücksichtigt sind. Berücksichtigt sind ebenso (bis Sommer 2024) die immer umfangreichere Rechtsprechung vom EuGH über das BVerfG bis hin zu den vielen weiteren (auch ausländischen) Gerichten sowie die Verlautbarungen der Datenschutzaufsicht. Somit behauptet sich der „Simitis“ als Grundlagen- und Standardwerk. Dies gilt sowohl für die wissenschaftliche Recherche als auch für die Anwendung des Datenschutzrechts in der Praxis: Sämtliche informationellen Eingriffsregelungen haben letztlich ihre Grundlage in den Artikeln 6 und 9 DSGVO und müssen sich an die dort festgehaltenen Vorgaben halten. Aber auch die Regelungen zu den Betroffenenrechten, zum technisch-organisatorischen Datenschutz oder zu Verfahrensfragen finden in der DSGVO ihre Grundlage. Während viele andere Kommentare insofern oft unterbelichtet sind, wird mensch im „Simitis“ regelmäßig fündig.

Auch ein Standardwerk ist angesichts der immer komplexer werdenden Rechtslandschaft mit vielen Bezügen zum Datenschutzrecht und den vielen bereichsspezifischen Konkretisierungen nicht in der Lage die Breite des gesamten Datenschutzrechts abzubilden. So orientiert sich auch diese Kommentierung streng an der DSGVO und dem BDSG, erwähnt die Seitenlinien allen-

falls am Rande. Dies gilt für die vielen Rechtsakte, die gerade in jüngster Zeit von der EU im Rahmen ihrer Digitalisierungsstrategie auf den Weg oder schon in Wirksamkeit gebracht wurden. Dies gilt auch für die datenschutzrechtlichen Spezialthemen – vom Telekommunikationsrecht über das Polizeirecht bis zum spezifischen Gesundheitsdatenschutz. Hierzu finden sich allenfalls Querverweise. Nötig wird dann der Zugriff auf Spezial-Literatur. Die umfangreichen Quellennachweise wie auch die erwähnten Schnittstellen machen den Kommentar zu den Grundsatzfragen zum wertvollen Nachschlagewerk des ersten Zugriffs.



Schwartmann, Rolf/Keber, Tobias O./Zenner, Kai (Hrsg.)  
**KI-VO Leitfaden für die Praxis**  
 C.F. Müller, Heidelberg  
 2. Auflage 2024, 325 S.,  
 ISBN 978-3-8114-6454-4, 85,00 €

(hdn) Dieser Leitfaden ist an dem Tag, am dem die Verordnung über Künstliche Intelligenz (KI-VO) in Kraft getreten ist, veröffentlicht worden, nämlich am 1. August 2024. Somit sind zum Beispiel Hinweise auf oder Kommentare von Urteilen hier nicht zu erwarten. Dagegen ist das Werk der 23 Autorinnen und Autoren bis in die Nebensätze mit wertvollen Kommentaren und Hinweisen zur KI-VO selbst prall gefüllt.

Der erste Teil liefert die Grundlagen und Begriffsbestimmungen und grenzt KI in verschiedenen Dimensionen zu benachbarten Handlungsfeldern ab. Hier finden sich auch Hinweise zu Praxisfällen (Biometrie, Arbeitsrecht und Straf-

verfolgung etc.), alles in sehr geraffter Form. Kern des Leitfadens ist jedoch der zweite Teil, der sich sehr akribisch und intensiv mit dem komplexen Thema KI-VO fundiert auseinandersetzt. Hier wird insbesondere eingehend auf den Risikoansatz in den verschiedenen KI-Systemen und die nicht zu unterschätzenden Anforderungen an Betreiber und Anwender eingegangen. An dieser Stelle wird auch auf die Transparenzpflichten, den technischen Datenschutz und die Grundrechte-Folgenabschätzung sowie auf die Datenschutz-Folgenabschätzung hingewiesen. Der dritte Teil schließlich beschreibt praxisrelevante Haftungsfragen und die Möglichkeiten der Durchsetzung durch die Aufsichtsorgane.

Die Gliederung mit sieben (!) Ebenen führt in Verbindung mit dem Stichwortverzeichnis nicht unbedingt zum schnellen Auffinden einer gesuchten Passage. Hier ist der Blick auf das detaillierte Inhaltsverzeichnis zielführender. Das Buch wendet sich ohnehin eher an Juristen und juristisch geschulte Entscheider in den vielfältigen Einrichtungen von Wirtschaft und Verwaltung. Diese Zielgruppen werden in diesem Werk sicherlich wertvolle Informationen zur gezielten Anwendung der KI-VO finden.



Martini, Mario/Wendehorst, Christiane  
**KI-VO: Verordnung über Künstliche Intelligenz – Kommentar**  
 Verlag C.H. Beck München, 2024, XXII,  
 1.178 Seiten,  
 ISBN 978-3-406-81136-4, 199,00 €

(hhs) Die KI-Verordnung (KI-VO) der EU ist im August 2024 in Kraft getreten.

Ihre Geltung entfaltet sie in der nächsten Zeit Stück für Stück. Die KI-VO stellt das erste umfassende Regelwerk zur Künstlichen Intelligenz weltweit dar und enthält Antworten, aber auch weitere Unbekannte, für die zahlreichen Anwendungsfragen dieser universell einsetzbaren Technologie. Kaum ist die KI-Verordnung im Amtsblatt der EU veröffentlicht, liegt sehr zeitnah der Großkommentar von Martini und Wendehorst zu der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz vor. Die Autorenschaft der Bearbeiter\*innen ist dabei sehr vielfältig gestreut, von Österreich über die Schweiz nach Deutschland, so dass man auch schon von einer europäischen Kommentierung sprechen kann. Einige der Bearbeiter waren wohl „in verschiedensten Funktionen“ in die Vorbereitung des Rechtsaktes eingebunden, was kein Nachteil sein kann.

Das Werk soll dem Anwender detaillierte und wissenschaftlich fundierte Erläuterungen, viele wertvolle Hinweise für die Praxis und einen übersichtlichen und strukturierten Aufbau bieten. Letzteres ist voll gelungen. Nach dem Inhaltsverzeichnis folgen die vollständigen Erwägungsgründe und dann die Kommentierung in der Reihenfolge der Artikel der KI-VO.

Für den Datenschutz-Interessierten stellt sich im Weiteren die Frage bezüglich der Hinweise für die Praxis. Immerhin verspricht der Verlag in seiner Werbung, dass die Bezüge zu anderen Regelwerken, wie zur DSGVO, berücksichtigt werden. So soll die KI-VO nach ErwG 9 KI-VO das bestehende Unionsrecht, das durch diese Verordnung ergänzt wird, unberührt lassen, also auch den Datenschutz und damit die DSGVO. Ja, die KI-Systeme sind im Einklang mit den geltenden Vorschriften zum Schutz der Privatsphäre und zum Datenschutz zu entwickeln und zu verwenden (ErwG 27 KI-VO). Schaut man nun in das Sachregister, so findet man unter dem Begriff Datenschutz auch etwas zum Verhältnis der DSGVO zur KI-VO. Die Verknüpfung zu beiden Normen steht in Art. 2 Abs. 7 KI-VO und dort findet sich in der Kommentierung der Hinweis für die Ausnahmen zu Art. 10 Abs. 5 und 59

KI-VO (Rn. 142), beides Normen, welche unabhängig von der DSGVO Anwendung finden. Unter dem Begriff „Datenschutz-Grundverordnung“ ist im Stichwortverzeichnis eine Verknüpfung zu Art. 8 KI-VO (Einhaltung der Anforderungen) zu finden. In der Kommentierung zu Art. 8 KI-VO erfährt man unter Rn. 15, dass die Anforderungen der DSGVO stets erfüllt werden müssen, auch wenn die KI-VO in einzelnen Bestimmungen wichtige Ausnahmen von der Anwendung der DSGVO vorsehe. Welche das jedoch sind, bleibt an dieser Stelle offen. Auch fehlt ein Verweis auf Art. 2 Rn. 142 und damit auf die Art. 10 und 59 KI-VO. Der Hinweis auf wichtige Ausnahmen – ohne diese zu benennen – hilft in der Praxis leider nicht sehr viel und gibt keine Antworten.

Unter dem Stichwort „DSGVO“ findet man noch eine Verknüpfung zu Art. 71 KI-VO (EU-Datenbank für die in Anhang III aufgeführten Hochrisiko-KI-Systeme), was sich aber nur auf die KI-Datenbank und auf die personenbezogenen Daten der Person bezieht, die für die Registrierung verantwortlich ist.

Alles in allem kann man dem vorliegenden Werk jedoch eine wissenschaftliche Basis in keiner Weise abstreiten, auch wenn man sich manchmal eine Vertiefung gewünscht hätte. So ähnelt das Recht auf Beschwerde (Art. 85 KI-VO), welches relativ spät in die VO aufgenommen wurde, dem Recht des Art. 77 DSGVO. Ob die Aussage in der Kommentierung allerdings richtig ist, dass eine betroffene Person keine Befassung mit ihrer Beschwerde bzw. dem gemeldeten Verstoß erzwingen könne (Rn. 10), erscheint sehr fraglich. Denn die Beschwerde ist nach den von den Marktüberwachungsbehörden „dafür eingeführten Verfahren“ zu behandeln. Welche das sind, verrät der Kommentar an dieser Stelle leider nicht. Zumindest steht Art. 85 KI-VO unter der Überschrift des Abschnittes 4 „Rechtsbehelfe“. Es dürfte daher höchst zweifelhaft sein, dass eine solche Beschwerde europarechtlich als Petition gewertet werden kann und nicht dem Rechtsschutz von Betroffenen dienen soll. Denn dann wäre es kein Rechtsbehelf. Es spricht vielmehr sehr viel dafür, dass es eine Befassung und Bescheidung von der Marktüberwachungsbehörde bedarf, so wie dies der EuGH zur DSGVO festge-

stellt hat (EuGH, Urteil vom 07.12.2023, C-26/22 und C-64/22 – SCHUFA Holding). Hier hätte sich der Rezensent eine vertiefere Betrachtung als Rechtsbehelf erhofft, zumal die Verarbeitung personenbezogener Daten im Rahmen eines KI-Systems wohl auch nicht ausgeschlossen werden kann.

Alles in allem kann man sagen, dass im Hinblick auf die Geschwindigkeit der Veröffentlichung des Kommentars im Verhältnis zu der Veröffentlichung der KI-VO eine bemerkenswerte Leistung vollbracht worden ist. Das vorliegende Werk enthält eine Kommentierung aller Normen der KI-VO und verschafft dem Leser die Möglichkeit sich zügig in einzelne Fragen der KI-VO einzuarbeiten. Dies auch, wenn das Ganze noch sehr stark im Fluss ist und sich auch die Meinungsbildungen zu einzelnen Fragen noch fortentwickeln dürften. Dies bleibt wohl einer der nächsten Auflagen des schon sehr umfangreichen Kompendiums vorbehalten. Dafür ist der vorliegende Kommentar der Erste auf dem Markt. Das Sachverzeichnis hilft bei der Erschließung der umfangreichen Verordnung nebst ihren Anlagen, welche im Amtsblatt bereits selbst 144 Seiten einnimmt.

Der vorliegende Kommentar ist als erster Kommentar zur KI-VO ein guter Einstieg, wenn man sich mit Fragen zu der KI-VO befasst und damit allen zu empfehlen, die sich mit diesem neuen Thema – aus welchen Gründen auch immer – befassen.

Mühleis, Niklas/Akinci, Nick (Hrsg.)  
**Rechtsleitfaden KI im Unternehmen**  
 Rheinwerk Verlag, Bonn 1. Auflage  
 2024, 308 S.,  
 ISBN 978-3-367-10098-9, 39,90 €

(hdn) Zehn Fachleute aus Technik und Justiz schreiben über die rechtlichen Grundlagen bei der Einführung von Künstlicher Intelligenz (KI) in Unternehmen. Ihnen gemeinsam ist die gut verständliche Sprache, in der die komplexen Sachverhalte beschrieben werden. Dargestellt werden auch die problematischen Aspekte im Bereich des Datenschutzes, die mit ihren Grundsätzen, Rechtsgrundlagen, Verantwortlichkeit sowie Hinweisen zur Einbindung von Datenschutzbeauftragten in



einem eigenen Kapitel wirklich gut beschrieben werden.

Das erste Kapitel beschäftigt sich auf gut 100 Seiten neben dem bereits erwähnten Datenschutz mit Funktion und Anwendung von KI, dem Urheberrecht bei der Verwendung von KI, den Haftungs- und Rechtsfragen sowie den Besonderheiten der KI-Compliance. Die gute Erläuterung von Aufbau und Funktion einer KI ist nachvollziehbar und trägt zum Verständnis ihrer Arbeitsweise bei.

Das ebenfalls sehr umfangreiche zweite Kapitel hilft bei der Nutzbarmachung der KI und weist auf die zu berücksichtigenden Nutzungsbedingungen hin. Das Urheberrecht mit seinen Problemstellungen speziell bei generativer KI, das Verwertungsrecht und damit verbundene weitere Rechte wie z. B. Vortrags- und Aufführungsrechte, Vervielfältigungsrechte oder Ausstellungsrechte sind Gegenstand eines separaten Kapitels. Nach nochmals vertiefendem Wissen über den Datenschutz liefern die Autoren Informationen rund um Persönlichkeitsrechte, Geschäftsgeheimnisse und Haftungsfragen. Der Abschnitt schließt mit Hilfestellungen zu KI-Unternehmensrichtlinien.

Weitere Kapitel beschreiben Individuallösungen, wobei die Autoren durchaus den Betrieb eigener Modelle unter Verwendung eigener Trainingsdaten empfehlen. Das vierte Kapitel liefert Anwendungen aus der Praxis, konkret die Arbeit mit Chatbots, Bild-KI, Personalarbeit und Softwareherstellung. Den Schluss bilden Hinweise über die KI-Verordnung, den Integrationsprozess von KI ins Unternehmen so-

wie einen Ausblick über die technische Entwicklung.

Das Buch ist gefüllt mit Praxishinweisen, Checklisten und Hintergrundwissen in allen Kapiteln. Die Zielgruppen, Anwender sowohl in Start-ups als auch in eingeführten Unternehmen, sind mit diesem Werk sehr gut bedient. Die leichte Verständlichkeit und auch der faire Preis sollten eine schnelle Verbreitung im Markt der Anwender begünstigen.



Windholz, Natascha et al  
**Praxishandbuch KI-VO. Künstliche Intelligenz rechtskonform im privaten und öffentlichen Bereich einsetzen**

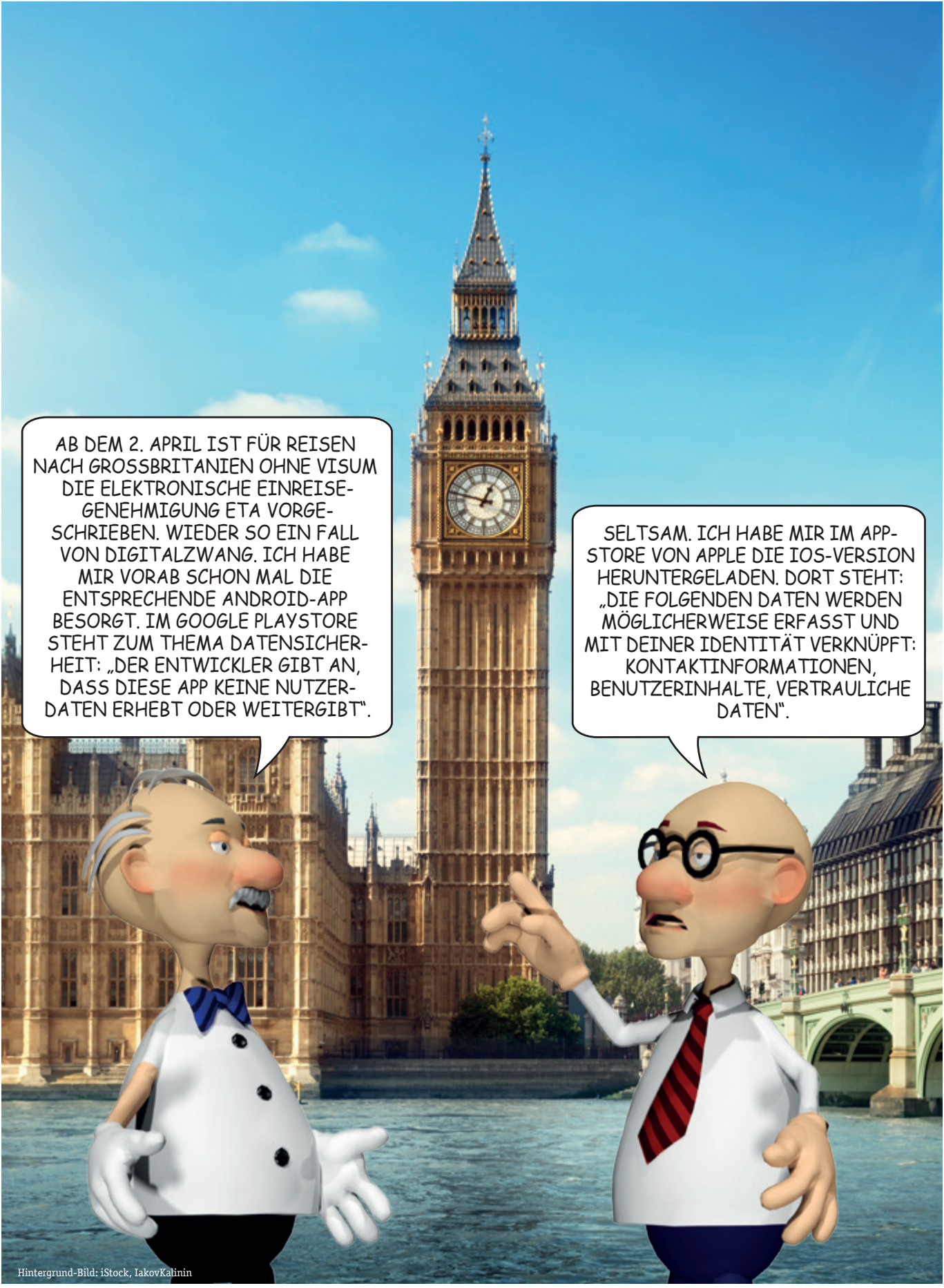
Carl Hanser Verlag, München 2025,  
521 S., ISBN 978-3-446-48194-7,  
69,90 €

(hdn) Das von siebzehn Fachautorinnen aus Wissenschaft und Praxis verfasste Werk besteht aus zehn inhaltvollen Kapiteln, die einen detaillierten Überblick über die Verordnung zur Künstlichen Intelligenz (KI-VO) und ihre Anwendung in der Praxis geben. Die stringente Gliederung umfasst alle wesentlichen Themen rund um die KI. Gleich zum Einstieg wird auf die Begriffe eingegangen, mit denen die verschiedenen Datenkategorien beschrieben und somit zielgerichtet eingeordnet werden können (z. B. Datenmanagement, Datenqualität, Datenanalytik, Data Governance). So wird auch gleich auf andere europäische Gesetze Bezug genommen. Die Autorinnen beziehen verwandte Rechtsgebiete genauso ein (Datenschutz-, IP- und IT-Recht) wie die Themen KI Governance, Risk und Compliance in Unternehmen – inklusive Blick

auf den risikobasierten Ansatz und die Grundrechte-Folgenabschätzung.

Eine Vielzahl von Anwendungsbeispielen von KI in der täglichen Praxis kennzeichnen das Werk. Für den privaten Bereich werden Auswirkungen u. a. auf Finanzwesen, Werbung, Hinweisgebung, Tourismus oder Bildung aufgeführt, nicht ohne zuvor die Probleme einer möglichen Diskriminierung und der verbotenen KI darzulegen. Im öffentlichen Bereich stehen Anwendungen bei Wahlen, Strafverfolgung und NIS bzw. NIS-2 im Fokus. Ausführungen zur Ethik für eine vertrauenswürdige KI und zur Governance im Unternehmen schließen das Buch ab. Dem Datenschutz wird ein eigenes Kapitel gewidmet. Auf den 35 Seiten sind alle wesentlichen Punkte der DSGVO dargelegt, für die in Betrieben empfohlenen Richtlinien in Bezug auf KI und Datenschutz wird ein Katalog mit Inhalten bereitgestellt. Der Abschnitt zur Technikgestaltung (Art. 25 DSGVO) ist knapp gehalten. Hier könnte ein Beispiel zur Umsetzung in die Praxis wie in anderen Kapiteln hilfreich sein. Auf die Probleme einer automatisierten Entscheidungsfindung in einer KI-Technologie wird dagegen eindringlich hingewiesen.

Weitgehend alle Kapitel weisen neben umfassenden Übersichten und Checklisten abschließend eine Quellenangabe auf. So können die Kapitel einzeln durchgearbeitet werden. Ausgewählte Themen können je nach Bedarf isoliert voneinander bearbeitet werden – sicherlich ein sehr praktischer Vorteil für dieses doch sehr umfangreiche Werk. Somit dürfte das Buch nicht nur für Anwender in den Betrieben und Behörden von Interesse sein. Auch Studierende aus betriebswirtschaftlichen, verwaltenden oder sozialen Fachgebieten, die sich mit der Materie beschäftigen müssen, finden einen schnellen Zugang. Dafür sprechen auch die wenigen juristischen Formulierungen, da vertiefende Informationen zur jeweiligen Rechtslage sehr gut in Tabellen, Quellenverzeichnissen und Fußnoten vorzufinden sind.



AB DEM 2. APRIL IST FÜR REISEN NACH GROSSBRITANIEN OHNE VISUM DIE ELEKTRONISCHE EINREISEGENEHMIGUNG ETA VORGESCHRIEBEN. WIEDER SO EIN FALL VON DIGITALZWANG. ICH HABE MIR VORAB SCHON MAL DIE ENTSPRECHENDE ANDROID-APP BESORGT. IM GOOGLE PLAYSTORE STEHT ZUM THEMA DATENSICHERHEIT: „DER ENTWICKLER GIBT AN, DASS DIESE APP KEINE NUTZERDATEN ERHEBT ODER WEITERGIBT“.

SELTSAM. ICH HABE MIR IM APPSTORE VON APPLE DIE IOS-VERSION HERUNTERGELADEN. DORT STEHT: „DIE FOLGENDEN DATEN WERDEN MÖGLICHERWEISE ERFASST UND MIT DEINER IDENTITÄT VERKNÜPFT: KONTAKTINFORMATIONEN, BENUTZERINHALTE, VERTRAULICHE DATEN“.