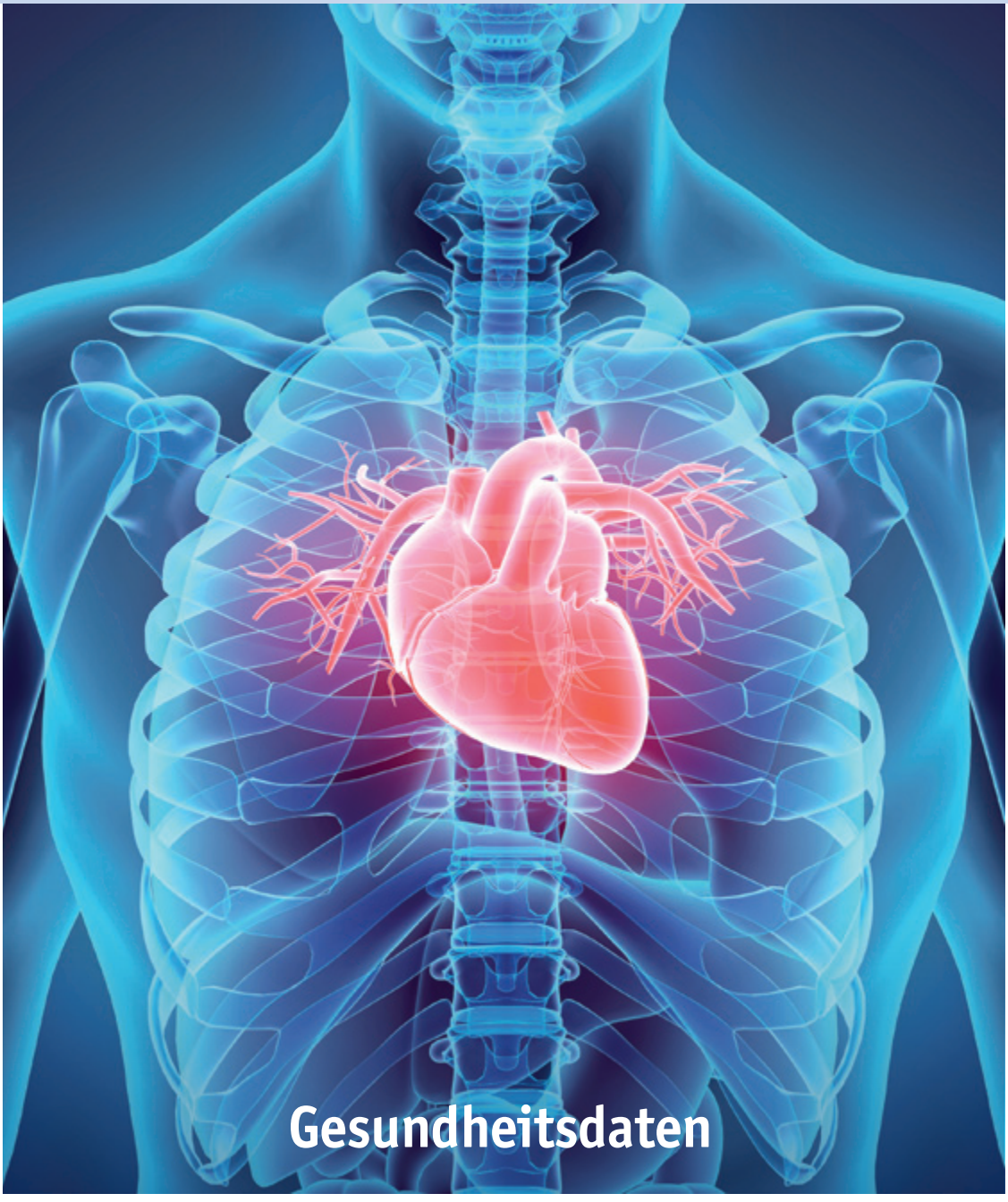
2/2024

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

47. Jahrgang
ISSN 0137-7767
16,00 Euro



■ Das Digital-Gesetz aus Sicht von Datenschutz und IT-Sicherheit ■ Gesundheitsdatennutzung ohne Datenschutz? Lauterbach auf Spahns Spuren der Verfassungswidrigkeit ■ Gesundheitsdaten bei Doctolib? So nicht! ■ Zum Grundrecht auf Informationelle Selbstbestimmung - und was daraus geworden ist ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

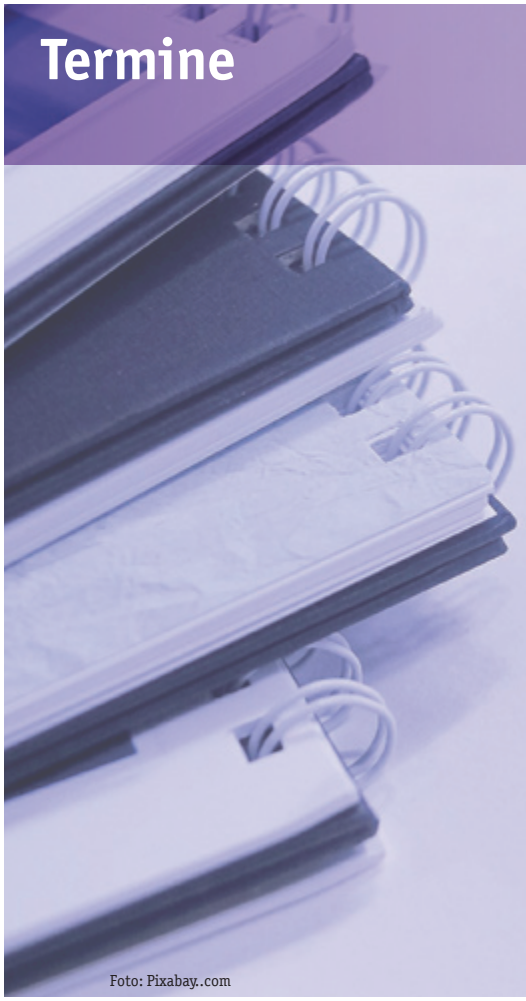


Foto: Pixabay..com

Donnerstag, 01.08.2024
Redaktionsschluss DANA 3/2024
„Nach der Europawahl"

Sonntag, 08.09.2024
Vorstandssitzung der DVD
Kiel

Montag, 09.09.2024
Sommerakademie „Von digitalen Datenräumen bis zu den Archiven – Treuhänder im Lebenszyklus der Daten"
Unabh. Landeszentrum für Datenschutz, Kiel

Mittwoch-Freitag, 25.-27.09.2024
Fachtagung Datenschutz im Gesundheitswesen
bitkom Frankfurt

Freitag, 11.10.2024
BigBrotherAwards – Die Oscars für Datenkraken
Digitalcourage, Bielefeld

Mittwoch-Freitag, 16.-18.10.2024
BvD-Herbstkonferenz & Behördentag
BvD, Stuttgart

Donnerstag/Freitag, 17./18.10.2024
Jahreskonferenz 2024, 9. Jahrestagung der Plattform Privatheit
Berlin

Freitag-Sonntag, 25.-27.10.2024
FIfF-Konferenz „Nachhaltigkeit in der IT"
Hochschule Bremerhaven

Freitag, 01.11.2024
Redaktionsschluss DANA 4/2024

Samstag, 09.11.2024
Vorstandssitzung der DVD
Bonn

Sonntag, 10.11.2024
Mitgliederversammlung der DVD
Bonn

DANA
Datenschutz Nachrichten
ISSN 0137-7767
47. Jahrgang, Heft 2

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
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert
c/o Deutsche Vereinigung für
Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
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.

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

Abbildungen, Fotos
Pixabay, iStock,
Frans Jozef Valenta
Titel: iStock – yodiyim

Editorial

Es gibt Zeiten, in denen es für den Datenschutz mau aussieht: Es wird nicht darüber diskutiert; er findet keine Beachtung. Keine Rede kann davon sein, dass aktuell über den Datenschutz nicht diskutiert würde. Ob er beachtet wird, steht aber mehr als oft zuvor in Frage: Das Ende der Legislatur des Europaparlaments hat zu einem Push bei Digitalthemen geführt, wobei Privacy und Data Protection immer mit dabei sind. Der Europäische Gerichtshof entscheidet zum Datenschutz schon fast am Fließband, was zweifellos dem Grundrechtsschutz und der Rechtssicherheit dient. In den USA sind diese Themen angesichts des anstehenden Präsidentschaftswahlkampfes im Fokus. Und in Deutschland werden gerade viele Gesetzesvorhaben erörtert und beschlossen, bei denen es auch um die Verarbeitung personenbezogener Daten geht.

Die intensive Diskussion ist keine Gewähr dafür, dass der Stellenwert des Datenschutzes gewahrt wird. Symptomatisch dafür ist ein Zitat unseres FDP-Digitalministers Volker Wissing, dessen Partei sich auf der einen Seite als Kämpferin für den Datenschutz zu profilieren versucht, indem sie sich gegen jede Form der IP-Datenspeicherung bei der Telekommunikation zur Wehr setzt, und die sich schon vor Jahren (2017) zu profilieren versuchte mit „Digital first – Bedenken second“. Wissing bekommt bei der Digitalisierung von Wirtschaft und Verwaltung kaum etwas gebacken, zugleich propagiert und legitimiert er Digitalzwang, etwa bei der Deutschen Bahn AG, für die er auch zuständig ist: „Wir müssen uns von analogen Strukturen trennen. Wir können es uns nicht erlauben Überflüssiges weiter fortzuführen. Ein Papierfahrschein generiert keine Daten. Wenn wir aber wissen wollen, wie viele Menschen zu welcher Uhrzeit von wo nach wo fahren, können wir den öffentlichen Nahverkehr effizienter und präziser planen – und das wollen ja alle. Das ist es, worum es bei der Digitalisierung wirklich geht: um das Generieren und Verknüpfen von Daten“ (SZ 10.04.2024, 13).

Es kommt also nicht von ungefähr, dass sich die DANA wieder mit der Datennutzung befasst – konkret mit der Nutzung von Gesundheitsdaten: Beim eben verabschiedeten Digitalgesetz und dem Gesundheitsdatennutzungsgesetz (wie dem ebenso beschlossenen European Health Data Space) geht es um das Generieren und Verfügbarmachen hochsensitiver Daten. Leider gilt auch hier „Bedenken second“ – oder gar noch weiter hintenan. Bernd Schütze und Thilo Weichert machen eine Bestandsaufnahme. Wie wenig nicht nur begründete Bedenken, sondern eklatanter Rechtsbruch ignoriert wird, das zeigt uns die immer weiter verbreitete Gesundheitsdatenkrake Doctolib. Das Unternehmen ist auch Gegenstand eines von der DVD angebotenen, am 16.07.2024 stattfindenden Videovortrags. Beachten Sie dazu unseren Hinweis auf Seite 86.

Angesichts der vielen Diskussionsthemen freut sich die DVD über Beiträge, innerhalb des Vereins und gerne auch über die DANA als Medium.

Das nächste DANA-Heft wird sich dann mit Europa befassen und der Frage, was die nächste Legislaturperiode des Europaparlaments zum Datenschutz bringen wird bzw. muss.

Die Redaktion

Autorinnen und Autoren dieser Ausgabe:

Dr. Rolf Gössner
Jurist und Publizist, Kuratoriumsmitglied der Internationalen Liga für Menschenrechte, Mitherausgeber von Ossietzky - Zweiwochenschrift für Politik/Kultur/Wirtschaft, Mitherausgeber des jährlich erscheinenden „Grundrechte-Report. Zur Lage der Bürger- und Menschenrechte in Deutschland“ (Fischer-TB),
https://rolf-goessner.de

Dr. Bernd Schütze
Leiter GMDS AG Datenschutz und IT-Sicherheit im Gesundheitswesen, Bonn,
schuetze@medizin-informatik.org

Dr. Thilo Weichert
Vorstandsmitglied der DVD, Netzwerk Datenschutzexpertise, Kiel,
weichert@datenschutzverein.de

Bernd Schütze

Das Digital-Gesetz aus Sicht von Datenschutz und IT-Sicherheit

Am 15. Juni 2023 wurde der Referentenentwurf des Bundesministeriums für Gesundheit (BMG) für ein Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) zur Kommentierung an Verbände entsprechend § 47 Abs. 3 der Gemeinsamen Geschäftsordnung der Bundesministerien verteilt; am 14. Dezember 2023 wurde das Gesetz vom Bundestag beschlossen, vom Bundesrat am 2. Februar 2024 angenommen und am 22. März 2024 im Bundesgesetzblatt veröffentlicht.[1] Im DigiG werden in 15 Artikeln acht bestehende Gesetze sowie fünf Verordnungen geändert, die meisten Änderungen betreffen das Fünfte Buch Sozialgesetzbuch (SGB V). Einige der geänderten Regelungen betreffen die Vergütung von Leistungen, andere die Art und Weise der Versorgung von Patienten. An dieser Stelle können nicht alle Regelungen besprochen werden, vielmehr beschränkt sich die Darstellung in diesem Artikel auf einige wenige ausgewählte Regelungen mit Bezug zu den Themen Datenschutz und IT-Sicherheit.

Gesundheitsgesetzgebung: Der deutsche Sonderweg

Die Gesetzgebungskompetenz hinsichtlich Gesundheitsrecht ist geteilt: Gemäß Art. 74 Abs. 1 Nr. 19a GG besteht eine konkurrierende Zuständigkeit von Bund- und Landesgesetzgeber, wobei Art. 74 Abs. 1 Nr. 19a GG der gesetzgeberischen Zuständigkeit des Bundes für das Gebiet der Krankenhäuser klare Grenzen setzt.[2] Aus Art. 74 Abs. 1 Nr. 19a GG ergibt sich das Primat der Länder für Fragen der Krankenhausplanung und -organisation[3] (Art. 70 Abs. 1 GG[4]). Aus Art. 2 Abs. 2 S. 1 GG i. V. m. dem Sozialstaatsprinzip folgt u. a., dass es Aufgabe des jeweiligen Bundeslandes ist, die stationäre Versorgung zu gewährleisten.[5] Die Länder erließen in Wahrnehmung ihrer Kompetenz jeweils eigene Krankenhausgesetze. Entsprechend Art. 74 Abs. 1 Nr. 19a GG stehen dem Bund lediglich die Regelungen der wirtschaftlichen Sicherung der Krankenhäuser und der Krankenhauspflegesätze zu.[6] Demgemäß darf der Bund Fragen, welche die Krankenhausplanung betreffen, nur regeln, wenn der Bezug zur wirtschaftlichen Sicherung der Krankenhäuser offensichtlich ist und den Ländern eigenständige und erhebliche Ausgestaltungsspielräume bleiben.[7]

Nach Art. 74 Abs. 1 Nr. 19 GG besteht u. a. bzgl. der Zulassung zu ärztlichen und anderen Heilberufen eine konkurrierende Gesetzkompetenz. Das Bundesverfassungsgericht urteilte, dass der Bund im Bereich des Gesundheitswesens seine begrenzten Regelungsmöglichkeiten nicht unter Berufung auf die öffentliche Fürsorge ausweiten darf: „Die Entscheidung der Verfassung (Art. 74 Nr. 19 und 19a GG), dem Bund für das Gesundheitswesen nur in eingeschränktem Maße Gesetzgebungskompetenzen zuzuweisen, darf nicht durch eine erweiternde Auslegung der Gesetzgebungskompetenz für die öffentliche Fürsorge unterlaufen werden“.[8]

Somit unterliegen insbesondere Änderungen, welche Fragen der Organisation oder Arbeitsweise von Krankenhäusern betreffen (wie beispielsweise Outsourcing inkl. Nutzung von Cloud-Diensten), ausschließlich der Gesetzgebungskompetenz der Bundesländer; Fragen mit Bezug zur wirtschaftlichen Sicherung der Krankenhäuser kann der Bund regeln, muss dabei aber den Ländern Gestaltungsspielräume lassen.

Niedergelassene Arzt- und Zahnarztpraxen wiederum sind freie Unternehmen, deren aus Art. 12 Grundgesetz (GG) abgeleitete Freiheit nur beschränkt werden darf, wenn es für das Allgemeinwohl unerlässlich ist. Jedoch hat der Bund Freiheiten bzgl. der Regelungen, welche Leistungen der Sozialstaat bezahlt und welche nicht.

Alle Regelungen des DigiG (wie auch des Gesundheitsdatennutzungsgesetzes, welches auch in diesem Heft besprochen wird) müssen im Kontext dieser Vorgaben des Grundgesetzes betrachtet werden. Widersprüche zum Grundgesetz, z. B. weil der Bundesgesetzgeber die Gesetzgebungskompetenz der Länder nicht beachtet, führen bei Rechtsanwendern wie Krankenhäusern, Arztpraxen oder Apotheken zu Unsicherheiten, denn man muss damit rechnen, dass bei einer Klage das Gesetz spätestens vom Bundesverfassungsgericht für nichtig erklärt wird und auf dem Gesetz beruhende Investitionen verloren sind.

Sicherheit in der ambulanten und stationären Versorgung

Die 2019 eingeführte Regelung zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung (§ 75b SGB V) sowie die im Oktober 2020 eingeführte Regelung zur IT-Sicherheit in Krankenhäusern (§ 75c SGB V) wurden aufgehoben, zugleich drei neue Paragrafen erlassen:

- § 390 SGB V: IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung
- § 391 SGB V: IT-Sicherheit in Krankenhäusern
- § 392 SGB V: IT-Sicherheit der gesetzlichen Krankenkassen

Die neuen Regelungen enthalten überwiegend den Wortlaut der alten Regelungen, wurden jedoch auch ergänzt:

- § 390 SGB V verpflichtet (wie zuvor auch § 75b SGB V) die Kassenärztliche Bundesvereinigung (KBV) dazu eine Richtlinie zur Sicherheit[9] in der vertragsärztlichen Versorgung zu veröffentlichen. Neu eingeführt wurde mit Abs. 2 Ziff. 2 die Pflicht für Maßnahmen, welche Beschäftigte bzgl. Informationssicherheit sensibilisieren.

- § 391 SGB V: Abs. 2 der neuen Regelung sieht vor, dass auch Maßnahmen zur Steigerung der Security-Awareness von Mitarbeiterinnen und Mitarbeitern verpflichtend sind.

Erfüllt werden können die Anforderungen des § 391 SGB V insbesondere dann, wenn Krankenhäuser den Vorgaben eines branchenspezifischen Sicherheitsstandards[10], wie ihn die Deutsche Krankenhausgesellschaft in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte, befolgen.

Kritik ruft insbesondere hervor, dass Verstöße gegen gesetzliche Auflagen nicht sanktioniert werden. Die Richtlinie der KBV entspricht sicherlich nicht dem Stand der Technik, insbesondere angesichts der Sensibilität der zu schützenden Patientendaten. Gesetzlich vorgeschrieben ist eine jährliche Aktualisierung der KBV-Richtlinie, die Richtlinie wurde zuletzt am 22. Januar 2021 überarbeitet.

Ein weiterer Kritikpunkt besteht darin, dass ambulante und stationäre Versorger die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur gewährleisten sollen, die Vorgaben jedoch von der Gesellschaft für Telematik (gematik) kommen. Diese ignoriert aber verschiedene Grundsätze der IT-Sicherheit wie beispielsweise einen Virenschutz für Daten in der ePA oder Prüfung von über die TI-Infrastruktur zu übermittelnden Daten auf Malware bzw. will entsprechende Maßnahmen nicht umsetzen.

Sicherheit bei den Kranken- und Pflegekassen

§ 392 SGB V ist vollständig neu und bestimmt auch gesetzliche Krankenkassen dazu einen Mindeststandard zur Gewährleistung der IT-Sicherheit zu befolgen. Die Regelungen entsprechen weitestgehend den Anforderungen der §§ 390, 391 SGB V. Entsprechend ist der Stand der Technik zu beachten, wobei die Angemessenheit von Maßnahmen am Aufwand bestimmt wird: Der Aufwand darf nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Arbeitsprozesse stehen. Auch hier wird auf einen branchenspezifischen Standard verwiesen.

Der neu eingeführte § 103a SGB XI verpflichtet Pflegekassen zur Gewährleistung von IT-Sicherheit analog zur Regelung § 392 SGB V. D. h., ein vom BSI als geeignet eingestufter branchenspezifischer Sicherheitsstandard soll erstellt werden. Darin sollen Anforderungen zur Gewährleistung eines Mindeststandards zur IT-Sicherheit formuliert werden, welche erfüllt werden müssen.

IT-Sicherheit und gematik

In der Vergangenheit zeigte sich mehrfach, dass Vorhaben der gematik ohne ausreichende Betrachtung der Anforderungen von Datenschutz und IT-Sicherheit erfolgten; erst bei Auftreten von Sicherheitsvorfällen erfolgten seitens der gematik Reaktionen.[11]

Immer wieder musste das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf die gematik einwirken, damit zumindest ein Mindeststandard der IT-Sicherheit eingehalten wird. Mit dem Patientendaten-Schutz-Gesetz wurde am 20. Oktober 2020 in § 311 Abs. 2 SGB V die gematik verpflichtet Festlegungen und Maßnahmen, die Fragen der Datensicherheit berühren, im Einvernehmen mit dem BSI zu treffen. Dies führte oft zu zeitlichen Verzögerungen: Offensichtlich wurde IT-Sicherheit seitens der gematik immer erst bei Besprechungen mit dem BSI adressiert, was dazu führte, dass die Pläne der gematik angepasst werden mussten.

Mit dem DigiG wurde das Einvernehmen mit dem BSI auf eine einfache Benehmensherstellung reduziert, d. h. die gematik muss Hinweise des BSI künftig nur noch zur Kenntnis nehmen, jedoch nicht länger berücksichtigen.

Dies mag Projekte aus Sicht der zeitlichen Vorgaben des BMG beschleunigen, jedoch stellt sich die Frage nach der Haftung der gematik für Sicherheitsvorfälle, wenn diese künftig Hinweise des BSI nicht befolgt und den Stand der Technik nicht einhält. Da gemäß § 310 Abs. 2 SGB V das BMG 51 % der Anteile der gematik besitzt, wird ggf. auch das BMG in die Haftung bei aufgrund unzureichender oder sogar fehlerhafter Vorgaben erfolgenden Sicherheitsvorfällen einzubeziehen sein.

Elektronische Patientenakte: Opt-Out inkl. Nutzung für Forschung

Nach § 342 Abs. 1 SGB V müssen gesetzliche Krankenkassen ab dem 15. Januar 2025 eine elektronische Patientenakte zur Verfügung stellen, wenn Versicherte dieser Bereitstellung nicht innerhalb von sechs Wochen nach Information durch die Krankenkasse widersprochen haben. Nach § 342 Abs. 2 Ziff. 4 SGB V müssen die Daten spätestens sechs Monate nach Bereitstellung der elektronischen Patientenakte zu Forschungszwecken bereitgestellt werden können.

Gemäß den §§ 347 und 348 SGB V müssen an der vertragsärztlichen Versorgung teilnehmende Leistungserbringer wie Krankenhäuser oder Arztpraxen Daten des Versicherten in die elektronische Patientenakte zur dortigen Speicherung übermitteln, soweit Versicherte dem nicht widersprachen. Daten der Krankenkasse selbst werden entsprechend § 350 SGB V ebenfalls in die Akte übermittelt und dort gespeichert, wenn die Versicherten nicht aktiv widersprochen haben.

Nach § 363 Abs. 1 SGB V müssen die Daten der elektronischen Patientenakte für die in § 303e Abs. 2 SGB V aufgeführten Sekundärzwecke zugänglich gemacht werden. Versicherte haben auch gegen diese Datenweitergabe lediglich ein Widerspruchsrecht. Gemäß § 363 Abs. 2 SGB V werden die Daten in pseudonymisierter Form automatisiert an das Forschungsdatenzentrum (§ 303d SGB V) übermittelt. Obwohl die Vorgabe der Pseudonymisierung seit 20. Oktober 2020 besteht, ist bis heute nicht bekannt, wie die Pseudonymisierung erfolgen soll: Die Sicherheit, die durch die Pseudonymisierung bezweckt wird, kann daher bis heute nicht eingeschätzt werden. Dies gilt insbesondere auch für das Re-Identifikationsrisiko.

Das Forschungsdatenzentrum, welches die Daten der elektronischen Patientenakte somit automatisiert erhält, wenn kein Widerspruch vorliegt, muss Nutzungsberechtigten die vorhandenen Daten für die in § 303e Abs. 2 SGB V genannten Zwecke zur Verfügung stellen. Nutzungsberechtigt sind nach der durch das DigiG erfolgten Änderung des § 303e Abs. 1 S. 2 SGB V natürliche und

juristische Personen im Anwendungsbereich der Verordnung (EU) 2016/679, also faktisch jeder EU-Bürger und jedes Unternehmen und jede Organisation innerhalb der EU; die Beschränkung erfolgt ausschließlich über die in § 303e Abs. 2 SGB V genannten Zwecke. Bisher waren Nutzungsberechtigte auf Krankenkassen bzw. deren Verbände, Leistungserbringer usw. beschränkt, privatwirtschaftliche Unternehmen und Organisationen waren jedoch ausgeschlossen.

Auch die erlaubten Zwecke wurden durch das BMG mit dem DigiG deutlich erweitert: Bisher sollte die Datennutzung zur Verbesserung der Qualität der Versorgung, zur Planung von Leistungsressourcen wie beispielsweise der Krankenhausplanung oder zur Forschung des Versorgungsgeschehens möglich sein. Durch das DigiG wurden nun u. a. auch Produktentwicklungen oder Produktweiterentwicklungen in den Katalog der gesetzlich legitimierten Zwecke aufgenommen. Somit können entsprechend § 303e Abs. 2 Ziff. 9 SGB V beispielsweise Hersteller von IT-Systemen oder Pharmaunternehmen die (wie auch immer) pseudonymisierten Daten der elektronischen Patientenakte über den Umweg des Forschungsdatenzentrums für die Entwicklung und Weiterentwicklung von Arzneimitteln, Medizinprodukten oder Systemen der künstlichen Intelligenz im Gesundheitswesen nutzen.

Google Inc. oder Amazon Web Services Inc. sind keine Nutzungsberechtigten i. S. v. § 303e Abs. 1 S. 2 SGB V, Google Ireland Limited hingegen ist eine juristische Person im Anwendungsbereich der Verordnung (EU) 2016/679, wird nutzungsberechtigt und könnte einen Antrag zur Nutzung der Daten zwecks Entwicklung von Systemen der künstlichen Intelligenz im Gesundheitswesen stellen.

Ab in die Cloud: Aber nur mit vielen Rechtsunsicherheiten …

Was ist „Cloud"? Nicht so einfach zu beantworten!

In § 385 Ziff. 5 SGB V findet sich die Definition eines Cloud-Computing-Dienstes, welcher weitestgehend der Begriffsbestimmung in Art. 6 Ziff. 30 Richtlinie (EU) 2022/2555 („NIS-2-Richtlinie") entspricht. Obwohl das SGB V an verschiedenen Stellen auf Rechenzentren verweist, findet sich im SGB V keine Begriffsbestimmung des Begriffs Rechenzentrum oder Rechenzentrumsdienst. Art. 6 Ziff. 31 Richtlinie (EU) 2022/2555 enthält zwar eine Definition, aber aufgrund der fehlenden Übernahme in die deutschen Begriffsbestimmungen ist eine rechtssichere Abgrenzung zwischen einem Cloud-Computing-Dienst und einem Rechenzentrumsdienst kaum möglich.

§ 385 Ziff. 5 SGB V definiert einen Cloud-Computing-Dienst als einen „digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind." Ist ein digitales Bildarchiv der Radiologie („PACS"), welches in einem über das Internet (= per Fernzugriff) erreichbaren Rechenzentrum eines Diensteanbieters betrieben wird und wo entsprechend des Bedarfs flexibel Platz zur Abspeicherung der medizinischen Bilddaten usw. hinzu gebucht werden kann (skalierbarer und elastischer Pool), ein Cloud-Computing-Dienst? In der Vorstellung vieler Anwender wohl nicht. Juristisch bereitet der fehlende Rechenzentrumsbegriff „Herausforderungen".

§ 393 SGB V: Erlaubnisnorm für Cloud-Verarbeitung? Auch nicht so einfach …

§ 393 Abs. 1 SGB V[12] erlaubt die Verarbeitung von Sozial- und Gesundheitsdaten: *„Leistungserbringer […] und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsdatenverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind."*

Wie einleitend dargestellt besitzt der Bundesgesetzgeber nur eine eingeschränkte Gesetzgebungskompetenz für Leistungserbringer. Im Bereich der Krankenhäuser muss zwingend vorrangig das entsprechende Landesrecht beachtet werden. Enthält das Landesrecht Vorgaben für ein Outsourcing, so müssen diese landesrechtlichen Anforderungen auch im Kontext der Nutzung eines Cloud-Computing-Dienstes beachtet werden.

Auch Apotheken gehören zu den im vierten Kapitel SGB V genannten Leistungserbringern und fallen somit unter die Regelung von § 393 Abs. 1 SGB V. Zumindest in Bezug auf ihre Abrechnung dürfen Apotheken gemäß § 300 Abs. 2 SGB V jedoch nur (die im SGB V nicht definierten) Rechenzentren nutzen. Ob zur Abrechnung Apotheken auch Cloud-Computing-Dienste nutzen dürfen, ist aufgrund des Wortlauts von § 300 SGB V zumindest zweifelhaft.

§ 393 SGB V: Art der Daten – Beschäftigtendaten?

§ 393 SGB V regelt die Verarbeitung von Sozial- und Gesundheitsdaten. Sozialdaten werden mit Verweis auf § 67 Abs. 2 SGB X definiert; der Begriff „Gesundheitsdaten" findet europaweit eine einheitliche Bestimmung in Art. 4 Ziff. 15 DSGVO.

§ 393 Abs. 1 SGB V enthält keine Regelung zu Beschäftigtendaten und ebenfalls nicht zu biometrischen Daten im Sinne von Art. 4 Ziff. 14 DSGVO. Biometrische Daten werden sehr häufig zur Authentifizierung von Personen benutzt, auch bei Cloud-Dienstleistungen wird der Zugriff häufig über biometrische Identifikationsmechanismen abgesichert. Grundsätzlich wird man argumentieren können, dass kein informationstechnisches System zur Verarbeitung von personenbezogenen Daten genutzt werden darf, ohne dass Mechanismen existieren, die gewährleisten, dass nur berechtigte Personen auf die personenbezogenen Daten zugreifen können. Eine Verarbeitung von Beschäftigtendaten zur Erreichung dieses Zieles wird also implizit in einer Erlaubnis zur Nutzung von IT-Systemen enthalten sein, auch bei der Nutzung von Cloud-Computing-Diensten.

Gemäß Art. 9 Abs. 1 DSGVO ist die Verarbeitung von „biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person" grundsätzlich verboten. Im Kontext der Richtlinie (EU)

2016/680[13] urteilte der EuGH[14], dass nationales Recht, welches eine Verarbeitung biometrischer Daten erlaubt, hinsichtlich der für diese Erlaubnis geltenden Voraussetzungen keine Unklarheit enthalten darf. Eine implizite Herleitung der Erlaubnis zur Nutzung biometrischer Daten von Beschäftigten dürfte diesen Anforderungen nicht genügen. Inwieweit Betriebsvereinbarungen genutzt werden dürfen, ist auch fraglich: Betriebsvereinbarungen sind keine gesetzlichen Normen[15] im eigentlichen Sinne; zudem wird die erforderliche Transparenz fehlen (z. B. wird in Einstellungsverfahren nicht darauf hingewiesen, dass entsprechend geschützte Daten aufgrund bestehender Betriebsvereinbarungen verarbeitet werden). Die Regelung im BDSG bzgl. Betriebsvereinbarungen wirft aus Sicht des EU-Rechts weitere Fragen auf.[16]

§ 393 SGB V: Art der Daten – Genetische Daten?

Der Begriff „genetische Daten" wird in Art. 4 Ziff. 13 DSGVO definiert, nimmt jedoch keinen Bezug auf den in Art. 4 Ziff. 15 DSGVO definierten Begriff der Gesundheitsdaten: Genetische Daten gehören entsprechend den in der DSGVO enthaltenen Begriffsbestimmungen nicht zu den Gesundheitsdaten, somit erlaubt § 393 SGB V nicht die Verarbeitung genetischer Daten in der Cloud.

Leistungserbringer müssen bei der Nutzung von Cloud-Computing-Diensten also streng darauf achten, dass keine genetischen Daten verarbeitet werden; gemäß der Regelung des § 393 SGB V ist eine entsprechende Verarbeitung nicht statthaft.

§ 393 SGB V: Ort der Cloud-Verarbeitung

§ 393 Abs. 2 SGB V legt den Ort der Verarbeitung auf die EU oder Drittländer mit Angemessenheitsbeschluss fest. Aktuell besteht für die USA noch ein Angemessenheitsbeschluss, jedoch liegen dem EuGH schon wieder Vorgänge zur Prüfung vor. In der Vergangenheit urteilte der EuGH[17], dass das Bestehen wirksamer Rechtsbehelfe im betreffenden Drittland im Kontext einer Übermittlung personenbezogener Daten in dieses Drittland zwingend zu gewährleisten ist; die Rechtsbehelfe müssen nach der Rechtsprechung des EuGHs den in der Charta der Grundrechte verankerten Rechten und insbesondere mit Art. 47 der Charta der Grundrechte der Europäischen Union[18] gleichwertig sein. D. h., ein „durch Gesetz errichtetes Gericht" (eine Executive Order ist nach US-amerikanischem Recht kein Gesetz) muss die Angelegenheit in „einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandeln", was in den USA ebenfalls nicht gegeben ist. Die Wahrscheinlichkeit, dass der EuGH in einem dritten Verfahren den Angemessenheitsbeschluss entsprechend den ersten zwei Beschlüssen des EuGHs für ungültig erklären wird, ist also sehr hoch.

US-amerikanische Anbieter errichten derzeit europäische Rechenzentren, um „souveräne" Clouds anbieten zu können, d. h. die Verarbeitung soll nur in diesen Rechenzentren erfolgen. Nach US-amerikanischem Recht ist der Ort der Verarbeitung jedoch egal, US-amerikanische Behörden haben auch in Europa Zugriff auf die Rechenzentren US-amerikanischer Cloud-Anbieter. 2024 bewertete der Wissenschaftliche Dienst des Deutschen Bundestages die Herausgabepflichten von Daten und Informationen an US-amerikanische Sicherheitsbehörden.[19] Darin heißt es: „Bereits aus US-amerikanischer Perspektive ist schließlich der Speicherort der Daten durch das US-amerikanische Unternehmen für Herausgabeverpflichtungen irrelevant. Auch aus einer datenschutzrechtlichen Perspektive erscheint diese Maßnahme, Daten vor Zugriffen aus den USA zu schützen, indem sie innerhalb der EU auf Servern gespeichert werden, entsprechend fraglich." Gleichzeitig wird im Papier festgestellt, dass Herausgaben von Daten gegen europäisches Recht verstoßen. US-amerikanische Cloud-Anbieter müssen sich bei Herausgabeanforderungen letztlich entscheiden, ob sie gegen geltendes US-Recht oder gegen geltendes EU-Recht verstoßen.

Ob in Europa befindliche Rechenzentren US-amerikanischer Cloud-Anbieter und deren Zusicherung, dass Daten nur in Europa verarbeitet werden, den Anforderungen des EU-Rechts und der Auslegung dieses Rechts durch den EuGH genügt, ist zumindest fraglich; eine eindeutige Antwort erscheint zumindest zum heutigen Zeitpunkt nicht möglich. Klar ist: Ist ein Zugriff aus den USA möglich (kann also nicht ausgeschlossen werden) und wurde der aktuelle Angemessenheitsbeschluss für die USA durch den EuGH wieder einmal für ungültig erklärt, so ist die Vorgabe von § 393 Abs. 2 SGB V nicht länger erfüllt: eine Nutzung von entsprechenden Cloud-Computing-Diensten ist dann illegal; eine Legalisierung der Verarbeitung durch entsprechend Art. 46 Abs. 2 lit. c DSGVO erlassene Standarddatenschutzklauseln der EU-Kommission oder andere der in Kap. V DSGVO genannten Maßnahmen ist nach deutschem Recht nicht möglich.

Letztlich müssen sich für die Datenverarbeitung Verantwortliche i. S. d. Art. 4 Ziff. 7 DSGVO entscheiden, ob sie diese mit § 393 Abs. 2 SGB V verbundene Rechtsunsicherheit eingehen wollen oder nicht.

§ 393 SGB V: Sicherheit der Cloud-Verarbeitung

Gemäß § 393 Abs. 3 SGB V müssen drei additive Bedingungen bei einer Cloud-Datenverarbeitung erfüllt werden:

1. Es müssen dem Stand der Technik entsprechende angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit ergriffen worden sein.
2. Es muss ein aktuelles C5-Testat[20] der datenverarbeitenden Stelle im Hinblick auf die C5-Basiskriterien für die im Rahmen des Cloud-Computing-Dienstes eingesetzten Cloud-Systeme und die eingesetzte Technik vorliegen.
3. Die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden müssen umgesetzt sein.

§ 393 Abs. 3 Ziff. 2 SGB V verlangt, dass die „datenverarbeitende Stelle" ein C5-Testat vorlegt. EuGH-Generalanwalt M. Bobek verwandte den Begriff „datenverarbeitende Stelle" in seinem Schlussantrag[21] vom 13. Januar 2021 als Synonym für den Verantwortlichen; Auftragsverarbeiter wie Cloud-Anbieter wären demzufolge „im Auftrag datenver-

arbeitende Stellen". Leistungserbringer und Kranken- und Pflegekassen müssen dem Wortlaut zufolge also ein C5-Testat nachweisen, was diese aber allein schon aufgrund der im C5-Katalog enthaltenen Anforderungen nicht können.

Mit § 393 Abs. 3 Ziff. 3 SGB V wird der Auftraggeber, also der Cloud-Kunde, adressiert. Im C5-Kriterienkatalog finden sich 46[22] Anforderungen für Cloud-Kunden, d. h. Anforderungen, die Cloud-Kunden und nicht die Cloud-Anbieter erfüllen müssen. § 393 Abs. 3 Ziff. 3 SGB V verpflichtet Leistungserbringer und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsdatenverarbeiter bei Nutzung von Cloud-Computing-Diensten, aber die Regelungen sind leider alles andere als rechtssicher formuliert, die Befolgung der Norm wird daher für Rechtsanwender nicht einfach sein.

§ 384 Ziff. 6 SGB V definiert ein aktuelles C5-Testat als „das positive Prüfergebnis über einen sicheren Cloud-Computing-Dienst anhand des Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils gültigen Fassung". Dabei handelt es sich um das Testat eines Wirtschaftsprüfers. Im Gegensatz zu Zertifikaten, die regelhaft eine begrenzte Gültigkeitsdauer haben, endet die Gültigkeit eines entsprechenden Testates nicht. Ein Wirtschaftsprüfer testiert die Übereinstimmung von Vorgaben(„Soll-Zustand") mit dem Ist-Zustand zu einem bestimmten Zeitpunkt. Es werden also keine Prozesse oder Arbeitsabläufe und daraus sich ergebende Ergebnisse bewertet, sondern ausschließlich ein Soll-Ist-Abgleich zu genau einem Datum.

Hat eine Firma beispielsweise am 1. Mai 2021 ein entsprechendes Testat erhalten, so ist dieses Testat auch am 31. März 2024 noch gültig und ist – sofern kein neueres Testat vorliegt – das aktuelle Testat. Mit dem Begriff „aktuell" wollte der Gesetzgeber vermutlich eine zeitliche Nähe zum Zeitpunkt der Auftragserteilung erreichen, jedoch ist formal die Begriffsbestimmung in § 384 Ziff. 6 SGB V anzuwenden, eine zeitliche Nähe zum Zeitpunkt der Auftragserteilung ist zur Erfüllung der Bedingung von § 393 Abs. 3 Ziff. 2 SGB V nicht erforderlich.

Beim C5-Testat unterscheidet das BSI Typ-1- und Typ-2-Testate:[23]

- Berichterstattungen vom Typ 1: Der Auditor gibt ein Prüfungsurteil darüber ab, ob die Kontrollen zum Zeitpunkt der Prüfung angemessen ausgestaltet und eingerichtet sind, um die Kriterien des C5 mit hinreichender Sicherheit zu erfüllen (englisch: „suitability of the design").
- Berichterstattungen vom Typ 2: Das Prüfungsurteil umfasst, neben der Aussage zur Angemessenheit, eine Aussage über die Wirksamkeit der Kontrollen in einem Prüfungszeitraum (englisch: „operating effectiveness").

Ein Typ-1-Testat bescheinigt somit nicht, dass wirksame Maßnahmen zur Sicherheit der Verarbeitung ergriffen wurden, sondern lediglich, dass Maßnahmen, Verfahrens- und Arbeitsanweisungen existieren, welche eine Sicherheit umsetzen könnten. Erst bei einem Typ-2-Testat wird geprüft, ob vorhandene Controls auch umgesetzt wurden. Trotzdem reicht entsprechend § 393 Abs. 4 SGB V bis zum 30. Juni 2025 ein Typ-1-Testat aus. Erst ab dem 1. Juli 2025 muss ein Typ-2-Testat vorliegen.

Fazit

Das DigiG wirft – wie die meisten Gesetze des Bundesministeriums für Gesundheit der letzten sechs Jahre – mehr Fragen auf als es Antworten auf bestehende Herausforderungen bei der Versorgung der Bürger bringt.

Das Bundesministerium für Gesundheit verfolgt mit den aktuellen Gesetzen unzweifelhaft das Ziel Daten der Patientenversorgung möglichst vielen natürlichen und juristischen Personen zu möglichst vielen Zwecken zur Verfügung zu stellen. Im DigiG wird dies mit der Etablierung von Opt-out-Vorgaben in der ePA und daraus abgeleiteten automatisierten Übermittlungen an Plattformen, welche die (pseudonymisierten) Patientendaten jeder natürlichen und juristischen Person in der EU zu diversen Zwecken auch abseits von Zwecken der medizinischen Forschung zur Verfügung stellen, besonders deutlich.

Datenschutz und IT-Sicherheit haben in diesem Kontext offensichtlich für das Bundesministerium für Gesundheit nur eine untergeordnete Bedeutung, denn anders lässt sich nicht erklären, dass das DigiG die Einflussmöglichkeiten des BSI im Kontext der gematik und der Telematik-Infrastruktur massiv beschneidet.

Formal wird die IT-Sicherheit in der ambulanten und stationären Versorgung im SGB V festgeschrieben. Dabei besitzen Verantwortliche keine Einflussmöglichkeiten in Bezug auf gematik-Komponenten wie den Konnektor, der aufgrund gesetzlicher Vorgaben zwingend einzusetzen ist. Die gematik wiederum adressiert Themen von Datenschutz und IT-Sicherheit nur unzureichend.

Ob und welche Sicherheitsvorfälle aus diesen Umständen, insbesondere auch aus der Gesetzgebung, erwachsen, kann zum jetzigen Zeitpunkt niemand absehen. Entsprechend Art. 85 Abs. 3 DSGVO haftet ein Verantwortlicher nicht, wenn er nachweisen kann, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Kommt es aufgrund der Vorgaben der gematik zu Sicherheitsvorfällen, wodurch betroffene Personen einen Schaden erleiden, haften Leistungserbringer wie Krankenhäuser oder niedergelassene Arztpraxen nicht. Wie der EuGH schon mehrfach ausführte, kann ein Schadenersatzanspruch aufgrund nationaler Gesetzgebung nicht ins Leere laufen. D. h., ggf. muss die gematik haften – letztlich auch als Mehrheitseigner der gematik das Bundesministerium für Gesundheit.

1 Bundesgesetzblatt: Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG). Online, zitiert am 2024-03-29; verfügbar unter https://www.recht.bund.de/eli/bund/bgbl-1/2024/101

2 Oeter S, Münkler l.: Art. 74, Rn. 140. In: Huber/Voßkuhle (Hrsg.) Grundgesetz, Band 2. C. H. Beck Verlag, 8. Auflage 2024. ISBN 978-3-406-79230-4

3 Siehe
- Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung, Seite 3. Online, zitiert am 2024-03-29; verfügbar unter https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf
- Wissenschaftliche Dienste Deutscher Bundestag. (2019) Gesetzgebungskompetenzen im Bereich des Krankenhausrechts; Seite 3. Online, zitiert am

2024-03-29; verfügbar unter https://www.bundestag.de/resource/blob/648488/7920b181e85756ccdedff0334a18145b/WD-3-094-19-pdf-data.pdf

- Wollenschläger, Seite 16/17. Online, zitiert am 2024-03-29; verfügbar unter https://www.stmgp.bayern.de/wp-content/uploads/2023/04/gutachten_verfassungskonformitaet_krankenhausplanung.pdf

4 Wollenschläger F, Schmidl A. (2016) Kompetentielle Grundfragen des Krankenhausstrukturgesetzes: das neue Qualitätsziel in der Krankenhausplanung. GesR: 542-550 (545)

5 Halbe B, Orlowski U.: § 13 Krankenhausrecht, Rn. 19. In: Clausen/Schroeder-Printzen (Hrsg.) Münchener Anwaltshandbuch Medizinrecht. C. H. Beck Verlag, 3. Auflage 2020. ISBN: 978-3-406-72937-9

6 BverfG, Urt. v. 1991-02-07, Az. 2 BvL 24/84, Rn. 72. Online, zitiert am 2024-03-29; verfügbar unter https://dejure.org/1991,41, Volltext unter https://openjur.de/u/176784.html

7 Wissenschaftliche Dienste Deutscher Bundestag. (2022) Verfassungsrechtlicher Rahmen für die Regelung der stationären medizinischen Versorgung, Seite 4. Online, zitiert am 2024-03-29; verfügbar unter https://www.bundestag.de/resource/blob/899852/e48e78cfe536ee972862bab82b8618e9/WD-3-054-22-pdf-data.pdf

8 BVerfG, Urt. v. 1993-05-28, Az. 2 BvF 2/90, 2 BvF 4/90, 2 BvF 5/92. Online, zitiert am 2024-03-29; verfügbar unter https://dejure.org/1993,2

9 KBV: Richtlinie zur Datensicherheit der Praxis-IT. Online, zitiert am 2024-03-29; verfügbar unter https://www.kbv.de/html/it-sicherheit.php

10 DKG: Informationssicherheit im Krankenhaus – Branchenspezifischer Sicherheitsstandard (B3S). Online, zitiert am 2024-03-29; verfügbar unter https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/

11 So z.B.: heise online (2011) Elektronische Gesundheitskarte: Gematik legt Bericht zur Sicherheitslücke vor. Online, zitiert am 2024-03-29; verfügbar unter https://www.heise.de/news/Elektronische-Gesundheitskarte-Gematik-legt-Bericht-zur-Sicherheitsluecke-vor-1266836.html

12 Gemäß Art. 2 Nr. 6 i. V. mit Art. 9 Abs. 4 des Gesetzes v. 22.03.2024 (BGBl 2024 Nr. 101) wird § 393 neu gefasst mit Wirkung v. 01.07.2024.

13 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates. Online, zitiert am 2024-03-29; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016L0680

14 EuGH, Urt. v. 2023-01-26, Rechtssache C-205/21, Rn. 66, 67. Online, zitiert am 2024-03-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0205

15 Das BVerfG beschrieb im sog. Volkszählungsurteil die Voraussetzung einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss.

16 Zu § 26 Abs. 4 BDSG ist anzumerken, dass der BAG dem EuGH am 8. Februar 2023 Fragen vorlegte, die letztlich auch eine Bewertung der Zulässigkeit von Betriebsvereinbarungen als Erlaubnistatbestand zur Verarbeitung personenbezogener Daten beinhaltet.

- Vorlagefragen: https://curia.europa.eu/juris/document/document.jsf?text=&docid=273715&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

- Verfahrensdokumentation: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=C%2D65%2F23

17 EuGH, Urt. v. 2020-07-16, Rechtssache C 311/18, Leitsatz 2 sowie Rn. 65, 103-105, 128. Online, zitiert am 2024-03-29; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62018CJ0311

18 Art. 47 Charta der Grundrechte der Europäischen Union. Online, zitiert am 2024-03-29 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012P/TXT#d1e697-393-1

19 Wissenschaftliche Dienste des Deutschen Bundestages. (2024) WD 3 – Herausgabepflichten von Daten und Informationen an US-amerikanische Sicherheitsbehörden. Zu den Auswirkungen auf die Nutzung von Cloud-Diensten durch Behörden. Online, zitiert am 2024-03-29 https://www.bundestag.de/resource/blob/990440/baf5c0d018ff7cdbfc08edf0f4ce6e64/WD-3-105-23-pdf.pdf

20 Bundesamt für Sicherheit in der Informationstechnik: Kriterienkatalog Cloud Computing C5. Online, zitiert am 2024-03-29 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

21 Schlussanträge des Generalanwalts M. Bobek vom 13. Januar 2021. Facebook Ireland Limited u. a. gegen Gegevensbeschermingsautoriteit. Rn. 27. Online, zitiert am 2024-03-29 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62019CC0645&qid=1713263721605

22 Zusammenstellung siehe GMDS, KH-IT, bvitg: Kommentierung der EVB-IT Cloud (Stand: 23. Oktober 2023), Seite 61-67. Online, zitiert am 2024-03-29 https://gesundheitsdatenschutz.org/html/evb-it-cloud

23 Bundesamt für Sicherheit in der Informationstechnik: Informationen für Prüfer, Abschnitt „zugrundeliegende Prüfmethodik". Online, zitiert am 2024-03-29 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/Pruefer/Pruefer_node.html

Thilo Weichert

Gesundheitsdatennutzung ohne Datenschutz?

Lauterbach auf Spahns Spuren der Verfassungswidrigkeit

Am 26.03.2024 wurde das Gesundheitsdatennutzungsgesetz (GDNG) im Bundesgesetzblatt veröffentlicht und trat damit in Kraft. Das Gesetz soll die Nutzung von Daten aus der ärztlichen Behandlung und aus der Pflege für sekundäre Zwecke ermöglichen, etwa für die Forschung, aber auch für Qualitätssicherung, Produktentwicklung, politische oder wirtschaftliche Planung. Trotz des Hinweises von Daten- und Patientenschützern, dass die Regelungen gegen Verfassungs- und Europarecht verstoßen, wurde das Gesetz innerhalb eines halben Jahres ohne wesentliche Änderungen verabschiedet.

1. Einleitung

Die Sinnhaftigkeit, ja die Notwendigkeit der Auswertung personenbezogener Gesundheitsdaten zur Verbesserung der Gesundheitsversorgung ist seit Jahrzehnten offensichtlich. Die dafür nötigen rechtlichen Regeln wurden aber nicht angepasst: Das strafbewehrte Patientengeheimnis (§ 203 StGB) monopolisierte diese Daten beim Arzt. Die europäische Datenschutz-Grundverordnung (DSGVO) erklärt ein generelles Verarbeitungsverbot, das nur unter engen gesetzlich definierten Voraussetzungen aufgehoben werden kann (Art. 9 DSGVO). Die Forderung von Medizinforschenden und wohlmeinenden Datenschützern, Gesundheitsdaten für gemeinnützige Sekundärnutzungen bereit zu stellen, blieb von der deutschen Politik lange ungehört.

Erst mit der Anfang 2020 einsetzenden *Corona-Pandemie* erkannte die Politik, dass die Datenlage bei der medizinischen Forschung wie für die Krisenbewältigung – faktisch wie rechtlich – ungenügend war. Politik und Medizin sahen sich gehindert, schnell adäquat zu reagieren. Während Israel oder Großbritannien einen fast tagesaktuellen Überblick über das dortige Pandemiegeschehen hatten, konnte bei uns die Epidemiologie zumeist nur mit Spekulationen sowie ad-hoc entstandenen Einzelstudien aufwarten.[1]

Der *rot-grün-gelbe Koalitionsvertrag* 2021 kündigte an die Gesundheitsdatennutzung zu verbessern: „Den Zugang zu Forschungsdaten für öffentliche und private Forschung wollen wir mit einem Forschungsdatengesetz umfassend verbessern. […] Zudem bringen wir ein Registergesetz und ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf."[2]

Parallel entwickelte die EU-Kommission eine Digitalstrategie. Deren primäres Ziel ist es, das Abhängen Europas von den USA und China im globalen Digitalisierungswettbewerb zu verhindern. Corona führte nun dazu, dass ein Europäischer Gesundheitsdatenraum dabei auf der Prioritätenliste nach vorne rückte. Die EU-Kommission präsentierte im Mai 2022 einen Gesetzgebungsvorschlag.[3] Zu diesem *European Health Data Space* (EHDS) einigten sich die EU-Gesetzgebungsorgane am 14.03.2024 im Trilog noch vor der EU-Parlamentswahl am 09.06.2024.[4]

Die Gesetzesinitiativen laufen auf einen *Paradigmenwechsel* hinaus: Das insbesondere in Deutschland hoch geschätzte Patientengeheimnis wird zugunsten einer umfassenden Möglichkeit, Gesundheitsdaten im öffentlichen Interesse nutz- und auswertbar zu machen, gelockert. Das Patientengeheimnis, also die berufliche Schweigepflicht der Heilberufe, soll dabei in seiner Substanz nicht angetastet werden: Zielsetzung dieses Patientengeheimnisses ist die Wahrung des allgemeinen Persönlichkeitsrechts in einem hochsensitiven und diskriminierungsträchtigen Bereich sowie der Schutz der Vertrauensbeziehung zwischen Arzt und Patient im Interesse eines umfassenden Austauschs und einer bestmöglichen medizinischen Behandlung.

Anfang Juni 2023 wurde ein erster Referentenentwurf eines *Gesundheitsdatennutzungsgesetzes* (GDNG) vorgelegt.[5] Mit Datum vom 08.09.2023 brachte die Bundesregierung den Entwurf überarbeitet in den Bundesrat ein.[6] Bei der Anhörung zum Entwurf am 15.11.2023 wurden offiziell 25 fast durchgängig lobbyinteressierte Stellungnahmen eingeholt. Nur eine, die des Bundesdatenschutzbeauftragten, befasste sich spezifisch mit dem Datenschutz.[7] Am 14.12.2023 verabschiedete der Bundestag das Gesetz in dritter Lesung weitgehend unverändert. Am 02.02.2024 bestätigte der Bundesrat das Gesetz.[8] Am 26.03.2023 trat das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten" mit dem GDNG sowie einigen Änderungen insbesondere im Sozialgesetzbuch (SGB) V in Kraft.[9] Der Gesetzgeber hatte es plötzlich ganz eilig. An dabei auftretenden wesentlichen verfassungsrechtlichen Fragen zeigte er kein Interesse. Diese Fragen stellten sich schon beim Digitale-Versorgung-Gesetz (DVG) von 2019 unter der vorherigen schwarz-roten Bundesregierung und dem damaligen Gesundheitsminister *Jens Spahn*.[10] Eine Verfassungsbeschwerde hiergegen wurde – aus formellen Gründen – zurückgewiesen, wobei das BVerfG bestätigte, dass die Beschwerde wichtige Fragen aufwirft. Eine Klage beim SG Berlin, die die Fragen thematisiert, ist weiterhin anhängig (s.u. 2.3.). Das nun in Kraft getretene Gesetz knüpft an das DVG an, ohne aber die schon dort aufgetretenen Fragen befriedigend zu beantworten.

2. Rahmenbedingungen

Das GDNG und die ergänzenden Regelungen des SGB V zielen darauf ab den individuellen wie den gesamtgesellschaftlichen *Gesundheitsschutz mit dem Datenschutz* in Einklang zu bringen. Dabei sind die Rahmenbedingungen des Europa- und des Verfassungsrechts,

aber auch weitere einfache Gesetze und die faktischen Gegebenheiten zu beachten.

2.1. Gesetzgebungskompetenz

Für die Gesetzgebung zur Sekundärnutzung von Gesundheitsdaten sind in Deutschland teilweise die Länder, teilweise der Bund zuständig: Der Bund erlässt Gesetze zur *„Sozialversicherung"* (Art. 74 Nr. 12 GG) insbesondere in den Sozialgesetzbüchern (SGB). Die Bundespolitik nutzt das SGB V mit seinen Regeln zur gesetzlichen Krankenversicherung (GKV), um die Digitalisierung im Gesundheitswesen generell voranzubringen. Mit dem DVG wurde das Forschungsdatenzentrum (FDZ) in den §§ 303a ff. SGB V geregelt, worüber sämtliche GKV-Abrechnungsdaten sowie die Daten der elektronischen Patientenakte (ePA, § 363 Abs. 2 SGB V) in pseudonymisierter Form für Sekundärzwecke zur Verfügung gestellt werden. Die vereinheitlichende Koordinierung der Datenschutzaufsicht bei länderübergreifenden Forschungsprojekten war von 2020 bis 2024 in § 287a SGB V-alt vorgesehen (jetzt § 5 GDNG). Das SGB V gilt für die Datenverarbeitung der 74,31 Mio. gesetzlich Versicherten, nicht für die der 8,7 Mio. privat Versicherten (2023). Für diese besteht bei Behandlung durch nicht-öffentliche Leistungserbringer im „Recht der Wirtschaft" (Art. 74 Nr. 11 GG) eine weitere Bundeszuständigkeit.

Die Länder sind aber für die wichtigen Bereiche der Universitätskliniken, der kommunalen Krankenhäuser, des öffentlichen Gesundheitswesens und für vieles mehr zuständig (Art. 70 Abs. 1 GG). Eine über die *„Förderung der wissenschaftlichen Forschung"* (Art. 74 Nr. 13 GG) begründete Bundeszuständigkeit[11] ist konstruiert und erfasst allenfalls die in Art. 5 Abs. 3 GG geschützte Forschung, aber nicht sonstige im GDNG geregelten Sekundärnutzungen, etwa zu Gesundheitsplanungen oder zur personalisierten Medizin. Der Gesetzentwurf beruft sich zum Teil auf Art. 74 Abs. 1 Nr. 19 GG, der dem Bund erlaubt „Maßnahmen gegen gemeingefährliche oder übertragbare Krankheiten" zu regeln. Damit wird nur ein kleiner weiterer Regelungsbereich des GDNG erfasst. Das GDNG soll aber sämtliche Sekundärnutzungen von Gesundheitsdaten regeln, nicht nur die in Bundeskompetenz normierten.[12] Versuche, hierfür das Grundgesetz zu ändern oder gemeinsame Regelungen für Bund und Länder zu erlassen, sind bisher unterblieben.

Das Problem der föderalen Kompetenzordnung des Grundgesetzes kann durch *verbindliche europäische Regelungen*, die Bund wie Länder binden (Art. 288 Abs. 2 AEUV), umgangen werden. Für das Gesundheitswesen hat die EU zwar nur eine die Politik der Mitgliedstaaten ergänzende Funktion (Art. 168 Abs. 1 AEUV). Die EU-Zuständigkeit für den EHDS begründen die EU-Gremien mit ihren Kompetenzen für den Binnenmarkt (Art. 114 AEUV) und für den Datenschutz (Art. 16 Abs.2 AEUV).[13]

Bis zum materiell-rechtlichen Wirksamwerden des EHDS gelten die Regelungen des GDNG uneingeschränkt, so dass die deutschen Kompetenzverwicklungen für eine gewisse Zeit bestehen bleiben. Die Länder, die oft ihre Landeszuständigkeiten mit Zähnen und Klauen verteidigen, haben diese hier im Bundesratsverfahren nicht einmal thematisiert.

2.2 Europa und Deutschland

Die Sekundärnutzung von Gesundheitsdaten wird neben dem nationalen GDNG parallel im europäischen EHDS geregelt sein, der zwei Jahre nach der Veröffentlichung im EU-Amtsblatt, also voraussichtlich im Frühjahr 2026, in Kraft treten wird (Art. 72 EHDS-E). Damit werden zumindest mittelfristig die deutschen kompetenzrechtlichen Probleme hinsichtlich der materiellen Regelungen gelöst. Europäisches Recht geht nationalem Recht vor, egal ob es sich um Verfassungs-, Bundes- oder Landesrecht handelt (Art. 288 AEUV). Keine nationale Regelungsbefugnis besteht bei abschließenden EU-Regelungen. Soweit im EU-Recht sog. Öffnungsklauseln bestehen, sind nationalstaatliche Spezifizierungen möglich oder sogar nötig. Deren Umsetzung hat dann gemäß den gesplitteten Gesetzgebungskompetenzen zu erfolgen (s.o. 2.1.). Viele Regelungen des GDNG, insbesondere soweit es dabei um nationale Prozeduren und Zuständigkeiten geht, werden Gültigkeit behalten.

2.3 *Spahns* Erbe

Das GDNG hat weitgehend das bisher in Deutschland geltende Regelwerk und die bestehenden Datenverarbeitungsstrukturen übernommen. Diese sind rechtlich angreifbar und teilweise wenig praktikabel. Derzeit wird im Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), einer dem Bundesgesundheitsministerium (BMG) nachgeordneten Behörde, das in den §§ 303a ff. SGB V geregelte *Forschungsdatenzentrum* (FDZ) aufgebaut. Das FDZ hat auch 4 Jahre nach Inkrafttreten des DVG seine Tätigkeit noch nicht aufgenommen. Die Bereitstellung der FDZ-Daten für Sekundärzwecke soll im Laufe des Jahres 2024 erfolgen, nachdem ein IT-Sicherheitskonzept erstellt und umgesetzt worden ist.[14] Im FDZ werden zunächst die GKV-Abrechnungsdaten in pseudonymisierter Form zusammengeführt und sollen für Sekundärnutzungen generell – nicht nur für die Forschung – bereitgestellt werden. Künftig sollen auch die pseudonymisierten elektronischen Patientenakten (ePAs) – jedoch nicht für Sekundärnutzung generell, sondern nur für Forschungszwecke – verfügbar sein (§ 363 SGB V). Geplant ist nun die Verknüpfung der FDZ-Daten mit Daten aus Krankheitsregistern, etwa den Krebsregistern (§ 4 GDNG), sowie mit weiteren Datenquellen.

Gegen eine solche Zentralstellenfunktion wäre grundsätzlich nichts einzuwenden, würden die Regeln und das gewählte Verfahren den datenschutzrechtlichen Mindestanforderungen genügen. Gemäß Art. 9 Abs. 2 lit. i u. j DSGVO müssen „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" geregelt und umgesetzt sein. Im Bereich der Gesundheitsversorgung müssen die Datenempfänger einem Berufsgeheimnis unterliegen (Art. 9 Abs. 2 lit. h i.V.m. Abs. 3 DSGVO). Nach europäischem und nationalem Verfassungsrecht dürfen Sekundärnutzungen nur „unter Wahrung des Grundsatzes der Verhältnismäßigkeit" vorgenommen werden; sie müssen notwendig sein und „dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen" (Art. 52 Abs. 1 S. 2 GRCh).

Schon im Spahn-Gesetz, dem DVG, sollten die Daten des FDZ nicht nur unabhängig Forschenden zur Verfügung gestellt werden, sondern auch und unter den gleichen rechtlichen Voraussetzungen zur Erreichung weiterer Zwecke, z.B. „Planung von Leistungsressourcen", „Unterstützung politischer Entscheidungsprozesse" oder „Analyse und Entwicklung von sektorenübergreifender Versorgungsformen sowie von Einzelverträgen der Krankenkassen" (§ 303e Abs. 1 u. 2 SGB V). Die Entscheidung über die Datenbereitstellung soll in einem weitgehend intransparenten Verfahren durch Mitarbeiter des direkt dem BMG unterstellten BfArM erfolgen. Betroffenenrechte, also ein Anspruch auf Auskunft, auf Widerspruch, auf Berichtigung oder Löschung, sind nicht vorgesehen und mangels eines Verfahrens (wegen der pseudonymisierten Verarbeitung) auch praktisch derzeit nicht umsetzbar. Die geltenden Regelungen zum FDZ sind offensichtlich verfassungswidrig.[15] In einem einstweiligen Rechtsschutzverfahren hat das BVerfG den sofortigen Antrag auf Schutz vor der DVG-Anwendung zurückgewiesen, zugleich aber darauf hingewiesen, dass „gewichtige Bedenken" gegen die angegriffenen Vorschriften bestehen, die „komplexe Fragen der verfassungsrechtlichen Datenschutzdogmatik" aufwerfen und aufgrund der Komplexität näherer Aufklärung bedürfen, die nicht in der für das Eilverfahren gebotenen Kürze der Zeit behandelt werden können.[16] Gemäß dem BVerfG liegt in den vorgesehenen Datenverarbeitungs- und Übermittlungsmaßnahmen „vor allem in Anbetracht des teils sensiblen und in hohem Maße persönlichkeitsrelevanten Charakters der genutzten Daten und der dabei breitflächigen Erhebung ein erheblicher Grundrechtseingriff", der verstärkt wird durch „die beträchtliche Menge an Daten".[17] Weitere Gerichtsverfahren, welche die Rechtmäßigkeit des FDZ-Verfahrens in Frage stellen, sind anhängig.[18]

3. Das Gesetz

Mit dem GDNG sollen bürokratische und organisatorische Hürden bei der Datennutzung abgebaut und die Nutzbarkeit von Gesundheitsdaten im Sinne eines die Datennutzung ‚ermöglichenden Datenschutzes' verbessert werden", indem „ein angemessener Ausgleich zwischen dem Schutz von Leben und Gesundheit, der Privatsphäre des Einzelnen sowie dem Recht auf informationelle Selbstbestimmung hergestellt" wird.[19]

Als zentrale Datenschutzgarantie wird die Einführung einer Strafnorm für Forschende bei Verletzung der Geheimhaltungspflicht aufgeführt. Eine im ersten Referentenentwurf noch vorgesehene „Einführung eines Zeugnisverweigerungsrechts für mit Gesundheitsdaten Forschende und eines Beschlagnahmeverbots"[20] schaffte es nicht mehr in den zweiten Referentenentwurf und auch nicht ins Gesetz. Konkrete Festlegungen, wie das bisherige, offensichtlich verfassungswidrige Gesetz verfassungskonform gemacht werden kann, finden sich nicht.

Das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten" ist ein Artikelgesetz mit dem GDNG mit 9 Paragrafen als Kernregelung. Weiterhin geändert werden das Gesetz über Nachfolgeeinrichtungen des Bundesgesundheitsamtes, das SGB V mit Modifikationen zum FDZ sowie das SGB X und das SGB XI.

Als Fremdköper in dem Gesetz ist in einem § 25b SGB V (im Referentenentwurf noch § 257a SGB V-E) vorgesehen, dass die Kranken- und Pflegekassen datengestützte Auswertung der dort vorliegenden Daten durchführen und die Versicherten „auf die Ergebnisse dieser Auswertung hinweisen" dürfen. Diese Regelung wurde trotz des massiven Protests von Ärztevertretungen, Daten- und Verbraucherschützern Gesetz.[21]

3.1 Das Organisationsmodell

Gemäß § 3 Abs. 1 GDNG wird beim BfArM eine „Datenzugangs- und Koordinierungsstelle für Gesundheitsdaten" (DZKG) eingerichtet, die Informationen bereithält, die berät und unterstützt, Anträge auf Zugang zu Gesundheitsdaten entgegennimmt und „an die datenhaltenden und den zuständigen Stellen" übermittelt, Anträge zur Verknüpfung von FDZ-Daten mit Krebsregistern genehmigt und Konzepte „zur Nutzung von sicheren Nutzungsumgebungen" erstellt ebenso wie Konzepte „zur Weiterentwicklung der zentralen Datenzugangs- und Koordinierungsstelle … als eigenständige Institution" (§ 3 Abs. 2 GDNG).

Ganz offensichtlich soll aus der DZKG die in Art. 36 EHDS-E vorgesehene zentrale nationale „Zugangsstelle für Gesundheitsdaten" werden, die mit Vertretern der Interessenträger zusammenarbeiten soll, „insbesondere mit Vertretern von Patienten, Dateninhabern und Datennutzern", und deren Personal Interessenkonflikte zu vermeiden hat (Art. 36 Abs. 3, 3a EHDS-E).

Schon hier ist erkennbar, dass das GDNG ein „Gesetz in Entwicklung" ist, nur ein erster Schritt zu einer umfassenderen Sekundärnutzung sein soll. Die DZKG soll zunächst nur für die Verknüpfung von Krebsregister und FDZ zuständig sein. Sie muss angesichts der EHDS-Vorgaben – auch gesetzlich – weiterentwickelt werden. Für die Weiterentwicklung bedarf es einer Gesetzesnovelle.

Wenig konsistent sind bisher die Planungen des BMG bzgl. des Zugangsverfahrens zu Gesundheitsdaten. Bisher sieht § 303d Abs. 1 SGB V das auch beim BfArM angesiedelte FDZ zugleich auch als Zugangsstelle zu den FDZ-Daten vor, die den Datenzugang nicht nur genehmigt, sondern auch selbst durchführt. Weitere Irritationen löste das BMG aus, als es mit Stand 17.01.2024 einen ersten Referentenentwurf eines „Medizinforschungsgesetzes" vorlegte, gemäß dem die Genehmigung des Datenzugangs für die Arzneimittel- und Medizinprodukteprüfungen bei einer erst noch beim BfArM einzurichtenden Bundes-Ethik-Kommission oder bei den schon auf Landesebene existierenden Ethik-Kommissionen liegen soll.[22]

Die Weiterentwicklung der DZKG ist dringend nötig. Die Ansiedelung der DZKG bei einer dem BMG nachgeordneten Behörde gewährleistet nicht deren unabhängige Entscheidung, zumal das BMG zu den Datenempfängern für Sekundärdatennutzungen gehört und hinsichtlich aller Zugangsgenehmigungen eigene Interessen im Spiel hat.[23] Was der bisherigen DZKG fehlt, ist neben der Unabhängigkeit die für die Aufgaben vom EHDS geforderte Fachkompetenz[24], wozu gesetzlich bisher nichts zu finden ist. § 303d Abs. 2 S. 1 SGB V sieht einen beratenden „Arbeitskreis zur Sekundär-

nutzung von Gesundheitsdaten“ vor, in dem GKV-Selbstverwaltungsverbände, Forschungseinrichtungen, Bundes- und Landesbehörden und Patientenorganisationen vertreten sein sollen.

Es ist unerfindlich, weshalb das BMG für die Datenzugangsgenehmigung nicht die „use-and-access-Committees“ etabliert, die im Rahmen der vom Bund finanzierten Medizininformatikinitiative etabliert wurden.[25]

3.2 Sekundärnutzungszwecke

Äußerst unbestimmt ist der Gesetzeszweck des GDNG, wonach die „Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens als lernendes System“ dienen soll (§ 1 Abs. 1 u. 2 GDNG). Was alles unter das „Gemeinwohl“ fällt, wird künftig hoch umstritten sein. Jede Stelle, die fremde Gesundheitsdaten nutzt, wird dieses für sich in Anspruch nehmen, selbst wenn die Hauptmotive profane eigene wirtschaftliche Interessen sind.[26] Selbst solche Interessen lassen sich als im Gesamtwirtschaftsinteresse liegend verbrämen. Da es insofern keine klaren Festlegungen geben kann, muss über die Unabhängigkeit der Genehmigungsbehörde, die Transparenz des Genehmigungsverfahrens, Betroffenenrechte, die Rechtskontrolle einer Aufsicht sowie der Gerichte gewährleistet sein, dass allein der Altruismus für das Datenzugangsrecht bestimmend ist.

Weitere Präzisierungen der Gemeinwohlzwecke nimmt das GDNG nicht vor. Lediglich hinsichtlich der Weiterverarbeitung von Versorgungsdaten durch die primär die Daten nutzenden Stellen selbst werden in § 6 Abs. 1 GDNG Zwecke genannt: Qualitätssicherung, Förderung der Patientensicherheit, medizinische, rehabilitative und pflegerische Forschung und Statistik einschließlich Gesundheitsberichterstattung. Da insofern die Daten in der die Daten haltenden Stelle bleiben, sind diese Zwecke relativ unproblematisch. Hinsichtlich einer Datenweitergabe für diese Zwecke verweist § 6 Abs. 3 GDNG auf sonstige Bundes- oder Landesgesetze.

Die Zurückhaltung des GDNG bzgl. der mit dem Gesetz im Vordergrund stehenden Sekundärnutzung durch Dritte erklärt sich wohl aus der Vorläufigkeit des Gesetzes. Die verfolgbaren konkreten Zwecke werden bisher hinsichtlich der Nutzung der FDZ-Daten in § 303e Abs. 2 SGB V normiert, der erweitert wurde: Steuerung durch die Kollektivvertragspartner, Qualitätssicherung und -verbesserung, Planung von Leistungsressourcen, wissenschaftliche Forschung, Unterstützung politischer Entscheidungsprozesse, Wirksamkeitsanalysen, Gesundheitsberichterstattung, gesetzliche Aufgabenwahrnehmung im Gesundheitsbereich, Nutzenbewertung, Entwicklung, Weiterentwicklung und Überwachung der Sicherheit von Arzneimitteln, Medizinprodukten und Behandlungsmethoden. Diese Zwecke sind schon uferlos. Sie sind aber gegenüber Art. 34 Abs. 1 EHDS-E noch nicht uferlos genug. Hier ist die Rede in Bezug auf Gesundheit und Pflege allgemein von Tätigkeiten aus Gründen des öffentlichen Interesses, der Unterstützung öffentlicher Stellen, „Bildungs- oder Lehrtätigkeiten im Gesundheits- und Pflegesektor“, „Training, Erprobung und Bewertung von Algorithmen“, auch von KI-Systemen, und der personalisierten Gesundheitsversorgung.

3.3 Datenempfänger

In § 303e Abs. 1 SGB V-alt gemäß dem DVG wurde noch eine Liste mit 18 Stellen aufgeführt, die Daten beim FDZ beziehen können sollten und jeweils einen Bezug zur Auswertung von GKV-Daten haben. Nun heißt es dort in Satz 2: „Nutzungsberechtigt sind natürliche und juristische Personen im Anwendungsbereich der Verordnung (EU) 2016/679, soweit diese nach Absatz 2 zur Verarbeitung der Daten berechtigt sind“. Anders gesagt: Jeder ist berechtigt, wenn er für die Datennutzung nur einen guten Zweck benennt. Dies geht zu weit.[27] Gegen einen weiten Empfängerkreises wäre weniger einzuwenden, wenn äußerst akribisch kontrolliert würde, ob die Zwecke berechtigt, die geplante Verarbeitung vertrauenswürdig und das Verfahren transparent und kontrolliert ist. Zusätzlich sollten aber an die Vertrauenswürdigkeit, Ausbildung und Qualifikation der Datenempfänger hinsichtlich der Auswertungskompetenz sowohl in fachlicher als auch in technischer Hinsicht hohe Anforderungen gestellt werden.

3.4 Pilot: Krebsforschung

§ 4 GDNG erlaubt für Forschungsvorhaben die Verknüpfung und Verarbeitung pseudonymisierter Daten des FDZ mit *Krebsregistern*. Die Genehmigung hierfür erfolgt durch die DZKG, sofern „schutzwürdige Interessen der betroffenen Personen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse überwiegt“ und die Risiken für die Betroffenen angemessen minimiert worden sind. Die Daten werden der Forschungseinrichtung in einer „sicheren Verarbeitungsumgebung einer öffentlich-rechtlichen Stelle verknüpft und den Antragstellenden als pseudonymisierte Einzeldatensätze, ohne Sichtbarmachung von Pseudonymen, verfügbar gemacht“ (§ 4 Abs. 5 S. 1 GDNG). Die Einzelheiten regelt das BMG in einer Rechtsverordnung (§ 4 Abs. 9 GDNG).

3.5 Geheimhaltungspflichten

§ 7 GDNG regelt, etwas verklausuliert, ein „Forschungsgeheimnis“, indem es eine strenge Zweckbindung und ein Weitergabe- und ein Re-Identifizierungsverbot statuiert, das aber durch sonstige Gesetze relativiert sein kann. Ähnlich wie § 203 Abs. 3 u. 4 StGB ist eine Einbindung von (internen) „Gehilfen“ und (externen) „Mitwirkenden“ erlaubt. § 9 GDNG erklärt einen Verstoß gegen § 7 GDNG zur Straftat, wobei – ebenso wie § 203 StGB – auch hier die Strafbarkeit von einem Strafantrag abhängig ist (§§ 205, 77 StGB).

Datenschützer verlangen seit Jahrzehnten die Einführung eines *Forschungsgeheimnisses*, mit dem das Vertrauen in die Forschenden bei Bereitstellung von Daten für wissenschaftliche Zwecke geschützt wird.[28] Ein solches Geheimnis, mit dem eine Geheimhaltungspflicht einhergeht, wird zumindest für Gesundheitsdaten nicht umfassend eingeführt. Dieser Ansatz ist zu eng. Es sind nicht nur Forschungsprojekte im Gesundheitsbereich, die auf vertrauliche Quellen angewiesen sind und an denen ein hohes öffentliches Interesse besteht.

Während im Datenschutzrecht zumindest noch ein Strafantragsrecht der Datenschutzaufsicht vorgesehen ist (§ 42 Abs. 3 BDSG), gilt dies für den ebenso öffentliche Interessen schützenden § 203 StGB und jetzt den § 9 GDNG nicht. Dieser Anachronismus ist bei Verletzung des Forschungsgeheimnisses besonders heikel, bei dem regelmäßig kein Bagatellbereich betroffen ist; es geht zumeist um große sensitive Datenmengen. Betroffene erlangen von Verstößen zumeist keine Kenntnis, so dass sie auch keinen Strafantrag stellen können.

Der Gesetzgeber unterlässt zudem den zweiten nötigen rechtlichen Schritt, indem er das Forschungsgeheimnis strafprozessual nicht durch ein Zeugnisverweigerungsrecht und ein Beschlagnahmeverbot flankiert.[29] Ein solcher Schutz ist verfassungsrechtlich geboten.[30] Weshalb dieser im ersten Referentenentwurf noch vorgesehene Schutz sang- und klanglos fallengelassen wurde und auch nicht im Entwurf eines Medizinforschungsgesetzes enthalten ist, ist nicht verständlich.

3.6 „Sichere Verarbeitungsumgebung"

Bisher ist in § 303e Abs. 4 S. 2 SGB V vorgesehen, dass die Nutzung von pseudonymen FDZ-Einzeldatensätzen „ohne Sichtbarmachung der Pseudonyme für die Bearbeitung unter Kontrolle des Forschungsdatenzentrums" bereitgestellt wird. D.h. die Datenverarbeitung muss unter der technischen Aufsicht des FDZ erfolgen; ein Datenexport ist nicht vorgesehen, selbst wenn eine Kombination mit weiteren Datensätzen für das Projekt nötig ist. Hierin liegt eine starke Einschränkung der wissenschaftlichen Nutzbarkeit der Daten. Um diese Behinderung etwas zu mildern, sieht nun ein neuer § 303 Abs. 4a SGB V vor, dass weiterhin unter FDZ-Kontrolle eine Verknüpfungserlaubnis mit „gesetzlich geregelten medizinischen Registern, die unter Bundesverwaltung stehen," erlaubt wird.

Einen Schritt weiter geht die Verknüpfungsmöglichkeit des FDZ mit Krebsregisterdaten, indem die Verknüpfung in einer „sicheren Verarbeitungsumgebung einer öffentlichen Stelle" erlaubt wird (§ 4 Abs. 5 S. 1 GDNG). Die DKZG soll Konzepte „zur Nutzung von sicheren Verarbeitungsumgebungen als Maßnahme zur Verbesserung des Datenschutzes und der Datensicherheit" erstellen (§ 3 Abs. 2 Nr. 9a GDNG). In § 4 Abs. 9 S. 2 GDNG ist geregelt, dass das Bundesamt für die Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bei der Festlegung der Anforderungen an die sichere Verarbeitungsumgebung durch eine Verordnung des BMG zu beteiligen sind.

Sämtliche Regelungen zur Informationstechnik haben gemein, dass sie äußerst unbestimmt sind und zugleich die Verknüpfung mit externen Forschungsdatenbeständen verhindern, was eine massive Behinderung für die Wissenschaftler zur Folge hat.[31] Sie sind der unbedarfte Versuch einer Selbstvergewisserung von Sicherheit, die in öffentlichen Umgebungen nicht besser und nicht schlechter hergestellt werden kann als unter nicht-öffentlicher Ägide. Konkrete Sicherheitsgarantien wären durch Zertifikate möglich (vgl. Art. 42 DSGVO).[32]

3.7 Verfahrenstransparenz

Wenig vertrauenerweckend ist bisher die bei den Zugangsgenehmigungen vorgesehene Transparenz. In § 303d Abs. 1 Nr. 6 SGB V ist „ein öffentliches Antragsregister mit Informationen zu den antragstellenden Nutzungsberechtigten, zu den Vorhaben, für die Daten beantragt wurden, und deren Ergebnissen" geplant. Dieses Antragsregister bezieht sich (nur) auf die Bereitstellung von FDZ-Daten. Wie konkret diese Datentransparenz sein soll, ist bisher mangels Präzisierung und Umsetzung nicht bekannt. § 8 GDNG enthält nun eine generelle Regelung, die auch zu einer Registrierung in einem Forschungsregister verpflichtet. Ergänzend ist vorgesehen, dass die Forschungsergebnisse innerhalb von 24 Monaten nach Forschungsabschluss in einer allgemein zugänglichen Weise veröffentlicht werden müssen. Eine solche Publikation ist bei Datenbeschaffung auf gesetzlicher Grundlage verfassungsrechtlich geboten.[33] § 8 S. 3 GDNG erlaubt den Verzicht auf eine Registrierung, wenn die Forschung im Auftrag oder unter Rechts- oder Fachaufsicht einer Behörde erfolgt und die Veröffentlichung „besondere öffentliche Belange" beeinträchtigen würde (vgl. § 3 IFG Bund).

Die Transparenzpflicht besteht nur, wenn die Verarbeitung im Forschungsvorhaben auf gesetzlicher Grundlage ohne die Einwilligung der Betroffenen erfolgt. Der Ausschluss von einwilligungsbasierten Projekten lässt sich schwerlich rechtfertigen. Dies gilt besonders, solange statt auf gesetzliche Grundlagen auf den sog. „broad consent" gesetzt wird, der den Anforderungen des Art. 7 DSGVO nicht genügt, die Betroffenen weitestgehend im Unklaren über die weitere Nutzung lässt und der derzeit als Königsweg für die medizinische Forschung genutzt wird.[34] Auch im Fall einer Einwilligung haben Betroffene keinerlei Kontrolle mehr über das, was mit ihren Daten geschieht. Eine nachträgliche Kontrolle wird so unmöglich gemacht.

Ein klassischer verfassungsrechtlicher Ansatz bei der Zulassung von informationellen Eingriffen in Grundrechte besteht darin die Berechtigten zu spezifischer Transparenz zu verpflichten.[35] Eine in § 8 GDNG angelegte nachträgliche Prüfmöglichkeit macht erfolgte informationelle Eingriffe nicht ungeschehen. Transparenzpflichten müssen früher, nämlich beim Antragsprozess, ansetzen und sie müssen zumindest die interessierte Fachöffentlichkeit, wenn möglich auch die potenziell Betroffenen, befähigen eine kritische Hinterfragung bei der Antragstellung bis hin zum Projektabschluss vorzunehmen. Nur so kann rechtzeitig interveniert werden, können Betroffene ihr – bisher weitgehend nicht bestehendes – Widerspruchsrecht wahrnehmen. Transparenz bei der Digitalisierung kommt in der öffentlichen Verwaltung generell zu kurz. Will man aber, wie beim GDNG, massenhaft Eingriffe in den sensitiven Bereich von Gesundheitsdaten ermöglichen, dann sind kompensatorische Transparenzmaßnahmen verfassungsrechtliche Pflicht, welche das GDNG ignoriert.

Als Minimalstandard für Transparenz gegenüber den Betroffenen gelten die Art. 12 ff. DSGVO. Die Regelung des § 6 Abs. 4 GDNG nimmt darauf Bezug, bleibt aber inhaltlich dahinter zurück. Um insofern eine Europarechtswidrigkeit der

Praxis zu verhindern, muss die GDNG-Regelung unter Hinzuziehung der DSGVO so ausgelegt werden, dass die Information auch konkret patientenbezogen erfolgt.[36]

3.8 Betroffenenrechte

Schon im DVG waren in den Regelungen zum FDZ keinerlei Betroffenenrechte vorgesehen, was als verfassungswidrig kritisiert wurde.[37] Angesichts des Umstands, dass die Betroffenenrechte in Art. 8 Abs. 2 S. 2 GRCh Grundrechtsschutz genießen, wäre zu erwarten gewesen, dass das schwarz-rote Versäumnis durch Rot-Grün-Gelb behoben würde. Doch auch im neuen Gesetz werden weder im GDNG noch durch Änderungen des SGB V Betroffenenrechte verankert.

Lediglich hinsichtlich der Nutzung der Daten aus den elektronischen Patientenakten (ePA), die für Forschungszwecke pseudonymisiert in das FDZ übertragen werden, ist in § 363 Abs. 5 SGB V ein Widerspruchsrecht vorgesehen. Für Betroffene besteht also zum einen das Recht eines Widerspruchs gegen die Einrichtung einer ePA wie auch ein Widerspruchsrecht einer Forschungsnutzung im Fall des Bestehens einer ePA.[38]

Ein Widerspruchsrecht gegen die Nutzung der pseudonymisierten GKV-Abrechnungsdaten im FDZ fehlt weiterhin. Von Art. 89 Abs. 2 DSGVO geforderte kompensierende Schutzvorkehrungen fehlen. Betroffenenrechte einzuschränken ist nur erlaubt, wenn anderenfalls die Verwirklichung der spezifischen Forschungszwecke unmöglich oder ernsthaft beeinträchtigt würden. Dies wird im Gesetz nicht umgesetzt.[39]

Das Fehlen eines Widerspruchsrechts im FDZ-Register mag noch mit der Notwendigkeit höchstmöglicher Repräsentativität der Datengrundlage begründbar sein. Dies gilt aber nicht für das Vorenthalten der weiteren Betroffenenrechte, insbesondere des Auskunftsrechts. Das in Art. 8 Abs. 2 S. 2 GRCh und in Art. 15 DSGVO garantierte Auskunftsrecht wird in Art. 89 Abs. 2 DSGVO, in § 27 Abs. 2 BDSG und in Bezug auf Sozialdaten in § 83 SGB X relativiert, aber nicht ausgeschlossen. Die Einzeldatensätze sind pseudonym und damit personenbeziehbar. Das Gesetz untersagt eine Re-Identifizierung von Transparenzdaten für Nutzungsberechtigte (§ 7 Abs. 2 GDNG; § 303e Abs. 5 S. 2, 3 SGB V). Dies kann aber nicht bei der Umsetzung des verfassungsrechtlich begründeten Auskunftsanspruchs[40] gelten. Dieser Anspruch besteht auch in Bezug auf pseudonymisierte Daten.[41] Hiergegen kann nicht argumentiert werden, eine Auskunft würde einen unverhältnismäßigen Aufwand erfordern (vgl. § 27 Abs. 2 S. 2 BDSG).[42] Gerade bei einem zentralisierten automatisierten Verfahren, wie vorliegend, kann durch entsprechend etablierte Abläufe der Aufwand auf ein Minimum reduziert werden. Beim FDZ findet ein individualisiertes Verknüpfen von Datensätzen für Sekundärzwecke statt. Es ist nicht zu rechtfertigen, dass diese Verknüpfung den Betroffenen selbst vorenthalten wird. Auch andere Erwägungen, die eine Auskunftsverweigerung begründen könnten (§ 83 Abs. 1 SGB X), sind nicht ersichtlich.

Es liegt auch kein Fall des Art. 11 DSGVO vor. Art. 11 Abs. 1 DSGVO ist nicht anwendbar, da das im FDZ gespeicherte Pseudonym zu einem Betroffenen nicht der „bloßen Einhaltung dieser Verordnung“ dient, sondern insbesondere einer späteren Zuordnung von weiteren Datensätzen. Art. 11 DSGVO entbindet von der Pflicht zur Wahrung der Betroffenenrechte, wenn der Verantwortliche nachweisen kann, dass er die betroffene Person nicht identifizieren kann, „es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesem Artikel niedergelegten Rechte zusätzliche Informationen bereit, die ihre *Identifizierung ermöglichen*“ (Art. 11 Abs. 2 S. 2 DSGVO). Da vom Betroffenen die Bereitstellung bestimmter, die Identifizierung ermöglichenden Daten problemlos gegenüber dem FDZ machbar ist, etwa indem von ihm individuelle Verschreibungs- oder Behandlungsdaten benannt werden, wodurch im Gesamtdatenbestand eine eindeutige Zuordnung möglich wäre, ist der Ausschluss des Auskunftsrechts nach Art. 11 DSGVO oft schon nach dem Wortlaut der DSGVO nicht gerechtfertigt. Relevant ist aber, dass Art. 11 DSGVO auf den Fall der Datentransparenzdaten gar nicht anwendbar ist, da die Regelung die Datenminimierung im Einzelfall fördern soll[43] und nicht für eine gesetzliche angeordnete pseudonyme Datenspeicherung anwendbar sein kann.

Eingriffe in das Auskunftsrecht sind nur auf gesetzlicher Grundlage zulässig, soweit diese sich als erforderlich erweisen. Sieht ein Gesetz eine Verschleierung der Personenidentität vor und dienen die verwendeten Pseudonyme einer eindeutigen Zuordnung zu einer Person, so muss das Gesetz auch einen Prozess festlegen, mit dem die Betroffenenrechte gewahrt werden können.[44]

Nach übergeordnetem Recht besteht ein *Auskunftsanspruch*, ohne dass in den §§ 303a ff. SGB V oder im GDNG ein Verfahren vorgesehen ist, mit dem dieser Anspruch umgesetzt werden kann. Ein geregeltes Verfahren wäre im Fall des FDZ unter Einbindung von Krankenkasse und Vertrauensstelle möglich.

Da die *Betroffenenrechte* verweigert werden, insbesondere das Widerspruchs- und das Auskunftsrecht, verstoßen die Regelungen gegen höherrangiges Recht und sind sowohl verfassungs- als auch europarechtswidrig.

3.9 Datenschutzkontrolle

§ 5 GDNG regelt die *Datenschutzaufsicht* bei länderübergreifender Gesundheitsforschung. Er knüpft an den bisherigen § 287a SGB V-alt an. Sind die Stellen nicht gemeinsam Verantwortliche, so kann für das Vorhaben eine „federführende Datenschutzaufsicht“ bestimmt werden. Örtlich zuständig ist die Aufsicht, wo die beteiligte Stelle mit dem größten Jahresumsatz bzw. mit den meisten Beschäftigten ihren Sitz hat (§ 5 Abs. 2 GDNG), wobei die federführende Aufsicht nur eine koordinierende Funktion wahrnimmt, wenn öffentliche Stellen beteiligt sind, während bei einer Beteiligung von nicht-öffentlichen Stellen in gemeinsamer Verantwortung eine alleinige Aufsichtszuständigkeit möglich ist (§ 5 Abs. 4 GDNG).

4. Was zusätzlich von Bedeutung ist

Bei der Regulierung der Sekundärnutzung von Gesundheitsdaten blieben bisher die Vorgaben des Gleichheitsgrundsatzes und die Besonderheit des

Schutzes wissenschaftlicher Forschung völlig unberücksichtigt.

Das GDNG soll für gesetzlich und für privat Versicherte gelten. Dies ist im Hinblick auf die meisten Sekundärnutzungen berechtigt: Daten von privat versicherten Patienten sind nur dann nicht nötig, wenn es um GKV-spezifische Auswertungen geht. Eine Ungleichbehandlung besteht also in den nur für gesetzlich Versicherte geltenden §§ 303a ff. SGB V, soweit dort mit der Datennutzung nicht-GKV-relevante Auswertungen vorgesehen sind. Für diese *Ungleichbehandlung von gesetzlich und privat Versicherten* gibt es keine tatsächliche, sondern allenfalls eine gesetzessystematische bzw. historische Begründung, welche aber die Ungleichbehandlung nach Art. 3 GG und Art. 20 GRCh nicht rechtfertigen kann.

Das GDNG unterlässt es, das bisher bestehende Defizit einer klaren Definition dessen vorzunehmen, was durch Art. 5 Abs. 3 GG grundrechtlich privilegiert ist und die Grundrechtseingriffe in den Datenschutz der Patienten rechtfertigt. Eine klare Bezugnahme auf die enge Forschungsdefinition des BVerfG[45] wird unterlassen. Der *Begriff der Forschung* wird nur ausschließend verwendet (so in § 303e Abs. 2 Nr. 4 GDNG); im GDNG etwa bzgl. der Einbeziehung von Krebsregisterdaten (§ 2 GDNG) oder bei der länderübergreifenden Datenschutzaufsicht bedarf es aber einer trenngenauen Definition.

Schon bisher beschränkten sich die Zwecke der Sekundärnutzung nicht auf die der wissenschaftlichen Forschung, sondern umfassten gemäß § 303e Abs. 2 SGB V auch operative Zwecke wie die Steuerung der GKV-Vertragspartner, Qualitätsverbesserung, Ressourcenplanung, die Unterstützung von politischen Planungen, die Entwicklung besonderer Behandlungsprogramme. Dabei bleibt unberücksichtigt, dass Forschungsnutzungen ein hoher grundrechtlicher Schutz zukommt, vielen der anderen Sekundärnutzungen aber nicht. Diese insbesondere im FDZ erfolgende Gleichbehandlung von Ungleichem verstößt gegen Art. 3 GG und Art. 20 GRCh.

5. Ergebnis

Die Hoffnung auf datenschutzgerechte gemeinwohlorientierte Sekundärnutzung von Gesundheitsdaten, die durch den Koalitionsvertrag begründet wurde, erhielt durch das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ einen Dämpfer. Das von der rot-grün-gelben Koalition gegebene Versprechen, in Deutschland klare datenschutzkonforme Regeln zur Auswertung von Gesundheitsdaten einzuführen, um unser Gesundheitswesen insgesamt und insbesondere die medizinische Forschung voranzubringen, wird bisher nicht eingelöst. Seine Einhaltung wird nicht nur von den Patientinnen und Patienten eingefordert, sondern – voraussichtlich zeitnah – auch vom Bundesverfassungsgericht und vom Europäischen Gerichtshof.

Während sich das DVG darauf beschränkte, dem FDZ GKV-Abrechnungsdaten für Sekundärnutzungen zur Verfügung zu stellen, sollen nun auch die Abrechnungsdaten der Pflegekassen erfasst werden. Hinzukommen sollen die Daten aus ePAs. Das FDZ ist darauf angelegt weitere Datenverknüpfungen, so mit den Krebsregistern (§ 2 GDNG), zu eröffnen. Der EHDS enthält die Perspektive, dass alles, was im weitesten Sinn als Gesundheitsdaten verstanden werden kann, für Sekundärzwecke nutzbar gemacht werden kann (Art. 33 EHDS-E). Eine umfassende Regelung der Sekundärnutzung von Gesundheitsdaten, wie sie im EHDS angelegt ist, lässt sich bei der deutschen Gesetzgebung nicht im Ansatz erkennen. Die zögerlichen Gesetzgebungsschritte sind inkohärent, vor allem aber europarechts- und verfassungswidrig. Dies kann nicht damit entschuldigt werden, dass die Praxis weit hinter der Gesetzgebung hinterherhinkt. Auch bei nur teilweiser Umsetzung etablieren sich Grundrechtsverstöße und schaffen so Fakten. Die Umsetzung des EHDS, zu dem erst nach dem GDNG der Trilog-Konsens gefunden wurde, macht eine Anpassung des eben erst in Kraft getretenen Gesetzes nötig. Dieses Mal darf sich der Gesetzgeber nicht aufs Weiterwurschteln beschränken. Er muss eine in sich stimmige, praktikable und zugleich verfassungskonforme Konzeption erarbeiten und in gesetzgeberische Regeln gießen.

1 Moreno GuP 2023, 189 f.

2 SPD/Bündnis 90/Die Grünen/FDP, Mehr Fortschritt wagen, 2021, S. 21, 83; dok. z.B. in Datenschutz-Nachrichten (DANA) 1/2022, 20 f.

3 EU-Kommission v. 3.5.2022, COM(2022) 197 final, 2022/0/140 (COD).

4 Zum Zeitpunkt des Verfassens des vorliegenden Artikels (Mai 2024) war noch keine Veröffentlichung erfolgt; es lag lediglich eine nicht bereinigte englische Fassung des Trilog-Ergebnisses vor, die hier als EHDS-E zitiert wird.

5 Im Netz veröffentlich durch Netzpolitik.org unter https://netzpolitik.org/2023/gesundheitsdaten-opt-out-digitalisierung-ohne-ruecksicht-auf-versicherte/#Gesundheitsdatennutzungsgesetz; dazu Weichert, Gesundheitsdatennutzung contra heilberufliche Vertraulichkeit, www.netzwerk-datenschutzexpertise.de 26.07.2023; zum zweiten Referentenentwurf Weichert GuP 2023, 183.

6 BR-Drs. 434/23 v. 08.09.2023 = BT-Drs. 20/9046 v. 01.11.2023.

7 https://www.bundestag.de/ausschuesse/a14_gesundheit/oeffentliche_anhoerungen/974686-974686; vgl. Netzwerk Datenschutzexpertise, Stellungnahme vom 14.11.2023, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/2023_stn_gdng.pdf.

8 Zum Ablauf des Gesetzgebungsverfahrens https://dip.bundestag.de/vorgang/gesetz-zur-verbesserten-nutzung-von-gesundheitsdaten-gesundheitsdatennutzungsgesetz-gdng/303310?f.deskriptor=Innerstaatliche Umsetzung von EU-Recht&rows=25&pos=2.

9 BGBl. N. 102 v. 26.03.2024.

10 DVG v. 09.12.2019, BGBl. I S. 2562; dazu Weichert MedR 2020, 539; Schulz SGb 2020, 536; Kühling/Schildbach NZS 2020, 41.

11 Von Kielmansegg VerwArch 2021, 132 ff.

12 BR-Drs. 434/23 S. 29.

13 Bernhardt/Ruhmann/Weichert, EHDS – der Europäische Gesundheitsdatenraum – Nutzungsrechte contra Vertraulichkeit, www.netzwerk-datenschutzexpertise.de, 27.02.2023, Kap. 3; diess., DANA 1/2023, 18.

14 Koch/Steiner, Lauterbachs Pläne für die Gesundheitsdaten-Revolution auf der Zielgeraden, www.heise.de 13.12.2023, Kurzlink: https://heise.de/-9573984, S. 4.

15 Weichert MedR 2020, 539 ff.; Schulz SGb 2020, 541.

16 BVerfG 19.03.2020 – 1 BvQ 1/20 Rn. 8, JZ 2020, 1012 f.

17 BVerfG 19.03.2020 – 1 BvQ 1/20 Rn. 13,

18 Krempl, Forschungsdatenzentrum soll Sicherheitskonzept vorlegen, www.medical-tribune.de 18.02.2023.

19 BR-Drs. 434/23, S. 3.

20 Dazu Weichert, Gesundheitsdatennutzung contra heilberufliche Vertraulichkeit, 09.08.2023, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2023_08_gdng.pdf, S. 8.

21 Moreno GuP 2023, 191 f.

22 §§ 41c ArzneimittelG-E, BMG-Referentenentwurf Stand 17.01.2024; Art. 36 Abs. 2 S. 2 EDHS-E erlaubt nur eine vorbereitende Einschaltung von Ethik-Kommissionen.

23 BfDI, Stellungnahme v. 29.09.2023. Deutscher Bundestag Ausschuss f. Gesundheit, Ausschussdrucksache 20(14)143, S. 17.

24 Art. 36 Abs. 2 S. 1 EHDS-E.

25 https://www.medizininformatik-initiative.de/de/nutzungsordnung.

26 BfDI, Stellungnahme (En. 23), S. 20.

27 BfDI, Stellungnahme (En. 23), S. 8.

28 Zuletzt DSK, Datenschutz in der Forschung durch einheitliche Maßstäbe stärken, 23.11.2023; weitere Nachweise bei Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, https://www.tmf-ev.de/sites/default/files/2023-10/tmf-schriftenreihe-band-19-datenschutzrechtliche-rahmenbedingungen-medizinischer-forschung.pdf, S. 114.

29 BfDI, Stellungnahme (En. 23), S. 4, 10.

30 BVerfG 25.09.2023 – 1 BvR 2219/20; dazu Pollähne Bürgerrechte & Polizei CILIP 134, April 2024, S. 97 ff. m.w.N; Kühne DÖV 2024, 27 ff.

31 Weichert MedR 2020, 544.

32 BfDI (En. 23), S. 8.

33 Weichert, Rahmenbedingungen (En. 28), S. 21 ff.

34 Weichert, Rahmenbedingungen (En. 28), S. 99 f.

35 Z.B. Fährmann/Aden/Arzt in Friedewald/Kreutzer/Hansen, Selbstbestimmung, Privatheit und Datenschutz, 2022, 303 ff.

36 BfDI, Stellungnahme (En. 23), S. 9 f.

37 Weichert MedR 2020, 542 f.

38 Kritisch dazu BfDI, Stellungnahme (En. 23), S. 21 ff.

39 Weichert MedR 2020, 543.

40 Däubler in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 3. Aufl. 2024, Art. 15 Rn. 1; Bäcker in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 15 Rn. 5, jeweils mit Verweis auf Art. 8 Abs. 2 S. 2 GRCh; zum nationalen Verfassungsrecht Weichert NVwZ 2007, 1005 f.

41 Dix in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 15 Rn. 12; Däubler in Däubler u.a. (En. 40), Art. 15 Rn. 4.

42 Vgl. VG Berlin 06.02.2024 – 1 K 187/21.

43 Weichert in Kühling/Buchner (En. 40), Art. 11 Rn. 11.

44 Weichert in Kühling/Buchner (En. 40), Art. 11 Rn. 1a.

45 BVerfG Urt. v. 29.05.1973, NJW 1973, 1176; BVerfGE 35, 112 f.; ausführlich Weichert, Rahmenbedingungen (En. 28), S. 18 ff.

Thilo Weichert

Gesundheitsdaten bei Doctolib? So nicht!

Die Zahl der Anfragen und Beschwerden von Ärzten und Patienten, die bei der Berliner Datenschutzbeauftragten (BlnBDI), bei weiteren Datenschutzaufsichtsbehörden und bei Ärztekammern eingegangen sind, ist nicht mehr überschaubar. Beispiele: Die Patientin eines Universitäts-Schlaflabors in Mannheim teilte mit, ihr sei die weitere Behandlung verweigert worden, nachdem sie erklärte, dass sie ihre Behandlungstermine nicht über den IT-Dienstleister Doctolib abwickeln möchte. Ein angestellter Arzt befürchtet, dass er sich durch seine Tätigkeit in einer Praxis, die ihre Terminvermittlung über Doctolib durchführt, strafbar macht. Patienten, die Termine mündlich und fernmündlich bei ihrem Arzt verabredet haben, erhalten überraschend von Doctolib eine Terminbestätigung per SMS oder Mail und fragen sich, weshalb das Unternehmen ihre vertraulichen Daten erhalten hat.

BigBrotherAward und andere Kritik

Diese Beschwerden landen nicht nur bei der zuständigen Datenschutzaufsicht und den Ärztekammern, sondern auch beim Netzwerk Datenschutzexpertise: Der Autor des vorliegenden Beitrags hielt am 11.06.2021 – in seiner Funktion als Vertreter dieses Netzwerks und der Deutschen Vereinigung für Datenschutz e.V. (DVD) – eine Laudatio zum BigBrotherAward (BBA) in der Kategorie Gesundheit für die Firma Doctolib GmbH, Berlin, wegen der Vermittlung von Arztterminen über deren Plattform: „Diese Daten werden unter Missachtung der Vertraulichkeitsverpflichtung verarbeitet und laut Datenschutzvereinbarung auch im Rahmen kommerzieller Marketingzwecke genutzt." Die Kritik: Doctolib lässt sich bei Einrichtung des Terminmanagements sämtliche im Arztinformationssystem gespeicherten Patientenstammdaten übertragen, unabhängig davon, ob diese einen Termin vereinbaren. Weitere Vorwürfe waren: Die Allgemeinen Geschäftsbedingungen (AGB) seien verwirrend, unklar und teilweise widersprüchlich. Unnötige Cookies, auch für Werbung, würden gesetzt. Social Media werde eingebunden. Die Patientendaten der einzelnen Gesundheitseinrichtungen würden nicht voneinander getrennt (sog. Mandantentrennung), wie dies für IT-Dienstleister Pflicht wäre. Fragwürdig sei auch die Einschaltung von Amazon Web

Services (AWS) als Cloud-Datenverarbeiter und die mögliche Datenübermittlung in unsichere Drittstaaten.[1] Zuvor war das Unternehmen – erfolglos – um eine Stellungnahme gebeten worden. Gesprächsangebote vom Netzwerk Datenschutzexpertise wurden seitdem von Doctolib bis Ende 2023 ignoriert.

Schon vor der BBA-Verleihung landete Doctolib im Rahmen einer Markt-Untersuchung der Stiftung Warentest zum Datenschutz bei Arztterminsoftware auf dem vorletzten Platz.[2] Im Dezember 2020 informierten der ChaosComputer-Club und ein Wissenschaftler über ein Datenleck, über das potenziell 150 Mio. Terminvereinbarungen hätten abgerufen werden können. Um seine BBA-Vorwürfe zu belegen, erarbeitete das Netzwerk Datenschutzexpertise ein 39-seitiges Gutachten und veröffentlichte dieses im Internet.[3] Zudem wurde bekannt, dass die Berliner Senatsverwaltung für Gesundheit Doctolib Ende 2020 beauftragt hatte, die Corona-Impftermine für Bewohner der Bundeshauptstadt zu vermitteln. Wie auch zwecks Terminvermittlung bei Ärzten mussten die Impfwilligen auf dem Webportal von Doctolib ein Konto einrichten, über das die Impftermine vergeben wurden. Dies führte dazu, dass 2,05 Mio. Berlinerinnen und Berliner sich bei dem Portal anmeldeten. Für die Stadt war das kostengünstig; sie erhielt die Dienstleistung angeblich unentgeltlich; es waren lediglich pro Terminerinnerung 0,16 Cent zu zahlen. Für Doctolib war dies eine wirksame Werbemaßnahme, erhielt doch seine illegale Verarbeitungspraxis den hoheitlichen Segen der Berliner Gesundheitsverwaltung. Gemäß dem etablierten fragwürdigen Internet-Geschäftsmodell „Zahlen mit Daten" erfasste das Unternehmen die Daten der zu Impfenden frei Haus.[4] Dass die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) diese hoheitlich geförderte Sammlung hochsensitiver Gesundheitsdaten als rechtswidrig kritisierte, störte weder die Gesundheitsverwaltung noch das Unternehmen. Die BlnBDI hatte schon in ihrem Tätigkeitsbericht für das Jahr 2019 die unzulässige Datenverarbeitung bei Ärzten – folgenlos – angeprangert.[5] In den Tätigkeitsberichten der Jahre 2021[6] und 2022[7] bekräftigte die Berliner Datenschutzaufsicht ihre Kritik.

Ganz folgenlos blieben die Verleihung des BigBrotherAwards, die Kritik der Aufsicht sowie Presseveröffentlichungen nicht: Anfang 2022 änderte Doctolib seine AGB, mit denen einige offensichtliche Rechtsverstöße behoben wurden, ohne dass aber das zu Grunde liegende illegale Geschäftsmodell verändert wurde. Die Cookie-Übermittlung an Google wurde gestoppt. Wahrscheinlich wurde bei der Datensicherheit nachgebessert.

Vom Startup zum Schwergewicht

Doctolib wurde 2013 als französisches Startup gegründet, das schon drei Jahre später in Frankreich an 30 Standorten ca. 230 Beschäftigte hatte. 2016 expandierte das Unternehmen nach Deutschland, es ist inzwischen auch in Italien und in den Niederlanden tätig. 2016 sammelte das Unternehmen rd. 23 Mio. Euro Wagniskapital ein. Nach einer weiteren Finanzierungsrunde wurde das Unternehmen 2019 zum „Unicorn"; es wurde mit mehr als 1 Mrd. Euro bewertet. 2023 kam Doctolib nach weiteren Finanzierungsrunden auf eine Bewertung von 5,8 Mrd. Euro.

Bei seiner Expansion scheute sich das Unternehmen nicht vor aggressiver Werbung und unlauteren Darstellungen. So meinte das Unternehmen, seine Datenschutzkonformität mit der Behauptung belegen zu können: „Wir arbeiten mit den Behörden, die für den Schutz von personenbezogenen Daten zuständig sind, zusammen." Wie diese „Zusammenarbeit" aussieht, ist den Jahresberichten der Berliner Datenschutzaufsicht zu entnehmen: Doctolib ignorierte Kritik der BlnBDI.

Eine weitere fragwürdige Methode der Selbstanpreisung zum Datenschutz bestand und besteht darin, dass sich das Unternehmen einer Vielzahl von Zertifikaten rühmt. Zu einem Zertifikat des TÜV Saarland „TÜV geprüfter Datenschutz v5.0" wollte der TÜV Saarland auf Nachfrage weder Nachweise noch Antworten vorlegen. Eine Zertifizierung durch datenschutz cert GmbH, bei der „internet privacy standards" (ips) zur Grundlage genommen wurden, wurde nicht erneuert, nachdem die Zertifizierungsstelle vom Netzwerk Datenschutzexpertise auf die festgestellten Datenschutzverstöße hingewiesen worden war. Eine Zertifizierung ISO/IEC 27001/27701 durch eine BSI-Group stammte nicht vom deutschen BSI, dem „Bundesamt für die Sicherheit in der Informationstechnik", sondern von einer „British Standards Institution", ohne dass hierzu vertiefte Nachweise vorgelegt wurden. Nach Intervention des Netzwerks Datenschutzexpertise wurde eine verfälschende Presseerklärung vom Unternehmen korrigiert. Zwei Zertifikate des TÜVIT, beworben u.a. mit „Datenschutz", beziehen sich lediglich auf das Doctolib-Angebot für Videosprechstunden. Auch vom TÜVIT wurden auf Nachfrage keine kritikfähigen Nachweise vorgelegt. Der TÜVIT vermittelt zudem auf seiner Webseite den falschen Eindruck, die Zertifizierung sei gemäß den inhaltlichen und formalen Anforderungen der europäischen Datenschutz-Grundverordnung erfolgt. Ein französisches HDS-Zertifikat (Hébergeur de Données de Santé), das sich auf die Cloud-Datenverarbeitung von AWS bezog, wird von dem Unternehmen in Deutschland nicht mehr beworben.[8] Stattdessen wirbt Doctolib mit dem deutschen C5-Testat, das aber nur auf einer gegenüber einem Wirtschaftsprüfer abgegebenen Selbstzertifizierung beruht. Das Unternehmen erweckt erneut fälschlich den Eindruck, das Testat werde vom deutschen BSI ausgestellt.[9] Dieses Testat Doctolibs, das übrigens nach neuer Rechtslage Voraussetzung für die Clouddatenverarbeitung von Gesundheits- und Sozialdaten ist (§ 393 SGB V), dürfte zumindest hinsichtlich des Einsatzes für das ärztliche Terminmanagement ungültig sein, da es nur für Auftragsverarbeiter gelten soll, Doctolib hier aber als Verantwortlicher die Daten verarbeitet.

Die Abmahnaktion Doctolibs und die Reaktion hierauf

Das Netzwerk Datenschutzexpertise veröffentlichte am 28.07.2022 nach einigen wesentlichen Änderungen durch Doctolib – etwa der AGB – ein neues Datenschutz-Gutachten, um auf die vielen Anfragen einzugehen, ob deren Angebot nun datenschutzkonform sei. Dies musste leider weiterhin verneint werden.[10] Gesprächsangebote zum Datenschutz-Gutachten blieben von Doctolib weiterhin unbeantwortet. Wohl aber nahm nicht nur eine kritische Öffentlichkeit von

den Gutachten Kenntnis. Im Medizinbereich tätige IT-Unternehmen verwiesen gegenüber Ärzten und Gesundheitsanbietern auf die Netzwerk-Gutachten, die zum Ergebnis kommen, dass Doctolib entgegen seiner eigenen Darstellung nicht als Auftragsverarbeiter, sondern als verantwortlicher Dienstleister tätig wird, was nicht nur einen Datenschutzverstoß darstellt, sondern auch eine Verletzung des Patientengeheimnisses. Nach § 203 StGB sind Heilberufe ebenso wie externe, an der ärztlichen Berufstätigkeit Mitwirkende, wozu Doctolib gehört, bei Offenbarung von Patientengeheimnissen sowie bei der Beihilfe und der Anstiftung hierzu, strafbar. Der Vorwurf der Strafbarkeit trifft nicht nur den Dienstleister, sondern auch die das Terminmanagement von Doctolib nutzenden Ärzte und sonstigen „Gesundheitsfachkräfte".

Die öffentliche Aufmerksamkeit und die Kritik an dem Gebaren Doctolibs nahm zu. Am 11.04.2023 berichtete die ARD.[11] Am 13.11.2023 wurde ein 30-minütiges Feature des Deutschlandfunks über Doctolib ausgesendet.[12] Der Gegenwind gefiel dem Unternehmen überhaupt nicht. Gegenüber Firmen, die sich auf die Gutachten des Netzwerks Datenschutzexpertise beriefen, versandte es Abmahnungen wegen „unlauterem Wettbewerb" und forderte zugleich z.B. einen Schadenersatz in Höhe von 50.000 Euro plus Anwaltskosten in Höhe von 2.700 Euro ein. Diese Abmahnaktionen zwangen das Netzwerk Datenschutzexpertise erneut zur Veröffentlichung eines dritten Gutachtens mit Datum vom 25.10.2023.[13] Darin wird akribisch nachgewiesen, dass die Abmahnungen unberechtigt sind.

Kurz darauf, am 21.11.2023, erfolgte etwas Überraschendes: Die Leiterin der Kommunikationsabteilung von Doctolib meldete sich beim Autor dieses Textes und bot diesem ein „Treffen in unserem Büro" in Berlin an. Dem wurde zugestimmt verbunden mit der erklärten Erwartung auf einen ausführlichen Austausch nicht nur mit der Geschäftsführung, sondern mit der Datenschutzbeauftragten und weiteren Vertretern des Unternehmens zwecks ernsthafter technischer und juristischer Erörterung der Doctolib-Praxis. Tatsächlich fand am 13.12.2023 ein Gespräch – aber nur mit dem Geschäftsführer Nikolay Kolev – statt, das in einer äußert freundlichen Atmosphäre stattfand. Dabei versicherte der Geschäftsführer wortreich, wie wichtig seinem Unternehmen der Datenschutz sei. Nach einer halben Stunde meinte er dann aber wegen weiterer Verpflichtungen das Gespräch beenden zu müssen. Der ausdrücklichen Forderung des Netzwerks Datenschutzexpertise, künftig keine weiteren Abmahnungen an Unternehmen zu versenden, die sich auf seine Gutachten beziehen, deren Stichhaltigkeit bisher qualifiziert nicht infrage gestellt wurden, wollte Herr Kolev nicht entsprechen. Zumindest sind aber seither keine weiteren Abmahnungen bekannt geworden.

Das raffinierte Geschäftsmodell

Doctolib ist ökonomisch bisher äußerst erfolgreich. Das Wachstum basiert darauf, dass das Unternehmen ein illegales Geschäftsmodell kopiert, welches insbesondere Internet-Unternehmen des Silicon Valley reich macht: Doctolib drängt Patienten bei ihrer Internet-Kommunikation mit Gesundheitsanbietern auf die eigene Plattform, sammelt die anfallenden Daten und nutzt diese für eigene Zwecke. Während z.B. Google oder Meta allgemeine Internetdaten auswerten und diese insbesondere für Werbezwecke lukrativ und rechtlich angreifbar vermarkten, zielt Doctolib spezifisch auf Gesundheitsdaten und die Internet-Kommunikation von Patienten und Heilberuflern. Die Internet-Plattformen des Silicon Valley hatten sich zunächst aus ihrer Verantwortung bei der Webseiten-Kommunikation dadurch zu entziehen versucht, dass sie sich als reine Dienstleister der Internetnutzenden präsentierten. Es könne klar getrennt werden zwischen der Verantwortlichkeit der Webseitenbetreiber und der Plattformen. Diesem Argument hat der Europäische Gerichtshof (EuGH) am 05.06.2018 mit seinem Facebook-Urteil eine Abfuhr erteilt und klargestellt, dass bei einer Kooperation eines Internetnutzers mit einer Plattform eine „gemeinsame Verantwortlichkeit" besteht, was Pflichten zu Folge hat, denen weder die US-Konzerne noch Doctolib genügen.[14]

Gesundheitseinrichtungen können Online-Terminvereinbarungen problemlos über ihre Webseite anbieten. In diesem Fall sind die IT-Dienstleister der Gesundheitseinrichtungen als Auftragsverarbeiter tätig; sie dürfen die dabei anfallenden Daten selbst nicht nutzen. Doctolib setzt aber auf umfassendes Datensammeln bei Patienten und Ärzten. Es macht die Nutzung seines Dienstes davon abhängig, dass sich die Patienten auf der Webseite von Doctolib anmelden. Damit erhält das Unternehmen die Nutzerdaten unabhängig vom direkten Arztkontakt und meint, diese wie jede andere Internet-Plattform für eigene Zwecke nutzen zu können. Die über den Doctolib-Account anfallenden Daten unterliegen nicht dem besonderen Schutz des Patientengeheimnisses.

Um möglichst viele Patientendaten zu erlangen, erklärt das Unternehmen gegenüber den Gesundheitseinrichtungen, dass die Übertragung der Stammdaten sämtlicher Patienten für den Betrieb des Terminmanagements nötig sei. Die E-Mail-Adresse bzw. die Handynummer auch von Patienten, die mündlich oder fernmündlich einen Termin vereinbaren, sei für das Versenden von Terminbestätigungen erforderlich. Für Gesundheitseinrichtungen ist das Online-Terminmanagement bequem. Einige weigern sich schon Terminanfragen über andere Wege als über Doctolib, etwa mündlich oder fernmündlich, zu behandeln. Patienten werden derart gezwungen bei Doctolib einen Internet-Account zu eröffnen, um mit ihrer Arztpraxis den Kontakt aufzunehmen.

Doctolib agiert also sowohl als Dienstleister der Patienten (als Internet-Portalanbieter) wie auch als Dienstleister von Ärzten und anderen Gesundheitseinrichtungen (als Terminmanager), ohne dabei zwischen diesen beiden Funktionen zu trennen. Für Patienten ist die Nutzung oft alternativlos. Bei der Terminvereinbarung erhebt das Unternehmen zwecks Vermittlung Namen, Geschlecht, Geburtsdatum, Telefonnummern, Patientennummern, Versichertenstatus sowie Notizen des Arztes wie die Termindaten, zu denen auch der „Besuchsgrund" gehört.[15]

So sammelt Doctolib arzt- und einrichtungsübergreifend in ganz Deutschland Daten von Patientinnen und Patienten. Nach Angaben des Unternehmens sind so inzwischen 80 Millionen Personen erfasst. Ca. 900.000 Angehörige von Heilberufen nutzen den Dienst. Mit-

te 2023 arbeiteten in Deutschland ca. 25.000 niedergelassene Ärzte und Therapeuten mit Doctolib zusammen, zudem 250 Krankenhäuser, darunter u.a. 34 Einrichtungen des Sana-Konzerns. Weitere Klinikkunden sind die St. Augustinus Gruppe, die Atos-Kliniken, die Paracelus-Kliniken, die Uni-Kliniken Köln und Mannheim, die Schön-Klinik, das Klinikum St. Georg und viele mehr.[16] Bei der Terminvermittlung von Ärzten hat das Unternehmen in Deutschland November 2023 einen Marktanteil von 60% erreicht;[17] in Frankreich soll der Marktanteil noch erheblich höher liegen. Gemäß dem Geschäftsführer kommen in Deutschland jeden Monat 300.000 Kunden hinzu.[18] Es ist also kein Wunder, dass das Unternehmen bei einer Investorenrunde 2022 weitere 500 Mio. Euro einsammeln konnte und mit 5,8 Mrd. Euro bewertet wurde. Zum Vergleich: Der umsatzbezogen weitaus größere Konkurrent Compugroup (CGM) wurde 2023 mit 2 Mrd. Euro bewertet.

Ausbau des Portfolios

Das Unternehmen erweitert kontinuierlich seine IT-Angebote für Gesundheitseinrichtungen. Dazu gehören Dienste für die Arztsuche, für Videosprechstunden, zur Dokumentation von Gesundheitsunterlagen und zur Kommunikation zwischen Patienten und Gesundheitseinrichtungen.[19] Anfang 2023 hat Doctolib mit „Siilo" den größten Anbieter für Gesundheitsmessenger in Europa gekauft, der angibt, 450.000 Gesundheitsanbieter zu vernetzen.[20] Die Einführung einer eigenen Praxissoftware wurde angekündigt.[21] Bei seinem Angebot „Doctolib Hospital" geht es nicht nur um Terminvermittlung, sondern „um mehr als nur ein Patientenportal", etwa durch eine „Optimierung des Zuweisermanagements und eine intersektorale Vernetzung". Dabei wird, so die Werbung, das Unternehmen „vollständig mit Ihrem Krankenhausinformationssystem (KIS) verbunden", wodurch z.B. Dokumente „vom Patientenportal ins KIS und zurück sowie in die elektronische Patientenakte (ePA) übertragen werden" können.[22] Am 14.03.2024 verkündete Doctolib, dass es die Ausschreibung der Charité, der europaweit größten Universitätsklinik mit Sitz in Berlin, zur Einführung eines KHZG[23]-fähigen Patientenportals gewonnen hat.[24] Der Hinweis des Netzwerks Datenschutzexpertise auf die Datenschutzprobleme bei Doctolib führten bisher zu keiner inhaltlichen Rückmeldung der Charité. Anfang 2024 teilte Doctolib zudem mit, dass es eine Kooperation mit dem ADAC eingegangen ist für einen gemeinsamen „niederschwelligen Zugang zur gesundheitlichen Versorgung", indem die Online-Arztterminbuchung von Doctolib in die „ADAC Medical App" integriert wurde.[25] Eine Suche nach Datenschutzhinweisen in der ADAC-App war nicht erfolgreich; auf der Seite des ADAC sind wenig vertrauenswürdige Social-Media-Anbieter eingebunden, etwa Tiktok, X und Facebook.

Sanktionen?

Die Berliner Datenschutzbeauftragte (BlnBDI) moniert in ihren Jahresberichten seit 2019 regelmäßig Datenschutzverstöße durch Doctolib. Man sollte denken, dass diese Verstöße auch sanktioniert würden. Dem ist bisher nicht so. Zwar mahnt die Aufsichtsbehörde auf ihrer Webseite Ärzte zu einem datenschutzkonformen Terminmanagement.[26] Auch andere Aufsichtsbehörden kritisieren die Doctolib-Praxis: die Bremische Datenschutzbeauftragte nennt in ihrem Jahresbericht ebenso wenig wie die BlnBDI in ihren Berichten explizit den Firmennamen.[27] Sanktionen wurden offenbar weder gegen Doctolib noch gegen die Doctolib nutzenden Ärzte oder sonstigen Gesundheitseinrichtungen verhängt.

Dass Doctolib auch im 5. Jahr nach der ersten öffentlichen Beanstandung durch die Datenschutzbehörden ungeschoren davonkommt, mag daran liegen, dass das Unternehmen behauptet, die BlnBDI sei für Sanktionen nicht zuständig; dies sei die französische Aufsicht, die „Commission Nationale de l'Informatique et des Libertés" (CNIL), da die Konzernmutter ihren Sitz in Frankreich hat. Diese Argumentation ist juristisch nicht haltbar, da die gesamte verantwortete Datenverarbeitung in Deutschland erfolgt und zudem teilweise spezifische deutsche Datenschutznormen – die Regeln zum Patientengeheimnis – gelten.[28]

Weniger verwunderlich ist, dass die Ärztekammern sowie sonstige Heilberufekammern bisher nicht tätig geworden sind. Diese können sich direkt nur an ihre Mitglieder wenden und haben keinen direkten Zugriff auf Doctolib. Wohl aber stehen deren Mitglieder als Gesundheitseinrichtungen in der Verantwortung für die Wahrung von Patientengeheimnis und Datenschutz, auch wenn sie dabei einzelne Aufgaben an Externe outsourcen. Noch weiter weg von den Rechtsverstößen scheinen Strafverfolger zu sein, also insbesondere die Staatsanwaltschaften. Diese können ohnehin nur auf Antrag der betroffenen Patientinnen oder Patienten tätig werden. Schließlich haben sich offenbar bisher auch die Verbraucherschutzorganisationen nicht eingeschaltet. Da Doctolib direkt Verbraucherinnen und Verbraucher adressiert, wären diese berechtigt, durch Abmahnungen gegen dessen unzulässige Praktiken vorzugehen.

Doctolib meint unantastbar zu sein. Da lässt der Deutschland-Geschäftsführer in Gesprächen gerne schon mal durchblicken, welche guten Beziehungen er in die Politik hat. Auch die Unternehmensvertreter vermitteln bei ihren Werbeterminen den Eindruck, dass Doctolib in der besonderen Gunst des Bundesgesundheitsministeriums stünde.

Was daraus folgt

Es mag Patienten geben, denen es egal ist, wenn ein Internet-Unternehmen von ihnen Daten über ihre Arztbesuche und Behandlungen sammelt. Diese sollen gerne das Angebot von Doctolib nutzen. Möchte aber ein Patient nicht, dass Doctolib über ihn Gesundheitsdaten sammelt, dann sollte er dies auch seinem Arzt oder der Gesundheitseinrichtung mitteilen. Wird dieser Widerspruch nicht respektiert, so besteht die Möglichkeit sich hierüber bei der zuständigen Datenschutzaufsichtsbehörde des Bundeslandes und bei der Heilberufekammer der jeweiligen Region zu beschweren. Verweigert ein Arzt gar die Behandlung wegen des unzulässigen Einforderns der Doctolib-Nutzung, dann ist eine Meldung gegenüber der Ärztekammer zu empfehlen. Denkbar wäre selbst eine Strafanzeige und ein Strafantrag gegen Doctolib wie gegen den Arzt. Wer sich dafür interessiert, welche Daten Doctolib gespeichert hat, der kann dort einen Auskunftsantrag gemäß Art. 15 DSGVO

stellen. Es ist jedoch zu vermuten, dass dabei nicht die Daten mitgeteilt werden, die das Unternehmen als vermeintlicher „Auftragsverarbeiter“ vom behandelnden Arzt mitgeteilt bekommen hat. Wer einen Account bei Doctolib eingerichtet hat und möchte, dass seine Daten dort gelöscht werden, dem wird empfohlen das Konto zu löschen. Dadurch ist Doctolib verpflichtet die gespeicherten Daten zu löschen. Hierauf sollte das Unternehmen ausdrücklich hingewiesen werden.

Es ist eine Binsenweisheit, dass es mit der Digitalisierung des Gesundheitswesens in Deutschland nicht zum Besten besteht. Nachdem sich insbesondere die Ärzteschaft lange Digitalisierungsbestrebungen der Gesundheitspolitik mit dem – falschen – Datenschutzargument verweigerte, hat sich der Wind für die ärztliche Vertraulichkeit gedreht: Es gibt in Deutschland offenbar massenhaft Gesundheitseinrichtungen, denen der Datenschutz und das Patientengeheimnis nicht wichtig zu sein scheinen. Informationstechnik ist heute aus der Gesundheitsversorgung nicht mehr wegzudenken – wegen der damit verbundenen Arbeitserleichterungen, der Kosteneinsparungen, der Synergiegewinne, auch wegen sinnvollen Sekundärnutzungen der digitalen Daten. Die Digitalisierung des Gesundheitswesens ist unter Wahrung von Patientengeheimnis und Datenschutz und unter Beachtung der dazu geltenden Regeln möglich.

Nominell bekennen sich alle IT-Dienstleister zum Datenschutz. Den meisten Anbietern im Gesundheitsbereich dürfte dies ein ernstes und in die Praxis umgesetztes Anliegen sein. Auch unter Einhaltung des Datenschutzes kann dabei Geld verdient werden. Bei Doctolib dient die Dienstleistung für Patienten und Gesundheitseinrichtungen vorrangig dem illegitimen und unzulässigen Datensammeln. Dabei werden die gesetzlich geforderten Grundsätze der Vertraulichkeit, der Zweckbindung, der Erforderlichkeit und der Transparenz zu disponiblen Aspekten. Es mag sein, dass das Angebot von Doctolib preisgünstig und funktional ist. Das könnte es auch sein, wenn es sich an das Datenschutzrecht halten würde.

Doctolib ist auf dem Weg die Datenverarbeitung im Gesundheitswesen von ethischen Prinzipien zu „befreien“. Das Patientengeheimnis dient dem Vertrauen der Patienten in die Heilberufler und in das gesamte Gesundheitssystem. Die Expansion Doctolibs erinnert an den „Erfolg“ der Unternehmen des Silicon Valleys seit über 20 Jahren. Diese sichern sich informationstechnische Dominanz und Profit zulasten der digitalen Grundrechte und gefährden dabei zugleich die Rechtsstaatlichkeit im digitalen Raum des Internets. Die Gesundheitsdatenverarbeitung in Europa war bisher von diesem Trend noch nicht erfasst. Das kann sich aber schnell ändern, wenn Anbietern wie Doctolib weiterhin freie Hand gelassen wird. Vorrangig sind die Aufsichtsbehörden, aber auch die Heilberufekammern, der Verbraucherschutz, die Standes- und die Patientenvertretungen aufgefordert dies zu verhindern.

1 Netzwerk Datenschutzexpertise, Arztterminvermittlung über Doctolib, 08.06.2021, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/bba_2021_doctolib.pdf.

2 test 1/2021, 92 ff., https://www.test.de/Arzttermin-Portale-im-Test-Ganz-schoen-unsensibel-5692512-0/; Risiken und Nebenwirkungen von Termin-Management-Systemen, www.zm-online.de 16.10.2021.

3 Netzwerk Datenschutzexpertise, Arztterminvermittlung über Doctolib, 08.06.2021 https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2021_doctolib.pdf, (NW DSE Gutachten 1).

4 Netzwerk Datenschutzexpertise, Doctolib geht gegen Konkurrenten wegen Datenschutzkritik vor, 25.10.2023 (NW DSE Gutachten 3), https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2023doctolib_update2.pdf, S. 3, 5; Netzwerk Datenschutzexpertise, Datenschutz bei Doctolib, 28.07.2022 (NW DSE Gutachten 2), https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2022doctolib_update.pdf, Kap. 7 (S. 16 f).

5 Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Jahresbericht (JB) 2019, Kap. 6.3 (S. 103 ff.).

6 BlnBDI, JB 2021, Kap. 1.3.1. (S. 30 ff.), 6.5 u. 6.6 (S. 92 ff.).

7 BlnBDI JB 2022, Kap. 52 (S. 57 ff.).

8 NW DSE Gutachten 1, S. 32.

9 https://media.doctolib.com/image/upload/mkg/file/doctolib_erhaelt_c5-testat_des_bsi.pdf.

10 NW DSE Gutachten 2.

11 https://www.youtube.com/watch?v=jwW8mNzBtcw.

12 https://www.ardaudiothek.de/episode/zeitfragen-feature-deutschlandfunk-kultur/patientendaten-das-faible-der-aerzte-fuer-doctolib/deutschlandfunk-kultur/12901239/.

13 NW DSE Gutachten 3.

14 EuGH 05.06.2028 – C-210/16.

15 Zur rechtlichen Bewertung s. Weichert MedR 2024, 84 ff.

16 https://info.doctolib.de/krankenhaus-mvz/.

17 Hoffmann, Patientenmanager von Doctolib, https://www.handelsblatt.com/inside/digital-health/doctolib-start-up-launcht-patientenmessenger/29530912.html, 29.11.2023.

18 Betz, Doctolib und der Datenschutz, SZ 09.08.2023, 12; Sana beauftragt Doctolib mit digitalen Patientenservices; www.sana.de März 2023.

19 Neuer Meilenstein auf dem Weg zur digitalen Arzt-Patienten-Kommunikation: Doctolib entlastet Ärzt:innen jetzt auch bei Patientenanfrage, https://about.doctolib.de/news 13.06.2023.

20 Hoffmann/Rybicki, Gesundheitsbranche Doctolib kauft Medizin-Messenger Siilo, www.handelsblatt.com 07.03.2023; www.crunchbase.com/organization/doctolib/company_financials, www.siilo.com/de/uber-siilo.

21 Doctolib bringt eigene Praxissoftware auf den Markt, www.apotheke-adhoc.de 16.03.2022.

22 https://info.doctolib.de/krankenhaus-mvz/.

23 KZHG steht für Krankenhauszukunftsgesetz.

24 https://about.doctolib.de/news/charite-universitatsmedizin-berlin-setzt-auf-das-patientenportal-von-doctolib/.

25 https://about.doctolib.de/news/doctolib-und-adac-kooperieren-fuer-einfachen-zugang-zur-digitalen-gesundheitsversorgung/.

26 https://www.datenschutz-berlin.de/themen/gesundheit/terminverwaltung/.

27 6. Jahresbericht der Landesbeauftragten für Datenschutz Bremen nach der Europäischen Datenschutzgrundverordnung-Berichtsjahr 2023, Kap. 8.3 (S. 48 f.).

28 NW DSE Gutachten 3, Kap. 7 (S. 13 ff.); NW DSE Gutachten 2, Kap. 3.2 (S. 12 f.).

Rolf Gössner

40 Jahre Volkszählungsurteil

Zum Grundrecht auf Informationelle Selbstbestimmung - und was daraus geworden ist[1]

Mit einem harmlos wirkenden Statistikvorhaben erzielten staatliche Planer in den 1980er Jahren der alten Bundesrepublik wider Willen ungeahnte gesellschaftliche Breitenwirkung: mit der berühmt-berüchtigten Volkszählung. Da alle Haushalte der Republik laut Volkszählungsgesetz gezwungen waren hieran teilzunehmen, lief es auf die Erfassung der gesamten Bevölkerung hinaus – mithilfe von Tür-zu-Tür-Befragungen und elektronischer Datenverarbeitung.

Nicht zuletzt aus diesem Grund war dieses staatliche Vorhaben geeignet das Bewusstsein der Bevölkerung zu sensibilisieren und den Massenprotest zu beflügeln. Unterschiedlichste gesellschaftliche Kräfte fanden sich zu Bürgerinitiativen zusammen, um sich zu informieren, darüber aufzuklären und den Protest zu organisieren. Es waren ohnehin Zeiten erstarkender politischsozialer Protest- und Widerstandsbewegungen, wie etwa der Anti-Atomkraft- oder der Friedensbewegung. Und so wirkte auf diesem widerständigen Hintergrund die Volkszählung wahre Wunder und erhitzte die Gemüter der damaligen Zeit bis hinein ins konservative Bürgertum.

Zum ersten Mal begannen damals unzählige Menschen zu erahnen, dass nicht allein soziale, politische oder gar kriminelle „Außenseiter" Subjekte staatlicher Erfassungs- und Kontrollbegierde sein können, sondern auch sie selbst mit all ihren normalen Alltagsleben und „abweichenden" Verhaltensweisen. Die detaillierten Fragen nach Ausbildung und Studium, Beruf und Erwerbstätigkeit, Arbeitsstelle und Arbeitsweg, Einkommen und Familienstand, Wohnungssituation und Miethöhe, Kinderbetreuung und Mobilität, Finanzen und Freizeit wurden jedenfalls rasch als Angriff auf Privatsphäre und Persönlichkeitsrechte empfunden. Zwar wurde den zu Befragenden per Gesetz Anonymität zugesichert, doch sollte es den Verwaltungen gleichwohl gestattet sein die erhobenen Daten mit ihren Einwohnermelderegistern hinsichtlich Namen, Anschriften, tatsächlichen Wohnsitzen, Geburtsdaten, Konfessionen und Staatsangehörigkeiten abzugleichen. Die versprochene Anonymität schien damit jedenfalls mehr als zweifelhaft.

Aus diesem Gefühl eigener Betroffenheit begann sich eine wahre Datenschutzbewegung zu entwickeln: Zahlreiche Volkszählungsboykott-Initiativen schossen aus dem Boden, massenweise versammelten sich Betroffene in Riesensälen und Stadthallen, um sich informieren zu lassen und zu debattieren. An etlichen dieser Initiativen und Großereignisse habe ich selbst aktiv mitgewirkt – just in der Anfangsphase meiner Berufstätigkeiten als Rechtsanwalt, Publizist und Referent. Die personenbezogene Nachfrage wurde insbesondere dadurch befördert, dass in jener Zeit mein erstes Buch „Der Apparat. Ermittlungen in Sachen Polizei" (Köln 1982), das ich zusammen mit dem damaligen Wallraff-Mitarbeiter Uwe Herzog verfasst hatte, zum Bestseller wurde. Die vielen besorgten Fragen, die uns seinerzeit erreichten, drehten sich insbesondere um staatliche Überwachungsmöglichkeiten, Datenaustausch und –missbrauch. Sie gingen auch weit über den konkreten Anlass der Volkszählung hinaus und zeugten nicht selten von mehr oder weniger diffusen Ängsten vor fortschreitender Computerisierung, Verdatung und Kontrolle. Kurz: vor dem drohenden „gläsernen Bürger", also vor zunehmender „Durchleuchtung" der Menschen und ihres Verhaltens.

Wir befanden uns schließlich, was wir seinerzeit nur erahnen konnten, am Beginn einer neuen Ära: auf dem Weg in eine moderne Informationsgesellschaft, die sich mit der beschleunigten digitalen Durchdringung von Staat und Gesellschaft herauszubilden begann und allmählich sämtliche Lebensbereiche tangierte. Die enormen Fortschritte und Vorteile einer solchen technologischen Entwicklung waren angesichts der ungewissen Entwicklungs- und Veränderungspotentiale und all ihrer problematischen bis gefährlichen Nebenwirkungen von starken Umwälzungs- und Zukunftsängsten begleitet. Was die gefährlichen Nebenwirkungen anbelangt: vollkommen zu Recht, wie wir mittlerweile längst erfahren mussten.

Doch trotz Widerstandsgeistes und Bereitschaft zum Zivilen Ungehorsam gegen die Volkszählung und gegen die damit verbundenen Risiken: Die Bewegung fokussierte sich immer mehr auf die bange Frage „Was tun, wenn der Zähler zweimal klingelt? Was tun, wenn im Falle der Verweigerung Zwangsgelder, Erzwingungshaft oder Ordnungswidrigkeitsverfahren drohen?" Und sie degenerierte damit in weiten Teilen still und leise zu einer bloßen Rechtshilfebewegung, die das Große und Ganze, also die staatlichen Ausforschungs- und Kontrollfunktionen und ihre gesellschaftlichen Folgen allmählich aus dem Blick zu verlieren drohte.

***

Und dennoch lieferte diese außerparlamentarische Opposition die kritische Grundstimmung, Einschätzung und Dynamik für eine erfolgreiche juristische Gegenwehr: Zahlreiche Verfassungsbeschwerden führten zu dem berühmten und wegweisenden Volkszählungsurteil, mit dem das Bundesverfassungsgericht am 15. Dezember 1983 (Az. 1 BvR 209/83) die Vollerfassung der Bevölkerung und das zugrunde liegende Volkszählungsgesetz wegen Verfassungswidrigkeit weitgehend kippte. Ich kann mich noch gut daran erinnern, wie ich wenige Tage vor der gerichtlichen Aussetzung der Volkszählungsdurchführung während einer Pressekonferenz der Fraktion „Die Grünen" im Bundestag nochmals eindringlich vor dieser Art

von Datenerfassung gewarnt hatte und deren Boykott begründete: ein Statement, das die „Tagesschau“ zu bester Sendezeit ausstrahlte mitsamt der abschließenden Mahnung: „Es ist fünf Minuten vor 1984“ – mit Bezug auf George Orwells dystopischen Roman „1984“, der in jener Zeit viel gelesen und zitiert wurde.

Mit dem Volkszählungsurteil wird der Datenschutz erstmals zum neuen Grundrecht gekürt: das Grundrecht auf „informationelle Selbstbestimmung“ als besondere Ausprägung des Persönlichkeitsrechts (Recht auf freie Entfaltung der Persönlichkeit, Art. 2 Abs. 1 Grundgesetz) und der unantastbaren Menschenwürde (Art. 1 Abs. 1 GG). Danach kann jeder Mensch grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten entscheiden. Seitdem gilt jede personenbezogene Datenerhebung, -speicherung, -verarbeitung und -verwendung als Eingriff in dieses Grundrecht und benötigt eine gesetzliche Rechtsgrundlage. In dieses Grundrecht durfte also fortan nur aufgrund bereichsspezifischer Gesetze, im überwiegenden öffentlichen Interesse und unter Beachtung der verfassungsmäßigen Verhältnismäßigkeit eingegriffen werden.

Wesentliche Leitsätze des Urteils, das weit über die Volkszählung hinaus Bedeutung hat, sind auch heute noch hoch aktuell. Deshalb seien sie hier kurz in Erinnerung gerufen:

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen…“

„Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“

„Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“

Nachdem die Volkszählung 1983 für weitgehend rechts- und verfassungswidrig erklärt worden war, fand sie 1987 auf neuer, nun verfassungskonformer Rechtsgrundlage statt. Es war die letzte „Vollerfassung“ in der Bundesrepublik – ebenfalls begleitet von zahlreichen Protesten, Bürgerinitiativen und Verweigerungsaktionen mit Parolen wie „Politiker fragen – Bürger antworten nicht“, „Lasst Euch nicht erfassen“, „meine Daten könnt ihr raten“ oder „meine Daten gehören mir“. Etliche Verweigerungen wurden mit Zwangs- und Bußgeldern sanktioniert und Boykott-Initiativen von Verfassungsschutz-Behörden unter Beobachtung gestellt.

Drei Jahre nach dieser Volkszählung und sieben Jahre nach dem Volkszählungsurteil als Meilenstein in der Geschichte des Datenschutzes folgte dann 1990 ein neues Bundesdatenschutzgesetz, das die verfassungsgerichtlichen Vorgaben weitgehend berücksichtigte. Dieses Gesetz ebnete fortan auch dem „Zensus“, also einer Teilzählung anstelle der zuvor üblichen Vollerfassung den Weg: so dem EU-weiten Zensus 2011 und dem letzten Zensus 2022. Mit Haushalte-Befragungen bei rund 10 Prozent der Bevölkerung soll alle zehn Jahre ermittelt werden, wie viele Menschen hierzulande leben, wie sie ausgebildet sind, wohnen und arbeiten etc. Um Ergebnisse für ganz Deutschland zu erhalten, werden diese Daten mithilfe statistischer Verfahren auf die gesamte Bevölkerung hochgerechnet. Damit sollen laut Bundesinnenministerium Fragen wie „Gibt es genügend Wohnungen? Brauchen wir mehr Schulen, Studienplätze oder Altenheime? Wo muss der Staat für seine Bürger:innen investieren?“ beantwortet werden, um den Planungsbedarf zu ergründen.

***

Zurück zum Volkszählungsurteil von 1983 und wie es weiterging: Diese bahnbrechende Entscheidung des Bundesverfassungsgerichts führte in der Folgezeit, anders als erwartet, nicht etwa dazu, den wuchernden Datenwildwuchs in allen möglichen staatlichen, kommerziellen und privaten Bereichen zu zügeln. Er wurde eher übersichtlicher und effizienter ausgestaltet und dann mit zahlreichen Gesetzesgrundlagen rechtlich abgesichert, wie es das Urteil ja verlangt. Tatsächlich kam es zu wahren Legalisierungswellen, mit denen immer mehr Eingriffs-, Überwachungs- und Datenübermittlungsbefugnisse verrechtlicht wurden – besonders für Polizei und Geheimdienste des Bundes und der Länder (inklusive etlicher verfassungswidriger Regelungen).

Letztlich sehen wir uns angesichts der digitalen und sicherheitsstaatlichen Entwicklung mit der Gefahr einer Unterhöhlung des Grundrechts auf Informationelle Selbstbestimmung konfrontiert, die auch verfassungsgerichtlich nur unzureichend gebannt werden kann. Dabei zeigte sich deutlich: Die Volkszählung der 1980er Jahre war wirklich harmlos gegen das, was uns seitdem mit der rasanten Entwicklung der modernen Informationsgesellschaft und der wachsenden digitalen Kontroll- und Überwachungsdichte im öffentlichen und privaten Raum drohte: nämlich ein präventiver Sicherheits- und Überwachungsstaat sowie eine kommerzielle Kontrollgesellschaft.

Im Zuge dieser technologischen Entwicklung haben sich auch die persönlichen Überzeugungen und Verhaltensweisen von Nutzern und Betroffenen gewandelt: Sie nutzen die neuen Techniken und Innovationen intensiv und

oft, aber auch oft recht freizügig und naiv – ohne sich groß um die damit verbundenen Gefahren des Überwachungs- und Kontrollpotentials zu scheren. Das Datenschutzbewusstsein scheint angesichts der Abstraktheit virtueller Bedrohung rapide zu verkümmern, ebenso die Achtung vor der eigenen und fremden Privat- und Intimsphäre – ganz besonders im Umgang mit „sozialen" Netzwerken wie Facebook, Instagram & Co.

Im Laufe der Entwicklung der Informationsgesellschaft haben sich regelrechte Datenkraken im privat-kommerziellen Bereich und im Öffentlichen Dienst herausgebildet. Und zwar mit einer ungeheuren Eingriffsmassivität und -intensität. Im Gegensatz zur Volkszählung und zum Zensus, die nur eine Augenblicksaufnahme darstellen, ist längst die permanente Erfassung von Daten über alltägliche Lebensvorgänge alltäglich geworden – etwa mittels unzähliger Überwachungskameras oder Verkehrsdaten, die u.a. bei Telekommunikation, Onlineshopping und der gesamten Internetnutzung anfallen. Die meisten Menschen hinterlassen pausenlos Datenspuren, die personalisierte Daten- und Persönlichkeitsprofile sowie Rückschlüsse auf ihr Surf- und Konsumverhalten ermöglichen, letztlich auf ihr gesamtes berufliches und privates Leben.

Wohl auch angesichts dieser weiteren Entwicklung hob das Bundesverfassungsgericht 2008 abermals ein neues Grundrecht für das digitale Zeitalter aus der Taufe: das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme" – kurz: „Computergrundrecht" genannt, das jedoch seither in der Praxis und per Gesetz ebenfalls immer wieder stark eingeschränkt worden ist. Auch hiergegen laufen wegen mutmaßlicher Verfassungswidrigkeit etliche Verfassungsbeschwerden.

1 Dieser Beitrag wurde zuerst veröffentlicht unter: https://www.ossietzky.net/artikel/40-jahre-volkszaehlungsurteil/1

Rolf Gössner

Der Weg in den digital-präventiven Sicherheits- und Überwachungsstaat[1]

Nach unserem Blick zurück ins letzte Jahrtausend, auf Volkszählung, Boykottbewegung und 40 Jahre Volkszählungsurteil (1983), fragen wir uns: Was ist aus dem seinerzeit vom Bundesverfassungsgericht aus der Taufe gehobenen neuen Grundrecht auf informationelle Selbstbestimmung eigentlich geworden? Schließlich handelte es sich dabei um eine wegweisende Entscheidung just in der Anfangsphase einer gesellschaftlichen und staatlichen Transformation, die uns mit einer rasanten Digitalisierung in die moderne Informationsgesellschaft katapultierte.

Bei der Beantwortung dieser Frage konzentrieren wir uns auf das staatliche System Innerer Sicherheit. Einen epochalen Einschnitt erfuhr die Sicherheitspolitik des Westens und damit auch der Bundesrepublik mit den staatlichen Reaktionen auf die Terror-Anschläge in den USA vom 11. September 2001. Hierzulande bescherte uns ein teils ausufernder Antiterrorkampf die umfangreichsten Sicherheitsgesetze, die in der bundesdeutschen Rechtsgeschichte jemals auf einen Streich verabschiedet worden sind (2002 ff.). Polizei- und Geheimdienstbefugnisse wurden stark ausgeweitet und Migranten, besonders Muslime unter ihnen, quasi unter Generalverdacht gestellt und einer noch intensiveren Überwachung unterzogen. Diesen „Sicherheitsgesetzen" folgten mehrere „Terrorismusbekämpfungsergänzungsgesetze", ein „Videoüberwachungsverbesserungsgesetz" sowie Verschärfungen der Polizeigesetze in Bund und Ländern (2016 ff.). Damit wurden Polizeiaufgaben und Überwachungsbefugnisse – wie heimliche Online-Durchsuchung von Computern mit Staatstrojanern oder elektronische Fußfesseln und Präventivhaft für „Gefährder" – weit ins Vorfeld konkreter Gefahren und möglicher Straftaten verlagert, zu Lasten von Grund- und Freiheitsrechten und rechtsstaatlichen Prinzipien.

Ein Beispiel zur Veranschaulichung der Problematik: Mit der inzwischen polizeirechtlich und auch geheimdienstlich zulässigen Online-Durchsuchung per Staatstrojaner bricht der Staat massiv in Privat- und Intimsphäre, Persönlichkeitsrechte und informationelle Selbstbestimmung der Betroffenen ein. So kann die Polizei unbemerkt auf Telekommunikation, gespeicherte Festplatteninhalte, intimste Informationen, Fotos und Filme zugreifen. Es handelt sich um einen schweren Grundrechtseingriff, einen Einbruch in alle Lebensbereiche bis hinein in Gedanken- und Gefühlswelten der Betroffenen und ihrer Kontaktpersonen, das heißt auch von unbeteiligten Dritten. Staatstrojaner öffnen darüber hinaus Missbrauch und gefährlichen Cyberattacken Krimineller Tür und Tor. Denn die Polizei nutzt dabei Sicherheitslücken in der Software längerfristig für die heimliche Einschleusung ihrer Staatstrojaner, anstatt diese Sicherheitslücken sofort schließen zu lassen. So gerät die gesamte Infrastruktur in Gefahr, zulasten der Allgemeinheit und unter Aushöhlung des *„Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität von IT-Systemen"*, das das Bundesverfassungsgericht 2008 angesichts der technologischen Entwicklung und ihrer Gefahren proklamiert hatte.

Man könnte angesichts dieser Gesetzesentwicklung auch von ausufernden „Notstandsgesetzen für den Alltag" sprechen und von einem präventiven Sicherheitsstaat, der sich auf den Weg zum Überwachungsstaat macht. Mit der zur Maßlosigkeit neigenden Präventionslogik verkehren sich auch die Beziehungen zwischen Bürger und Staat: Die Unschuldsvermutung, eine der wichtigsten rechtsstaatlichen Errungenschaften, büßte so ihre Staatsmacht begrenzende Funktion ein. Der Mensch mutiert tendenziell zum potentiellen Sicherheitsrisiko, und muss unter Umkehr der Beweislast seine Harmlosigkeit und Unschuld nachweisen; auf der anderen Seite wird die „Sicherheit" quasi zum „Supergrundrecht", das die Grundrechte mehr und mehr in den Schatten zu stellen droht. Dabei gerät in Vergessenheit, dass es weder in einer hoch technisierten Risikogesellschaft, in der wir ja leben, noch in einer offenen, liberalen Demokratie absoluten Schutz vor Gefahren und Gewalt geben kann.

Terror und Terrorangst stärken die Staatsgewalt und entwerten Freiheitsrechte – das hat sich seit 9/11 immer wieder deutlich gezeigt. Tatsächlich mussten Bundesverfassungsgericht (BVerfG) und Europäischer Gerichtshof für Menschenrechte mehrfach maßlose Antiterrorgesetze und Sicherheitsmaßnahmen und deren digitale Potentiale ganz oder teilweise für verfassungswidrig erklären. Erinnert sei nur an den „Großen Lauschangriff" mit elektronischen Wanzen in und aus Wohnungen (in diesem Zusammenhang hat das BVerfG 2004 den *„Kernbereich privater Lebensgestaltung"* unter absoluten Schutz gestellt), an die präventive Telekommunikationsüberwachung oder den Fluggast-Datentransfer an US-Sicherheitsbehörden. Auch die exzessiven Rasterfahndungen nach „islamistischen Schläfern" sind für verfassungswidrig erklärt worden, ebenso präventive Terrorabwehrbefugnisse des Bundeskriminalamtes und die anlasslose Vorratsspeicherung von Telekommunikationsdaten der gesamten Bevölkerung. Zu diesen ohne Verdacht auf Vorrat gespeicherten Massendaten gehörten Verkehrs-, Standort-, Teilnehmer- und andere Daten aller Telekommunikationsvorgänge (mit Ausnahme des eigentlichen Inhalts). Könnte ja sein, dass sie später eventuell zu Strafermittlungszwecken benötigt werden.

Hiergegen hatte ich 2008 in Kooperation mit dem *Arbeitskreis Vorratsdatenspeicherung* (AK Vorrat) und dem Datenschutz- und Bürgerrechtsverein *„Digitalcourage"* Verfassungsbeschwerde vor dem BVerfG eingelegt – und zwar zusammen mit fast 35.000 Menschen. Es war die bis dahin größte Massenbeschwerde in der bundesdeutschen Rechtsgeschichte. Daraufhin erklärte das BVerfG 2010 diese Regelung für weitgehend verfassungswidrig, so dass die Unmengen auf Vorrat gespeicherter Kommunikationsdaten wieder gelöscht werden mussten. Auch die daraufhin abgeänderte Vorratsdatenspeicherung (2015) ist rechtswidrig sowie mit EU-Recht unvereinbar, so der Europäische Gerichtshof für Menschenrechte im September 2023. Eine allgemeine und unterschiedslose Speicherung und Sammlung von Kommunikationsdaten sei mit den Grundrechten auf Privatsphäre, Datenschutz und Meinungsfreiheit unvereinbar. Auch gegen die gesetzliche Ermächtigung von Polizei und Geheimdiensten, heimlich Staatstrojaner in Computersysteme zur Online-Durchsuchung einschleusen zu können, haben wir 2018 Verfassungsbeschwerde eingelegt; weitere Beschwerden sind anhängig.

2020 erklärte das BVerfG die weltweite Massenüberwachung („strategische Auslandsaufklärung") durch den Auslandsnachrichtendienst BND für weitgehend verfassungswidrig und stärkte damit internationale Menschenrechte und Pressefreiheit (Urteil, Mai 2020). Auch die „Bestandsdatenauskunft", also der staatliche Zugriff auf personenbezogene Daten von Telekommunikationsdienste-Anbietern über ihre Kund:innen ist schon zum zweiten Mal für verfassungswidrig erklärt worden (letztes Urteil, Mai 2020); und eine Norm des „Antiterrordatei- Gesetzes" (ATDG) verstößt, so das BVerfG, gegen das *Grundrecht auf Informationelle Selbstbestimmung* und ist damit verfassungswidrig und nichtig (Urteil, Nov. 2020). Auch Datenübermittlungsbefugnisse im Nachrichtendienstrecht (Verfassungsschutz, BND, Militärischer Abschirmdienst), mit denen das Gebot der Trennung von Geheimdiensten und Polizei unterlaufen werden kann, hielten den verfassungsrechtlichen Vorgaben und Ansprüchen des Gerichts nicht Stand (2022). Ob die daraufhin erfolgte Neuregelung der Befugnisse vom November 2023 tatsächlich in Gänze verfassungskonform geraten ist, ist allerdings mehr als fraglich.

Wie oft hatte ich im Laufe der Jahrzehnte als parlamentarischer Sachverständiger die Abgeordneten vor der Verfassungswidrigkeit einzelner Sicherheitsgesetze oder Bestimmungen gewarnt. Zumeist allerdings ohne durchschlagenden Erfolg – wurde jedoch in mehreren Fällen etliche Jahre später verfassungsgerichtlich ganz oder teilweise bestätigt. Die Verfassungsgerichte rügten in all diesen Fällen, dass Regierungen und Parlamentsmehrheiten Grund- und Bürgerrechte, die Menschenwürde und den Kern privater Lebensgestaltung unhaltbaren Sicherheitsversprechen und einer vermeintlichen Sicherheit geopfert hatten. Die ausgesprochen hohe Anzahl verfassungswidriger Gesetze dokumentiert letztlich ein bedenklich verkümmertes Verfassungsbewusstsein in der politischen Klasse und in mancher Sicherheitsbehörde. Strenggenommen ein Fall für den „Verfassungsschutz", der jedoch eher harsche Kritik an verfassungsverletzenden Institutionen zum Anlass nimmt, um gegen Kritiker wegen *„verfassungsschutzrelevanter Delegitimierung des Staates"* vorzugehen.

Wir mussten durch die Jahrzehnte hindurch erleben, dass mit Staatsschutz-, Sicherheits-, Überwachungs- und Antiterror-Gesetzen, aber auch mit Asyl- und Migrationsgesetzen die Menschenwürde, Grund- und Freiheitsrechte immer wieder schwer beschädigt werden. Insgesamt und strukturell betrachtet machte sich der demokratische Rechtsstaat, wie bereits angedeutet, auf den Weg in Richtung eines präventiv-autoritären Sicherheits- und Überwachungsstaats – eines Staates, der demokratisch immer schwerer kontrollierbar ist, in dem der Mensch zum Sicherheitsrisiko zu mutieren droht, in dem Rechtssicherheit und Vertrauen der Bürger allmählich verloren gehen. Mit einem weiteren ungezügelten Siegeszug „Künstlicher Intelligenz" (KI) wird sich die Problematik noch potenzieren.

Zwar lässt sich die Mehrheit der Bevölkerung mit Angstpolitik und durch unhaltbare Sicherheitsversprechen von

Parteien und Regierungen immer wieder beschwichtigen – oder besser gesagt: hintergehen. Dennoch regte und regt sich durch die Jahrzehnte hindurch auch immer wieder außerparlamentarischer Protest, der zuweilen Abertausende Menschen auf die Straßen treibt. Getragen und betrieben wird die Oppositionsarbeit von durchaus breiten zivilgesellschaftlichen Bündnissen unter Beteiligung vieler Bürgerrechts- und Datenschutz-Organisationen, aber auch von Friedens-, Klima- und Umweltvereinigungen. Erinnert sei etwa an die großen Demos und Kundgebungen *„Freiheit statt Angst“* sowie an die Gründung und Arbeit von Datenschutzorganisationen und Gruppen, wie *ChaosComputerClub, Digitalcourage, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Deutsche Vereinigung für Datenschutz* oder *Gesellschaft für Freiheitsrechte*. Sie alle kümmern sich um die Grundrechte auf Privat- und Intimsphäre, auf informationelle Selbstbestimmung und Anonymität in digitalen Sphären und betreiben „digitale Selbstverteidigung“. Unter anderem auch, wie *Digitalcourage* in Bielefeld, mithilfe der jährlichen Verleihung des Negativpreises *BigBrotherAward* (BBA) an Datenschutzfrevler in Staat, Wirtschaft und Gesellschaft. 20 Jahre lang durfte ich an diesem Aufklärungsprojekt als Jurymitglied und Laudator teilhaben und mitwirken. Die prekäre Entwicklung in dieser Zeitspanne von 2000 bis 2020 habe ich in *„Datenkraken im Öffentlichen Dienst. ‚Laudatio‘ auf den präventiven Sicherheits- und Überwachungsstaat“* (PapyRossa, Köln 2021) Revue passieren lassen und zwar anhand der BBA-Verleihungen an Datenfrevler in Politik, Regierungen und Staatsapparat. Auch im jährlichen *„Grundrechte-Report. Zur Lage der Bürger- und Menschenrechte in Deutschland“* sind regelmäßig Fälle gravierender Grundrechtsverletzungen im digitalen Zeitalter dokumentiert und nachzulesen.

Solche Aufklärungs- und Oppositionsaktivitäten lassen jedenfalls hoffen, gerade weil selbstbewusster und starker Protest und Widerstand dringender sind denn je. Grund- und Freiheitsrechte müssen Tag für Tag verteidigt, fortentwickelt oder aber neu erkämpft werden. Und es ist höchste Zeit für eine längst überfällige unabhängige Evaluierung aller bisherigen Sicherheits- und Antiterror-Gesetze und ihrer konkreten Anwendung, und zwar als Basis für eine „Überwachungsgesamtrechnung“, wie sie vom BVerfG bereits 2010 angemahnt worden ist (Az 1 BvR 256/08, Rn. 1). Eine solche Bilanzierung und Evaluierung, die auch demokratische Transparenz schaffen soll, wird übrigens von der Ampelregierung angestrebt und soll bis Ende 2024 umgesetzt werden. Dann ist auch die Einrichtung einer „Freiheitskommission“ geplant, die auf Grundlage der jeweiligen Überwachungsgesamtrechnung bei künftigen sicherheitspolitischen Gesetzesvorhaben beraten soll. Es bleibt abzuwarten und kritisch zu begleiten, wie dieses durchaus sinnvolle Gesamtvorhaben umgesetzt wird – schließlich geht es um die Gewährleistung einer grundrechtsbasierten Innen- und Rechtspolitik, die in der Summe ihrer Sicherheitsgesetze das für eine Demokratie erträgliche Maß an Überwachung (aus Sicherheitsgründen) nicht überschreiten darf. Nur so lässt sich vermeiden oder rückgängig machen, dass das freiheitliche demokratische Gemeinwesen allmählich unterminiert und von innen heraus geschädigt wird, wie es in der Realität wohl längst passiert.

1 Dieser Beitrag wurde zuerst veröffentlicht unter: https://www.ossietzky.net/artikel/digital-praeventiver-sicherheitsstaat/

Offener Brief: Moderne ePrivacy-Gesetzgebung muss Grundrechte schützen

Am 24.04.2024 forderten EDRi und 13 weitere Organisationen, darunter die DVD und Digitalcourage, die künftige Europäische Kommission auf, umfassende Pläne zur Reform der ePrivacy-Gesetzgebung der Europäischen Union wieder aufzunehmen und die Datenschutz-Grundverordnung (DSGVO) zu ergänzen und zu präzisieren.

Brüssel, den 24.04.2024

Zur Kenntnis des Binnenmarktkommissars der Europäischen Union, Thierry Breton, der Vizepräsidentin der Europäischen Kommission, Věra Jourová, und der Kommissarin für Inneres, Ylva Johansson

CC/ Kabinett des Europäischen Kommissars für Justiz

Für den Schutz der Grundrechte ist die Modernisierung der Gesetzgebung zum Datenschutz bei der elektronischen Kommunikation von zentraler Bedeutung

Im Januar 2017 schlug die Europäische Kommission eine Aktualisierung der aus dem Jahr 2002 stammenden Datenschutzrichtlinie für elektronische Kommunikation vor – wodurch neue Regeln für die Vertraulichkeit elektronischer Kommunikation und die Verwendung von Cookies und anderen Online-Tracking-Technologien festgelegt werden sollten. Sieben Jahre später haben die EU-Mitgliedstaaten und Unternehmen (insbesondere Werbefirmen, Verlage und Telekommunikationsbetreiber) diese wichtige Reform erfolgreich blockiert – entgegen den Forderungen aus der Zivilgesellschaft und von Einzelpersonen, die sich offen für mehr Datenschutz und Sicherheit in der Online-Kommunikation einsetzen [1]. Gemäß den Schlussfolgerungen des Rates über die Zukunft der EU-Digitalpolitik bestehen nach wie vor weit verbreitet Probleme im digitalen Sektor. Wir, die unterzeichnenden Organisationen, bekräftigen weiterhin die Notwendigkeit einer soliden Gesetz-

gebung. Diese ist dringender denn je, um die Datenschutz-Grundverordnung (DSGVO) zu ergänzen und zu spezifizieren. Wir fordern daher die kommende Europäische Kommission auf umfassende Pläne für die Reform der ePrivacy-Gesetzgebung der EU vorzulegen.

In den letzten Jahren gab es besorgniserregende Debatten über einige von der Datenschutzrichtlinie für elektronische Kommunikation behandelte Aspekte in verwandten Gesetzen wie dem Gesetz über digitale Dienste (Digital Services Act – DSA) und dem politischen Druck der Mitgliedstaaten zur Beibehaltung ihrer nationalen Gesetze zur Vorratsdatenspeicherung [2]. Die bestehenden Regelungen sind unzureichend, um die erwiesenen Schäden durch kommerzielle und staatliche Überwachungstechnologien zu bekämpfen. Wir haben bereits in der Vergangenheit darauf hingewiesen, dass einige Mitgliedstaaten geneigt zu sein scheinen den einseitigen Geschäftsinteressen einiger weniger großer Technologieunternehmen und der pauschalen Ausnahme für die nationale Sicherheit, die staatliche Eingriffe und Missbräuche ermöglichen kann, Vorrang vor den Grundrechten des Einzelnen einzuräumen. Wir sind zudem beunruhigt, dass Maßnahmen gefördert werden, die keinen umfassenden Grundrechtsschutz bieten wie z.B. freiwillige Selbstverpflichtungen von Unternehmen oder die zunehmende Akzeptanz des Musters „pay or okay“ (Bezahlen oder Akzeptieren), mit dem echte und freie Wahlmöglichkeiten ausgehöhlt werden, und dass sich eine Zukunft abzeichnet, in der die Privatsphäre zur Ware verkommt. Nicht zuletzt erinnern der Einsatz von Spyware und wiederkehrende Skandale im Zusammenhang mit staatlicher Überwachung daran, wie der Einsatz von Überwachungssoftware das in der Datenschutzrichtlinie für elektronische Kommunikation verankerte Recht auf Schutz von Endgeräten verletzt. Dieses Verbot sollte in jedem Fall in künftigen Regelungen bestehen bleiben.

Die durch die Beibehaltung unserer Online-Datenschutzstandards auf dem Niveau von 2002 bestehenden Wirkungen zeigen sich in alarmierender Weise im jüngsten Vorschlag zur Verlängerung der angeblich befristeten Ausnahmeregelung für bestimmte Abschnitte der Datenschutzrichtlinie für elektronische Kommunikation aus dem Jahr 2002 [3]. Diese Verlängerung zielt vorrangig darauf ab, dass Online-Material über sexuellen Kindesmissbrauch durch Kommunikationsunternehmen erkannt wird. Dieser Ansatz führt jedoch zu einer Massenüberwachung, da den Unternehmen erlaubt wird, die private Kommunikation von Einzelpersonen dauernd automatisch zu scannen. Ihm fehlt zudem eine solide Rechtsgrundlage; der Ansatz wurde gegenüber weniger einschneidenden Maßnahmen vorgezogen, über welche die Überwachung auf legitime Verdächtige beschränkt würde, was mit den Grundsätzen eines ordnungsgemäßen Verfahrens und den vom Europäischen Gerichtshof immer wieder hervorgehobenen Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit im Einklang stünde.

Will die EU die Grundfreiheiten stärken und einen funktionierenden digitalen Binnenmarkt gewährleisten, so ist eine Aktualisierung der Datenschutzrichtlinie für elektronische Kommunikation unumgänglich. Die Datenschutzstandards für die Vertraulichkeit der Kommunikation und den Schutz vor Online-Tracking in der Datenschutzrichtlinie für elektronische Kommunikation von 2002 müssen beibehalten und zugleich modernisiert werden, um den technologischen Entwicklungen seit 2002 Rechnung zu tragen. Es muss dringend verhindert werden, dass der durch die Datenschutz-Grundverordnung gewährleistete Schutz personenbezogener Daten durch vorherrschende kommerzielle Interessen an Tracking-basierter Werbung und anderen datengesteuerten Geschäftsmodellen oder durch staatliche Eingriffe, die auf der massiven Erhebung personenbezogener Daten beruhen, untergraben wird. Wir wissen, dass dies durch verschiedene Maßnahmen und auf legislativem Wege erreicht werden kann. Daher fordern wir die Europäische Kommission auf Pläne für folgende Schutzmaßnahmen in der nächsten Legislaturperiode aufzunehmen:

- Aufnahme solider Bestimmungen für einen wirksamen Schutz der Privatsphäre und der Sicherheit der Kommunikation, einschließlich verbindlicher Standards für den eingebauten Datenschutz bei Software und Hardware (Privacy by Design und by Default).
- Verbot von Tracking-Walls, über die ein Preis für die Wahrnehmung der Grundrechte verlangt wird.
- Schutz der Verschlüsselung (einschließlich Ende-zu-Ende-Verschlüsselung) und der Vertraulichkeit der Kommunikation.
- Abschaffung der Überwachungswerbung zugunsten datenschutzfreundlicherer Formen des Ad-Targeting wie z.B. kontextbezogene Werbeadressierung.
- Beschränkung der Verarbeitung elektronischer Kommunikationsdaten auf konkrete, genau definierte Zwecke.
- Einführung eines soliden Schutzes gegen invasive Online-Überwachung und gegen Eingriffe bei den Endgeräten.
- Gewährleistung, dass die Rechtsprechung des Europäischen Gerichtshofs zum Schutz der Vertraulichkeit der Kommunikation vor unrechtmäßigen staatlichen und kommerziellen Eingriffen umgesetzt wird.
- Förderung von Sammelklagen zivilgesellschaftlicher Gruppen gegen Verstöße gegen die Rechtsvorschriften.

Mit freundlichen Grüßen

EDRi European Digital Rights, IT-Pol Denmark, Homo Digitalis, Zavod Državljan D, ApTI, Access Now, Privacy International, Politiscope, ARTICLE 19, Digital Rights Ireland, Bits of Freedom, Aspiration, Digitalcourage, **Deutsche Vereinigung für Datenschutz e.V. (DVD)**

Die englischsprachige Originalfassung dieses offenen Briefes finden Sie unter
https://edri.org/our-work/open-letter-modernised-eprivacy-legislation-must-protect-fundamental-rights/

[1] https://europa.eu/eurobarometer/surveys/detail/2124

[2] https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/

[3] https://edri.org/our-work/a-beginners-guide-to-eu-rules-on-scanning-private-communications-part-1/

Presseerklärung der DVD – Bonn, 13.03.2024

Datenschutzvereinigung fordert entschiedenen Widerstand gegen „Pay or Consent“ – Internet-Nutzer dürfen nicht geschröpft werden!

In einem offenen Brief wendete sich die Deutsche Vereinigung für Datenschutz e.V. (DVD) gemeinsam mit zwölf Bürgerrechtsorganisationen am 07.03.2024 erneut an die Datenschutzaufsichtsbehörden in der Europäischen Union, um zu verhindern, dass eine datenschutzfreundliche Nutzung des Internets nur noch gegen Bezahlen hoher Gebühren möglich ist. Hintergrund des offenen Briefs ist, dass der Europäische Gerichtshof das bisherige Gebührenmodell des Facebook- und Instagram-Konzerns Meta beanstandet hat, das auf „Einwilligungen“ zur Werbenutzung der Daten basiert, welche tatsächlich nicht freiwillig und daher unwirksam sind.

Anstelle dessen bietet Meta jetzt die Alternative Datenwerbenutzung oder Bezahlen – „Pay or Okay“. Hiergegen und gegen „Pay or Consent“-Modelle allgemein laufen Datenschützer in Nichtregierungsorganisationen (NGO) schon seit Monaten Sturm. Die Frage liegt nun beim Europäischen Datenschutzausschuss (EDSA), dessen Mitglieder unter massivem Lobbydruck von Meta und anderen Big-Tech-Unternehmen mit dem gleichen Geschäftsmodell stehen.

In dem durch Access Now initiierten offenen Brief fordern die NGO den EDSA und alle Aufsichtsbehörden auf „Pay or Consent“-Modelle entschieden abzulehnen.

Dazu erklärt der DVD-Vorsitzende Frank Spaeing: „‚Pay or Consent‘-Modelle wie das Modell ‚Pay or Okay‘ von Meta drohen europaweit etabliert zu werden. Letztlich wird diese Entwicklung, wenn sie von den Datenschutzbehörden jetzt nicht gestoppt wird, dazu führen, dass die großen Internet-Plattformen mit der Gebührenandrohung die Internet-User zu weiter zunehmenden Werbenutzungen drängen können. Damit wird der Kommerzialisierung des Internets weiter Vorschub geleistet; Nutzer werden entweder finanziell oder mit ihren Daten geschröpft; die digitale Trennung zwischen arm und reich wird weiter vorangetrieben. Die Datenschutz-Grundverordnung verlangt, dass Datenverarbeitung ‚fair‘ sein muss. Der digitale Kommunikationsbedarf der Menschen ist ein Grundrechtsbedürfnis; Betroffene müssen das Internet diskriminierungsfrei nutzen können.“

Den offenen Brief (in deutscher Übersetzung) finden Sie unter
https://www.datenschutzverein.de/wp-content/uploads/2024/03/Pay-or-okay2_de.pdf
(siehe auch die Meldung mit der Reaktion des EDSA auf S. 96)

Offener Brief

Protest gegen die Beschädigung des Amtes des/der Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI)

Berlin u.a., den 19.03.2024
An die Bundesregierung, insbesondere die Bundesministerin des Innern und für Heimat, Frau Nancy Faeser,
den Chef des Kanzleramtes, Herrn Wolfgang Schmidt,
An die Fraktionsvorsitzenden der Parteien SPD, Bündnis90/Die Grünen, FDP, Herrn Rolf Mützenich MdB, Frau Katharina Dröge MdB,
Frau Britta Hasselmann MdB und Herrn Christian Dürr MdB,
An die Präsidentin des Deutschen Bundestages, Frau Bärbel Bas MdB

Sehr geehrte Damen und Herren,

die Bundesregierung der Bundesrepublik Deutschland hat sich in ihrem Koalitionsvertrag 2021-2025 „Mehr Fortschritt wagen - Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit“ zur Aufgabe gemacht den Datenschutz zu stärken. Ihre eigenen Worte lauten auf Seite 104: „Den Rechtsschutz sowie die Datenaufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) stärken wir deutlich.“

Die Vorgänge in Bezug auf die Neu- oder Weiterbesetzung des Bundesbeauftragten

für Datenschutz und Informationsfreiheit (BfDI) schaden dem Amt jedoch in noch nie dagewesener Weise. Eine Unklarheit über die Fortführung der Amtsgeschäfte schwächt den gesamten Datenschutz in Bund und Ländern. Nichts fügt dem Datenschutz in Deutschland jedoch einen größeren und nachhaltigeren Schaden zu, als das verheerende Zeichen, dass der BfDI sich bei seinen unabhängigen Amtsgeschäften nicht sicher vor politischer Sanktion und damit vor politischer Einflussnahme sein kann. Es entsteht der Eindruck, der bisherige Amtsinhaber könnte sich eine mögliche zweite Amtszeit nicht durch den Einsatz für die Sache erarbeiten, sondern insbesondere durch politische Gefügigkeit. So erginge es jedoch auch jeder nachfolgenden Person im Amt der oder des BfDI.

Laut DSGVO und BDSG handelt die Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. Sie oder er unterliegt weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisung noch nimmt sie oder er Weisungen entgegen. Zum Verfahren zur Besetzung der Datenschutzaufsicht führt die DSGVO in Art. 53 aus: „Die Mitgliedstaaten sehen vor, dass jedes Mitglied ihrer Aufsichtsbehörden im Wege eines transparenten Verfahrens ernannt wird." Ein transparentes Verfahren zur Benennung ist in Deutschland aktuell nicht vorgesehen. Dieser Umstand wird von Fachverbänden zu Recht bemängelt. Die aktuell entstandene Verunsicherung ist eine unmittelbare Auswirkung dieser fehlenden Transparenz.

Es ist bekannt, dass sich der kommissarisch amtierende BfDI für eine weitere Amtszeit bewirbt. Es gibt keine Äußerung der Bundesregierung, warum eine nochmalige Benennung nicht geplant ist oder wer anstelle des amtierenden BfDI der Vorschlag ist. Ein transparentes Verfahren gibt es nicht. Dies gibt Raum für Spekulationen, die der Person, der Behörde, dem Datenschutz als solchem und nicht zuletzt auch dieser Bundesregierung selbst schaden. Die unterschreibenden Organisationen eint die Sorge um die Unabhängigkeit des BfDI und damit um die Effektivität des Datenschutzes in Deutschland.

Wir fordern die Bundesregierung und den Bundestag auf den bereits in erheblicher Weise entstandenen Schaden nach allen Kräften zu begrenzen und schnellstmöglich Klarheit über die Fortführung zu schaffen. Um die Beschädigung nicht als Dauerzustand fortzusetzen, müssen außerdem die Weichen für die Stärkung der Unabhängigkeit des Bundesbeauftragten für Datenschutz und Informationsfreiheit durch das Festschreiben eines transparenten Benennungsverfahrens gestellt werden.

Mit freundlichen Grüßen

Ann Cathrin Riedel und Teresa Widlok für LOAD e.V., Caroline Krohn für die AG Nachhaltige Digitalisierung, Padeluun für Digitalcourage e.V., Lilli Iliev für Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens e. V., Henriette Litta für die Open Knowledge Foundation Deutschland, Bianca Kastl für den Innovationsverbund Öffentliche Gesundheit e.V. (InÖG), Max Schrems für noyb – Europäisches Zentrum für digitale Rechte, Dr. Stefan Brink für das Wissenschaftliche Institut für die Digitalisierung der Arbeitswelt – wida, Christine Regitz für die Gesellschaft für Informatik e.V., Prof. Dr. Daniel Loebenberger für den Fachbereich Sicherheit – Schutz und Zuverlässigkeit der Gesellschaft für Informatik e.V. / Fraunhofer AISEC, Dr. Martin Weigele für den Arbeitskreis Datenschutz und IT-Sicherheit der Gesellschaft für Informatik e.V., Elisa Lindinger für SUPERRR Lab, Prof. Dr. Dennis-Kenji Kipker für das cyberintelligence.institute, Matthias Spielkamp für die AW AlgorithmWatch gGmbH, Jennifer Herbert für Netzbegrünung e.V., Stefan Hügel & Rainer Rehak für das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Chaos Computer Club e.V. (CCC), Svea Windwehr für D64 - Zentrum für Digitalen Fortschritt, Johannes Näder für die Free Software Foundation Europe e.V., Frederick Richter, LLM für die Stiftung Datenschutz, Peter Schaar für die Europäische Akademie für Informationsfreiheit und Datenschutz (EAID) – ehemaliger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Tom Jennissen für die Digitale Gesellschaft e.V., Robert Peter, Weizenbaum Institut e.V.

(siehe auch die Meldung zur Benennung von Louisa Specht-Riemenschneider, S. 88)

Presseerklärung vom 11.03.2024

Netzwerk Datenschutzexpertise warnt vor dem Einsatz von Standard-IT durch Journalisten

Medienunternehmen, Rundfunkanbieter und Presseredaktionen nutzen Bürokommunikationswerkzeuge wie z. B. Microsoft 365, die zwar ein Sorglospaket bei Installation und Betrieb bieten, aber keine Gewähr dafür, dass die verarbeiteten Daten vertraulich bleiben. Anbieter wie z. B. Microsoft nehmen für sich vielmehr in Anspruch Daten für eigene Zwecke zu nutzen. Eine solche Sekundärnutzung verstößt im Medienbereich gegen Verfassungs-, Medien- und Datenschutzrecht. Journalisten erfüllen in unserer Demokratie die Funktion einer „vierten Gewalt". Wird die Ver-

traulichkeit ihrer Arbeit beeinträchtigt, so bedroht dies Informationsquellen, sonstige Betroffene sowie die unbeeinflusste Tätigkeit von Redaktionen und deren Mitarbeitern.

Hat der Software-Anbieter seinen Sitz in einem Staat, der sich aus Sicherheitsgründen den heimlichen Zugriff auf verarbeitete Daten vorbehält, wie dies bei den USA der Fall ist, so drohen die Daten journalistischer Kommunikation und Recherchen direkt bei dortigen Behörden und Geheimdiensten zu landen. Dies kann nicht nur einen massiven Vertrauensbruch, sondern eine direkte Gefährdung der Journalisten und ihrer Quellen zur Folge haben. Um dies zu vermeiden, haben Journalisten gegenüber ihren Arbeitgebern in Deutschland einen Anspruch auf die Bereitstellung vertrauenswürdiger IT.

Ein umfangreiches Gutachten des Netzwerks Datenschutzexpertise nimmt eine umfassende rechtliche Analyse vor und begründet, weshalb und wie sich angestellte Journalisten gegen nicht vertrauenswürdige IT zur Wehr setzen können. Karin Schuler vom Netzwerk Datenschutzexpertise erklärt: „Medienunternehmen und Journalisten nutzen bisher oft arglos Informationstechnik, mit der sie sich schutzlos einem IT-Unternehmen ausliefern und dadurch zudem Gefahr laufen von diesem Unternehmen oder Dritten ausspioniert zu werden. Die Auswahl der richtigen Software gehört ebenso zu einer standesgemäßen journalistischen Arbeit wie die gründliche objektive Recherche und Berichterstattung."

Das Gutachten des Netzwerks Datenschutzexpertise finden Sie unter: https://www.netzwerk-datenschutzexpertise.de/dokument/vertraulichkeit-beim-cloudcomputing.

Einladung zu einer DVD-Videoveranstaltung

Das im letzten Jahr gestartete Format der DVD-Videoveranstaltung wurde im April DVD-intern mit dem Thema „Internet der Dinge" fortgeführt. In Zukunft wollen wir diese Videoveranstaltungen generell auch für Nicht-Mitglieder zugänglich machen.

Nächster Termin: **16. Juli 2024, 18:00-19:30 Uhr.**

Zum Thema „Doctolib und Datenschutz" referiert Thilo Weichert, der im Jahr 2021 die Laudatio bei der Vergabe des BigBrotherAwards an Doctolib hielt.

Wer den Link aus den letzten Veranstaltungen nicht mehr hat, kann sich gerne per E-Mail an dvd@datenschutzverein.de anmelden. Ein Passwort ist nicht erforderlich.

Neuigkeiten aus der DVD

DVD-Blog

Mit den einleitenden Worten „Alles neu macht der Mai" hat die DVD in ihrem Mitglieder-Newsletter Mitte Mai darüber informiert, dass es auf der DVD-Webseite einen neuen Inhaltstyp, den DVD-Blog, gibt. Der Vorstand will in Zukunft häufiger aktuelle Inhalte auf der DVD-Webseite veröffentlichen und startete den DVD-Blog mit einer Blog-Reihe, die beim Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. schon eine längere Tradition hat, mit „Menschen, Daten, Sensationen – Rudis Bericht aus dem Datenzirkus, ergänzt um Franks Zugabe", allerdings nun in der DVD-Edition. Sie finden den DVD-Blog unter https://www.datenschutzverein.de/kategorie/blog/.

RSS-Feed

Falls Sie automatisiert mitbekommen möchten, sobald sich etwas Relevantes auf der DVD-Webseite ändert, dann können Sie den DVD-RSS-Feed abonnieren, dann bekommen Sie in dem RSS-tauglichen Programm Ihrer Wahl (einige Mailprogramme unterstützen z.B. RSS-Feeds) automatisch eine Mitteilung, sobald wir etwas Relevantes auf der DVD-Webseite publiziert haben (zum Beispiel Blog-Beiträge). Sie finden den RSS-Feed unter https://www.datenschutzverein.de/kategorie/_rss/feed.

DVD-Mitglieder-Newsletter

Der klassische Kanal für die Information der Öffentlichkeit ist für die DVD der elektronische Versand von Pressemitteilungen an alle E-Mail- Adressen auf dem Presseverteiler. Von Zeit zu Zeit werden seit letztem Jahr auch Vereinsmitglieder per E-Mail über aktuelle Themen informiert, wenn sie sich in den Mitglieder-Verteiler aufnehmen lassen. Da es sich um unterschiedliche Listen handelt bitten wir interessierte Vereinsmitglieder, die noch keine „DVD-Mitglieder-News" erhalten haben, uns ihre E-Mail-Adresse mitzuteilen.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Bundesregierung beschließt BDSG-Änderungen

Das Bundeskabinett hat am 07.02.2024 den von Bundesinnenministerin Nancy Faeser vorgelegten Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes beschlossen (BR-Drs. 72/24). Damit wird die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder institutionalisiert, das Auskunftsrecht der Betroffenen eingeschränkt und ein Urteil des Europäischen Gerichtshofs (EuGH) zum Scoring umgesetzt. Die neue Scoring-Regelung wurde gemeinsam mit dem Bundesministerium für Umwelt und Verbraucherschutz erarbeitet.

Der Gesetzentwurf der Bundesregierung enthält folgende Punkte: Die Datenschutzkonferenz (DSK) wird im Bundesdatenschutzgesetz verankert. Die DSK hat den Zweck die Datenschutzgrundrechte zu schützen sowie eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Unternehmen sowie Einrichtungen, die Daten für wissenschaftliche, historische oder statistische Zwecke verarbeiten, können künftig bei länderübergreifenden Vorhaben, für die eine gemeinsame datenschutzrechtliche Verantwortung besteht, statt mehrerer Aufsichtsbehörden nur eine Aufsichtsbehörde als Ansprechpartner wählen. Darüber hinaus wird klargestellt, dass sich die Aufsichtsbehörden des Bundes und der Länder im Rahmen der europäischen Zusammenarbeit frühzeitig innerstaatlich abstimmen müssen. Damit soll auch in EU-Angelegenheiten die Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder gestärkt werden (zu den Stellungnahmen zum Referentenentwurf hierzu Alenfelder DANA 1/2024, 6 ff., vgl. DANA 4/2023, 216 f.).

Zudem werden die rechtlichen Grundlagen für das Scoring neu geregelt. Hintergrund ist die Entscheidung des Europäischen Gerichtshofs vom 07.12.2023 (DANA 1/2024, 45 f.). Danach folgt aus Art. 22 der EU-Datenschutz-Grundverordnung (DSGVO) das Verbot Personen einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zu unterwerfen, die ihnen gegenüber rechtliche Wirkung entfaltet. Bereits die Bildung eines Score-Wertes durch eine Auskunftei ist eine solche automatisierte Entscheidung, wenn von diesem Score-Wert die Entscheidung eines Dritten maßgeblich abhängt. Von der in der DSGVO vorgesehenen Möglichkeit für nationale Ausnahmen von diesem Verbot wird jetzt Gebrauch gemacht.

Damit wird z.B. für das Kreditscoring eine rechtliche Grundlage geschaffen, die dem Schutz von Verbraucherinnen und Verbrauchern dient. So ist vorgesehen, dass für die Bildung von Wahrscheinlichkeitswerten beim Scoring folgende Daten nicht verwendet werden dürfen:

- besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 DSGVO, wie die ethnische Herkunft, biometrische Daten und Gesundheitsdaten,
- der Name der betroffenen Person oder personenbezogene Daten aus ihrer Nutzung sozialer Netzwerke,
- Informationen über Zahlungseingänge und -ausgänge von Bankkonten,
- Anschriftendaten,
- Daten, die minderjährige Person betreffen.

Der Gesetzentwurf enthält zudem die von der DVD kritisierte Einschränkung des Auskunftsanspruchs von Betroffenen (DANA 4/2023, 210 f.). Er muss nun vom Bundestag und vom Bundesrat behandelt werden (Bundesministerium des Innern – BMI, PE v. 07.02.2024, Bessere Durchsetzung des Datenschutzrechts und Rechtssicherheit beim Scoring).

Bund

DSK kritisiert BDSG-Novellierungs-Entwurf

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert zahlreiche Nachbesserungen am Regierungsentwurf zur BDSG-Novelle. Bislang dürfen staatliche Datenschutzkontrolleure gemäß § 43 Bundesdatenschutzgesetz (BDSG) keine Geldbußen gegen Behörden und öffentliche Stellen verhängen. Selbst bei massiven Datenschutzverstößen z.B. durch die Polizei kann in der Regel nicht viel mehr als eine öffentliche Rüge erteilt werden. Die DSK fordert daher die entsprechende BDSG-Privilegierung zu streichen. Die Praxis habe gezeigt, „dass ein Bedarf für Geldbußen auch im öffentlichen Bereich besteht, um die Schwere eines Verstoßes gegenüber der beaufsichtigten Stelle hinreichend deutlich zu machen“. Geldbußen hätten „die am meisten abschreckende Wirkung und dienen folglich der Sicherstellung der Einhaltung“. Damit könnte Datenschutzverletzungen „aktiv vorgebeugt werden“. Die Möglichkeit, Geldbußen zu verhängen, sei zudem „aus Gründen der Gleichbehandlung“ von öffentlichen und privaten Stellen erforderlich. Die Ansicht des Bundesinnenministeriums, dass bei einer solchen Strafe letztlich nur Steuergelder hin- und hergeschoben würden, greife zu kurz: Der Sanktionscharakter eines Bußgeldes bestehe aufgrund der eigenen Haushaltsbetroffenheit der jeweiligen Stelle uneingeschränkt. Die Bundesdatenschutzaufsichtsbehörde benötige ferner die Option Zwangsmittel gegen Behörden und juristische Personen des öffentlichen Rechts erlassen und Anweisungen so vollstrecken zu können.

Die Bundesregierung plant anlässlich der BDSG-Novelle eine Überarbeitung der Regeln zum Scoring. Auslöser war ein Urteil des Europäischen Gerichtshofs (EuGH) gegen die Schufa (DANA 1/2024, 45 f.; s.o.). Die DSK weist auf zahlreiche Unklarheiten bei der geplanten Regulierung hin. Sie hält es für erforderlich ein Verbot der Nutzung von Daten zum Alter und zum Geschlecht der betroffenen Person als Basis für eine maschinelle Bonitätsbewertung zu prüfen. Ferner seien Verfahren zur Sicherstellung richtiger und aktueller Daten für das Scoring zu implementieren.

Mit dem Regierungsvorhaben soll die DSK im BDSG institutionalisiert werden, was die Ampel im Koalitionsvertrag vereinbart hat. Für die DSK selbst enthält der ins Spiel gebrachte Ansatz aber „nicht viel Neues“: Man arbeite bereits seit mehreren Jahren auf Basis einer eigenen Geschäftsordnung, die sich als tragfähig erwiesen habe: „Darin sind auch Anwendungsbereich und Verfahren von Mehrheitsentscheidungen definiert.“ Vorteilhaft wäre es aber die Ziele der DSK zur Koordinierung der Arbeit der Aufsichtsbehörden ins Gesetz aufzunehmen und eine ständige Geschäftsstelle einzurichten. Sie solle als Kontaktpunkt für andere Behörden und Institutionen dienen und die Konferenz bei der Aufgabenerfüllung unterstützen.

Bei gemeinsamer Verantwortlichkeit im nicht öffentlichen Bereich will es die Exekutive den beteiligten Unternehmen ermöglichen eine einzige Aufsichtsbehörde festzulegen. Die DSK hält es in solchen Fällen aber für nötig zumindest vorab zu prüfen, ob dafür die Berechtigungen vorliegen und wie sich eine gemeinsam verantwortete Verarbeitung abgrenzen lässt. Zugleich weist die DSK auf offene Fragen beim vorgesehenen hoheitlichen Tätigwerden in anderen Ländern hin.

Sie äußerte zudem Zweifel, ob die geplanten Vorgaben zum Schutz von Betriebs- und Geschäftsgeheimnissen bei Auskunftsansprüchen von Bürgern mit der DSGVO vereinbar sind (vgl. DVD-PE, DANA 4/2023, 210 f.): Die europarechtlichen Optionen, entsprechende Betroffenenrechte einzuschränken, seien eng auszulegen. Der Europäische Datenschutzausschuss (EDSA) prüft die Beachtung dieser Vorschrift gerade (Krempl, Datenschützer fordern Geldbußen gegen Behörden und öffentliche Stellen, www.heise.de 22.04.2024, Kurzlink: https://heise.de/-9694133; Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12.04.2024, https://www.datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdf).

Bund

Louisa Specht-Riemenschneider wird die neue BfDI

Nach monatelanger Suche haben sich FDP und Grüne auf eine Kandidatin für die Nachfolge des bisherigen Bundesdatenschützers Ulrich Kelber geeinigt, der spätestens Anfang Juli endgültig aus dem Amt ausscheidet. Die Informationsrechtlerin Louisa Specht-Riemenschneider von der Rheinischen Friedrich-Wilhelms-Universität Bonn wird neue Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Gemäß dem formellen Verfahren nach dem Bundesdatenschutzgesetz (BDSG) muss Innenministerin Nancy Faeser (SPD) die Kandidatin dem Bundeskabinett offiziell vorschlagen. Anschließend muss der Deutsche Bundestag die neue Datenschutzbeauftragte mit einer Mehrheit bestätigen.

Die 1985 geborene Specht-Riemenschneider ist Juristin und lehrt als Professorin für Rechtswissenschaften an der Universität Bonn, wo sie auch eine Forschungsstelle für Rechtsfragen neuer Technologien und Datenrecht leitet. Ihre wissenschaftliche Arbeit geht weit über das Feld des Datenschutzrechts hinaus; sie ist auch Expertin für Themen wie dem Handel mit Daten, Dateninfrastrukturen sowie Urheberrecht. Der neue Arbeitsplatz für sie als BfDI ist nur wenige Bahnstationen entlang der alten Bonner Diplomatenrennbahn entfernt. Sie ist keine Unbekannte in Berliner Politikkreisen, sie berät seit Jahren Bundesministerien und Parteien, etwa als Vorsitzende des Sachverständigenrats für Verbraucherfragen oder zuletzt als Mitglied im Digitalbeirat der Bundesregierung. Sie war unter anderem auch Mitglied der Gründungskommission für das geplante Dateninstitut – eine neue Einrichtung des Bundes, die zu rechtlichen und praktischen Fragen beim Umgang mit und Teilen von Daten beraten soll. Specht-Riemenschneider gilt als hervorragend vernetzt und fachlich kompetent. Sie gehört keiner Partei an.

Die SPD hatte die Nachfolgesuche den beiden Koalitionspartnern überlassen, da sie den ersten unabhängigen Polizeibeauftragten des Bundestages stellen wollte (DANA 1/2024, 24 f.). Der wurde Mitte März gewählt – der langjährige SPD-Bundestagsabgeordnete Uli Groetsch. Das SPD-Mitglied Kelber war bei seiner Partei und insbesondere bei Fraktionschef Rolf Mützenich in Ungnade gefallen, weil er sich immer wieder kritisch zu Projekten aus SPD-geführten Ministerien geäußert hatte (dazu DVD-PE DANA 4/2023, 214). Vorangegangen war ein monatelanges Ringen in der Ampelkoalition um die BfDI-Nachfolge. Kelbers Amtszeit wäre eigentlich am 06.01.2024 ausgelaufen. Branchenvertreter und Datenschützer hatten die Regierungsparteien davor gewarnt, das Amt nicht durch weiteres Hinauszögern zu beschädigen (s.o. Offener Brief S. 84). Geeignete Kandidaten für die Nachfolge Ulrich Kelbers zu finden, war offenbar recht schwierig, nachdem die SPD mit dem „Aus“ für Kelber signalisiert hatte, dass sie von diesem Amt kein allzu engagiertes Eintreten für den Datenschutz erwartet. Reihenweise hagelte es Absagen. Teils aus persönlichen Gründen, teils aber auch dem Prozess geschuldet. Einige Kandidaten waren aufgrund der Umstände der Nichtverlängerung des bisherigen Amtsinhabers nicht bereit die Aufgabe zu übernehmen.

Das Erbe Ulrich Kelbers, der das Amt noch bis zur offiziellen Amtsübergabe an seine Nachfolgerin ausübt, wiegt schwer. Ein Ausrufezeichen bei der Durchsetzung des Datenschutzes auch gegenüber staatlichen Stellen setzte Kelber mit einer Anordnung gegenüber dem Bundespresseamt, dem er die Nutzung von Facebook untersagen wollte. Das anhängige Gerichtsverfahren vor dem zuständigen Verwaltungsgericht ist bis heute nicht abgeschlossen. Zudem wirkte Kelber an den Entscheidungen des Europäischen Datenschutzausschusses (EDSA) mit, der etwa die

irische Datenschutzaufsicht zu einem härteren Vorgehen gegen den Meta-Konzern, der Facebook, Instagram und WhatsApp verantwortet, verpflichtete.

Der Bonner Informatiker und langjährige SPD-Bundestagsabgeordnete Kelber sah noch im März vor allem eine Beschädigung des Amtes durch die Ampelkoalition – insbesondere im internationalen Kontext sei die Position des BfDI geschwächt worden, da er der künftigen Leitung nicht vorgreifen könne. Die Datenschutz-Grundverordnung (DSGVO) wird 2026 zehn Jahre alt. Es gibt nicht wenige, die sie für überarbeitungsbedürftig halten. Es stehen also intensive politische und öffentliche Auseinandersetzungen an. Auch die Debatten um KI-Regulierung und die Frage, welche Stelle in Deutschland die Aufsicht über die KI-Verordnung ausübt, dürfte einige Aufmerksamkeit erfordern – genau wie die Ausgestaltung der Teilaufgaben aus dem Digital Services Act, die bei der Datenschutzaufsicht liegen, etwa zu Dark Patterns.

Die DSGVO verpflichtet die Politik bei der Benennung des BfDI zu einem transparenten Verfahren. Davon konnte bisher nie und nun wieder keine Rede sein. Mit einer qualifizierten Wahl von Specht-Riemenschneider besteht die Hoffnung, dass dieses Manko keine schwereren Folgen hat (Rusch, Regierung einigt sich: Bonner Professorin wird neue Datenschutzbeauftragte, www.tagesspiegel.de 15.04.2024; Steiner, BfDI: Koalition einigt sich auf Nachfolge für Kelber, www.heise.de 15.04.2024; Kurzlink: https://heise.de/-9685907).

Bund

Offizielle Regierungsstellen bespielen verstärkt Social Media Kanäle

Das Presse- und Informationsamt der deutschen Bundesregierung (BPA) folgt dem Bundestag und ist nun auch auf WhatsApp aktiv. Das Amt informiert über aktuelle politische Entscheidungen und Vorhaben der Regierung. Das BPA folgt dem Beispiel des Bundestages, der sein WhatsApp-Angebot Anfang 2024 eröffnet hat. Der Bundestag hat inzwischen 18.000 Abonnenten. Der neue Kanal „Bundesregierung“ konnte am 17.04.2024 binnen Stunden 8.000 Abonnenten gewinnen. Den WhatsApp-Kanal betreut die Social-Media-Redaktion des Presse- und Informationsamtes. Sie ist zuständig für mehrere weitere Auftritte der Bundesregierung und des Bundeskanzlers bei Diensten von Meta Platforms (Instagram, Facebook) sowie bei Tiktok, X, Youtube und Mastodon.

Bei WhatsApp sind Kanäle im Reiter „Aktuelles“ zu finden. Vor dem ersten Zugriff müssen Nutzer separate Geschäftsbedingungen von Meta Platforms akzeptieren. Auf Mobilgeräten, auf denen WhatsApp installiert ist, kann der Kanal der Bundesregierung auch über den Link https://bpaq.de/whatsapp angesteuert werden.

Die Mastodon-Auftritte öffentlicher Stellen der Bundesrepublik Deutschland und mancher Länder sind auf einem Server des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), social.bund.de, eingerichtet. Dort gibt es bereits einhundert verschiedene aktive Konten, darunter gleich zwei des Bundestages (@bundestag und @hib_Nachrichten, wobei hib für „Heute im Bundestag“ steht).

Die Bandbreite reicht vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem deutschen Datenportal Govdata über den Deutschen Wetterdienst bis zum Deutschen Zentrum für Luft- und Raumfahrt (DLR) und dem Zoll. Gerichte, Ministerien, Landtage, Stiftungen, Institute, Ämter, Beiräte, Versicherungen, Bundeswehr, Technisches Hilfswerk und andere mehr informieren auf Mastodon frei von Drittwerbung. Ein strukturiertes Verzeichnis der Angebote gibt es offenbar noch nicht (Sokolov, Deutsche Bundesregierung bespielt Whatsapp-Kanal, www.heise.de 17.04.2024, Kurzlink: https://heise.de/-9688836).

Bund

BfDI gegen Regierungspräsenz auf Tiktok

Nachdem Bundeskanzler Olaf Scholz am 29.02.2024 von einer Bürgerin bei einem Bürgerdialog in Dresden darauf angesprochen worden war, dass die AfD auf dem Videoportal Tiktok „kackbraune Soße“ über die Leute gieße und die demokratischen Parteien dort gar nicht existieren, gab der Kanzler ihr mikrofonend recht und erklärte, dass die Bundesregierung darüber diskutiere dort ebenfalls aktiv zu werden. Diese Äußerung rief den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) auf den Plan. Der BfDI-Sprecher Christof Stein erklärte: „Sollte die Bundesregierung einen Account betreiben, wie der Bundeskanzler es angekündigt hat, dann wird der BfDI sich noch einmal verstärkt mit dem Thema befassen. Grundsätzlich haben öffentliche Stellen bei sozialen Medien eine Vorbildfunktion und sollten diese nur nutzen, wenn es rechtskonform möglich ist.“

Schon 2021 hatte der BfDI die Bundesministerien und -behörden auf seine Bedenken hingewiesen, die mit potenziellen Datenschutzverletzungen bei Tiktok begründet wurden. Von einer Installation der App auf Diensthandys riet man damals ab. Die Diskussion um Aktivitäten auf dem bei Jugendlichen beliebten Tiktok schwelt schon länger. Der Regierungssprecher Hebestreit wurde Ende 2022 mit Hinweisen auf einen Prüfvermerk des Bundespresseamtes zur chinesischen Plattform zitiert, das vor einer Präsenz dort warnt (Siering, Des Bundeskanzlers Hin und Her bei TikTok, www.heise.de 02.03.2024, Kurzlink: https://heise.de/-9644451).

Nachdem sich Tiktok zunehmend der „Beliebtheit“ von Vertretern der Bundesregierung erfreut, wandte sich eine Redakteurin des Springer-Blattes „Bild“ an die DVD mit der Frage, wie mit Blick auf den Datenschutz der Auftritt aller Parteien, mehrerer Minister und des Bundeskanzlers zu bewerten sei. Hier die Antwort:

„Tiktok ist aus Sicht von Datenschützern, Verbraucher- und Kinderschützern massiv zu kritisieren: Die Datenauswertung von Tiktok verstößt in vieler Hinsicht gegen Vorgaben der Datenschutz-Grundverordnung; die Transparenz für die Nutzenden ist katastrophal; insbesondere Kindern wird durch die genutzten Algorithmen erheblich geschadet. Das stört u.a. die AfD in keiner Weise, die Tiktok für Hassinhalte und Desinformation nutzt. Dass nun seriösere Poli-

tiker versuchen dieses Medium auch zu bespielen, ist zumindest insofern nachvollziehbar, dass der AfD etwas entgegengesetzt werden soll. Eine gute Idee ist es aber nicht. Solange Politiker Tiktok als Privatpersonen nutzen, ist dies ihre persönliche Freiheit. Anders zu bewerten ist es aber, wenn sie dies in ihrer Funktion als Regierungsmitglieder, also in ihrer offiziellen Funktion, tun: Insofern sind sie an die Beachtung der rechtlichen Vorgaben gebunden. Es kommt nicht von ungefähr, dass der Bundesdatenschutzbeauftragte dem Bundespresseamt als öffentlicher Einrichtung in einem Musterverfahren die Nutzung von Facebook untersagte, was derzeit gerichtlich geklärt wird. Facebook verstößt ähnlich wie Tiktok weiterhin eklatant gegen Datenschutzregeln und gegen weitere rechtliche Vorgaben. Der Europäische Gerichtshof hat klargestellt, dass durch den Betrieb eines Accounts eine Mitverantwortlichkeit für die Rechtsverstöße der Plattform besteht. Das Problem: Das Umsetzungsdefizit des Datenschutzes und generell des Rechts bei Social Media ist gewaltig. Es ist traurig, dass die Regierung hiervor die Augen verschließt und diesen Medien wie Tiktok mit der offensiven Nutzung sogar noch Vorschub leistet und diese unterstützt."

Die Bild-Zeitung berichtete nicht über diese Stellungnahme.

Bund

Einigung der Koalition über TK-Vorratsdatenspeicherung wohl nur vorläufig

Nach langem Streit über die Vorratsspeicherung von Telekommunikations-(TK-)Daten haben sich SPD und FDP am 10.04.2024 auf die Einführung des sogenannten Quick-Freeze-Verfahrens geeinigt. Quick Freeze soll zum Einsatz kommen können, wenn es um schwere Straftaten wie z.B. Mord und Totschlag geht. Kommunikationsunternehmen sollen dann beauftragt werden, bestimmte Verkehrsdaten, etwa IP-Adressen und Telefonnummern, „einzufrieren", damit sie für spätere Ermittlungen zur Verfügung stehen. Nötig ist ein richterlicher Beschluss. Anschließend sollen Strafverfolgungsbehörden einen Monat Zeit haben, um einen weiteren Richterbeschluss zu erwirken und die eingefrorenen Daten zur Auswertung zu bekommen.

Der Streit über Ermittlungsmethoden im Internet ist alt. Die Vorratsdatenspeicherung führte der Bundestag erstmals 2007 ein. In großem Umfang verpflichtete das Gesetz Unternehmen zur Aufzeichnung von Verkehrs- und Standortdaten, also der Informationen darüber, wer wann wo auf welche Weise kommuniziert hat. Drei Jahre später kassierte das Bundesverfassungsgericht die Regelung. 2015 versuchte es die große Koalition noch einmal. Sie erließ eine Regelung, die Unternehmen verpflichtete zehn Wochen lang zu speichern, wer sich wann mit welcher IP-Adresse ins Internet eingeloggt hatte. TK-Unternehmen sollten festhalten, wer wem wann Nachrichten geschrieben oder wer wann mit wem telefoniert hatte. Doch noch ehe die Speicherpflicht galt, setzte die Bundesnetzagentur das Gesetz außer Kraft.

Im September 2022 bestätigte der Europäische Gerichtshof (EuGH) die Zweifel und erklärte die deutsche Regelung größtenteils für unionsrechtswidrig; nur unter bestimmten Voraussetzungen sei eine allgemeine und unterschiedslose Vorratsdatenspeicherung zulässig (DANA 2/2022, 125 ff.). FDP-Bundesjustizminister Buschmann warb seitdem besonders für Quick Freeze. Im Oktober 2022 legte er einen Gesetzentwurf vor und stieß damit in der SPD auf Widerstand. Sozialdemokraten (und Union) machten vor allem auf ein Problem aufmerksam: Manche TK-Unternehmen speichern die Daten mittlerweile nicht mal mehr ein paar Tage; in diesen Fällen gibt es wenig einzufrieren. Wohl auch deshalb verwiesen die stellvertretenden SPD-Fraktionsvorsitzenden, Dirk Wiese und Verena Hubertz, nach dem Kabinettsbeschluss auf nun anstehende „intensive Beratungen" im parlamentarischen Verfahren. Man werde erörtern, wie Quick Freeze den „Anforderungen einer effizienten Strafverfolgung im Internet gerecht wird".

Die Einigung auf Quick Freeze wurde nur möglich, weil die FDP der SPD beim Mietrecht entgegengekommen ist. Die 2025 auslaufende Mietpreisbremse soll nunmehr bis 2029 verlängert werden. Sie sorgt dafür, dass die Miete bei Abschluss eines neuen Vertrags grundsätzlich nicht mehr als zehn Prozent über der ortsüblichen Vergleichsmiete liegen darf. SPD, Grüne und FDP hatten sich darauf schon im Koalitionsvertrag geeinigt, nach dem Widerstand gegen Quick Freeze verknüpfte Buschmann beide Vorhaben jedoch. In der SPD war der Ärger darüber groß. Immer wieder war die Rede davon, dass Buschmann den Mieterschutz „in Geiselhaft" nehme.

Wenige Tage nach der Verständigung in der Koalition wurde klar, dass der Streit noch lange nicht beendet ist. So erklärte Faeser, das Quick-Freeze-Verfahren sei zwar „ein gutes neues Instrument": „So können Ermittler bei schwerer Kriminalität Daten einfrieren lassen, damit wichtige Ermittlungsansätze nicht verloren gehen." Abgeschlossen seien die Gespräche dazu nicht: „Über diese Frage verhandeln wir deshalb weiter. Das haben wir ausdrücklich vereinbart." Da immer mehr Verbrechen über das Internet angebahnt werden, habe die Aufklärung der Identität von Verdächtigen eine weiter zunehmende Relevanz, insbesondere, wenn diese verschlüsselt kommunizierten. Da Telekomfirmen die Daten ihrer Nutzenden nach geltender Rechtslage nur kurz oder gar nicht speichern, blieben den Ermittlern bestenfalls wenige Tage, um ihnen auf die Spur zu kommen.

In Sicherheitskreisen war der Ärger über die Koalitionseinigung groß. Sie halten es für unerlässlich, die Verkehrsdaten für eine gewisse Zeit zu speichern, wobei es nicht um die Inhalte, sondern um die Identität der Kommunikationspartner und um den Zeitpunkt geht, v.a. in Fällen des Kindesmissbrauchs, der Hasskriminalität und des Terrorismus. Faeser assistiert: „Es besteht bei allen Ermittlungsbehörden und Innenministern in den Ländern wie im Bund und in der EU völlige Einigkeit, dass wir eine kurzzeitige Speicherung der IP-Adressen bei den Anbietern brauchen." Der Europäische Gerichtshof habe die Speicherung von IP-Adressen ausdrücklich für zulässig erklärt. „Das ist unser Maßstab" (Grunert, Was ist Quick-Freeze? www.faz.net 10.04.2024; Balser, Faeser will IP-Adressen speichern, SZ 15.04.2024, 7).

Bund

Russia Today veröffentlicht WebEx-Kommunikation zu Taurus

Die Chefin des russischen Staatssenders RT (Russia Today), Margarita Simonjan, veröffentlichte am 01.03.2024 einen Audiomitschnitt eines 38-minütigen, abgehörten, über WebEx geführten Gesprächs von Beratungen deutscher Luftwaffen-Offiziere über das Waffensystem Taurus und dessen umstrittenen Einsatz in der Ukraine. Bundesverteidigungsminister Boris Pistorius (SPD) gab an eine „lückenlose Aufklärung" über das Bundesamt für den militärischen Abschirmdienst (BAMAD) in die Wege geleitet zu haben. Zu prüfen sei, ob der Inhalt des Gesprächs richtig eingestuft worden sei. Von WebEx gebe es „zertifizierte Formen", diese könnten „bis zu einer bestimmten Vertrauens- und Geheimhaltungsstufe genutzt werden". Ob das der Fall war, müsse das BAMAD herausfinden.

Von der Bundeswehr wird Ciscos WebEx offenbar häufig eingesetzt. Mit der Implementation von WebEx in Sicherheitsbereichen vertraute Personen bestätigten, dass das System zumindest bei der Einwahl per Telefon oder über einen Browser keine Ende-zu-Ende-Verschlüsselung bietet. Und tatsächlich erwies sich die Fahrlässigkeit der Teilnehmenden als primäre Ursache für das Datenleak: Brigadegeneral Frank Gräfe hatte sich offenbar von einem Hotelzimmer in Singapur in die Videoschalte eingewählt. Nach diesem „individuellen Anwendungsfluss" ist es nach Angaben von Pistorius zum „Datenabfluss" gekommen.

Der Offizier hatte sich während der Flugmesse „Singapore Airshow" in der Stadt aufgehalten. Dort waren auch hochrangige Militärs westlicher Staaten vertreten ebenso wie vermutlich russische Geheimdienst-Mitarbeiter. Bei solchen Veranstaltungen finden, so Verteidigungsminister Pistorius im Rahmen einer Sondersitzung des Verteidigungsausschusses am 11.03.2024, flächendeckende Abhöraktionen statt. Daher müsse man davon ausgehen, dass die abgehörte Konferenz „ein Zufallstreffer im Rahmen einer breit angelegten Vorgehensweise war".

Pistorius teilte weiter mit, dass auch Luftwaffeninspekteur Ingo Gerhartz als Zweiter der vier Teilnehmer über eine nicht sichere Leitung zugeschaltet war. Neben dem grundsätzlichen Sicherheitsproblem, dass per traditionellem Telefonanruf in Konferenzen zugeschaltete Teilnehmer keine verschlüsselten Verbindungen aufbauen können, muss in WebEx Ende-zu-Ende-Verschlüsselung von IT-Verantwortlichen für die Client- und Server-Software eingerichtet und aktiviert werden. Zudem müssen alle Nutzer diese Optionen dann zugewiesen bekommen, was bei einer Einwahl über ein Hotel wohl nicht möglich ist. Spione haben sich möglicherweise Zugang zu dem Router des Hotels in Singapur verschafft. IT-Experten warnen seit Jahren davor in öffentlichen Netzen wie Hotels, Bahnhöfen oder Cafés unverschlüsselt zu kommunizieren. Welche der potenziellen Schwachstellen von pro-russischen Schnüfflern zum Abhören missbraucht wurde, war zunächst unklar.

WebEx vom US-Konzern Cisco war während der Pandemie aus Datenschutzgründen ins Gerede gekommen. Wie bei anderen Kommunikationsplattformen von US-Anbietern auch, etwa Teams von Microsoft oder Zoom, äußerten Datenschützer Bedenken. Cisco teilte damals mit an einem Tag mehr als 4,2 Millionen Konferenzen bereitgestellt zu haben. In der Software, besonders in den Erweiterungen für Browser, wurden schon mehrmals Sicherheitslücken festgestellt.

Das abgehörte Gespräch soll der Vorbereitung auf eine Unterrichtung für Verteidigungsminister Pistorius gedient haben. In dem in der Audiodatei dokumentierten Austausch geht es unter anderem um die Frage, ob Taurus-Marschflugkörper technisch in der Lage wären die von Russland gebaute Brücke zur völkerrechtswidrig annektierten ukrainischen Halbinsel Krim zu zerstören. Ein weiterer Punkt ist, ob die Ukraine den Beschuss ohne Bundeswehrbeteiligung bewerkstelligen könnte.

In dem Mitschnitt ist auch zu hören, dass es auf politischer Ebene kein grünes Licht für die Lieferung der von Kiew geforderten Marschflugkörper gibt. Brisant ist, dass die Rede davon ist, dass die Briten im Kontext des Einsatzes ihrer an die Ukraine gelieferten Storm-Shadow-Marschflugkörper „ein paar Leute vor Ort" hätten. Gerade erst hatte es in Großbritannien Verärgerung über eine Äußerung von Kanzler Olaf Scholz gegeben, die ihm von einigen als Indiskretion ausgelegt wurde. Er sagte: „Was an Zielsteuerung und an Begleitung der Zielsteuerung vonseiten der Briten und Franzosen gemacht wird, kann in Deutschland nicht gemacht werden."

Nach der Veröffentlichung forderten Sicherheitspolitiker Konsequenzen, etwa die Vorsitzende des Verteidigungsausschusses des Bundestags, Marie-Agnes Strack-Zimmermann: „Wir müssen dringend unsere Sicherheit und Spionageabwehr erhöhen, denn wir sind auf diesem Gebiet offensichtlich vulnerabel." Der stellvertretende Unionsfraktionsvorsitzende Johann Wadephul forderte die Bundesregierung auf die Vorschriften für den Schutz von Kommunikation nachzuschärfen. Der Grünen-Politiker und Vorsitzende des Parlamentarischen Kontrollgremiums, Konstantin von Notz, meinte: „Es stellt sich die Frage, ob es sich hier um einen einmaligen Vorgang oder ein strukturelles Sicherheitsproblem handelt." Er erwarte „umgehende Aufklärung aller Hintergründe".

Roderich Kiesewetter sagte mit Blick auf die Veröffentlichung: „Man muss davon ausgehen, dass das Gespräch ganz gezielt durch Russland zum jetzigen Zeitpunkt geleakt wurde, in einer bestimmten Absicht. Diese kann nur darin liegen eine Taurus-Lieferung durch Deutschland zu unterbinden." Russland wolle Scholz abschrecken, indem man „öffentlich zeigt, wie tief Russland die deutschen Entscheidungsvorbereitungen dazu bereits aufgeklärt hat". Auch Strack-Zimmermann sieht als Grund für die Veröffentlichung, dass Russland Bundeskanzler Olaf Scholz (SPD) davon abschrecken will doch noch grünes Licht für die Lieferung von Taurus zu geben. Spionage gehöre „zum Instrumentenkasten Russlands hybrider Kriegsführung". Es sei weder überraschend noch verwunderlich, dass Gespräche abgehört würden. „Es war nur eine Frage der Zeit,

wann es öffentlich wird.“ Kiesewetter rechnet damit, dass noch etliche andere Gespräche abgehört wurden und gegebenenfalls später im Sinne Russlands geleakt werden. Er vermutete zudem wegen der zeitlichen Überschneidung: „Dieses Bundeswehr-Leak kann ein russischer Versuch sein die öffentliche Debatte wegzulenken von den Wirecard-Enthüllungen und der Beerdigung von Alexej Nawalny“ (Ernst, Bundeswehr wurde bei Diskussion über Taurus per WebEx abgehört, www.heise.de 02.03.2024, Kurzlink: https://heise.de/-9644487; Ernst, Taurus-Leak: Bundeswehr nutzte angeblich ungesichertes System, www.heise.de 03.03.2024, Kurzlink: https://heise.de/-9644680; Martin-Jung, Wie funktioniert Webex? SZ 04.03.2024, 2; Koopmann, Schwachstelle Mensch, SZ 06.03.2024, 4; TaurusLeaks: Auch Inspekteur war über unsichere Leitung zugeschaltet, www.heise.de 12.03.2024, Kurzlink: https://heise.de/-9651939).

Bund

Erneut mehr Kontodatenabfragen

Im Jahr 2023 hat das Bundeszentralamt für Steuern gemäß einer Antwort der Bundesregierung zur Anzahl und Entwicklung von Kontoabfragen durch Behörden (BT-Drs. 20/10841) auf eine Kleine Anfrage der AfD-Fraktion (BT-Drs. 20/10589) hin 169.901 Kontoabfragen für die Finanzämter vorgenommen. Den Angaben zufolge gab es 2023 insgesamt 1,4 Millionen Abfragen gemäß § 93b der Abgabenordnung (AO) und damit eine weitere Steigerung gegenüber den Vorjahren 2022 (1, 14 Mio.) und 2020 (1,01 Mio.). 342.505 Abfragen erfolgten gemäß § 93 Absatz 7 AO. Im Bereich der Grundsicherung für Arbeitssuchende nach dem Sozialgesetzbuch II waren es demnach 23.600 Abfragen. Für die Finanzämter nahm das Bundeszentralamt für Steuern 169.901 Abfragen vor, für Gerichtsvollzieher 844.427 (Deutscher Bundestag, PM vom 02.04.2024; Kontoabfragen für die Finanzämter: Zahl für 2023 veröffentlicht, www.steuerzahler.de 03.04.2024; Nachgezählt Der Spiegel Nr. 15 06.04.2024, 19).

Bundesweit

Ex-RAF-Mitglied Klette gefasst – Journalisten waren mit Pimeyes schneller

Am 27.02.2024 klingelten die Zielfahnder des Landeskriminalamts (LKA) Niedersachsen an der Tür einer Wohnung in Berlin, in der eine Frau unter dem Namen Claudia Ivone wohnte. Sie zeigte ihren italienischen Pass vor, musste aber dennoch zur Personalienüberprüfung zur Wache, wo ihr Fingerabdrücke genommen wurden. Dabei bestätigte sich der Verdacht, dass es sich bei Frau Ivone um Daniela Klette handelte, mutmaßliche Ex-Terroristin der Roten Armee Fraktion (RAF), seit mehr als 30 Jahren im Untergrund lebend und eine der meistgesuchten Personen des Landes. Ihr werden mehrfacher versuchter Mord, Teilnahme an Sprengstoffanschlägen und vieles mehr vorgeworfen.

Zwischenzeitlich hatten die Zielfahnder versucht Klette mit Hilfe der Rasterfahndung zu finden, die in der heißen Phase des RAF-Terrorismus in den 70er Jahren entwickelt und eingesetzt worden war. Das LKA ließ sich von den Meldeämtern in Niedersachsen anonymisiert die Passbilder aller Einwohner zuschicken, die der Altersgruppe der Gesuchten entsprachen und führte mit einer Gesichtserkennungssoftware einen Abgleich mit den Fahndungsfotos durch, was keinen Erfolg zeigte. Die Verhaftung Klettes ging letztlich auf einen Tipp aus der Bevölkerung vom November 2023 zurück.

Kurz zuvor, im Oktober 2023, hatte schon der kanadische Journalist Michael Colborne der Investigativplattform Bellingcat Klette mit Hilfe einer frei verfügbaren Gesichtserkennungssoftware ausfindig gemacht. Die Macher des ARD-Podcasts „Legion“ produzierten damals eine Sendung mit dem Titel „most wanted: Wo ist die RAF-Terroristin Daniela Klette?“ Dafür baten sie zunächst Colborne Fotos einer Frau aus Köln mit Fahndungsbildern von Klette abzugleichen, was erfolglos war. Da er die Bilder schon mal hatte, speiste er sie in die Software Pimeyes ein, die das Internet nach Fotos abgrast, mit dem Ziel dieselbe Person zu finden. Colborne erhielt zahlreiche Bilder einer Frau, die sich offenkundig in Berlin aufhielt und in einem Verein Capoeira tanzte: „Die Suche hat mich nicht mehr als eine halbe Stunde nach Feierabend gekostet.“ Die Podcast-Macher gingen zum Kampftanz-Training in Berlin-Treptow, wo man eine Claudia Ivone kannte, die aber nach der Pandemie nicht mehr dort aufgetaucht war. Die Journalisten verfolgten die Spur nicht weiter, erläutert Produzent Patrick Stegemann: „Wir glaubten schon, dass wir sie gefunden hatten – und konnten es eigentlich auch nicht glauben, sie lebte seit 30 Jahren im Untergrund.“

Pimeyes ist eine Bildersuchmaschine, die man mit einem Foto von einem Gesicht füttern kann und deren Algorithmus Millionen Bilder aus dem Internet nach denselben Gesichtsmerkmalen durchforstet. Pimeyes behauptet dabei keine Social-Media-Fotos zu verwenden. Solche Programme sind höchst umstritten. Der damalige Landesbeauftragte für Datenschutz Baden-Württemberg Stefan Brink warnte 2020, diese Programme zu nutzen sei ein „eklatanter Rechtsverstoß“. Die Datenschutz-Grundverordnung „untersagt, biometrische Daten zur eindeutigen Identifizierung zu nutzen“, insbesondere wenn der Datensatz aus Bildern besteht, die ohne Einwilligung der betreffenden Personen gesammelt wurden. Deshalb dürfte die Polizei Pimeyes und ähnliche Suchmaschinen auch nicht nutzen.

Eine spätere Reproduktion der Recherche von Colborne im Internet war erfolglos. Pimeyes fand nur weitere Fahndungsfotos. Colborne vermutet, weil ursprünglich vorhandene Bilder von Websites gelöscht worden sind, konnte er das Ergebnis vom vorangegangenen Herbst nicht wiederholen. Sucht man allerdings mit einem aktuelleren Foto, das Klette auf ihrem Facebook-Profil veröffentlicht hat, tauchen weitere Fotos von ihr auf. Eines zum Beispiel zeigt sie 2011 auf dem Karneval der Kulturen in Berlin, das auf einem privaten Blog veröffentlicht ist und wo Klette zufällig vor die Linse geriet. Neuere Aufnahmen der nach wie vor flüchtigen RAF-Terroristen Ernst-Volker Staub und Burkhard Garwig waren mit Pimeyes übrigens nicht zu finden (Glüsing/Großekemper/Gude/Höfner/Lehberger/Rosenbach/Schwarze/Siemens/Wiedmann-Schmidt,

Die nette Frau Ivone, Der Spiegel Nr. 10 02.03.2024, 28 ff; Erb/Koopmann, Die Spur der Bilder, SZ 02./03.03.2024, 7).

Bundesweit

Datenleck mit Spenderangaben beim BSW

Informationen von 35.000 Unterstützern und Interessenten des Bündnis Sahra Wagenknecht (BSW) sind offenbar in unbefugte Hände geraten. Neben den Namen sind davon auch konkrete Zahlungsinformationen betroffen. Es geht u.a. um eine Liste mit Daten von rund 5.000 Parteispendern. Sie umfasst Zahlungen an die Wagenknecht-Partei, die bis zum 13.01.2024 mittels eines Formulars auf der Webseite des BSW eingegangen sind. Neben den Spender-Informationen gelangten auch 30.000 E-Mail-Adressen von Newsletter-Empfängern in die Öffentlichkeit. Der BSW-Schatzmeister Ralph Suikat erklärte, dass bei der Überprüfung einer überlassenen Stichprobe des Datensatzes sich diese als unvollständig entpuppten beziehungsweise die Angaben sich nicht mit tatsächlichen Spenden deckten. Bei dem Leck seien neben Namen, E-Mail-Adressen und der Unterscheidung, ob mehr oder weniger als 500 Euro gespendet wurden, keine weiteren Daten betroffen – also auch keine Kontoverbindungen. Insgesamt habe das BSW seit seiner Gründung 3,1 Millionen Euro an Spenden gesammelt. Man habe den Vorfall sofort nach Bekanntwerden an die Staatsanwaltschaft und die Datenschutzbehörde weitergeleitet. Zudem habe der Verein BSW mit seinen Dienstleistern Kontakt aufgenommen, um die Sicherheitsmaßnahmen „noch einmal überprüfen" zu lassen. Zu den ersten Gegenmaßnahmen zur besseren Absicherung der IT-Systeme gehören etwa die Überwachung kompromittierter Systeme und die Aktualisierung von Passwörtern.

Das BSW war formal im Januar 2024 als neue Partei gegründet worden. Zuvor hatte sich das BSW im Oktober 2023 offiziell als Verein konstituiert, der die Parteigründung vorbereiten und dafür auch Spenden einwerben sollte. Das Datenleck soll bei den Strukturen dieses vorgeschalteten Vereins passiert sein. Die Vereinskonstruktion hatte damals einiges an Kritik hervorgerufen. Das BSW versicherte zwar, dass die Spenden genau wie Parteispenden behandelt würden, Experten monierten aber, dies sei kaum nachprüfbar. Auch andere Parteien wurden gelegentlich Opfer von Datenlecks. Mitte 2023 standen etwa Mitgliedsanträge der AfD frei zugreifbar im Netz. Schuld waren da jedoch keine Datendiebe und Einbrecher (Knop, Datenleck bei Bündnis Sahra Wagenknecht: Unbekannte hatten Zugriff, www.heise.de 14.03.2024, Kurzlink: https://heise.de/-9654796; Slavik, Datenleck beim BSW SZ 15.03.2024, 8).

Bundesweit/Baden-Württemberg

Ortung von 110-Anrufenden im Probebetrieb

Das baden-württembergische Innenministerium hat sich mit dem Datenschutzbeauftragten des Landes, Prof. Tobias Keber, auf eine Lösung bei der Frage nach der Ortung von Notrufen unter der Nummer 110 verständigt. Danach soll die Weitergabe der Standortdaten in einem „vorläufigen bundesweiten Pilotbetrieb" möglich sein, sofern diese „nur zur Hilfe und nicht zur Strafverfolgung" genutzt wird.

Die Polizei arbeitet an einer schnellstmöglichen technischen Umsetzung zur Nutzung der mitunter lebenswichtigen Informationen. Wegen rechtlicher Hürden in Baden-Württemberg kann die Polizei bisher 110-Notrufe bundesweit nicht schnell zurückverfolgen. Die Ortungsdaten aus ganz Deutschland fließen zentral nach Baden-Württemberg. Die Rechtslage im Südwesten erlaubt aber bisher nicht den Abruf und die Weitergabe. Es ist zumindest unklar, ob das Polizeigesetz dafür eine ausreichende Rechtsgrundlage bietet.

Wer in Not gerät, die 110 wählt und nicht mehr in der Lage ist, seinen genauen Standort mitzuteilen, den können die Beamten deshalb nicht so schnell finden, wie es eigentlich möglich und oft nötig wäre. Während bei der Rufnummer 112 eine Ortung erlaubt ist, ist das bei der 110 nicht der Fall, wie das Innenministerium Schleswig-Holstein beklagt: „Die föderale Struktur Deutschlands ist hier zurzeit aus rechtlichen Gründen hinderlich."

Technisch ist die Ortung über das Verfahren „Advanced Mobile Location" (AML) schnell und präzise machbar. Dabei werden auf einem Smartphone beim Wählen des Notrufs verschiedene Sensoren wie WLAN und GPS eingeschaltet und die Daten über die Mobilfunknetze automatisch übertragen. Die Übertragung funktioniert auch – alle Daten landen in Baden-Württemberg. Im Schwarzwald steht der zentrale AML-Server für ganz Deutschland, der für den 112-Bereich genutzt wird.

Der baden-württembergische Landesbeauftragte für den Datenschutz monierte bisher, dass für den Umgang mit den Informationen die Rechtsgrundlage fehlt. Nur im Einzelfall dürfe der Standort hilfloser Menschen ermittelt werden. Für die automatische Übermittlung sei eine Rechtsgrundlage nötig, die klarstellt, was mit den Daten genau gemacht werden darf, so ein Sprecher: „Dies gilt insbesondere im Falle der Polizei, die nicht nur dafür zuständig ist, in Notlagen zu helfen, also Gefahren abzuwehren, sondern auch im Falle von Anhaltspunkten für Straftaten zu ermitteln." Die Standortdaten dürften ausschließlich zur Hilfeleistung verwendet werden: „Dies auch mit Blick darauf, dass Menschen nicht aus Angst vor der automatisierten Standortübermittlung von einem Anwählen des Notrufs absehen sollten." Im Gegensatz zum Polizeinotruf 110 besteht für die Ortung der 112-Anrufer eine klare Rechtsgrundlage. Geht es um eine konkrete Gefahr für Leib und Leben, können die Beamten auch bei der 110 bereits jetzt über die sogenannte Funkzellenabfrage Verletzte und Vermisste orten, was aber aufwändiger und zeitintensiver ist.

Nach dem Okay des Datenschutzbeauftragten startet ein Pilotbetrieb. Gleichzeit will das Innenministerium Baden-Württemberg eine Rechtsgrundlage schaffen. Der Landeschef der Deutschen Polizeigewerkschaft, Ralf Kusterer, kommentierte: „Der Normalbürger versteht unseren Staat manchmal nicht mehr. Gerade bei der Ortung von 110 ist in der Regel höchste Eile geboten. Wer diese Ortung nicht zulässt, gefährdet Leib und Leben." Er kritisierte, dass die

Prüfung beim Ministerium schon viel zu lange andauere (Streit um 110: Datenschützer erlauben bundesweite Notruf-Ortung, www.heise.de 20.03.2024, Kurzlink: https://heise.de/-9659860).

Nordrhein-Westfalen

Erste DSGVO-Akkreditierung für und erstes DSGVO-Zertifikat durch EuroPriSe

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat die Bonner EuroPriSe Cert GmbH als erste Stelle in Deutschland als Zertifizierungsstelle gemäß der Datenschutz-Grundverordnung (DSGVO) Art. 43 DSGVO akkreditiert. EuroPriSe ist damit befugt Datenverarbeitungsprozesse auf gesetzlicher Grundlage zu zertifizieren. Ab sofort können Auftragsverarbeiter ihre Datenverarbeitungsprozesse von dieser Stelle zertifizieren lassen.

Bereits Ende 2022 wurden die Zertifizierungskriterien, die die Grundlage der Zertifizierungsstelle für ihre Tätigkeit darstellen, durch die LDI NRW als zuständige Behörde genehmigt. Daran schloss sich das mehrstufige, von der LDI NRW gemeinsam mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) durchgeführte Akkreditierungsverfahren an. Die Befugniserteilung war der letzte notwendige Verfahrensschritt, damit die Zertifizierungsstelle ihre Arbeit beginnen kann. Eine Akkreditierung wird zeitlich befristet für eine Höchstdauer von fünf Jahren erteilt. Eine anschließende Re-Akkreditierung ist möglich.

Praktisch zeitgleich erteilte EuroPriSe der RISER ID Services GmbH als erstem Auftragsverarbeiter gemäß dem DSGVO-Kriterienkatalog das erste Zertifikat. Konkret wird damit bestätigt, dass RISER ID bei der Erbringung des RISER-Dienstes für digitale Melderegisterauskünfte alle einschlägigen rechtlichen und technisch-organisatorischen Anforderungen für Auftragsverarbeiter erfüllt. Das Datenschutzzertifikat ist drei Jahre gültig.

Die LDI NRW, Bettina Gayk, erklärte: „Zertifikate sind ein wichtiges Instrument, um ein hohes Datenschutz-Niveau zu gewährleisten. Wer einen zertifizierten Auftragsverarbeiter auswählt, trifft eine gute Wahl und erhält Sicherheit, dass dessen Datenschutzkonformität in einem transparenten Verfahren überprüft und überwacht wird." Zertifikate sollen zu einem Instrument werden, um auf dem Markt eine Orientierung zu datenschutzkonformen Produkten zu schaffen. Zertifikate bedeuten für alle, deren Daten verarbeitet werden, mehr Transparenz. Sie liefern einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen (LDI NRW erteilt die Befugnis für erste deutsche Zertifizierungsstelle, PE 02.02.2024; EuroPriSe, Erste Datenschutzzertifizierung für Auftragsverarbeiter nach von der LDI NRW genehmigtem Kriterienkatalog, PE 17.01.2024).

Sachsen-Anhalt

Christina Rost ist neue Landesdatenschutzbeauftragte

Nach einer seit 2018 dauernden Hängepartie wurde am 24.04.2024 die Juristin Maria Christina Rost vom Landtag Sachsen-Anhalt gleich im ersten Wahlgang zur neuen Landesdatenschützerin gewählt. Eine Neubesetzung war zuvor mehrfach misslungen (DANA 2/2018, 108 f.; 1/2019, 40; 4/2022,262 f.; 3/2023, 94 f.). Bei der Wahl erhielt die 49-Jährige 66 Ja-Stimmen. 26 Abgeordnete stimmten mit Nein, zwei enthielten sich. Für die Wahl waren mindestens 49 Stimmen notwendig. Die Koalitionsparteien von CDU, SPD und FDP verfügen zusammen über 56 Stimmen. Rost war zuvor beim hessischen Datenschutzbeauftragten in Wiesbaden in der Rechtsabteilung und der Öffentlichkeitsarbeit tätig. CDU-Fraktionsvize Sandra Hietl-Heuer hatte bereits vor der Wahl erklärt, Rost verfüge über ein ausgezeichnetes Netzwerk und kenne sich im Datenschutz aus. Auch die SPD sowie die Oppositionsparteien Linke, Grüne und AfD hatten sich anerkennend geäußert.

Das Amt des Landesdatenschutzbeauftragten war in Sachsen-Anhalt seit 2018 unbesetzt. Mehrere Kandidaten hatten sich seitdem auf den Posten beworben. Keiner von ihnen konnte im Landtag die notwendige Stimmenmehrheit auf sich vereinen. Die Verfassungsregelung des Landes wurde zu diesem Thema geändert.

Zuletzt hatte der Jurist Daniel Neugebauer im Juni 2023 im Landtag in drei Anläufen nicht die erforderliche Mehrheit erhalten. Im dritten Wahlgang hatte der Rechtsanwalt 48 Ja-Stimmen bekommen. Warum es am Ende nicht geklappt hatte, blieb nach den geheimen Wahlgängen offen. Die CDU hatte Neugebauer, der Mitarbeiter der Anwaltskanzlei von FDP-Fraktionschef Andreas Silbersack ist, vorgeschlagen. Die Opposition hatte den Vorschlag heftig kritisiert.

Vor der erfolglosen Wahl 2023 hatte sich extern Malte Engeler, Richter am schleswig-holsteinischen Verwaltungsgericht, beworben: „Ich bewerbe mich hiermit formell um eine Berücksichtigung im Wahlverfahren. Meine fachliche und persönliche Qualifikation darf ich angesichts langjähriger Befassung mit rechtlichen und technischen Fragen der Digitalisierung und des Datenschutzrechts, zahlreicher Veröffentlichungen in der Fachliteratur, wiederholter Tätigkeit als Sachverständiger auf Bundes- und Landesebene sowie konstantem, zivilgesellschaftlichen Engagement als gegeben annehmen." Die Koalitionsfraktionen von CDU, SPD und FDP hatten im April 2023 für einen neuen § 21 des Landesdatenschutzgesetzes gestimmt, wonach die Stelle als Datenschutzbeauftragter nicht mehr offiziell ausgeschrieben werden muss und nur die Fraktionen des Landtages vorschlagsberechtigt sind. Da Engeler das Verfahren ohne Ausschreibung für unzulässig ansah, zog er vor das Verwaltungsgericht Magdeburg, das jedoch seinen Eilantrag mit Beschluss vom 25.04.2023 ablehnte.

Engeler wurde damals von der gemeinnützigen Organisation „Frag Den Staat" unterstützt: „Grundsätzlich soll das Land Sachsen-Anhalt ein transparentes Verfahren etablieren – so wie im EU-Recht vorgeschrieben. Ein solches Verfahren müsste mindestens eine öffentliche Ausschreibung der Stelle, eine öffentliche Anhörung der Bewerberinnen und Bewerber, Transparenz bezüglich der Qualifikationen und die Dokumentation des Auswahlverfahrens beinhalten." Im Zweifel wolle man hierfür auch den Europäischen Gerichtshof bemühen, so Arne

Semsrott von „Frag Den Staat“ (Wahl im Landtag: Sachsen-Anhalt hat neue Landesdatenschutzbeauftragte, www.mdr.de 24.04.2024; Neue Kandidatin für Amt des Datenschutzbeauftragten, www.mdr.de 14.03.2024; Frohmüller, Geplante Wahl des Datenschutzbeauftragten: Externer Bewerber vor Gericht vorerst gescheitert, www.mdr.de 27.06.2023; Fahnert, Heftige Kritik an Kandidaten-Auswahl für Amt des obersten Datenschützers, www.mdr.de 26.04.2023).

Datenschutznachrichten aus dem Ausland

Weltweit

Europarat besorgt über Journalistenüberwachung

Der Europarat sieht die Arbeit von Journalistinnen und Journalisten in Europa teilweise bedroht. Gemäß einem Bericht einer Partnerorganisation des Europarats zum Schutz von Journalisten, der am 05.03.2024 in Straßburg und Thessaloniki veröffentlicht wurde, gehören der rechtswidrige Einsatz von Spähsoftware gegen Medienschaffende, einschüchternde Klagen und die prekäre Lage von Reportern im Exil zu den größten Hindernissen für die Pressefreiheit. Die digitale Sicherheit von Journalisten sei durch den anhaltenden Einsatz von Spyware-Technologie gefährdet. Deshalb sollen die Mitgliedsstaaten des Europarats Journalistinnen und Journalisten den größtmöglichen Schutz vor Spionageprogrammen und Abhörmaßnahmen einräumen. Der Europarat wurde 1949 zum Schutz von Demokratie, Menschenrechten und Rechtsstaat in Europa gegründet. Er ist von der Europäischen Union unabhängig. Ihm gehören 46 europäische Staaten an.

Gemäß dem Europarat wird eine „beispiellose Zahl von Medienschaffenden“ insbesondere aus Russland und Belarus mit Drohungen und Einschüchterungen ins Exil getrieben. Die Mitgliedsstaaten des Europarats sollen für solche Fälle humanitäre Visaregelungen einführen und die Ausstellung von Arbeitsvisa erleichtern. Weiter werde die Medienfreiheit durch sogenannte Slapp-Klagen eingeschränkt. Die Kurzform Slapp steht im Englischen für „Strategische Klagen gegen öffentliche Beteiligung“. Die Klagen zielen darauf ab Menschen, die sich zu Themen von öffentlichem Interesse äußern, einzuschüchtern oder zum Schweigen zu bringen. Die Generalsekretärin des Europarats, Marija Pejčinović Burić, erklärte: „Wir brauchen entschlossenes Handeln der Staaten, um Journalisten zu schützen und Bedrohungen der Medienfreiheit wie missbräuchliche Klagen und illegaler Überwachung entgegenzuwirken“ (Europarat besorgt über Einsatz von Spähsoftware gegen Journalisten, https://web.de/magazine/panorama/europarat-besorgt-einsatz-spaehsoftware-journalisten-39398554 05.03.2024).

Europa

Hohes Niveau von Anträgen zum Recht auf Vergessenwerden

Aus einer Studie des IT-Sicherheitsunternehmens Surfshark, das die Transparenzberichte der Suchmaschinenbetreiber Google und Microsoft für die Länder des Europäischen Wirtschaftsraums (EWR) sowie Großbritannien und die Schweiz auswertete, geht hervor, dass die beiden Unternehmen 2022 über 155.000 Anforderungen rund um das Recht auf Vergessenwerden, das in der Datenschutz-Grundverordnung (DSGVO) verbrieft ist, erhielten. Dabei gingen die meisten Anfragen mit 147.000 (96%) an Google. Die Gesamtzahl ist 2022 im Vergleich zu 2021 um 16% zurückgegangen, was das erste Minus seit Beginn der Corona-Pandemie im Jahr 2020 darstellt. Microsoft verzeichnete für seine Suchmaschine Bing einen leichten Anstieg der Löschanträge von 7.700 auf 8.200.

Auf Frankreich, Deutschland und das Vereinigte Königreich entfielen laut der Analyse 2022 über 50% aller Anträge zum Recht auf Vergessenwerden. Franzosen reichten mit insgesamt 43.000 die meisten Ersuchen ein (rund 25%). Allerdings war die Gesamtzahl der französischen Anfragen um 12% niedriger als 2021. Deutschland und das Vereinigte Königreich belegten mit 24.166 beziehungsweise rund 16.000 Anfragen den 2. und 3. Platz, was einem Rückgang von 24% bzw. 15% gegenüber dem Vorjahr entspricht. Italien und Spanien belegten den 4. und 5. Rang. Rechnet man die Zahl der Anfragen auf die Bevölkerung um, lagen Schweden und Frankreich mit 7 Löschanträgen pro 10.000 Einwohner an der Spitze der Liste.

Das Recht auf Vergessenwerden ermöglicht es Einzelpersonen die Löschung namensbezogener Informationen von den Ergebnisseiten europäischer Suchmaschinen zu beantragen. Dabei geht es der Untersuchung zufolge um eine breite Palette von Angaben, die von beruflichen Daten bis zu Verbindungen mit kriminellen Aktivitäten reichen. Die 155.000 Anfragen bezogen sich den Forschern zufolge auf etwa 600.000 URLs, von denen die beiden großen Betreiber 56% beziehungsweise 50% heruntergenommen hätten. Als Begründung dafür, die angeforderten Links nicht aus den Suchmaschinen zu entfernen, gaben die Betreiber etwa technische Probleme sowie ein starkes öffentliches Interesse und das Recht an online auf die Informationen zuzugreifen. Politische Inhalte bleiben am häufigsten in den Trefferlisten.

Seit dem Urteil des Europäischen Gerichtshofs (EuGH) vom 13.05.2014 (C-131/12) entfernte allein Google der Studie zufolge sechs Milliarden URLs aufgrund von Löschanträgen. Soziale Netzwerke waren demnach das häufigste Ziel solcher Ersuchen, wobei Inhalte auf Facebook besonders umstritten waren. 129.000 Links zur Meta-Tochter sollten nicht mehr angezeigt werden; zwei Fünfteln der Anforderungen kam Google hier nach. Am zweit- beziehungsweise

dritthäufigsten betrafen die Anfragen Beiträge auf X und YouTube. Die Daten zeigen für Surfshark, dass sich das Interesse am Recht auf Vergessenwerden in den vergangenen Jahren auf vergleichsweise hohem Niveau eingependelt habe. Da während der Pandemie viele alltägliche Dinge in den Cyberraum verlagert worden seien, hätten sich Nutzer damals offenbar zu einer bewussteren „digitalen Hygiene" ermutigt gesehen und mehr auf ihre Online-Privatsphäre geachtet (Krempl, Vergessenwerden: 24.000 Löschanträge bei Google stammten 2022 aus Deutschland, www.heise.de 04.04.2024, Kurzlink: https://heise.de/-9675711).

EU

Einigung über PNR-Daten

Unterhändler des EU-Parlaments und des EU-Rats haben sich am 01.03.2024 darauf geeinigt, welche Fluggastdaten (Passenger Name Records – PNR-Daten) wie gespeichert und mit den nationalen Behörden in der EU geteilt werden sollen. Die Regelung betrifft die sog. erweiterten Fluggastdaten (API). Diese enthalten den Namen des Fluggastes, sein Geburtsdatum, seine Staatsangehörigkeit, seine Reisepassdaten sowie grundlegende Fluginformationen. Sie müssen vor und nach dem Abflug an die Behörden am Ankunftsort übermittelt werden.

Die API sollen mit weiteren PNR-Daten kombiniert werden, die von Fluggesellschaften erfasst und gespeichert werden. Dazu gehören Informationen wie der Name des Fluggastes, Reisedaten, Reiserouten, Sitznummern, Gepäckangaben, Kontaktangaben und Zahlungsarten. So sollen im Kampf gegen Terrorismus und schwere Kriminalität besonders gefährliche Passagiere entdeckt werden können. Gespeichert werden sollen die Daten in der Regel 48 Stunden. Fluggesellschaften müssen die in Reisedokumenten enthaltenen Daten automatisiert sammeln, zum Beispiel, indem sie maschinenlesbare Pässe scannen. Wenn das nicht möglich sein sollte, können Airlines die Daten im Online-Check-in oder im Check-in am Flughafen manuell sammeln. Dafür soll es eine Übergangszeit von zwei Jahren geben. Die Daten werden zentral gesammelt; eine EU-Agentur soll die dafür nötige Technik entwickeln. Die dort gesammelten Daten gehen dann an die zuständigen Grenzüberwachungs- und Strafverfolgungsbehörden.

Zu der 2016 beschlossenen PNR-Richtlinie für die Übermittlung dieser Daten hatte im Juni 2022 der Europäische Gerichtshof entschieden, dass viele EU-Mitgliedsstaaten ihre nationalen Gesetze zu deren Umsetzung neu fassen müssen (DANA 3/2022, 201 f.). Grundsätzlich sind von den nun beschlossenen Regeln nur Flüge betroffen, die außerhalb der EU starten. Die Mitgliedsstaaten könnten jedoch beschließen auch Flüge innerhalb der EU zu erfassen. Eine solche Entscheidung hänge ab von spezifischen Bedürfnissen – wie einer terroristischen Bedrohung – der Strafverfolgungsbehörden, wozu mithilfe der Daten eine Risikobewertung unterstützt werden kann (Wilkens, Fluggastdaten: EU-Rat und EU-Parlament einigen sich auf Erfassung und Weitergabe, www.heise.de 01.03.2024, Kurzlink: https://heise.de/-9644242).

EU

EDSA gegen „Pay or Okay"

Der Europäische Datenschutzausschuss (EDSA, European Data Protection Board – EDPB) hat mit einer Stellungnahme vom 17.04.2024 große Online-Plattformen dazu aufgefordert ihren Nutzern bei ihren Diensten mehr Alternativen anzubieten. Vielfach werden Anwender nur vor die Wahl gestellt entweder zu zahlen oder zuzustimmen, dass sie ihre Daten für personalisierte Werbung freigeben. Der EDSA verlangt eine weitere Alternative zu Online-Gebühren oder Abonnements, ohne oder mit geringerer Datenfreigabe.

Datenschützer Deutschlands, Norwegens und der Niederlande hatten die Diskussion im EDSA formell angeregt. Bei der Stellungnahme handelt es sich lediglich um eine Positionierung ohne bindende Wirkung. Der EDSA als Ausschuss der europäischen Aufsichtsbehörden ist für die einheitliche Anwendung der Datenschutz-Grundverordnung (DSGVO) zuständig. Diese dürften bei ihren Tätigkeiten dieser Meinung folgen und könnten Online-Plattformen entsprechend abmahnen.

Große Online-Plattformen wie die von Meta, z.B. Facebook oder Instagram, bieten entweder ein kostenpflichtiges Abo oder verlangen von den Nutzern das Einverständnis zur Freigabe persönlicher Daten, damit für Werbetreibende personalisierte Anzeigen ausgespielt werden können. Wenn ein Anwender auf Datenschutz Wert legt und den Dienst nutzen möchte, muss er eine Gebühr zahlen.

Der EDSA kritisiert dies, da Anwender oft umgehend die kostenlose Option wählen, ohne sich der Konsequenzen für den Datenschutz bewusst zu sein. Deshalb fordert der Datenschutzausschuss eine weitere Option von den großen Online-Plattformen. Statt lediglich „Zustimmen oder zahlen" anzubieten, sollen diese eine zusätzliche Alternative vorlegen. Diese soll gebührenfrei sein und keine oder weniger Daten von den Anwendern fordern.

Der EDSA beruft sich auf Artikel 5 DSGVO, der Zweckbindung, Datenminimierung und Fairness als Prinzipien des Datenschutzes anführt. Große Online-Plattformen sollten zudem die Einhaltung der Grundsätze der Notwendigkeit und Verhältnismäßigkeit berücksichtigen und nachweisen können, dass die Datenverarbeitung DSGVO-konform erfolgt.

Die Leiterin der finnischen Datenschutzbehörde und Rechtswissenschaftlerin Anu Talus ist seit knapp einem Jahr EDSA-Vorsitzende. Sie erklärte dazu: „Online-Plattformen sollten den Nutzern eine echte Wahlmöglichkeit bieten, wenn sie Einwilligungs- oder Bezahlmodelle anwenden. Die heutigen Modelle erfordern in der Regel, dass Einzelpersonen entweder alle ihre Daten preisgeben oder dafür bezahlen. Infolgedessen stimmen die meisten Benutzer der Verarbeitung zu, um einen Dienst zu nutzen, und sie verstehen nicht die vollständigen Auswirkungen ihrer Entscheidungen. Verantwortliche sollten stets darauf achten, dass das Grundrecht auf Datenschutz nicht zu einer Funktion wird, für deren Inanspruchnahme der Einzelne zahlen muss. Einzelpersonen sollten sich des Werts und der Konsequenzen ihrer Entscheidungen voll bewusst sein."

Meta Platforms steht bereits seit Jahren unter ständiger Beobachtung. 2023 hatten EU-Datenschützer Facebook und Instagram personalisierte Werbung untersagt. In der Folge führte der Konzern kostenpflichtige Abos dieser Dienste ein, um deftige Strafen der EU abzuwenden (Schräer, EU verlangt von Online-Plattformen Gratis-Dienste ohne personalisierte Werbung, www.heise.de 18.04.2024, Kurzlink: https://heise.de/-9688890; siehe auch den Aufruf auf S. 84; Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf).

EU

Transparenzpflicht bei politischer Werbung

Gemäß einer EU-Verordnung über die Transparenz und das Targeting politischer Werbung, die am 09.04.2024 in Kraft trat, muss bezahlte politische Werbung für die Bürgerinnen und Bürger als solche und deren Hintergrund einfacher zu erkennen sein. Es muss deutlich werden, so die Mitteilung der Europäischen Kommission, „wer wie viel dafür bezahlt hat, an welche Wahlen, welches Referendum oder welchen Regulierungsprozess sie geknüpft ist und ob Techniken zur gezielten Werbung verwendet wurden". „Die neuen Regeln gelten ab sofort und damit auch für die Wahlen zum Europäischen Parlament vom 6. bis 9. Juni 2024." Sie seien Teil der Maßnahmen, um die Integrität von Wahlen zu schützen. Weiter sollen sie „eine offene demokratische Debatte fördern". Věra Jourová, Vizepräsidentin der EU-Kommission für Werte und Transparenz, erläuterte, dies fördere nicht nur die Transparenz politischer Werbung: „Das neue Gesetz [...] bietet einen besseren Schutz vor ausländischer Einflussnahme und Manipulation."

Gemäß der Verordnung muss jede politische Anzeige „in klarer, hervorgehobener und eindeutiger Weise" deutlich machen, dass es sich um eine politische Anzeige handelt, wer diese finanziert und welche Einrichtung den Sponsor gegebenenfalls kontrolliert. Ebenso braucht es einen Hinweis auf den etwaigen Anlass, auf den die Anzeige zurückgeht, ob die politische Anzeige Teil von Targeting- oder Anzeigenschaltungsverfahren ist, sowie eine Transparenzmitteilung, wo diese Informationen zu finden sind. Die neue Verordnung umfasst auch das politische Targeting, also die sehr auf die ausgewählte Zielgruppe zugeschnittene Ausspielung und Anzeige von Werbung. Techniken dafür stünden ausschließlich auf Basis personenbezogener Daten, erhoben von der betroffenen Person, und nur mit deren Zustimmung zur Verfügung. Sensible personenbezogene Daten, etwa die sexuelle Orientierung, Religion oder politische Einstellung, dürfen die Akteure nicht verwenden. Die Kommissions-Mitteilung erläutert: „Dadurch wird die missbräuchliche Verwendung personenbezogener Daten eingeschränkt, die darauf abzielt Wählerinnen und Wähler zu manipulieren." Zudem werde politische Online-Werbung künftig in einem Online-Verzeichnis gespeichert. Ein Sponsoring seitens Akteuren außerhalb der EU wird künftig ebenfalls eingeschränkt: Dieses wird in den drei Monaten vor der Wahl verboten (VO (EU) 2024/900 v. 13.03.2024, ABl. EU v. 20.03.2024; Reckeweg, EU-Verordnung: Politische Werbung muss als solche zu erkennen sein, www.heise.de 10.04.2024, Kurzlink: https://heise.de/-9680758).

EU

EDSB beanstandet Microsoft-365-Einsatz durch Kommission

Der EU-Datenschutzbeauftragte (EDSB) Wojciech Wiewiórowski hat am 11.03.2024 das Ergebnis seiner im Mai 2021 gestarteten und am 08.03.2024 mit einer Entscheidung abgeschlossenen Untersuchungen des Einsatzes von Microsoft Office 365 (MS 365) durch die EU-Kommission bekanntgegeben. Demnach hat die Brüsseler Regierungsinstitution mit der Nutzung des Cloud-Pakets des US-Softwareriesen gegen mehrere Vorgaben aus der speziellen Datenschutzverordnung für die EU-Institutionen verstoßen. Der Kontrolleur reibt sich demnach besonders daran, dass die Kommission kein hinreichendes Schutzniveau persönlicher Informationen gewährleistet habe, die über MS 365 in Drittstaaten wie die USA gehen. Die sogenannten Standardvertragsklauseln für Transfers an Microsoft, die der Konzern schon mehrfach überarbeitet hat, seien nicht klar genug gewesen.

Ferner hat die Kommission in ihrem Vertrag mit Microsoft generell nicht ausreichend spezifiziert, welche Arten personenbezogener Daten zu welchen expliziten und festgelegten Zwecken bei der Nutzung von MS 365 erhoben werden. Die Verstöße der Kommission in ihrer Funktion als verantwortliche Stelle für die Datenverarbeitung betreffen auch deren Datenübermittlung. Sie habe keine effektiven technischen und organisatorischen Schutzmaßnahmen ergriffen, die auch jenseits der EU und des Europäischen Wirtschaftsraums (EWR) eine Verarbeitung im Einklang mit dem Grundsatz der Integrität und Vertraulichkeit gewährleisten.

Wiewiórowski leitete die Ermittlungen nach dem „Schrems-II-Urteil" des Europäischen Gerichtshofs (EuGH) ein, womit dieser das „Privacy Shield" zwischen der EU und den USA kippte (DANA 3/2020, 199 ff.). Viele Verträge für Cloud-Dienste waren vor dieser Grundsatzentscheidung abgeschlossen worden und mussten im Lichte der Rechtsprechung überprüft werden. Inzwischen gibt es mit dem EU-US-Datenschutzrahmen zwar ein Nachfolgeabkommen, das Kritikern zufolge aber ebenfalls auf tönernen Füßen steht und nicht lange halten dürfte (DANA 3/2023, 164 f.).

Der EDSB hat mit seiner Entscheidung die Kommission angewiesen, 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 EWR ergeben. Ausnahmen gelten nur für Drittstaaten, die laut der Kommission ein vergleichbares

Datenschutzniveau wie die EU haben. Die Exekutivinstanz muss zudem bis zu dem Stichtag nachweisen, dass sie die Schutzverordnung einhält. Die Abhilfemaßnahmen hält Wiewiórowski „angesichts der Schwere und Dauer der festgestellten Verstöße" für „angemessen, notwendig und verhältnismäßig". Viele der Rechtsverletzungen beträfen eine große Zahl von Einzelpersonen. Weitere Sanktionen hat sich der Kontrolleur vorbehalten. Er prüfte damit die Verträge der EU-Einrichtungen mit Microsoft bereits wiederholt. Auch 2020 war er zu dem Ergebnis gelangt, dass die Zwecke der Datenverarbeitung beim Nutzen von Windows oder Microsoft Office viel zu offen definiert sind. Die Regeln für Unterauftragsverarbeiter seien unzureichend, Daten könnten ohne Kontrolle der EU-Institutionen in Drittstaaten übertragen werden. Am besten sollten sich Nutzer daher laut dem Beauftragten nach Alternativen umschauen, die höhere Datenschutzstandards erlauben. Hierzulande unterstrich in Deutschland die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder im Jahr 2022 auch, dass Einrichtungen wie Ämter, Schulen und Unternehmen das Office-Paket von Microsoft mit Cloud-Anschluss nicht ohne Weiteres rechtskonform einsetzen könnten (Krempl, EU-Datenschutzbeauftragter: EU-Kommission hat Microsoft 365 rechtswidrig genutzt, www.heise.de 11.03.2024, Kurzlink: https://heise.de/-9651423).

EU/Niederlande

Bußgeld gegen Uber wegen ungenügender Auskunftserteilung

Die niederländische Datenschutzbehörde Autoriteit Persoonsgegevens (AP) hat mit Beschluss vom 11.12.2023 ein Bußgeld in Höhe von 10 Millionen Euro gegen Uber verhängt, weil der Konzern Fahrern nicht angemessen Auskunft im Sinne der Datenschutz-Grundverordnung (DSGVO) erteilt hat. Der US-Konzern mit europäischem Hauptsitz in den Niederlanden hat den Kontrolleuren zufolge nicht ausreichend transparent gemacht, wie lange er Daten europäischer Fahrer aufbewahrt und in welche Drittländer diese übermittelt werden. Uber habe es den Fahrern ferner schwergemacht ihre Datenschutzrechte wahrzunehmen und einen Antrag auf Einsicht oder Herausgabe ihrer Daten zu stellen. Zwar habe es in der App ein digitales Formular gegeben, mit dem Chauffeure Zugang beantragen konnten, dieses sei aber „in allen Arten von Menüs" versteckt gewesen. Fanden die Fahrer den Menüpunkt trotzdem, habe Uber die angeforderten Daten nicht in einem leicht zugänglichen Format bereitgestellt. Uber hatte den Mitarbeitern eine Datei übermittelt, in der die personenbezogenen Angaben „nicht immer strukturiert und daher schwer zu interpretieren waren". Antragsteller erhielten Informationen über die Verarbeitung, der sie unterliegen, zudem nur in englischer Sprache.

Das Unternehmen habe in seinen Datenschutzbestimmungen auch nicht ausreichend angegeben, wie lange es Fahrerdaten speichert. Bei der Festsetzung der Höhe der Sanktion berücksichtigte die AP nach eigenen Angaben die Größe des Unternehmens sowie die Schwere der Verstöße. Zum Zeitpunkt der Beschwerde waren in Europa rund 120.000 Fahrer für die Plattform aktiv. Uber habe, so AP-Vorsitzender Aleid Wolfsen „eine hohe Hemmschwelle gesetzt, wenn Fahrer ihr Recht auf Privatsphäre wahrnehmen wollten. Das ist nicht erlaubt."

Uber hat mittlerweile gegen die Entscheidung Rechtsmittel eingelegt und muss die Strafe zunächst bis zu einer endgültigen Entscheidung nicht zahlen. Die Aufsichtsbehörde erkannte an, dass der Konzern inzwischen Maßnahmen ergriffen habe, um den Auskunftsrechten der Fahrer besser nachzukommen. Auslöser war eine Sammelbeschwerde der Menschenrechtsorganisation La Ligue des Droits de l'Homme, die über 170 Uber-Fahrer vertritt, bei der französischen Datenschutzbehörde CNIL. Die CNIL hatte den Fall an die hauptsächlich zuständige AP weitergeleitet (Krempl, Fahrerrechte missachtet: Uber soll 10 Millionen Euro DSGVO-Strafe zahlen, www.heise.de 01.02.2024, Kurzlink: https://heise.de/-9616016).

Frankreich

Über 33 Mio. Krankenkassendaten kompromittiert

Die Commission Nationale de l'Informatique et des Libertés (CNIL) untersucht als französische Datenschutzbehörde zwei riesige Datenlecks bei den Dienstleistern Viamedis und Almerys, von denen mit über 33 Millionen Personen knapp die Hälfte der Bevölkerung Frankreichs betroffen ist. Die beiden Dienstleister für Kranken- und Sozialversicherungen haben die Behörde über Cyberangriffe informiert, bei denen die persönlichen Daten Versicherter und ihrer Angehöriger im großen Stil kompromittiert worden seien. Von dem Ende Januar 2024 erfolgten Datenzugriff betroffen sind Informationen zu Familienstand, Geburtsdatum, Sozialversicherungsnummer, Krankenversicherer, die Leistungsdetails der abgeschlossenen Verträge. Bankverbindungen, medizinische Daten, erfolgte Erstattungen, Adressen, Telefonnummern und E-Mails sollen von dem Leck nicht betroffen sein.

Die CNIL betonte, dass es den jeweiligen Krankenkassen, die Viamedis und Almerys nutzen, obliegt „alle betroffenen Personen individuell und direkt zu informieren, wie es insbesondere die Datenschutz-Grundverordnung (DSGVO) vorsieht." Sie will dafür sorgen, „dass dies so schnell wie möglich geschieht", und auch ihre eigene Untersuchung schnell vorantreiben. Es gelte vor allem zu klären, ob die von den Unternehmen vor und nach dem Vorfall ergriffenen Sicherheitsmaßnahmen der Unternehmen angemessen waren.

Die CNIL empfiehlt Betroffenen vorsichtig zu sein bei potenziellen Anfragen, „insbesondere wenn es um die Erstattung von Gesundheitskosten geht". Es sei ratsam „regelmäßig die Aktivitäten und Bewegungen auf Ihren verschiedenen Konten zu überprüfen". Die kompromittierten Informationen könnten mit Beständen aus früheren Datenpannen kombiniert werden. 2021 waren in einem von Cyberkriminellen frequentierten Internet-Forum medizinische Daten von fast 500.000 Franzosen zum Verkauf angeboten worden. Berichten zufolge stammten diese Informationen

aus den Akten von etwa dreißig medizinischen Analyselabors.

Viamedis gab den Cybersicherheitsvorfall Anfang Februar 2024 auf LinkedIn bekannt. Die Webseite des Unternehmens war nach der Attacke nicht mehr erreichbar. Die Firma betreut Daten von 20 Millionen Versicherten und 84 angeschlossenen Gesundheitsorganisationen. Die Zahl der Betroffenen wollte Viamedis nicht offenlegen, da dies noch untersucht werde. Über die Panne bei Almerys berichteten anfangs nur lokale Medien unter Verweis auf anonyme Quellen. Das Unternehmen, dessen Homepage weiterhin abrufbar war, äußerte sich zu dem Leck zunächst nicht öffentlich. Almerys arbeitet nach eigener Darstellung mit über 2.000 Partnern zusammen, von denen 400 in Frankreich sitzen. Als Kunden nennt die Firma neben französischen Versicherungen etwa auch den Lebensversicherungskonzern Swiss Life, als hauptsächlichen IT-Dienstleister IBM (Krempl, Cyberangriff: Gesundheitsdaten von 33 Millionen Franzosen betroffen, www.heise.de 09.02.2024, Kurzlink: https://heise.de/-9624548).

Polen

Abhöraffäre wird aufgeklärt und bedrängt PiS

Die alte PiS-Regierung Polens hat offenbar nicht nur politische Gegner, sondern auch eigene Leute systematisch abgehört. Dies wird, wie vor seiner Wahl vom jetzigen Premierminister Donald Tusk angekündigt, untersucht und führt zu einer Zerreißprobe für die PiS-Partei. Tusk teilte dem der PiS nahestehenden polnischen Präsident Andrzej Duda mit, dass die Liste der Abgehörten „sehr, sehr lang“ sei. Der Justizminister werde eine Reihe von Dokumenten vorlegen, die nicht nur den Kauf der Spionage-Software Pegasus belegen, sondern auch den legalen und illegalen Einsatz zu 100 Prozent nachvollziehbar machen. Der Fall Pegasus spielt eine wichtige Rolle im Ringen der neuen Regierung darum das Vermächtnis der alten aufzuarbeiten und sich davon zu befreien. Schon 2023 war eine Untersuchungskommission zu dem Schluss gekommen, mit Pegasus seien systematisch Menschen überwacht worden, gegen die kein Verdacht auf ein Verbrechen bestand. Juristische Folgen hatte dieser Bericht jedoch nicht.

Tusk erklärte: „Das Dokument hier bestätigt leider, was wir befürchtet haben: Dass auf Initiative des Zentralen Antikorruptionsbüros der Kauf von Pegasus aus Mitteln des Gerechtigkeitsfonds beantragt und von Minister Ziobro bestätigt wurde. Ich muss sagen, das macht mich sehr traurig.“ Die PiS-Regierung hatte also in Gestalt des damals amtierenden Justizministers Zbigniew Ziobro den Kauf der Spionagesoftware Pegasus für umgerechnet 9,6 Millionen Euro beauftragt und im Geheimen finanziert – ausgerechnet mit Mitteln, die eigentlich für die Unterstützung von Verbrechensopfern gedacht waren.

Am 19.02.2024 kam der Pegasus-Untersuchungsausschuss des polnischen Abgeordnetenhauses Sejm zur ersten inhaltlichen Sitzung zusammen. Die neuen Regierungsparteien hatten vor der Wahl versprochen alle Regelbrüche und Gesetzesverstöße aus acht Jahren PiS-Regierung zu untersuchen und Verantwortliche zur Rechenschaft zu ziehen. Untersucht wird etwa die Visa-Affäre, bei der ohne größere Überprüfungen möglicherweise Tausende Arbeitsvisa ausgegeben wurden – die den Einwanderern teils dazu dienten, innerhalb Europas aber auch bis in die USA weiterzureisen. Ebenfalls untersucht wird die Briefwahl-Affäre aus dem Jahr der Präsidentschaftswahl 2020, wobei es um Verstöße gegen das Wahlrecht und den Datenschutz geht. Die Pegasus-Affäre könnte für die PiS-Partei die größte Sprengkraft haben: Es sieht so aus, als habe die Partei im Stile von Diktatoren nicht nur den Gegner, sondern auch die eigenen Leute abgehört. Selbst der frühere Ministerpräsident Mateusz Morawiecki soll auf der Liste stehen. Er wird voraussichtlich zu den Zeugen gehören, die von der Untersuchungskommission einbestellt werden, ebenso wie seine Vorgängerin, die frühere Ministerpräsidentin Beata Szydło und möglicherweise auch der Parteivorsitzende Jarosław Kaczyński. Für Kaczyński ist die Affäre ein „übel aufgeblasener Ballon“: „Nach allem, was ich weiß – wobei ich in dieser Sache nichts Genaues weiß – wurde Premierminister Morawiecki mit Sicherheit nicht abgehört.“ Alles, was unternommen worden sei, sei im Interesse der polnischen Nation gewesen.

Dass Gegner ausspioniert wurden, ist schon länger bekannt (DANA 1/2022, 47). Bereits Anfang 2022 – noch unter der PiS-Regierung – forderte Donald Tusk einen Untersuchungsausschuss. Der Oberste Rechnungshof hatte damals öffentlich gemacht, dass Pegasus im September 2017 angeschafft worden war. Die Regierung hatte offenbar den Kauf vor den eigenen Behörden verschleiert. Mit der Abhöraktion hatte PiS anscheinend versucht sich Vorteile im Wahlkampf 2019 zu verschaffen. So wurde unter anderem Krzysztof Brejza abgehört, der Kampagnenleiter der von Donald Tusk geführten Partei Bürgerplattform, außerdem eine Staatsanwältin, die wiederholt den Justizumbau kritisiert und aktiv dagegen gearbeitet hatte. Auch Journalisten sollen ausspioniert worden sein. Der Einsatz der Spähsoftware in Polen war so exzessiv, dass sogar der Hersteller – das israelische Unternehmen NSO – Polen die Lizenz wieder entzog.

Es musste erst zum Regierungswechsel kommen, damit die Vorwürfe aufgeklärt werden. Der elfköpfigen Kommission gehören auch vier Abgeordnete der PiS-Partei an. Sie stellt im Sejm die größte Fraktion. Zudem befasst sich die Staatsanwaltschaft mit dem Fall. Premier Donald Tusk betonte die Unabhängigkeit der Ermittler und des Untersuchungsausschusses. Er werde keine Erwartungen bezüglich des Ergebnisses formulieren und den Fall auch nicht für politische Kämpfe nutzen: „Alles, was offengelegt werden kann, wird auch offengelegt werden.“ Er stelle dem Präsidenten gern alle Informationen und Unterlagen zur Verfügung. Duda hatte sich bis dahin inhaltlich nicht zu Pegasus geäußert. Er sei für eine Untersuchung, sagt das PiS-nahe Staatsoberhaupt – allerdings nicht ohne Einschränkung: „Ich erwarte vom Staat vor allem Rechtschaffenheit. So ein rechtschaffener Mensch ist für mich Minister Mariusz Kaminski.“ Kaminski war der PiS-Innenminister, der

die Pegasus-Abhöraktion, wenn nicht gesteuert, dann doch mutmaßlich genutzt hat. Er wurde wegen Amtsmissbrauchs zu einer Haftstrafe verurteilt und war von Präsident Duda vor der Polizei versteckt und später begnadigt worden.

Die Vorsitzende des parlamentarischen Untersuchungsausschusses, Magdalena Sroka, gehört einer der neuen Regierungsparteien an und erklärte, sie habe nicht vor die PiS-Partei zu schonen. Sroka hatte früher selbst mit PiS zusammengearbeitet. Sie gehörte einer kleinen Partei an, die 2021 die Regierungskoalition mit PiS verließ. Vorangegangen war unter anderem ein Streit um den Ablauf der Präsidentschaftswahlen. Sroka erklärte, es erscheine ihr völlig einleuchtend, dass PiS auch die eigenen Leute oder Verbündete abhörte, um die Kontrolle zu behalten.

Die Sitzung des Untersuchungsausschusses am 19.02.2024 konnte live im Internet verfolgt werden. Sroka sagte, sie wolle so transparent wie möglich arbeiten und viele Informationen zugänglich machen. Das sei im Interesse der Öffentlichkeit: „Sie haben versucht das Leben von Menschen zu zerstören." Der Fall von Krzysztof Brejza, jenem Wahlkampfleiter der Bürgerplattform von 2019, zeige das deutlich. PiS spricht nun von ungeschickten Versuchen der Regierung die Partei zu zerstören. Dass die Spionage-Software benutzt wurde, streiten aber auch PiS-Leute nicht ab. Wie der Oberste Rechnungshof nachweist, hat die Regierung damals 25 Millionen Złoty für das Programm ausgegeben, umgerechnet knapp sechs Millionen Euro.

Die Generalstaatsanwaltschaft nannte inzwischen Zahlen zum Umfang der Abhöraktionen: Von 2017 bis 2023 sei die Software zu Beobachtung von 578 Personen eingesetzt worden. Justizminister Adam Bodnar kündigte an, dass 31 Personen, gegen die es Angriffe mit Pegasus gab, eine Vorladung der Staatsanwaltschaft bekommen, um als Zeugen auszusagen (PiS soll spioniert haben, SZ 17.04.2024, 6; Großmann, Abhörskandal bringt PiS in Bedrängnis. SZ 20.02.2024, 7; Adam, Abhöraffäre in Polen „Auf Schritt und Tritt begleitet", www.tagesschau.de 19.02.2024).

Schweden

noyb-Beschwerde gegen Pseudo-Medienunternehmen MrKoll

Die Bürgerrechtsorganisation noyb (none of your business) mit Sitz in Wien hat eine Beschwerde bei der schwedischen Datenschutzbehörde (IMY) zu einem der größten Datenhändler Schwedens, MrKoll, eingereicht („koll" ist schwedisch für „überprüfen"). Das Unternehmen verfügt über die Daten fast aller Schwed:innen und schlägt Profit daraus ohne deren Einwilligung einzuholen oder anderweitige datenschutzrechtliche Kontrollmechanismen zu beachten. Das Unternehmen nutzt eine Ausnahmeregelung der Datenschutz-Grundverordnung (DSGVO), wonach bei Vorliegen einer Medienlizenz vom dort geregelten Datenschutz eine Freistellung erfolgt. Diese Ausnahmeregelung dient ursprünglich dem Schutz von Journalisten. Artikel 85 DSGVO erlaubt es Mitgliedsstaaten die Anwendung einiger Elemente der DSGVO im Sinne der Pressefreiheit einzuschränken. Schweden wendet diese Privilegierung extensiv an. Gemäß dem dort geltenden Recht können u.a. Datenhändler, also Privatunternehmen, die persönliche Daten von Millionen Menschen kaufen und verkaufen, eine Medienlizenz erhalten und sich somit der Datenschutzkontrolle gemäß der DSGVO entziehen. Unter den von MrKoll gehandelten Daten befinden sich nicht nur die Namen, Geburtsdaten, Telefonnummern, Wohn- und Arbeitsadressen der Menschen. Das Unternehmen verfügt auch über Informationen zum Wert von Immobilien, zum gefahrenen Auto, zu anhängigen Zivilverfahren, Bußgeldern oder Strafregistereinträgen. Sollte die Datenschutzbehörde die Beschwerde auf Basis der nationalen Rechtslage abweisen, behält sich noyb vor Berufung beim Stockholmer Gericht einzulegen.

Stefano Rossetti, Datenschutzjurist bei noyb, erklärte: *„Das Geschäftsmodell von Datenhändlern wie MrKoll hat nichts mit Journalismus zu tun. Im Gegenteil, das Unternehmen gefährdet Menschen, indem es ihre persönlichen Daten ohne jegliche Schutzmaßnahmen zum Verkauf anbietet. Die schwedischen Behörden müssen diesem Missbrauch des Gesetzes, das ursprünglich zum Schutz von Journalist:innen gedacht war, endlich einen Riegel vorschieben."* Persönliche Daten würden von Gangs und Kriminellen genutzt. Ein Extrembeispiel dafür, welche Folgen der Verkauf persönlicher Daten durch Datenhändler wie MrKoll nach sich ziehen kann, zeigt ein Bericht, wonach sich rivalisierende Banden bei Datenhändlern bedienten, um den Standort ihrer Kontrahenten auszuforschen und Anschläge zu begehen (noyb, So umgehen schwedische Datenhändler die DSGVO, https://noyb.eu/de 14.03.2024).

Großbritannien

„Intelligente" Videoüberwachung erweist sich als unzuverlässig

Der Betreiber der Londoner U-Bahn „Transport for London" (TfL) hat die Videoüberwachung tausender Personen täglich von Künstlicher Intelligenz (KI) auf auffälliges Verhalten untersuchen lassen, um Straftaten oder unsichere Situationen zu erkennen. Die bestehenden Überwachungskameras wurden hierfür mit Machine-Learning-Software kombiniert. So sollten Waffen und Schwarzfahrer entdeckt werden, aber auch aggressives Verhalten oder wenn die Gefahr besteht, dass Personen auf die Gleise stürzen. In solchen Fällen wurde das Personal unmittelbar informiert.

Der Test wurde von Oktober 2022 bis Ende September 2023 an der oberirdischen U-Bahnstation namens Willesden Green getestet. Diese Station zählte vor der Coronapandemie rund 25.000 Besucher täglich. Es war das erste Mal, dass die Transportgesellschaft KI mit Live-Videoüberwachung kombiniert hatte und Mitarbeiter dabei entsprechend benachrichtigt wurden. Gemäß Berichten über den Untersuchungsbericht wurden innerhalb des Testzeitraums von fast einem Jahr mehr als 44.000 Alarme ausgelöst, wobei das Personal in 19.000 Fällen in Echtzeit informiert wurde. Die restlichen 25.000 Fälle wurden zu Analysezwecken gespeichert. Das KI-System sollte vor allem kriminelles und

unsoziales Verhalten erkennen. Es wurde aber auch darauf trainiert Rollstühle und Kinderwagen, Raucher und Personen zu erkennen, die unbefugte Bereiche betreten oder sich zu nahe am Rand des Bahnsteigs befinden.

Die KI erwies sich als äußerst fehlbar. So wurden Kinder, die ihren Eltern durch die Ticketschranken folgen, als potenzielle Schwarzfahrer identifiziert. Das System machte keine Unterscheidung zwischen einem zusammengeklappten und einem normalen Fahrrad; nur letzteres darf nicht in die U-Bahn mitgenommen werden. Die Polizei unterstützte den Test. Beamte, die bei geschlossener Station eine Machete und eine Schusswaffe offen trugen, sollten die KI auf die Erkennung von Waffen trainieren. Im Rahmen des Tests wurden allerdings keine Alarme wegen Waffen ausgelöst. Laut TfL-Bericht war auch die gewünschte Aggressionserkennung nicht erfolgreich, weil nicht ausreichend Daten für das KI-Training zur Verfügung standen. So wurden Alarme ausgelöst, wenn jemand die Arme nach oben streckt, was die Dokumente als „häufiges Verhalten im Zusammenhang mit aggressiven Handlungen" bezeichnen. Dies hat die KI während der Testphase in lediglich 66 Fällen mit potenziell aggressivem Verhalten festgestellt.

Alarme wurden ausgelöst, weil ein- und aussteigende Zugführer als Personen identifiziert wurden, die sich in unbefugten Bereichen befinden. Auch habe Sonnenlicht die KI-Auswertung der Videoüberwachung beeinträchtigt, wenn es direkt in die rund 20 Jahre alten Kameras schien. Besser erkannt wurden Schwarzfahrer. Die KI habe laut Bericht in 26.000 Fällen Alarm ausgelöst, weil jemand ohne Fahrschein fahren wollte. Datenschutzexperten stellen allerdings die Genauigkeit der Algorithmen zur Objekterkennung infrage. Sie warnen auch davor, dass eine solche KI-Videoüberwachung in Zukunft ausgeweitet werden könnte, etwa auf Gesichtserkennung. Die TfL versichert, dass während der Testphase alle Gesichter aufgenommener Personen verwischt und die Daten maximal 14 Tage vorgehalten wurden. Sechs Monate nach Beginn des Tests beschloss die TfL jedoch die Gesichter potenzieller Schwarzfahrer wieder erkennbar zu machen und bewahrte diese Daten länger auf (Schräer, KI-Videoüberwachung in Londoner U-Bahn zur Erkennung von Straftaten in Echtzeit, www.heise.de 09.02.2024, Kurzlink: https://heise.de/-9623370).

Großbritannien

Regierung will Erstellung von Nackt-Deepfakes unter Strafe stellen

Das britische Justizministerium kündigte an, die Regierung werde die Generierung von sexualisierten Deepfakes unter Strafe stellen, auch wenn die Inhalte nicht mit anderen geteilt würden. Die neuen Vorgaben sollen über eine Ergänzung zum Criminal Justice Bill umgesetzt werden. Das hätte zur Folge, dass die Generierung solcher Darstellungen und die – bereits verbotene – Verbreitung als zwei unterschiedliche Straftatbestände gelten, die getrennt voneinander verfolgt werden können. Die möglichen Konsequenzen gehen von der Einstufung als vorbestraft und Geldstrafen ohne eine Begrenzung nach oben bis hin zu Gefängnis. Der Schritt sei Teil mehrerer Maßnahmen, mit denen Frauen besser vor unterschiedlichsten Arten von Missbrauch geschützt werden sollen.

Die für den Gesetzentwurf zuständige Parlamentarische Staatssekretärin für Schutzmaßnahmen, Laura Farris, begründet den Plan damit, dass die Erstellung solcher Bilder „verwerflich und völlig inakzeptabel" sei. Es sei dann unerheblich, ob die Bilder geteilt würden oder nicht. Es zeige einmal mehr wie bestimmte Menschen versuchen würden, andere – und dabei vor allem Frauen – zu erniedrigen und zu entmenschlichen. Gleichzeitig könne es „katastrophale Folgen" haben, wenn solches Material verbreitet wird. Das werde die Regierung nicht tolerieren. Sie mache mit dem geplanten Straftatbestand eindeutig klar, dass die Herstellung solcher Inhalte „unmoralisch, oft frauenfeindlich und ein Verbrechen ist".

Deepfakes sind Videos oder Bilder, in denen Software die Gesichter der Dargestellten austauscht. Mit dem Aufkommen leistungsfähiger KI-Bild- und -Videogeneratoren ist die Erstellung solcher Inhalte sehr einfach geworden. Angebote zum „digitalen Entkleiden" beliebiger Personen anhand von normalen Fotos haben sich längst zu einem einträglichen Geschäftszweig entwickelt. Opfer sind vor allem Frauen und Mädchen (vgl. DANA 1/2024, 44 f.; 4/2023, 232; Holland, KI-Nacktbilder: Großbritannien will Erschaffung von Deepfakes separat verbieten, www.heise.de 16.04.2024, Kurzlink: https://heise.de/-9686412).

Belarus

Cyberangriff auf Geheimdienst

Einer Gruppe von Hacktivisten ist es nach eigenen Angaben gelungen den staatlichen Geheimdienst von Belarus, der sich nach der Unabhängigkeit des Landes weiterhin KGB nennt, zu infiltrieren und Personalakten zu mehr als 8.600 Angestellten einzusehen. Laut den „Cyber Partisans" (auf belarussisch „кіберпартызаны") ist die Internet-Seite des KGB schon seit zwei Monaten nicht mehr erreichbar. Auf der Startseite heißt es inzwischen lediglich, dass sich das Portal „in der Entwicklung" befinde. Der Gruppe ist es angeblich bereits im Herbst 2023 gelungen dort einzudringen und „alle verfügbaren Informationen" abzugreifen. Zum Beweis werden Datenbanken publik gemacht.

Yuliana Shametavets, eine Art Sprecherin der Gruppe, teilte mit, die Veröffentlichung einer Liste von Administratoren der Internetseite, der gesamten Datenbank und von Server Logs sei eine Reaktion auf den Vorwurf des KGB-Chefs, dass die „Cyber-Partisanen" Angriffe auf kritische Infrastruktur des Landes planten. Der Geheimdienstchef habe vorher behauptet, dass die Hacktivisten sogar Atomkraftwerke ins Visier nehmen würden: „Der KGB führt die umfangreichste Repression in der Geschichte des Landes durch und muss sich dafür verantworten. Wir setzen uns dafür ein die Leben der Menschen in Belarus zu schützen und nicht sie zu zerstören, wie die repressiven Sicherheitsdienste."

Gemäß Shametavets ist es der Gruppe schon vor Jahren gelungen in das Netz-

werk des KGB einzudringen. Seitdem sei versucht worden die Datenbank zu erbeuten. Nachdem das gelungen ist, hat die Gruppe nun einen Telegram-Bot eingerichtet, mit dem Menschen aus Belarus Geheimdienstangestellte identifizieren können. Dazu müssen sie demnach lediglich Fotos für eine Gesichtserkennung hochladen. Die Sprecherin kündigt an, dass es für das Regime immer schlimmer werden würde, wenn die Repression nicht eingestellt werde. Man werde die Attacken fortführen und dem Regime maximal möglichen Schaden zufügen.

Die „Cyber-Partisans" haben sich im Zuge der später blutig unterdrückten Proteste gegen das Regime von Alexander Lukaschenko nach den umstrittenen Wahlen vom August 2020 zusammengefunden. Seit ihrer Gründung haben sie mit mehreren Hacks unter anderem von Sicherheitsbehörden auf sich aufmerksam gemacht. Mit den koordinierten Angriffen wollen sie „die Gewalt und Repression des terroristischen Regimes in Belarus beenden und das Land zurückbringen zu demokratischen Prinzipien und zur Rechtsstaatlichkeit". Kurz vor dem umfangreichen Einmarsch russischer Truppen in die Ukraine hatte die Gruppe einen Cyberangriff auf die Bahngesellschaft von Belarus ausgeführt, um unter anderem den Transport russischer Waffen und Truppen durch das Land zu erschweren (Holland, KGB von Belarus angeblich gehackt: Telegram-Bot soll Angestellte deanonymisieren, www.heise.de 29.04.2024, Kurzlink: https://heise.de/-9701449).

Russland

Moskaus Videoüberwachung wird aus Holland trainiert

Die Firma Toloka aus den Niederlanden, eine Tochter des russischen Suchmaschinen-Konzerns Yandex, hat die seit Juli 2023 sanktionierten russischen Unternehmen NTechLab und Tevian dabei unterstützt Gesichtserkennung zu verbessern. Dies fand eine journalistische Recherchegruppe heraus. Russland baut auf Crowd- und Clickworker, um Software für automatisierte Gesichtserkennung zu trainieren und Videoüberwachung vor allem in Moskau schlagkräftiger zu machen. Toloka hat auch einen Ableger in der Schweiz. NTechLab und Tevian liefern Software für das öffentliche Überwachungssystem Moskaus, das mit geschätzten 227.000 Kameras zu einem der umfangreichsten der Welt zählt. Die elektronischen Augen, die in der ganzen Stadt und der U-Bahn verteilt sind, scannen vorbeikommende Gesichter und suchen nach Übereinstimmungen mit Beobachtungslisten.

Die aufdeckende Recherchegruppe besteht aus The Bureau of Investigative Journalism (TBIJ), Follow the Money und Paper Trail Media in Kooperation mit dem Spiegel und dem ZDF. Nach Angaben der russischen Bürgerrechtsorganisation OVD-Info sollen allein nach der Beerdigung des Kreml-Kritikers Alexei Nawalny Anfang März 649 Personen im ganzen Land verhaftet worden sein. Mindestens 19 seien festgehalten worden, nachdem ihre Gesichter auf Basis einschlägiger Aufnahmen identifiziert wurden.

Schon seit 2017 ist bekannt, dass Bilder der damals rund 178.000 Überwachungskameras der russischen Hauptstadt mit Software zur biometrischen Gesichtserkennung ausgestattet werden (DANA 4/2017, 214). Die Verwaltung der Metropole setzte schon damals auf Technik von NTechLab. Das Unternehmen hat auch die vor allem in sozialen Netzwerken populäre einschlägige App FindFace entwickelt. 2020 gab das russische Innenministerium bekannt, dass das Kamera-Netzwerk damals in Moskau während der Covid-19-Beschränkungen etwa 200 „Quarantäneverletzer" erfasst habe.

TBIJ fand u.a. in YouTube-Videos zahlreiche Beispiele von Gig-Arbeitern, die seit 2019 für NTechLab und Tevian Aufgaben über Toloka erledigt haben. Dabei ging es z.B. darum Fotos von Menschen mit der ethnischen Zugehörigkeit „Afro, Latino, Asiat" ausfindig zu machen beziehungsweise zu labeln, um die Leistung der Erkennungssysteme bei bestimmten ethnischen Gruppen zu steigern, bei denen diese sonst oft versagen. Die von Tevian geposteten Aufgaben betrafen hauptsächlich die Erkennung der „Lebendigkeit des Gesichts". Dabei handelt es sich um eine Funktion, die beide Ausrüster als Kernbestandteil ihrer einschlägigen Produkte verkaufen. Sie dient dazu, eine reale Person von einem Bild oder Video beziehungsweise Deepfake zu unterscheiden. Die Kooperationen gehen über den Juli 2023 hinaus. Yandex hat bestätigt, bis dato mit NTechLab zusammenzuarbeiten.

Ein EU-Diplomat sieht hierin einen Regelverstoß: „Wenn diese Unternehmen sanktioniert werden, ist es verboten ihnen Ressourcen zur Verfügung zu stellen. Sobald sie Zahlungen von einem sanktionierten Unternehmen erhalten, also sobald dieser Transfer in ein EU-Bankensystem gelangt, sollte er eingefroren werden." Als Schlupfloch könnte Yandex Sanktionsexperten zufolge Geschäfte zwischen dem zweiten Toloka-Ableger in der Schweiz und NTechLab genutzt haben. In der Alpenrepublik ist der Softwarelieferant bisher nicht sanktioniert. In Yandex, das u.a. eine Suchmaschine betreibt, haben auch westliche Banken und Vermögensverwalter wie UBS, JP Morgan Chase und Goldman Sachs investiert. Yandex findet sich in der EU oder in den USA auf keinen Sanktionslisten – im Gegensatz zu drei seiner früheren Manager. Toloka erklärte, NTechLab habe nur einen Vertrag mit der russischen Firma Toloka RU LLC gehabt. Auch diese gehörte laut den Berichten zum fraglichen Zeitpunkt aber einem niederländischen Unternehmen (Krempl, Moskaus Massenüberwachung hat Hilfe aus Holland, www.heise.de 27.03.2024, Kurzlink: https://heise.de/-9669436).

Kanada

Supreme Court: IP-Adressenherausgabe entspricht einer Durchsuchung

Der Oberste Gerichtshof Kanadas, der in Ottawa ansässige Supreme Court, hat am 01.03.2024 in einem Grundsatzurteil festgestellt, dass die kanadische Polizei einen Durchsuchungsbefehl benötigt, um an die Internetkennung einer Person zu gelangen. In der knappen 5:4-Entscheidung befand er, dass Nutzer davon ausgehen können, dass eine ihnen zugeteilte dynamische IP-Adresse ein privates Datum darstellt. Mit der Internetkennung gehe eine gewisse Erwartung an den Schutz der Privatsphäre

im Sinne der zur Verfassung gehörenden Grundrechtecharta, der Charter of Rights and Freedoms, einher. Schon das Ermitteln dieser Nummern komme einer Durchsuchung gleich, sodass eine entsprechende Anordnung dafür nötig sei.

Für die Mehrheit des Gremiums hob Richterin Andromache Karakatsanis hervor, dass eine IP-Adresse „die entscheidende Verbindung zwischen einem Internetnutzer und seiner Onlineaktivität" bildet. Gegenstand der Suche in dem verhandelten Fall seien die Informationen gewesen, die diese Internetkennungen „über bestimmte Internetnutzer preisgeben könnten, darunter letztlich auch deren Identität". Zu berücksichtigen sei auch, was IP-Adressen „in Kombination mit anderen verfügbaren Informationen, insbesondere von Webseiten Dritter", offenbaren könnten. Wenn die Charta die Online-Privatsphäre der Bürger in der heutigen überwiegend digitalen Welt sinnvoll schützen solle, müssten ihre IP-Adressen mit abgedeckt sein. Die Richterin Suzanne Côté erklärte dagegen in der abweichenden Stellungnahme im Namen auch ihrer drei weiteren Kollegen: „Eine IP-Adresse allein verrät nicht einmal die Surfgewohnheiten." Nur der Provider eines Nutzers werde enthüllt. Das sei „kaum eine privatere Information als der Stromverbrauch oder die über Wärmeemissionen".

Klage erhoben hatte in dem Fall Andrei B., der in 14 Betrugsdelikten in einem Onlineshop eines Spirituosenladens in Alberta für schuldig befunden worden war. 2017 stellte die Polizei von Calgary fest, dass das Geschäft seine E-Commerce-Aktivitäten über den Zahlungsdienst Moneris abwickelte. Dort fragte sie, ohne einen Durchsuchungsbeschluss vorzulegen, die mit den Käufen verbundene IP-Adresse ab. Der Dienstleister gab daraufhin zwei IP-Adressen an die Ermittler heraus. Diese wandten sich daraufhin mit einer richterlichen Anordnung an den Zugangsanbieter, um die mit den IP-Adressen verknüpften Bestandsdaten in Form von Namen und Adressen zu erhalten. Sie führten zu B. und seinem Vater. Der Verdächtige wurde nach einer Wohnungsdurchsuchung verhaftet und wegen Missbrauch einer Kreditkarte und eines Ausweises eines Dritten angeklagt.

Kanadische Strafverfolgungsbehörden bedauerten in Folge der höchstrichterlichen Entscheidung umgehend, dass Teile ihrer Arbeit wie der Kampf gegen sexuelle Ausbeutung von Kindern im Internet dadurch erheblich erschwert werde. Bürgerrechtler begrüßen das Urteil als überfällig.

In Europa wurde 2016 durch den Europäischen Gerichtshof (EuGH) klargestellt, dass es für den Personenbezug von IP-Adressen ausreicht, wenn sich der Anbieter von Online-Mediendiensten insbesondere bei Cyberattacken an die zuständige Ermittlungsbehörde wenden kann (DANA 4/2016, 201). Dieser obliege es dann „die nötigen Schritte" etwa mithilfe einer Bestandsdatenabfrage zu unternehmen, „um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten". Der deutsche Bundesgerichtshof (BGH) bestätigte wenig später in diesem Sinne, dass dynamische IP-Adressen von Website-Besuchern grundsätzlich geschützte personenbezogene Informationen sind, die nicht ohne Einwilligung monatelang getrackt werden dürfen (Krempl, Polizeizugriff: Oberstes kanadisches Gericht stärkt Schutz von IP-Adressen, www.heise.de 02.03.2024, Kurzlink: https://heise.de/-9644463).

USA

KI-bearbeitete Videos haben keinen gerichtlichen Beweiswert

Ein Richter in den USA hat die Nutzung einer Videoaufnahme als Beweismittel in einem Gerichtsverfahren untersagt, weil der Film zu sehr mit KI-Technik verändert wurde. Die „neuartige" Technologie greife auf „undurchsichtige Methoden" zurück. Damit würde lediglich dargestellt, was die Technik „denkt", was auf dem Ausgangsfilm zu sehen ist. Die Zulassung des Films würde zu einer zu großen Verwirrung führen und außerdem zeitaufwändige Debatten nach sich ziehen, die nichts mit dem eigentlichen Verfahren zu tun hätten. Einem NBC-News-Bericht zufolge dürfte es sich um den ersten Fall handeln, in dem sich ein US-Gericht mit einer derartigen Frage befasst hat.

In dem Verfahren im US-Bundesstaat Washington geht es um einen Mann, der drei Menschen erschossen hat. Der plädierte auf Notwehr und hatte das mit einem Video beweisen wollen, das mit einem Mobiltelefon aufgenommen wurde. Weil das aber nicht aussagekräftig genug war, hätten sich seine Anwälte an jemanden mit Erfahrung in „kreativer Videobearbeitung" gewandt, der keine Erfahrung mit solchen Rechtsstreitigkeiten hat. Mithilfe der Software von Topaz Labs habe die Person das Video nachbearbeitet und der Angeklagte fühle sich durch das Ergebnis bestätigt. In einem Statement seiner Anwälte steht demnach, dass es sich um eine „originalgetreuere Darstellung des Originals" handle.

Ein Experte habe für das Verfahren die beiden Videos verglichen. Dieser kam zu dem Schluss, dass die überarbeitete Fassung Daten enthalte, die im Original nicht vorkommen. Jeder Bildpunkt in dem angeblich verbesserten Video sei neu, das Ergebnis sei ein Film, der zwar für das Auge angenehmer erscheine, aber Klarheit und eine verbesserte Auflösung lediglich vortäusche und die Begebenheiten des Originals nicht akkurat wiedergebe. Der Experte, der 30 Jahre als Videoanalyst für das FBI gearbeitet habe, habe auch ergänzt, dass es seines Wissens keine wissenschaftlich anerkannte Methode für die Verbesserung von Videos mit KI-Technik gebe. Auch Topaz Labs hat demnach deutlich davor gewarnt die eigene Technik für forensische Zwecke zu verwenden.

Das Thema könnte künftig immer wieder erörtert werden. In aktuellen Smartphones kommen immer mehr Funktionen zum Einsatz, die mit KI-Unterstützung für eine bessere Fotoqualität sorgen sollen. Auch wenn die so vorgenommenen Änderungen noch vergleichsweise minimal sind, könnte es bald immer schwieriger werden solche Aufnahmen vor Gericht zu verwenden, auch wenn sie nicht manuell nachbearbeitet wurden. Als besonders weitgehende Beispiele dienen schon seit Jahren Fotos des Mondes, die mit Smartphones von Samsung gemacht wurden und mehr Details zeigen, als tatsächlich vorhanden sind (Holland, US-Gericht: Von KI „verbessertes" Video nicht als Beweismittel zugelassen, www.heise.de 04.04.2024, Kurzlink: https://heise.de/-9675312).

USA

Gewaltiger Gesundheitsdaten-Angriff auf Change Healthcare

Nach einem Cyberangriff auf die Online-Plattform „Change Healthcare" teilte der Versicherungskonzern UnitedHealth Group mit Lösegeld gezahlt zu haben. Der Angriff soll das Unternehmen im ersten Quartal 2024 bereits 1 Milliarde US-Dollar gekostet haben. Dieser könne „einen erheblichen Teil der Menschen in den USA betreffen". Die genaue Zahl der Betroffenen nennt das Unternehmen nicht. Der Versicherer schätzt, dass er „mehrere Monate kontinuierlicher Analyse" benötigt, um betroffene Kunden zu identifizieren und zu benachrichtigen. Damit sich möglicherweise Betroffene über den Vorfall informieren können, richtete UnitedHealth eine Hotline ein.

Alles deutet darauf hin, dass persönliche Daten und Gesundheitsdaten von einem bedeutenden Teil der US-Bevölkerung abgeflossen sind. Doch gebe es bisher keine Beweise, dass Arztakten oder vollständige Krankengeschichten kompromittiert wurden. Das Unternehmen überwacht laut eigenen Angaben das Darknet, um festzustellen, ob mehr Daten online veröffentlicht wurden. Im Darknet seien 22 Screenshots aus „angeblich abgezogenen Dateien" aufgetaucht, von denen einige sensible Informationen enthielten. Weitere Daten seien bisher nicht veröffentlicht worden.

UnitedHealth gab zu Lösegeld gezahlt zu haben „als Teil der Verpflichtung des Unternehmens, alles in seiner Macht Stehende zu tun, um Patientendaten vor der Offenlegung zu schützen". Hinter dem im Februar 2024 von UnitedHealth gemeldeten Angriff steckt offenbar die Ransomware-Gruppe AlphV (auch als Blackcat bekannt), die das Lösegeld erhalten haben soll. RansomHub, eine weitere kriminelle Bande, hat kürzlich mutmaßlich persönliche Patientendaten aus dem Datenleak veröffentlicht und ebenfalls ein Lösegeld gefordert. RansomHub behauptet als einzige Zugriff auf die Daten zu haben.

Parallel laufen die Wiederaufbauarbeiten. Das amerikanische E-Rezept funktioniert seit März 2024 wieder. Für das gesamte Jahr wird wegen des Angriffs mit Kosten von 1,6 Milliarden US-Dollar gerechnet. Schon seit Februar kämpfen Apotheken in den USA aufgrund des Vorfalls mit IT-Störungen. In der Folge hatten auch schon die Cybersecurity and Infrastructure Agency (CISA) und das FBI Maßnahmen ergriffen. Auch das Weiße Haus hatte Druck auf UnitedHealth ausgeübt. Im US-Gesundheitssystem ist Change Healthcare die größte Plattform für den Datenaustausch zwischen Ärzten, Apotheken, Gesundheitsdienstleistern und Patienten, über die auch Transaktionen laufen. Bemerkbar macht sich der Vorfall bei dem zentralen Dienstleister nicht nur in Apotheken im ganzen Land, sondern auch in Krankenhäusern des US-Militärs weltweit (Koch, eHealth: Nach Cyberangriff droht US-Bevölkerung großer Datenleak, www.heise.de 23.04.2024, Kurzlink: https://heise.de/-9695208).

USA

Genetischer Promi-Exhibitionismus

Als Gast in der US-Fernsehsendung „Finding Your Roots" erfuhr der 79-jährige Schauspieler Michael Douglas, dass er ein entfernter Cousin der 39-jährigen Kollegin Scarlett Johansson ist. Für diese Sendung wird die DNA, werden also die Gene von Promis untersucht und verglichen und das Ergebnis öffentlich präsentiert. Seine Reaktion: „Oh, das ist unglaublich!" Er freue sich darauf Scarlett bald wieder zu sehen. Die Show hatte zuvor bereits enthüllt, dass der Schauspieler Bob Odenkirk und König Charles II. entfernt verwandt seien (Scarletts Vetter, SZ 06.07.2024, 12).

USA

Per Kfz-Daten des LexisNexis-Reports zu teurer Versicherung

Es ist nicht neu und wird auch in Deutschland schon seit einigen Jahren praktiziert, dass Kfz-Fahrinformationen von Versicherten per OBD-Dongle (On-Board-Diagnose) oder Smartphone-App an den Versicherer übermittelt werden, um so bessere Konditionen (Telematik-Tarife) zu bekommen. In den USA werden die Daten allerdings schon seit langer Zeit direkt vom Autohersteller an ein Datenanalyseunternehmen übertragen, das wiederum die Versicherer beliefert – oftmals ohne Wissen des Fahrzeugbesitzers. Dies hat Auswirkungen auf die Versicherungsprämien, die US-Autofahrer zahlen müssen.

• LexisNexis protokolliert die Kfz-Nutzung

Ein 65-jähriger Softwareunternehmer aus Seattle, der sich selbst als „vorsichtigen Fahrer" seines geleasten Chevrolet Bolt von General Motors (GM) einstuft, war überrascht, als er vor zwei Jahren 21% mehr für seine Versicherung zahlen musste. Vergleiche mit anderen Versicherungsgesellschaften fielen ähnlich höher aus als zuvor. Ein Faktor für die höheren Policen, erklärte ihm ein Versicherungsvertreter, sei sein LexisNexis-Report. Gemäß einem Bericht der New York Times (NYT) ist LexisNexis ein in New York ansässiger globaler Datenmakler, der Autounfälle und Strafzettel erfasst sowie Informationen zum Fahrstil direkt von den Autoherstellern bekommt und die Kfz-Versicherer mit den gesammelten Daten versorgt. Der betroffene Softwareunternehmer forderte dort seinen „Consumer Disclosure Report" an und bekam von LexisNexis eine 258-seitige detaillierte Auswertung von jeder Fahrt der vergangenen sechs Monate, die er oder seine Frau mit dem Bolt unternommen hatte.

Von 640 Fahrten in dem Zeitraum seien minutengenau etwa Fahrtbeginn und -ende, zurückgelegte Strecken, Geschwindigkeitsüberschreitungen, Vollbremsungen und starke Beschleunigungen von jeder Fahrt dokumentiert worden. Einzig die Standorte sollen nicht enthalten gewesen sein. All die Informationen wurden demzufolge direkt vom Hersteller über dessen App Smart Drive von OnStar, das zum Autohersteller GM gehört, zur Verfügung gestellt. LexisNexis analysiere, so ein Sprecher des Unternehmens, die Fahrdaten und erstelle Risikobewertungen, „die Versicherer als [...] Faktoren verwenden

können, um einen individuelleren Versicherungsschutz zu schaffen".

Für den betroffenen Softwareunternehmer ist es „Verrat", dass derartige Informationen, von denen er nicht gewusst habe, weitergegeben und von den Versicherungen verwendet werden. Acht Versicherer hätten in einem Monat seine Daten bei LexisNexis angefordert.

Spezielle Dongles für die On-Board-Diagnose und Smartphone-Apps zeichnen mit Zustimmung der Versicherten ebenfalls die Fahrweise auf – allerdings sind sich die Versicherten dessen meistens bewusst. Die App „Smart Driver" von OnStar scheint in den USA andere Wege zu gehen. Der OnStar-Fahrzeug-Kommunikationsdienst gehört zu GM und wurde schon im Jahr 1996 eingeführt. Damals nutzte OnStar, das zuerst in Cadillac-Fahrzeugen eingeführt wurde, laut einem Bericht bereits Mobilfunk- und Satellitentechnologie für die Kommunikation mit einem Fahrer oder beim Auslösen des Airbags in Unfallsituationen. 2003 stand der Service auch für Fahrzeuge von Volkswagen, Toyota und Honda zur Verfügung und hatte den Angaben von GM zufolge zwei Millionen Kunden. Im selben Jahr machte GM erstmals Geld mit OnStar und wollte den Umsatz von 750 Millionen Dollar (2001) auf 4 Milliarden Dollar bis 2005 steigern.

• Hersteller liefern direkt

In einer 2022 veröffentlichten Patentanmeldung von Ford heißt es zu den erfassten Daten der OBD-Dongle, die für Telematik-Tarife von den Versicherern ausgegeben und ans Fahrzeug angebracht werden: „In der Vergangenheit haben sich die Fahrer nur ungern an diesen Programmen beteiligt". Versicherer – die in dem Patentantrag als Kunden bezeichnet werden – könnten bestimmte Fahrzeugmerkmale wie die Fahrgestellnummer missinterpretieren und der Credit Score lasse nicht zwingend auf das Fahrverhalten schließen. Diese Daten nutzen Versicherer demzufolge in den USA zur Risikoeinschätzung. Die Autohersteller sammeln die Informationen nun direkt von den mit dem Internet verbundenen Fahrzeugen, die dann von der Versicherungsbranche genutzt werden können, so dass Dongle oder Smartphone-App zur Überwachung der Fahrgewohnheiten überflüssig werden.

Mit dem Internet verbundene Fahrzeuge bieten Zugang zu Diensten wie etwa Navigation, Pannenhilfe oder auch Smartphone Apps. Letztere ermöglichen den Autobesitzern z.B. die Ver- und Entriegelung aus der Ferne und bieten Informationen zum Füllstand des Tanks, der Reichweite oder Fahrdaten und Fahrzeugzustand sowie Terminierung eines Werkstattbesuchs bei einem Servicepartner. Zusätzlich können über die jeweiligen Fahrzeugs-Apps kostenpflichtige Dienste hinzugebucht werden. Das wird auch in Deutschland schon seit einiger Zeit praktiziert.

In den USA haben die Autohersteller, darunter GM, Honda, Kia und Hyundai, damit begonnen, in den Connected-Car-Apps optional die Bewertung der Fahrweise des Fahrers anzubieten. Wird diese Funktion aktiviert, werden gemäß einem Bericht der New York Times die so gesammelten Daten über das Fahrverhalten an Datenmakler wie LexisNexis weitergegeben – oftmals ohne das Wissen der Fahrzeugbesitzer. Die Zustimmung erfolge über die kleingedruckten und undurchsichtigen Datenschutzbestimmungen, die Autoherstellern und Datenbrokern das Sammeln detaillierter Informationen von Millionen US-amerikanischer Autofahrer ermögliche.

Ein Rechtsprofessor der Cornell University zeigte sich überrascht: „Da der Durchschnittsverbraucher dies nicht erwarten kann, sollte es in der Branche üblich sein darauf hinzuweisen." Die Politik hat ebenfalls ihre Besorgnis darüber zum Ausdruck gebracht. Die kalifornische Datenschutzbehörde untersucht derzeit die Datenerfassungspraktiken der Autohersteller. Senator Edward Markey aus Massachusetts hat im Februar 2024 die Federal Trade Commission (Handelskommission) aufgefordert, diesbezüglich eine Untersuchung durchzuführen: „Das ‚Internet der Dinge' dringt wirklich in das Leben aller Amerikaner ein. Wenn es jetzt eine Absprache zwischen Autoherstellern und Versicherungsgesellschaften gibt, die die von einem unwissenden Autobesitzer gesammelten Daten nutzen, um dessen Versicherungstarife zu erhöhen, ist das aus meiner Sicht per se ein potenzieller Verstoß gegen Abschnitt 5 des Federal Trade Commission Act." Das Bundesgesetz verbietet unlautere und betrügerische Geschäftspraktiken, die den Verbrauchern schaden.

Werden diese Daten auf professionellen Rennstrecken erfasst, die mit dem eigenen Kfz zulässigerweise befahren werden dürfen, so entsteht ein Problem: So schrieb im Jahr 2022 z.B. ein Corvette-Besitzer in einem US-Forum, dass er „am Arsch sei", weil er auf so einer Rennstrecke die Grenzen seiner Corvette ausgetestet hatte: „Ich habe die Daten gesehen, bevor ich Smart Drive ausgeschaltet habe. Mal sehen, was bei der Erneuerung der Versicherung in ein paar Monaten passiert".

• Situation in Deutschland

Fahrzeuge von deutschen Herstellern bieten auch für in Deutschland zugelassene Kfz Smartphone-Apps, die Informationen über den Fahrzeugzustand geben. Bei Volkswagen etwa kann über die Volkswagen-App das Fahrzeug nach erfolgreicher Anmeldung und einem Ident-Verfahren aus der Ferne ver- und entriegelt sowie ein „Hupen & Blinken" ausgelöst werden, wenn die Standortdaten aktiviert sind. Zusätzlich zeigt die App Langzeit-Fahrdaten und Fahrdaten seit dem letzten Tanken inklusive Tankfüllstand und Reichweite, die Laufleistung, den nächsten Service und Ölservice sowie mögliche Probleme mit Antrieb, Bremsen, Fahrlicht, Assistenten, Reifen und weitere Details an. Kostenpflichtige Dienste können ebenfalls über die App gekauft und aktiviert werden.

Die mit entsprechender Technik ausgerüsteten Fahrzeuge von Volkswagen erfassen auch die aktuelle Position des Autos (inklusive Abstellort) und übermitteln diesen zusammen mit der Fahrzeug-Identifizierungsnummer, der Art des Fahrzeugantriebs und dem Fahrzeugtyp beim Absetzen eines Notrufs. Mindestens in Modellen mit Geschwindigkeitswarnung wird auch die Geschwindigkeit erfasst. Auch andere Hersteller erfassen diese Daten von ihren Fahrzeugen. Damit sind alle Informationen, die in den USA an die Versicherungen weitergegeben werden und sich auf die Höhe der Versicherungspolice auswirken können, auch in Deutschland bei den Autobauern vorhanden.

Die in Deutschland geltende Datenschutz-Grundverordnung (DSGVO) macht die Erfassung und Übermittlung dieser Informationen von einer expliziten Zustimmung abhängig. Aktuell werden offenbar keine Fahrdaten der Hersteller für die Prämien-Einstufung durch Versicherungen herangezogen. Einzig bei den fahrabhängigen Telematik-Tarifen, die unter Zustimmung des Versicherten bewusst abgeschlossen werden und eine App oder einen Dongle voraussetzen, werden die vertraglich festgelegten Daten erfasst. Neben der Vertragsunterschrift muss der Kunde zusätzliche Maßnahmen ergreifen, um den speziellen Versicherungsschutz zu erhalten, so dass für ihn eine gewisse Transparenz besteht.

Die Fahrzeughersteller in Europa unterliegen der DSGVO. Mercedes-Benz Deutschland erklärte auf Anfrage, „dass der sichere und verantwortungsvolle Umgang mit Daten die Basis für die Akzeptanz des vernetzten Fahrens ist". Doch ohne Datenübertragung funktioniert in den modernen Fahrzeugen auch in Deutschland kaum noch ein Service. So werden nicht nur beim obligatorischen eCall, bei dem Mercedes-Benz Notrufsystem und Mercedes-Benz Info- und Pannenruf Daten zur Hilfe und Unterstützung übertragen, sofern dies vom Fahrer oder automatisch, etwa nach einem Unfall, ausgelöst wurde. Fahrzeuge würden laufend Daten verarbeiten, „um einen sicheren Betrieb zu gewährleisten, Fehler zu finden und um Assistenz- und Komfortfunktionen anbieten zu können". Informationen zur Datenspeicherung habe Mercedes-Benz an prominenter Stelle in der Einleitung in die Betriebsanleitung aufgenommen. Mit dem „Mercedes me", den Mercedes auch als App anbietet, bestimmt – so Mercedes – der Kunde, welche Dienste er nutzen möchte. Welche Daten zu den jeweiligen Diensten benötigt werden, stelle das Unternehmen transparent dar. Über die ausgewählten Funktionen hinaus erfasse Mercedes keine weiteren Daten.

Die Navigation inklusive Stauumfahrung in Echtzeit funktioniert ohne eine permanente Erfassung und Verwendung von Standortdaten nicht. Das sollte jedem, der diese Funktion nutzt – egal bei welchem Fahrzeughersteller – klar sein. Allerdings werden auch in dem Fahrzeug selbst viele Informationen auf lokale Speicher geschrieben, die später etwa in der Werkstatt zu Auswertungen und Reparaturen herangezogen werden. Mit immer komplexeren Funktionen und unzähligen Sensoren in den Fahrzeugen steigt auch die Menge der gespeicherten Daten. Allein für das automatische Umschalten von Tagfahr- auf Abblendlicht werden entsprechende Sensoren benötigt, die funktionieren sollten. Will man all dies nicht, muss man sich nach einem älteren Fahrzeug ohne entsprechenden „Komfort" umsehen.

Unabhängig von der Dienste-Auswahl erfassen auch Fahrzeuge von Mercedes-Benz sämtliche Informationen, auf die Versicherer vermutlich gerne Zugriff hätten. Anders als in den USA schützt die DSGVO Autofahrer in Europa vor der Weitergabe dieser Daten.

Der Datenschutz ist bei Mercedes-Benz, so das Unternehmen, schon im Entwicklungsprozess integriert, an dem die Ingenieure gemeinsam mit den Kollegen des Konzerndatenschutzes und anderer Rechtsbereiche arbeiteten, um die Produkte und Services datenschutzfreundlich zu gestalten und somit den Grundätzen Privacy by design und Privacy by default gerecht zu werden. Das bedeute auch, „dass wir die für die Dienste-Erbringung erforderlichen Daten nur so lange speichern, wie dies für die Dienste-Erbringung erforderlich ist und anschließend löschen". So werde etwa der Tankfüllstand laufend überschrieben, sobald ein neuer Wert vom Fahrzeug gesendet wird.

• Zukunft ungewiss

In den US-Foren häufen sich Beschwerden über steigende Prämien von unwissenden Versicherten. Ein Cadillac-Fahrer aus Florida erwägt eine Klage gegen GM, weil ihm im Dezember 2023 sieben Versicherer eine Kfz-Versicherung verweigert hätten – aufgrund seines LexisNexis-Berichts, wonach er zu häufig stark gebremst und stark beschleunigt hat. LexisNexis Definition einer Vollbremsung kenne der Cadillac-Fahrer nicht, der Kopf des Beifahrers würde jedenfalls nicht gegen das Armaturenbrett schlagen, gleiches gelte für die Beschleunigung. Auf der Homepage bewirbt OnStar Smart Driver damit, „wie Sie ein intelligenter und sicherer (und besserer) Fahrer werden können". Dank Belohnungsprinzip könne man Abzeichen wie etwa „Brems-Genie" oder „Grenzwert-Held" erreichen. Die steigenden Versicherungsprämien haben offenbar dafür gesorgt, dass viele Betroffene sich abgemeldet und die App deinstalliert haben.

GM betätigte die Praxis des Datensammelns und nannte mit Verisk einen weiteren Datenbroker, mit dem das Unternehmen zusammenarbeitet. Kunden schalten Smart Driver „zum Zeitpunkt des Kaufs oder über die mobile App ein". Aus einem GM-Handbuch gehe hervor, dass Autoverkäufer Boni für die erfolgreiche Anmeldung bei OnStar erhalten können. So ist es möglich, dass Käufer unwissentlich angemeldet werden. Der Cadillac-Besitzer aus Florida hatte in seinen unterschriebenen Unterlagen zum Kauf des Autos zumindest keine Hinweise darauf gefunden.

Jen Caltrider, eine Forscherin bei Mozilla, hat 2023 Datenschutzrichtlinien von mehr als 25 Automarken überprüft. Autofahrer hatten kaum eine Vorstellung davon, wozu sie ihre Zustimmung geben, wenn es um die Datenerfassung geht. Es sei „unmöglich für die Verbraucher zu versuchen die mit Gesetzestexten gefüllten Richtlinien der Autohersteller, ihrer vernetzten Dienste und ihrer Apps zu verstehen". Sie nannte Autos „einen Alptraum für die Privatsphäre". Dabei kam heraus, dass Autos z.B. auch Daten zum Einwanderungsstatus und zu sexuellen Aktivitäten sammeln (Mewes, App ermittelt Fahrdaten von US-Versicherten und beschert teurere Prämien, www.heise.de 16.02.2024, Kurzlink: https://heise.de/-9653169).

Vietnam

Ausweiskarten mit biometrischen Daten

Ab Sommer 2024 sollen in Vietnam für neue Ausweiskarten u.a. biometrische Daten gesammelt werden: Iris-Scans, Stimmaufnahmen und DNA-Informationen. Gemäß einer Mitteilung der staatlichen Government News beginnt die Sammlung der Daten am 1. Juli. Die Aufnahme der umfangreichen biomet-

rischen Daten wird nebenbei erwähnt, hauptsächlich geht es um Änderungen bei den auf den Ausweisen abgedruckten Informationen. Gleichzeitig wird darauf hingewiesen, dass auf der Rückseite der Karten keine Fingerabdrücke des Besitzers oder der Besitzerin sowie keine Informationen zu deren Charakteristiken mehr abgedruckt werden. Die Abgabe der DNA-Informationen und der Aufnahmen der Stimme seien laut dem zugrundeliegenden Gesetz für die meisten Menschen freiwillig.

Die Speicherung von Daten zur DNA und zu Stimmen in den Ausweiskarten war bereits vor anderthalb Jahren angekündigt worden. Die Exilzeitung Thòi Báo hat damals Kritik zusammengetragen. So erklärte ein Anwalt den Plan für verfassungswidrig. Es wurde darauf hingewiesen, dass Menschen vor allem mit Iris-Scans und Stimmaufzeichnungen bestimmte Zugänge absichern könnten, also Wohnungseingänge, Bankkonten oder ihre Smartphones. Wenn die Regierung solche Daten in großem Umfang einsammele, steige die Gefahr, dass die Daten an solch einer zentralen Stelle abgegriffen werden und z.B. für Identitätsdiebstahl benutzt werden können. Das ließe sich dann auch nicht mehr rückgängig machen, da diese biometrischen Merkmale nicht geändert werden können.

In dem zugrundeliegenden, Ende November 2023 verabschiedeten Gesetzesartikel heißt es, dass die Daten zur DNA und Stimme gesammelt werden, wenn sie freiwillig von den jeweiligen Personen „oder der zuständigen Strafverfolgungsbehörde beziehungsweise der zuständigen Behörde“ eingereicht werden. Das legt nahe, dass die Freigabe der Informationen nicht in allen Fällen freiwillig erfolgt. Zudem ist offenbar vorgesehen, dass Kinder unter 14 Jahren einen solchen Ausweis bekommen, was aber nicht verpflichtend sei. Der Einparteienstaat wird seit Jahrzehnten von der Kommunistischen Partei beherrscht (Holland. Biometrie: Vietnams Ausweise enthalten bald Daten zu DNA, Iris und Stimme, www.heise.de 20.02.2024, Kurzlink: https://heise.de/-9632970).

Technik-Nachrichten

Facebook-Marketplace-Datenbank geleakt

Bei Metas Facebook Marketplace gab es einen IT-Sicherheitsvorfall, bei dem unbekannte Angreifer persönliche Daten von 77.267 Marketplace-Nutzenden mit mehr als 200.000 Einträgen erlangen und in einem Hacking-Forum veröffentlichen konnten. Die Website „Have I Been Pwned?“ hat die Daten in ihren Onlineservice aufgenommen. Dort kann man prüfen, ob etwa die eigene Mailadresse in diesem oder anderen Datenleaks vorkommt. In dem Leak finden sich unter anderem Namen, E-Mail-Adressen, Passwörter und Telefonnummern. Die Passwörter sind über die Hashfunktion bcrypt geschützt. Das Verfahren gilt derzeit als sicher. Dementsprechend sind die Kennwörter nicht im Klartext einsehbar und Kriminelle können damit nichts anfangen. Unklar ist, ob diese Kennwörter auch zu den jeweiligen Facebook-Accounts gehören. Andere Daten haben Sicherheitsforscher stichprobenartig validiert und für echt befunden.

Im Hacking-Forum gibt der Verfasser des Beitrags zum Leak an, dass die Daten im Oktober 2023 von einem Cyberkriminellen mit dem Pseudonym „algoatson“ kopiert wurden. Um an die Daten heranzukommen, soll er über den Chatdienst Discord einen Dienstleister, der die Cloud-Dienste von Facebook verwaltet, kompromittiert haben. Mittels der erbeuteten Daten können Kriminelle Rückschlüsse auf Facebook-Marketplace-Nutzende ziehen und die Daten für Phishing-Attacken, die für mehr Glaubwürdigkeit mit persönlichen Details ausgestattet werden, missbrauchen. Im Zuge von SIM-Swap-Attacken ist aber auch das Abfangen von Zwei-Faktor-Authentifizierungs-Codes vorstellbar. Damit ausgestattet, können Angreifer Accounts übernehmen. Es handelt sich nicht um das erste Datenleak bei Facebook. So wurde z.B. Anfang 2021 bekannt, dass Cyberkriminelle Daten von mehr als 500 Millionen Nutzern veröffentlicht haben (vgl. DANA 2/2021, 134 f.; Schirrmacher, Persönliche Daten von über 77.000 Facebook-Marketplace-Nutzern geleakt, www.heise.de 22.02.2024, Kurzlink: https://heise.de/-9635749).

Airbnb verbannt Kameras aus Apartments

Airbnb teilte mit, dass ab dem 30.04.2024 Sicherheitskameras innerhalb vermieteter Apartments untersagt sein sollen. Bisher geltende Ausnahmeregelungen für bestimmte Bereiche werden abgeschafft. In vermieteten Apartments dürfen auch keine Kameras in Gemeinschaftsbereichen wie Fluren oder Wohnzimmern mehr installiert sein, was bislang erlaubt war, wenn auf der Angebotsseite darauf hingewiesen wurde und die Geräte gut sichtbar waren. Nur in Schlafbereichen und Badezimmern waren Kameras auch bisher schon verboten. Mit der Neuregelung soll das Vorgehen vereinheitlicht werden. Sicherheitskameras, die nach außen zeigen, sind weiterhin zulässig. Außenkameras dürfen aber nicht auf Bereiche gerichtet werden, in denen ein höheres Maß an Privatsphäre erwartet wird, also etwa eine Dusche oder eine Sauna.

Laut einem Blogeintrag, in dem die neuen Vorgaben erklärt werden, bleiben etwa Kameras an Türklingeln oder Geräte zur Überwachung der Lautstärke erlaubt – die dürfen aber keine Audioaufzeichnungen übertragen. Dabei handele es sich um „effektive, die Privatsphäre schützende“ Möglichkeiten vermietete Räumlichkeiten zu überwachen und beispielsweise gegen unerwünschte Feierlichkeiten vorzugehen. Gegenüber den Mietern müsse aber auf das Vorhandensein hingewiesen und der ungefähre Standort deutlich gemacht werden.

Airbnb erklärte, nur ein kleiner Teil dürfte von der Neuregelung betroffen sein, weil die meisten Angebote zur Ver-

mietung von Apartments keine Angaben zu einer Sicherheitskamera enthalten. Künftig würden Hinweise auf Verstöße überprüft und könnten die Entfernung eines Angebots oder gar die Löschung des verantwortlichen Accounts zur Folge haben. Gegen möglicherweise versteckt installierte Kameras wird die Neuregelung voraussichtlich wenig helfen. Doch fallen damit mögliche Erklärungsversuche weg, sollte solch eine entdeckt werden. Laut Airbnb sind der Regeländerung intensive Gespräche mit verschiedenen Interessengruppen vorausgegangen (Holland, Privatsphäre: Airbnb verbannt Sicherheitskameras ganz aus vermieteten Apartments, www.heise.de 12.03.2024, Kurzlink: https://heise.de/-9651901).

Rechtsprechung

EGMR

Schwächung der Ende-zu-Ende-Verschlüsselung verstößt gegen Menschenrechte

Der Europäische Menschenrechtsgerichtshof (EGMR) hat mit Urteil vom 13.02.2024 eine Schwächung der sicheren Ende-zu-Ende-Verschlüsselung wegen Verstoß gegen den Schutz der Privatsphäre nach Art. 8 Europäische Menschenrechtskonvention (EKMR) für unzulässig erklärt (Application No. 33696/19). Im Verfahren Case of Podchasov v. Russia begründete die 3. Sektion des EGMR dies damit, dass die Verschlüsselung Bürger und Unternehmen vor Hackerangriffen, Diebstahl von Identitäts- und personenbezogenen Daten, Betrug und unbefugter Weitergabe vertraulicher Informationen schützt. Eigens dafür eingerichtete Hintertüren für behördliche Zwecke könnten auch von kriminellen Netzwerken ausgenutzt werden. Backdoors würden die Sicherheit der elektronischen Kommunikation aller Nutzer ernsthaft gefährden. Es gebe andere Lösungen zur Überwachung verschlüsselter Kommunikation ohne den Schutz aller Nutzer generell zu schwächen. Als Beispiel nennt das Urteil den Einsatz von Staatstrojanern oder die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Das Urteil des EGMR dürfte auch erhebliche Auswirkungen auf die geplante Chatkontrolle haben bzw. die Pläne der EU-Kommission unmöglich machen. Nach Ansicht des bisherigen EU-Abgeordneten Patrick Breyer ist dies ein klares Signal, dass die von der EU-Kommission „zur Chatkontrolle geforderte ‚client-side scanning'-Überwachung auf allen Smartphones eindeutig illegal" ist (Sobiraj, Ende-zu-Ende-Verschlüsselung durch Urteil EU-weit geschützt, https://tarnkappe.info 14.02.2024).

EuGH

Rechtliche Klarstellungen zum Real Time Bidding

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 07.03.2024 die Regeln für die Versteigerung von personenbezogenen Informationen für gezielte Online-Werbung per Real Time Bidding (RTB) auf Basis der Datenschutz-Grundverordnung (DSGVO) erläutert. Wenn ein Nutzer eine Website oder eine Anwendung mit einem Werbeplatz aufruft, können Werbeunternehmen, Datenbroker und Werbeplattformen, die Tausende von Werbetreibenden vertreten, anonym in Echtzeit Gebote abgeben, um diesen Werbeplatz zu erhalten und dort auf das Profil des Nutzers abgestimmte Werbung anzuzeigen (DANA 3/2019 120, ff.).

Die belgische Datenschutzbehörde APD erklärte das vom Verband IAB Europe entwickelte TCF 2022 auf Basis der DSGVO für unzulässig und verhängte ein Bußgeld von 250.000 Euro. Die Behörde verhängte gegen IAB Europe zudem mehrere Abhilfemaßnahmen. IAB Europe focht diese Entscheidung an und wandte sich an den Appellationshof Brüssel, der dem Gerichtshof Fragen zur Vorabentscheidung vorgelegt hat. Die Luxemburger Richter bestätigen die APD-Auffassung, dass der TC-String Informationen über einen identifizierbaren Nutzer enthält und so ein personenbezogenes Datum im Sinne der DSGVO darstellt. Ferner hat der EuGH festgestellt, dass IAB Europe als „gemeinsam Verantwortlicher" im Sinne der DSGVO anzusehen ist.

IAB Europe ist ein Verband ohne Gewinnerzielungsabsicht mit Sitz in Belgien, der Unternehmen der digitalen Werbe- und Marketingindustrie auf europäischer Ebene vertritt. IAB Europe hat eine Lösung entwickelt, die dieses Versteigerungssystem mit der DSGVO in Einklang bringen können soll. Die Nutzerpräferenzen werden in einem aus einer Kombination von Buchstaben und Zeichen bestehenden String kodiert und gespeichert, der als „Transparency and Consent String" (TC-String) bezeichnet wird und der mit Brokern für personenbezogene Daten und Werbeplattformen geteilt wird, damit diese wissen, worin der Nutzer eingewilligt oder wogegen er Widerspruch eingelegt hat. Auf dem Gerät des Nutzers wird auch ein Cookie gespeichert. Miteinander kombiniert, können der TC-String und das Cookie der IP-Adresse dieses Nutzers zugeordnet werden.

Sobald Nutzer bei einem Cookie-Banner auf „Akzeptieren" klicken, wird der TC-String erzeugt und an alle Partner geschickt, die auf das sogenannte OpenRTB-System setzen. Auf Basis dieser Zeichenkombination werden unter Einbezug eines Cookies und der IP-Adresse Nutzerprofile erstellt, die als Grundlage für Echtzeit-Werbeauktionen dienen. Bevor eine gezielte Werbung angezeigt wird, muss die vorherige Einwilligung des Nutzers zur Erhebung und Verarbeitung seiner Daten (insbeson-

dere seinen Standort, sein Alter, den Verlauf seiner Suchanfragen und seine zuletzt getätigten Einkäufe betreffend) für bestimmte Zwecke, wie u.a. Marketing oder Werbung, oder zum Austausch dieser Daten mit bestimmten Anbietern eingeholt werden. Der Nutzer kann dem auch widersprechen.

Mit seinem Urteil bestätigt der Gerichtshof, dass der TC-String Informationen über einen identifizierbaren Nutzer enthält und somit ein personenbezogenes Datum im Sinne der DSGVO darstellt. Anhand der in einem TC-String enthaltenen Informationen kann nämlich, wenn sie einer Kennung wie insbesondere der IP-Adresse des Geräts des Nutzers zugeordnet werden, ein Profil dieses Nutzers erstellt und die betreffende Person identifiziert werden.

Die gemeinsame Verantwortlichkeit wird vom EuGH damit begründet, dass IAB Europe bei der Speicherung der Einwilligungspräferenzen der Nutzer im TC-String auf die Verarbeitungen personenbezogener Daten Einfluss zu nehmen und gemeinsam mit ihren Mitgliedern sowohl die Zwecke als auch die zugrundeliegenden Mittel festzulegen scheint. Dies müsse der Appellationshof aber noch nachweisen. Die Brüsseler Kollegen sollen zudem untersuchen, ob IAB Europe auch als gemeinsamer Verantwortlicher zusammen mit den TCF-Teilnehmern rund um die nachfolgende Datenverarbeitung zur Verfolgung der TCF-Zwecke angesehen werde, also etwa das Ausspielen digitaler Werbung, Zielgruppenmessung oder Personalisierung. Die belgischen Datenschützer waren davon zunächst ausgegangen.

Der IAB Europe sieht sich als kleiner, nicht gewinnorientierter Verband außerstande die Datenverarbeitung für alle Empfänger der Werbeinformationen zu übernehmen. Dabei geht es um Hunderte Firmen, die wiederum teils eigene Banner-Netzwerke betreiben. Johnny Ryan von der irischen Bürgerrechtsorganisation ICCL, die zu den Beschwerdeführern gehört, wertet die EuGH-Klarstellungen als großen Erfolg: Die Entscheidung werde „die größte Spam-Aktion der Geschichte beenden“ und der „Tracking-basierten Werbebranche eine tödliche Wunde zufügen“. Der IAB Europe gab sich dagegen nach außen hin gelassen und will das angerufene Brüsseler Gericht zunächst seine Arbeit weiter verrichten lassen. Bis dahin gelte die Aussetzung des APD-Beschlusses weiter. Der EuGH habe TCF-basierte Cookie-Banner nicht pauschal als illegal eingestuft. Die aktuelle, unter anderem von Google verlangte TCF-Version besagt etwa, dass der Widerruf der Einwilligung genauso einfach sein muss wie die Zustimmung (Krempl, Personalisierte Werbung: EuGH untermauert Probleme mit Cookie-Bannern, www.heise.de 07.03.2024, Kurzlink: https://heise.de/-9649245; EuGH, PM Nr. 44/24, 07.03.2024, Versteigerung von personenbezogenen Daten für Werbezwecke: Der Gerichtshof stellt die Regeln auf der Grundlage der DSGVO klar).

EuGH

Lebenslange polizeiliche Biometriedatenspeicherung grds. unzulässig

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 30.01.2024 zum Recht auf Löschung nach den Datenschutzgesetzen der EU festgestellt, dass Polizeibehörden biometrische Merkmale wie Fingerabdrücke oder DNA-Profile nicht ohne weitere zeitliche Einschränkung unterschiedslos bis zum Tod eines strafrechtlich Verurteilten aufbewahren dürfen (Az. C-118/22). Auch wenn eine allgemeine Speicherung solcher sensiblen Daten für die Verfolgung und Prävention von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen prinzipiell gerechtfertigt ist, müsse regelmäßig geprüft werden, ob dieser Grundrechtseingriff noch notwendig sei. Gegebenenfalls sind die Einträge im Anschluss zu löschen.

In dem Fall wurde in Bulgarien eine Person im Rahmen eines Ermittlungsverfahrens wegen falscher Zeugenaussage polizeilich registriert. Ein Gericht befand den Betroffenen schließlich dieser Straftat für schuldig und verurteilte ihn zu einer einjährigen Bewährungsstrafe. Nach der Verbüßung galt die Person grundsätzlich als rehabilitiert. Sie beantragte daher ihre einschlägigen Daten aus dem Polizeiregister zu streichen. Nach bulgarischem Recht werden bislang aber unter anderem Fingerabdrücke und DNA-Profile weiter gespeichert. Sie können von den Behörden verarbeitet werden, die ohne zusätzliche zeitliche Einschränkung bis zum Tod von Betroffenen Zugang zu ihnen haben und Abgleiche durchführen dürfen.

Dies ist gemäß den Luxemburger Richtern in der Rechtssache nicht mit dem EU-Recht vereinbar. Die umstrittenen Daten könnten ihnen zufolge zwar unerlässlich sein, um zu prüfen, ob die betroffene Person früher oder später in andere Straftaten verwickelt ist. Nicht bei allen Verurteilten sei dieses Risiko aber gleich hoch. Die Frist der lebenslangen Speicherung sei nur unter besonderen Umständen angemessen, die sie gebührend rechtfertigten (Krempl, EuGH: Biometrie-Daten Verurteilter dürfen nicht lebenslang gespeichert werden, www.heise.de 30.01.2024, Kurzlink: https://heise.de/-9613643).

EuGH

Fingerabdrücke auf Personalausweis sind rechtens

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 21.03.2024 entschieden, dass die europaweite Verpflichtung zur Aufnahme von zwei Fingerabdrücken in den Personalausweis mit den Grundrechten auf Achtung des Privatlebens (Art. 7 GRCh) und auf Schutz personenbezogener Daten (Art. 8 GRCh) vereinbar ist (C-61/22). Zugleich haben die Luxemburger Richter aber festgestellt, dass der Gesetzgeber bei der EU-Verordnung, die die Speicherpflicht für alle Mitgliedsstaaten vorschreibt, die falsche Rechtsgrundlage zugrunde gelegt hat. Bis zum 31.12.2026 müssen die europäischen Gesetzgebungsgremien eine neue Verordnung auf der richtigen Rechtsbasis erlassen.

Die Pflicht zur Abgabe und Speicherung der biometrischen Fingerabdrücke ist nach Ansicht des EuGHs grundrechtskonform: „Sie ist durch die Ziele, die Herstellung gefälschter Personalausweise und den Identitätsdiebstahl zu bekämpfen sowie die Interoperabilität der Überprüfungssysteme zu gewährleisten, gerechtfertigt.“ Die damit verbundenen Einschränkungen der Normen aus der europäischen Grundrechte-Charta (GRCh)

seien durch Zielsetzungen gerechtfertigt, die dem Gemeinwohl dienen, und dafür geeignet, erforderlich sowie „nicht unverhältnismäßig“ sind.

Durch die Aufnahme der Fingerabdrücke sei es möglich, gegen Fälschungen sowie die missbräuchliche Nutzung personenbezogener Daten vorzugehen. Die Pflicht könne so einen Beitrag „sowohl zum Schutz des Privatlebens der betroffenen Personen als auch im weiteren Sinne zur Bekämpfung von Kriminalität und Terrorismus“ leisten. Sie erlaube es EU-Bürger auf zuverlässige Weise zu identifizieren und so die Reisefreiheit und das Aufenthaltsrecht zu gewährleisten. Diese Zwecke hätten für die Gemeinschaft und die Individuen eine besondere Bedeutung. Die Alternative, nur ein biometrisches Gesichtsbild auf dem Funkchip im Ausweis zu speichern, wäre den Richtern zufolge „ein weniger wirksames Identifizierungsmittel“. Alterung, Lebensweise, Erkrankung oder ein chirurgischer Eingriff könnten nämlich die anatomischen Merkmale des Gesichts verändern. Der EuGH legt aber Wert darauf, dass die Fingerabdrücke allein auf den Ausweisen selbst gespeichert werden.

Das EU-Parlament und der Ministerrat hätten die Verordnung aber fälschlich auf Grundlage von Artikel 21 des Vertrags über die Arbeitsweise der EU (AEUV) gestützt. Dieser betreffe das Recht der Bürger sich im Hoheitsgebiet der Mitgliedsstaaten frei zu bewegen und aufzuhalten. Richtig wäre die spezifischere Bestimmung des Artikels 77 gewesen, die sich auf „den Raum der Freiheit, der Sicherheit und des Rechts“ bezieht und dabei konkret auf die Politik im Bereich Grenzkontrollen, Asyl und Einwanderung. Diese Bestimmung sieht ein besonderes Gesetzgebungsverfahren und vor allem die Einstimmigkeit im Rat vor, was die Hürde für einen neuen Verordnungsbeschluss höher legt. Die gewährte Frist bis Ende 2026, bis das derzeitige EU-Gesetz ungültig wird, begründet der EuGH damit, dass ein Kippen mit sofortiger Wirkung schwerwiegende negative Folgen für eine erhebliche Zahl von EU-Bürgern und für ihre Sicherheit haben könnte.

In Deutschland gilt die Pflicht, dass Bundesbürger beim Beantragen eines neuen Personalausweises mit einem Scanner Abdrücke des linken und rechten Zeigefingers abgeben müssen, seit August 2021. Der frühere Geschäftsführer der Bürgerrechtsorganisation Digitalcourage, Detlef Sieber, klagte im Dezember 2021 gegen diese Auflage. Das Verwaltungsgericht (VG) Wiesbaden befragte dazu Anfang 2022 den EuGH wegen erheblicher Zweifel an der Rechtmäßigkeit der Bestimmungen. Das VG hielt diese für unvereinbar mit den Artikeln 7 und 8 GRCh.

Das VG Hamburg erließ am 22.02.2023 eine einstweilige Anordnung, wonach die zuständige Behörde der Hansestadt einem Antragsteller einen Personalausweis auch ohne die auf dem Chip zusammen mit dem biometrischen Gesichtsbild gespeicherten Fingerabdrücke ausstellen muss (Az. 20 E 377/23). Das hoheitliche Dokument sollte zunächst befristet für ein Jahr gelten, bis die Rechtslage höchstrichterlich geklärt ist. In Deutschland müssen Personen über 16 Jahren einen Personalausweis oder Reisepass besitzen. Sonst drohen Bußgelder bis zu 5.000 Euro.

Der Wiesbadener Kläger begründete seinen Gang vor Gericht damit, es fühle „sich für mich so an, wie ein Tatverdächtiger für ein Verbrechen behandelt zu werden“. Er empfinde das Anlegen entsprechender Karteien als Verletzung der Menschenwürde: „Die Menschen nehmen teils Bußgelder in Kauf“, um der erkennungsdienstlichen Behandlung auf dem Bürgeramt zu entgehen, ergänzte Digitalcourage-Gründerin Rena Tanges im Vorfeld der EuGH-Entscheidung. Dass die Ausweise ausstellenden Behörden die biometrischen Merkmale 90 Tage lang aufheben könnten, erhöhe das Risiko, dass diese Daten bei Cyberangriffen Kriminellen oder ausländischen Geheimdiensten in die Hände fallen. Fachanwalt Wilhelm Achenpöhler unterstrich, dass andere Verfahren wie 3D-Hologramme mehr zur Fälschungssicherheit beitrügen. Die Mitgliedsstaaten dürften die erhobenen Abdrücke zudem für schier beliebige Zwecke nutzen, was hochproblematisch sei (Krempl, EuGH: Fingerabdruckpflicht im Ausweis ist rechtens, Verordnung aber ungültig, www.heise.de 21.03.2024, Kurzlink: https://heise.de/-9661552; Janisch, Einmal Hand auflegen, SZ 22.03.2024, 6).

EuGH

DSA für Amazon vorläufig anwendbar

Der Vizepräsident des Europäischen Gerichtshofs (EuGH), Lars Bay Larsen, verkündete am 27.03.2024 seinen Beschluss, dass der Digital Services Act (DSA) für Amazon Services Europe nicht ausgesetzt wird (Az. C-639/23 P (R)). Das Unternehmen gehört zum Amazon-Konzern mit geschäftlichen Aktivitäten im Online-Einzelhandel sowie weiteren Dienstleistungen wie Cloud Computing und Online-Streaming. Die Online-Marktplatzdienste ermöglichen Drittverkäufern Waren im Amazon Store zum Kauf anzubieten.

Am 23.04.2023 hatte die EU-Kommission gemäß der Verordnung über einen Binnenmarkt für digitale Dienste (DSA) beschlossen, dass der Amazon Store als sehr große Online-Plattform einzustufen ist, was u.a. bedeutet, dass Amazon Store ein Werbearchiv mit detaillierten Informationen über ihre Online-Werbung öffentlich zugänglich machen und u.a. Algorithmen offenlegen muss. Mit der Einstufung hat die EU-Kommission Amazon mehrere Pflichten zur Minderung systemischer Risiken auferlegt.

Dem erwiderte Amazon, der DSA sei zum Einhegen völlig anderer Geschäftsmodelle gedacht, was auch Zalando in einer ähnlichen Klage vorbringt. Auf der eigenen Plattform bestehe kein „systemisches Risiko“ der Verbreitung schädlicher oder illegaler Inhalte Dritter. Amazon beantragte deshalb beim Gericht der Europäischen Union (EuG) die Nichtigerklärung dieses Beschlusses und stellte zudem einen Antrag auf vorläufigen Rechtsschutz. Der Präsident des EuG ordnete mit Beschluss vom 27.09.2023 die Aussetzung des Beschlusses der Kommission an, soweit Amazon Store damit verpflichtet wird das Werbearchiv öffentlich zugänglich zu machen (Az. T-367/23). Hiergegen legte die Kommission beim EuGH Rechtsmittel ein, dem der Vizepräsident des EuGHs statt gab und den Antrag auf vorläufigen Rechtsschutz Amazons endgültig zurückwies.

Larsen begründete seine Entscheidung damit, dass das Vorbringen von Amazon, die Pflicht sein Werbearchiv

öffentlich zugänglich zu machen, seine Grundrechte auf Achtung des Privatlebens und auf unternehmerische Freiheit rechtswidrig einschränken könne, nicht unerheblich und auch nicht völlig haltlos sei. Amazon würde, wenn keine Aussetzung erfolgt, in Fall eines im Hauptsacheverfahren obsiegenden Urteils wahrscheinlich auch einen schwerwiegenden und nicht wiedergutzumachenden Schaden erleiden.

Dies sei aber nicht entscheidend. Die Abwägung sämtlicher beteiligter Interessen rechtfertige die Versagung der Aussetzung. Amazon habe nicht dargetan, dass in diesem Fall die Existenz oder die langfristige Entwicklung von Amazon auf dem Spiel stünden. Die Aussetzung würde bedeuten, dass das vollständige Erreichen der Ziele des DSA möglicherweise über mehrere Jahre hinausgeschoben würde. So könne sich evtl. ein Online-Umfeld weiterentwickeln, „das eine Bedrohung für die Grundrechte darstellt". Die Bemühungen der EU-Gesetzgeber, Online-Portale sicherer zu machen, würden gefährdet. Der Unionsgesetzgeber hatte den sehr großen Online-Plattformen in diesem Umfeld eine wichtige Rolle zugesprochen. Dies gehe im vorliegenden Fall den materiellen Interessen von Amazon vor.

Ein Amazon-Sprecher zeigte sich enttäuscht über die Entscheidung. Der Konzern betreibe keine sehr große Plattform im Sinne des DSA und hätte nicht so eingeordnet werden dürfen. Die Sicherheit der Kunden habe für Amazon oberste Priorität (EuGH PM 60/24 v. 27.03.20234, Online-Werbung: Der Antrag von Amazon auf Aussetzung ihrer Pflicht, ein Werbearchiv öffentlich zugänglich zu machen, wird zurückgewiesen; Krempl, EuGH setzt DSA durch: Amazon muss Werbearchiv öffentlich machen, www.heise.de 27.03.2024, Kurzlink: https://heise.de/-9669467)

BVerwG

Keine Informationsfreiheit bei anonymen Anfragen

Das Bundesverwaltungsgericht (BVerwG) in Leipzig hat in einem Rechtsstreit mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), der von fragdenstaat.de unterstützt wurde, am 20.03.2024 entschieden, dass es zulässig ist, die Postanschrift einer Person zu verarbeiten, die eine Anfrage nach dem Informationsfreiheitsgesetz (IFG) stellt (Az. 6 C 8.22): „Nach dem Informationsfreiheitsgesetz sind anonyme Anträge unzulässig." Deshalb müsse die Behörde den Namen und auch die Anschrift des Antragstellers kennen. Das Bundesministerium des Innern (BMI) habe sich „ermessensfehlerfrei" für die Schriftform und die Bekanntgabe per Post entschieden, obwohl der Antragsteller einen elektronischen Zugang gemäß § 3a Abs. 1 VwVfG eröffnet hatte. Ein Antragsteller müsse es hinnehmen, dass die Behörde trotz eines eröffneten elektronischen Zugangs mit ihm auf dem Postweg kommuniziere.

fragdenstaat.de wird von der Open Knowledge Foundation Deutschland betrieben. Sie will es seit 2011 Nutzenden erleichtern ihr Recht auf Zugang zu amtlichen Informationen wahrzunehmen. fragdenstaat.de meint nun, das BVerwG habe mit seinem Urteil „einen Grundpfeiler des Informationszugangs" entfernt: „Die neue Regelung dürfte zahlreiche Menschen davon abschrecken Anfragen an Behörden zu richten. Gerade marginalisierte Gruppen möchten verständlicherweise nicht für Anfragen nach Informationen ihre privaten Adressen herausgeben. Das Gericht ignoriert dies komplett." Selbst wenn es Behörden über fragdenstaat.de einfach möglich sei per E-Mail zu antworten, müssten es Menschen nun hinnehmen, dass „die Behörde trotz eines eröffneten elektronischen Zugangs mit ihm auf dem Postweg kommuniziert". Dabei werde allerorts über die Digitalisierung der Verwaltung gesprochen.

In der Vorinstanz hatte das Oberverwaltungsgericht (OVG) Münster in dem Streit zwischen dem BMI und dem BfDI Ulrich Kelber noch anders entschieden. Die Postanschrift zu erheben sei für das BMI nicht erforderlich gewesen, als es die Daten verarbeitete. Es gehe nicht aus dem IFG, auch nicht aus den Grundsätzen des Allgemeinen Verwaltungsrechts hervor, dass zu einem IFG-Antrag immer die Postanschrift angegeben werden müsse. Es gebe in diesem Einzelfall auch keine Anhaltspunkte dafür, dass eine Datenerhebung erforderlich gewesen sei.

Anlass für den Rechtsstreit war ein IFG-Auskunftsantrag eines Bürgers, den dieser über fragdenstaat.de mit einer dort generierten, nicht personalisierten E-Mail-Adresse beim BMI gestellt hatte. Das BMI forderte ihn dann dazu auf, seine Postanschrift mitzuteilen, sonst könne das Verfahren nicht ordnungsgemäß durchgeführt werden. Daraufhin sprach Kelber dem BMI eine datenschutzrechtliche Verwarnung aus. Das BMI klagte dagegen, das Verwaltungsgericht Köln gab dem Ministerium Recht. Kelber wiederum hatte vor dem OVG mit seiner Berufung Erfolg.

Das Urteil des BVerwG sollte nach Meinung von fragdenstaat.de ein „Weckruf für den Gesetzgeber sein endlich ein Transparenzgesetz zu schaffen, das seinen Namen verdient". Die Ampel-Koalition verspreche seit Jahren einen Gesetzentwurf, der dieses Jahr endlich kommen soll. Er müsse sicherstellen, dass Anträge auf Informationen auch pseudonym möglich sind: „Unser Ziel ist es sicherzustellen, dass der Zugang zu Informationen allen Menschen zugutekommt. Dazu werden wir unsere Plattform erweitern und, wo möglich, klagen."

Die FDP hatte im März 2021 in den Bundestag einen Antrag eingebracht, in dem sie unter anderem fordert „das Informationsfreiheitsgesetz zu einem echten Bundestransparenzgesetz nach Vorbild des Hamburger Transparenzgesetzes (HmbTG) weiterzuentwickeln und dabei einen besonderen Fokus auf maschinelle Lesbarkeit der Daten zu legen". Der Antrag wurde vom Bundestag abgelehnt. Die Grünen unterstützen die Forderung von fragdenstaat.de nach einem Bundestransparenzgesetz. Der auch von der SPD unterschriebene Koalitionsvertrag enthält den Passus: „Die Informationsfreiheitsgesetze werden wir zu einem Bundestransparenzgesetz weiterentwickeln" (Wilkens, Informationsfreiheit: Behörden dürfen Anschrift eines Antragstellers abfragen, www.heise.de 22.03.2024, Kurzlink: https://heise.de/-9662831).

OLG Düsseldorf

Meta-Bezahl-Button ist rechtswidrig

Der Bestellprozess für das kostenpflichtige Abo von Facebook bezie-

hungsweise Instagram ist in seiner gegenwärtigen Form gemäß einem Urteil des Oberlandesgerichts Düsseldorf (OLG) vom 08.02.2024 rechtswidrig und muss überarbeitet werden (I-20 UKlaG 4/23). Meta hatte nach einem Urteil des Europäischen Gerichtshofes (EuGH) in Europa werbefreie Versionen von Facebook und Instagram mit Bezahlpflicht eingeführt (DANA 3/2023, 175 f.). Auf Antrag der Verbraucherzentrale (VZ) Nordrhein-Westfalen (NRW) urteilte das OLG, dass ein kostenpflichtiges Abo nicht mit Schaltflächen beworben werden darf, auf denen es keinen eindeutigen Hinweis auf die zahlungspflichtige Bestellung gibt. Bei Meta hieße es lediglich „Abonnieren" und anschließend „Weiter zur Zahlung", wobei man einen Bezahlweg auswählen muss.

Gemäß dem Bürgerlichen Gesetzbuch (BGB) müssen Bestell-Buttons eindeutig auf eine Kostenpflicht hinweisen. Die Verbraucher müssen bei einer Bestellung ausdrücklich bestätigen, dass diese mit einer Zahlungsverpflichtung verbunden ist. Auf der Schaltfläche muss dann die Formulierung „Zahlungspflichtig bestellen" oder ein ähnlich eindeutiger Text stehen (§ 312j BGB). Meta hat das nicht getan, was aus umfangreichen Erläuterungen zum Abschluss des Abos hervorgeht. Der 20. Zivilsenat am OLG Düsseldorf schloss sich der Kritik der VZ an. Der Kontext sei unerheblich, maßgeblich ist allein der Text auf der Schaltfläche. Die VZ NRW meint, dass Meta die Buttons nicht nur rechtmäßig beschriften muss, sondern dass bereits abgeschlossene Abos ungültig sind. Eventuell müssten gezahlte Gebühren gar zurückbezahlt werden. Eine entsprechende Klage werde geprüft.

Mit der Gerichtsentscheidung hat die Verbraucherzentrale einen ersten Erfolg gegen mehrere behauptete Rechtsverstöße in Zusammenhang mit dem neuen Abo errungen. Für mindestens 9,99 Euro im Monat kann man damit Facebook und Instagram benutzen, ohne dass in den Diensten Werbung angezeigt wird. Zudem sichert Meta zu, dass die Nutzerinformationen während des Abozeitraums nicht für Werbung benutzt werden, eine Verwendung für andere Zwecke wird damit wohl nicht ausgeschlossen. Bei der VZ ist man zudem überzeugt, dass Meta keine hinreichende Einwilligung in die Datennutzung zu Werbezwecken einholt, wenn man nicht für die beiden Dienste bezahlt. Dafür habe man ein Abmahnverfahren eingeleitet, das noch andauere. Schließlich geht die Organisation davon aus, dass die Umsetzung des Abomodells gegen die Datenschutz-Grundverordnung (DSGVO) verstößt, weil weiterhin umfangreiche Nutzerprofile erstellt werden, Partnerfirmen von Meta weiterhin Daten von bezahlenden Usern erhalten und die Wahlmöglichkeit zwischen einem kostenfreien Account und einem für mindestens 120 Euro Jahresgebühr nicht der Vorgabe für Freiwilligkeit entspreche. Über diese Kritikpunkte muss noch entschieden werden (siehe dazu auch S. 84, 96).

Eine Meta-Sprecherin erklärte, dass das rechtskräftige OLG-Urteil sich nur darauf beziehe, wie das Abonnement ohne Werbung mit sehr spezifischen Aspekten des deutschen Verbraucherrechts interagiere: „Viele Online-Dienste bieten ähnliche Abo-Modelle an, und wir sind zuversichtlich, dass unser Abo-Modell mit dem europäischen Recht übereinstimmt" (Abo für Facebook und Instagram: Meta muss nachbessern, https://www.verbraucherzentrale.nrw 08.02.2024; Holland, Ungültige Buttons: Verbraucherzentrale erringt Teilerfolg gegen Metas Abo-Modell, www.heise.de 08.02.2024, Kurzlink: https://heise.de/-9622862).

OLG Köln

Rechtswidriges Cookie-Banner bei „wetteronline.de"

Das Oberlandesgericht (OLG) Köln bestätigte mit Urteil vom 19.01.2024 auf die Klage der Verbraucherzentrale Nordrhein-Westfalen NRW (VZ NRW) hin, dass die Cookie-Banner auf der reichweitenstarken Website „wetteronline.de" der WetterOnline Meteorologische Dienstleistungen GmbH auf unerlaubte Weise gestaltet waren (6 U 80/23). Die VZ NRW monierte, dass die Nutzenden der Seite durch die unzulässige Gestaltung der Cookie-Banner dazu verleitet wurden Analyse- und Marketingcookies eher zu akzeptieren als abzulehnen.

Statt einer gleichwertigen Ablehnungsoption verwies die Website „wetteronline.de" in ihrem Cookie-Banner auf ein untergeordnetes Menü zur Abwahl von Analyse- und Marketing-Cookies. Mit solchen Cookies können Unternehmen das Surfverhalten analysieren und kommerziell nutzen, etwa für personalisierte Werbung. Für das Funktionieren der Website sind sie nicht notwendig, deshalb ist für Analyse- und Marketing-Cookies eine Einwilligung der Websitebesucher nötig. Die Möglichkeit, solche nicht notwendigen Cookies mit nur einem Klick abzulehnen, fehlte auf der ersten Ebene des Banners. Zudem zeichnete sich der „Einstellungen"-Button, der auf die zweite Ebene mit Ablehnmöglichkeiten von Analyse- und Marketing-Cookies führte, kaum vom Hintergrund ab, der „Akzeptieren"-Button hingegen deutlich. Das OLG bestätigte die Auffassung der VZ NRW, dass Nutzer aufgrund der Gestaltung des Banners keine echte Wahlfreiheit hatten zwischen dem Akzeptieren und Ablehnen solcher Cookies. Das Gericht befand auch ein Kreuzchen in der rechten oberen Ecke des Cookie-Banners mit der Aufschrift „Akzeptieren & Schließen" für rechtswidrig. Klickten Nutzende der Website auf dieses Kreuzchen, gaben sie wie beim Akzeptieren-Button ihre Einwilligung zur Verarbeitung von Analyse- und Marketing-Cookies. Die Beklagte hat inzwischen ihr werbefinanziertes Geschäftsmodell um ein kostenpflichtiges Abomodell erweitert und das Banner im Zuge dessen angepasst.

Christine Steffen, Juristin und Datenschutzexpertin bei der Verbraucherzentrale NRW, erläutert: „Bei einer solchen Gestaltung reden wir von sogenannten ‚Dark Patterns', die die Verbraucher:innen unterbewusst bei einer Entscheidung beeinflussen sollen. Unternehmen versuchen immer wieder die Grenzen rechtmäßiger Gestaltung von Cookie-Bannern auszureizen. Ein Zeichen dafür, wie wichtig den Anbietern Nutzerdaten sind." Das Urteil ist noch nicht rechtskräftig (VZ NRW, Cookie-Banner auf wetteronline.de rechtswidrig gestaltet, PE 01.02.2024).

OVG Niedersachsen

Geburtsdatum als Webshop-Pflichtfeld grds. unzulässig

Das Niedersächsische Oberverwaltungsgericht (OVG) hat mit Beschluss vom 23.01.2024 die Ansicht des Landesbeauftragten für den Datenschutz Niedersachsen (LfD) bestätigt, dass beim Einkaufen in Online-Shops im Rahmen eines Bestellprozesses nicht ohne Weiteres das Geburtsdatum als zwingende Angabe abgefragt werden darf (Az. 14 LA 1/24). Mit dem Beschluss hat das OVG die Zulassung zur Berufung gegen das Urteil des Verwaltungsgerichts Hannover, das entsprechend entschied, verweigert. Hintergrund des Verfahrens ist eine Unterlassungsanordnung der Datenschutzaufsicht gegenüber einer Online-Apotheke. Diese hatte das Geburtsdatum im Bestellprozess erhoben. Die Abfrage erfolgte unabhängig von der Art der bestellten Ware, also nicht nur bei Medikamenten, sondern auch bei allgemeinen Drogerieprodukten.

Die Verarbeitung des Geburtsdatums ist i.d.R. datenschutzrechtlich nicht zur Erfüllung eines Vertrags erforderlich. Für eine Prüfung, ob Minderjährige im Webshop bestellen und der Vertrag daher schwebend unwirksam sein könnte, kann der Betreiber die Volljährigkeit abfragen und benötigt nicht das genaue Geburtsdatum. Der Betreiber eines Webshops kann auch nicht die Erfüllung einer rechtlichen Verpflichtung geltend machen, um später Kunden bei der Ausübung ihrer Betroffenenrechte eindeutig identifizieren zu können. Verantwortliche dürfen explizit keine zusätzlichen Daten allein für die Erfüllung ihrer Auskunftspflicht speichern.

Das OVG stellte klar, dass der Verantwortliche das standardmäßige Erheben und Verarbeiten des Geburtsdatums auch nicht mit seinem berechtigten Interesse begründen kann. Zwar kann die Vorsorge für ein gegebenenfalls notwendiges Eintreiben offener Zahlungen ein berechtigtes Interesse darstellen, jedoch nur, wenn überhaupt ein Ausfallrisiko hinsichtlich der Zahlung besteht. Ein solches Risiko liegt beispielsweise nicht bei der Bezahlung per Vorkasse vor.

Dies gilt auch für den Sonderfall einer Online-Apotheke. Zwar sind Apotheken in besonderem Maße verpflichtet den Käufer zu beraten, zu informieren und aufzuklären. Doch diese Pflichten gelten nur für bestimmte Produktkategorien. Eine Sonderreglung nach der Arzneimittelverschreibungsordnung für rezeptpflichtige Medikamente ist für die sonstigen Vertriebsprodukte der Online-Apotheke nicht anwendbar. Ein Argument gegen die verpflichtende Angabe des Geburtsdatums war im aktuellen Fall zudem, dass der Bestellprozess dieses zwar für den Käufer abfragte, nicht jedoch für die Person, die das Produkt später verwenden sollte.

Der LfD Niedersachsen Denis Lehmkemper erläutert: „Während sich eine Anschrift durch einen Umzug verändern kann, ist das Geburtsdatum ein besonders dauerhaftes Datum. Ich begrüße daher die Klarheit, mit der die Gerichte die Argumente der Beklagten zurückgewiesen haben." Betreiber von Webshops sollten überprüfen, ob sie im Bestellprozess das Geburtsdatum als zwingende Angabe abfragen, zu welchen Zwecken dieses erforderlich ist und auf welcher Rechtsgrundlage es verarbeitet wird. Sollte die Abfrage nur auf die Einwilligung als Rechtsgrundlage gestützt werden können, ist das entsprechende Eingabefeld im Bestellformular eindeutig als „freiwillig" zu kennzeichnen. Die Kundinnen und Kunden seien über die Verwendung dieses Datums umfassend zu informieren. Geben diese kein Geburtsdatum an, so müsse der Bestellprozess fortgesetzt werden können (Vorinstanz VG Hannover, U. v. 09.11.2021, Az.: 10 A 502/19; Der Landesbeauftragte für den Datenschutz Niedersachsen, Geburtsdatum als Pflichtfeld in Webshops oft rechtswidrig, PM Nr. 6/2024 v. 20.03.2024).

ArbG Hamburg

ChatGPT im Betrieb nicht immer mitbestimmungspflichtig

Das Arbeitsgericht (ArbG) Hamburg hat mit Beschluss vom 16.01.2024 entschieden, dass die Einführung von Systemen Künstlicher Intelligenz (KI) wie ChatGPT oder Gemini nicht in jedem Fall mitbestimmungspflichtig sei, weil die Mitarbeitervertretung es bereits in einer Vereinbarung über Webbrowser ausgeübt hat (Az. 24 BVGa 1/24). Der Betriebsrat eines global agierenden Hamburger Herstellers im Bereich der Medizintechnik mit rund 1.600 Mitarbeitern am Stammsitz wollte im Rahmen einstweiligen Rechtsschutzes den in dem Konzern seit Mitte Dezember 2023 möglichen Einsatz von ChatGPT und den weiterer KI-Lösungen verbieten lassen. Dies wiesen die Hamburger Richter als teils unbegründet und teils unzulässig zurück.

Das Unternehmen will generative KI für die Mitarbeiter als neues Werkzeug zur Unterstützung nutzbar machen. Zwar sperrte es zunächst kurz den Zugang zur Webseite von ChatGPT, veröffentlichte dann aber auf seiner Intranet-Plattform einschlägige Richtlinien für den Dienst von OpenAI und ähnliche Services. Die Systeme werden nicht auf den Computersystemen des Konzerns installiert. Ihre Nutzung erfolgt über Webbrowser durch ein Konto auf dem Server des jeweiligen Anbieters. Dienstliche Nutzerkonten werden zurzeit nicht eingerichtet. Etwaige Kosten müssen die Arbeitnehmer selbst tragen. Der Arbeitgeber weiß nach eigenen Angaben nicht, wer von derlei Optionen wie lange und wann Gebrauch macht und welche Daten dabei an die Systembetreiber fließen.

Der Betriebsrat verlangte, neben ChatGPT auch vergleichbare Programme zu sperren, solange eine Rahmenvereinbarung zum Thema KI nicht fertig sei. Mit der Veröffentlichung von Richtlinien zur Nutzung generativer KI würden die Mitbestimmungs- und Mitwirkungsrechte verletzt. Es könne nicht ausgeschlossen werden, dass weitere personenbezogene Daten neben der Anmeldeinformationen eingegeben würden. Auch sei nicht ersichtlich, wie der Arbeitgeber überprüfen wolle, dass die internen Vorgaben eingehalten werden und ChatGPT nur im „Non-Training-Modus" läuft. Im schlimmsten Fall könnten Arbeitsschritte der Beschäftigten „lückenlos überwacht werden".

Das ArbG meinte dagegen, dass die Vorgaben zur Nutzung von ChatGPT und vergleichbarer Werkzeuge hier „unter

das mitbestimmungsfreie Arbeitsverhalten“ falle. Zwar werde der verwendete Browser die Nutzung des Chatbots regelmäßig aufzeichnen. Die Parteien hätten jedoch zur Nutzung solcher Navigationsmittel im Web schon eine Konzernbetriebsvereinbarung abgeschlossen; damit habe der Betriebsrat sein Mitbestimmungsrecht bereits ausgeübt. OpenAI zeichne die bei ChatGPT eingegebenen Daten zwar wohl auf. Dies führe aber nicht zur Mitbestimmung, da „der dadurch entstehende Überwachungsdruck nicht vom Arbeitgeber ausgeübt“ werde. Schließlich könne der Antragsgegner auf die vom Diensteanbieter gewonnenen Informationen nicht zugreifen.

Die Arbeitsrichter diskutierten zudem das Mitbestimmungsrecht „in Fragen der Ordnung“ der Firma „und des Verhaltens der Arbeitnehmer“. Es gehe um das „Zusammenleben und kollektive Zusammenwirken der Beschäftigten“. Der Arbeitgeber habe hier „nur Anordnungen getroffen“, wie die Arbeit zu leisten sei. Die Entscheidung erfolgte konkret auf die Gegebenheiten des Einzelfalls bezogen. KI im Betrieb dürfte in den meisten Fällen mitbestimmungspflichtig sein. Die Erwägungen des ArbGs sind aber praxisrelevant. Im Betriebsrätemodernisierungsgesetz von 2021 wird klargestellt, dass die Rechte der Beschäftigtenvertretung bei der Gestaltung der Arbeitsumgebung und von Abläufen im Unternehmen auch dann greifen, wenn dort algorithmische Entscheidungssysteme etwa zu Personalauswahl und -bewertung eingesetzt werden sollen. Der Betriebsrat darf einen Sachverständigen hinzuziehen, um die Einführung oder Anwendung von KI beurteilen zu können (Krempl, Arbeitsgericht: Betriebsrat darf nicht mitbestimmen über Einsatz von ChatGPT, www.heise.de 14.02.2024, Kurzlink: https://heise.de/-9627556).

Buchbesprechungen

Specht, Louisa/Hennemann, Moritz
Data Governance Act: DGA
Handkommentar
Nomos Verlagsgesellschaft Baden-Baden 2023, 718 S.
ISBN 978-3-8487-8340-3, 129,00 Euro

(ak) Schon kurz nach Abschluss des Gesetzgebungsvorgangs zum neuen EU Data Governance Act legen die Autorin und der Autor einen Handkommentar vor, der versucht, dieses neue Regelwerk zugänglich zu machen. Zum Zeitpunkt des Erscheinens dieses Werks war der Gesetzgebungsprozess für die Elemente das Digitalpaketes der Europäischen Kommission noch nicht abgeschlossen. Insbesondere der Data Act war noch in der Verhandlung zwischen den Gesetzgebungsorganen. Dies ist inzwischen geschehen; mit der Verordnung zum Europäischen Gesundheitsdatenraum (European Health Data Space, EHDS) ist auch bereits ein weiteres Instrument zur Datennutzung verabschiedet worden. Entsprechend diesen Entwicklungen wurde die Kommentierungsarbeit nicht eingestellt, sondern ein Nachfolgewerk desselben Teams ist vom Verlag bereits für Juli 2024 angekündigt.

Der Kommentar stellt fest, dass der DGA nicht die Erwartung erfüllt, einen wirklich umfassenden und vollständigen Rahmen für die Weitergabe und Weiternutzung von Daten innerhalb des EU-Binnenmarktes zu schaffen, was nach den Ankündigungen vielleicht die Erwartung mancher Beobachter war. Die Verordnung konzentriert sich nur auf einige Teilbereiche, und zwar insbesondere die Weitergabe von Daten öffentlicher Stellen, auf Datenvermittlungsdienste und das neu eingeführte Modell des „Datenaltruismus“. Wesentlich zum Verständnis des DGA und seiner vorgesehenen Funktion für eine gesamtgesellschaftliche Datengovernance ist daher seine Interaktion mit den anderen bereits bestehenden Instrumenten über die Behandlung von Daten, also Instrumenten wie der DSGVO, der PSI-Richtlinie, aber auch den anderen Teilen des Digitalpaketes, also DSA, DMA und DA. Hier bietet das Werk eine umfassende und kenntnisreiche Analyse.

Aus der Perspektive des Datenschutzes ist natürlich besonders das Verhältnis des DGA zur DSGVO interessant. In seinen Artikeln und Erwägungsgründen ist der DGA in dieser Hinsicht zwar sehr viel wortreicher und detaillierter als etwa DSA und DMA, aber die Komplexität des Zusammenwirkens der verschiedenen Rechtsinstrumente bedarf dennoch weiterer Klarstellung. Der vorliegende Kommentar geht dieses Thema an und bietet eine sehr klare Position. Vor allem bietet der DGA keine zusätzliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Das ist eine ganz wichtige Feststellung für alle, die mit der Rechtmäßigkeit der Verarbeitung personenbezogener Daten in Unternehmen oder öffentlichen Organisationen zu tun haben, auch um sich – wenn nötig – den Ansprüchen der enthusiastischen Datenschatz-Sucher entgegenzustellen.

Für die vorliegende erste Auflage gilt wie bei anderen bereits in der DANA besprochenen „frühen“ Kommentaren der neuen EU-Digitalgesetzgebung, dass ein Kommentar, der wenige Monate nach der Verabschiedung eines

Rechtsakts erscheint, naturgemäß nur ein erster Einstieg in die Thematik sein kann, insbesondere wenn notwendige ergänzende Regelungen der EU und auf nationaler Ebene noch in der Entwicklung sind. Der vorliegende Band zeigt aber bereits, dass das Autorenteam der Aufgabe voll gewachsen ist und das komplexe Rechtsgebiet überblickt.

Zu erwarten sind in der nächsten Zeit umfassende Kommentierungen zu den gesamten neuen Regelungen zum Teilen von Daten, insbesondere zum Data Act und zum Europäischen Gesundheitsdatenraum (EHDS), die für Datenschützer sehr wichtig sein werden. Der vorliegende Band hilft auch zu erkennen, wo die mit Blick auf nicht personenbezogene Daten geschaffenen neuen Regeln zum Teilen von Daten durch den Datenschutz begrenzt sind.

Maties, Martin
StichwortKommentar eSport-Recht
Beratungs- und Anwendungswissen, alphabetische Gesamtdarstellung
Nomos, Baden-Baden 2023, 1080 S.,
ISBN 978-3-8487-5966-8, 149,00 Euro

(ha) Bereits mehrmals wurden an dieser Stelle Bücher vorgestellt, die das Thema „Spielen" behandeln oder zumindest streifen (siehe DANA 2/2023 S. 123, 3/2022 S. 210 und 1/2021 S. 62 f.). Jetzt liegt mit dem „Stichwort-Kommentar eSport-Recht" aus dem Nomos-Verlag ein umfassendes Werk vor, das seinem Untertitel „Alphabetische Gesamtdarstellung" durchaus gerecht wird. Herausgeber ist Prof. Dr. Martin Maties von der Universität Augsburg, der dort 2019 die Forschungsstelle für eSportRecht gründete. Im Vorwort begründet er die Wahl des Formates damit, dass aufgrund der Vielzahl der Rechtsmaterien eine klassische Kommentierung nicht zielführend sei.

Für das Stichwort „Datenschutz" zeichnen Dirk Heckmann und Jakob Auer verantwortlich. Sie behandeln das Thema ausführlich und liefern eine grundsätzliche juristische Aufarbeitung mit einzelnen Beispielen. Nur stellen sie ab und zu den Bezug zum eSport mit teils lapidaren Bemerkungen her, wie zum Beispiel bei der Erläuterung der Datenschutzerklärung: „Die Anforderungen an die Datenschutzerklärung sind im Bereich des eSports ebenso wichtig wie in anderen Bereichen …"

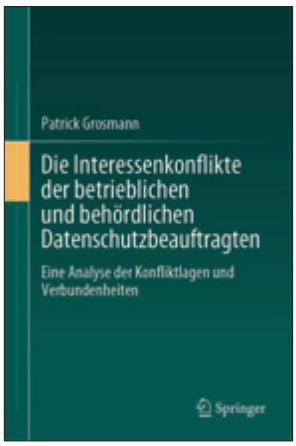
In Beiträgen anderer Autoren wird ebenfalls des Öfteren auf Datenschutz eingegangen. Dabei wiederholt sich naturgemäß die Grundinformation zum Anwendungsbereich der DSGVO – nebst vielen Verweisen auf das o.a. Kapitel Datenschutz –, doch sind hier die Spiele-Bezüge deutlich ausgeprägter, was den nicht juristisch vorgebildeten Leserinnen und Lesern sicher entgegenkommt. So wird unter dem Stichwort „Account, Datenschutz" an einem Beispiel ausführlich dargestellt, wie informative Webseiten über öffentliche Spiele von eSportlern genutzt werden können, um daraus „detaillierte Rückschlüsse auf die Lebensgewohnheiten" des Sportlers zu ziehen. Verantwortlich für dieses Kapitel und für „Clan, Datenschutz" sowie „Sportverein, Datenschutz" sind Ulrich M. Gassner und Daniel Schmid. Schmid alleine verfasste „Cloud Gaming" und „Beschäftigtendatenschutz". In letzterem Beitrag findet über die übliche Spieler-Situation hinaus eine hilfreiche Betrachtung der Situation von Spiele-Profis statt. Ganz konkret problematisiert der Autor dort beispielsweise unter Bezug auf das BDSG (§ 26) die Sammlung von Leistungsdaten durch den Arbeitgeber, um damit im Fall eines etwaigen Spieler-Transfers „die Ablösesumme in die Höhe zu treiben". Auch in weiteren Beiträgen wird das Thema Datenschutz im konkreten Zusammenhang wiederholt aufgegriffen, etwa beim Punkt „Social Media", den Roman Deringer verfasst hat, und der ausführlich die Nutzung der sog. sozialen Medien betrachtet.

Nicht verschwiegen werden soll an dieser Stelle, dass die Autoren Heckmann und Auer in einem Punkt völlig anderer Meinung zu sein scheinen als Gassner und Schmid: Während im Hauptbeitrag „Datenschutz" in Bezug auf den Widerruf der Einwilligung die Meinung vertreten wird, „dass bei Zusammentreffen der Einwilligung mit einem anderen Rechtfertigungsgrund durch den Widerruf dennoch eine Verarbeitung personenbezogener Daten … möglich ist", wird unter „Beschäftigtendatenschutz" und „Clan, Datenschutz" empfohlen, die Einwilligung solle „nur für Datenverarbeitungsvorgänge eingeholt werden, für die nicht sowieso ein anderer Erlaubnistatbestand gegeben ist". Gassner und Schmid sehen nämlich in der von Heckmann und Auer vertretenen Position ein widersprüchliches Verhalten und bewerten sie mit der Feststellung, die eSportler würden damit in den Irrglauben versetzt, „über die Verarbeitung der Daten bestimmen zu können". Ähnlich unterschiedlich ist auch die Einschätzung bei den sensiblen Daten, bei denen es im „Datenschutz"-Beitrag heißt, es werde im eSport-Bereich „nur in sehr seltenen Fällen" zu ihrer Verarbeitung kommen. Das wird im Beitrag von Schmid zum Beschäftigtendatenschutz anders gesehen, der dort als Beispiele für den Fitnesszustand des eSportlers „Herz- und Atemfrequenz, Tastanschläge oder Klicks pro Minute" nennt.

Wer sich also nicht auf das Kapitel „Datenschutz" beschränkt, in dem übrigens das BDSG beim Datenschutzbeauftragten (§ 38) nicht erwähnt wird, findet aufgrund der immerhin 122 Stichworte die Persönlichkeitsrechts-Problematik unter verschiedenen Gesichtspunkten umfassend betrachtet. Als Beispiel dafür sei das Thema „Recht am eigenen Bild" genannt, das sowohl als eigenes Stichwort als auch in weiteren Zusammenhängen behandelt wird. Vor allem Verantwortlichen aus dem Bereich des eSports kann dieses Werk durchaus empfohlen werden.

Grosmann, Patrick
Die Interessenkonflikte der betrieblichen und behördlichen Datenschutzbeauftragten
Springer, Berlin 2024, 221 S.
ISBN 978-3-662-68386-6, 119,99 Euro

(tw) Der betriebliche/behördliche Datenschutzbeauftragte (bDSB) – ein ursprünglich deutsches Instrument des Datenschutzes – hat seine europaweite



Ausformung in den Art. 37 bis 39 DSGVO gefunden. Hierzulande ist der bDSB in der Datenschutzkultur bestens integriert und erfüllt eine zentrale Funktion als Mittler zwischen Verantwortlichem, Betroffenen und Aufsichtsbehörde. Mit Urteil vom 09.02.2023 fanden diese Regelungen auch den Segen des Europäischen Gerichtshofs (EuGH), der Kriterien benannte, wann ein Interessenkonflikt bei der Wahrnehmung der Aufgaben des bDSB besteht (C-453/21). Auch das Bundesarbeitsgericht (BAG) befasste sich in jüngerer Zeit immer wieder mit dem Thema (zuletzt BAG 06.06.2023 – 9 AZR 383/19). Diese Urteile konnten von Patrick Grosmann in seiner Promotion zum judizierten Thema nicht mehr berücksichtigt werden. Die Arbeit wurde im Juni 2022 eingereicht und nun 2024 gedruckt und als eBook verfügbar gemacht.

Das Thema hat Relevanz, ja Brisanz. So war der Versuch des Innenausschusses des Bundesrats nicht überraschend, anlässlich der jüngsten Novellierung des Bundesdatenschutzgesetzes (BDSG), die „bürokratische" Erforderlichkeit des bDSB zurückzufahren. Und erfreulich war es, dass der Bundesrat dieses Ansinnen Anfang 2024 zurückwies. Offenbar ist die Erkenntnis, dass die Institution des bDSB als ehrlicher Makler zwischen den Fronten eine zentrale Rolle spielt bei der Wahrung des Datenschutzes in Verwaltung und Wirtschaft, bis in die Spitzen der Landespolitiken vorgedrungen.

Diese Erkenntnis hat zweifellos einen Hintergrund in der organisatorischen Verfestigung des bDSB in der deutschen Datenschutzkultur, die ein recht klares Berufsbild des bDSB hervorgebracht hat und dessen Erhalt auch im Interesse der Wirtschaft zu liegen scheint. Einen wesentlichen Beitrag hierfür leistet der EuGH mit seinen Urteilen, wonach Unternehmen im Fall des Verstoßes gegen den Datenschutz saftige Sanktionen oder Schadenersatzforderungen drohen und der bDSB als unabhängiger Berater des Verantwortlichen, also de facto der Unternehmensleitung, als eine wirksame Schutzmaßnahme erkannt wird.

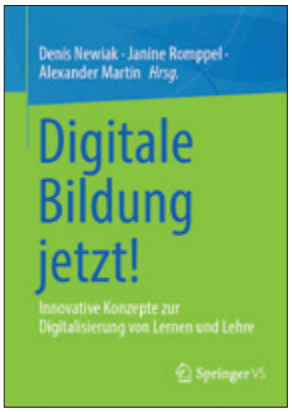
Das Thema der Arbeit von Grosmann ist, welche Wirksamkeitsvoraussetzungen hierfür bestehen. Dabei kann er auf eine umfangreiche Literatur zurückgreifen, die er auch umfassend ausgewertet hat. Systematisch dekliniert der Autor die möglichen Interessenkonflikte sowohl des internen wie des externen bDSB durch. Systematisch erfreulich ist, dass sauber zwischen dem Grundverhältnis des bDSB und dem datenschutzrechtlichen Verhältnis zwischen Verantwortlichem und bDSB unterschieden und die Wechselwirkung beschrieben wird. Besonders berücksichtigt wird der Umstand, dass als externe bDSB tätige Anwälte spezifischen Interessenkonstellationen ausgesetzt sind. Der Autor beschränkt sich nicht auf eine formale Betrachtung, wie sie zunächst im Gesetz angelegt ist, sondern widmet sich auch weniger justiziablen, in die Psyche gehenden „Verbundenheiten". Dabei stellt er hohe Anforderungen an die Neutralität und Unabhängigkeit des bDSB, die in der Realität oft nicht anzutreffen sind. Dies ist eine Stärke des Buchs, das so der Selbstversicherung des bDSB dienen kann. Es ist aber fraglich, ob diese Erkenntnisse vor Gericht umsetzbar sind. Dessen ungeachtet ist die Entwicklung eines Idealbilds des bDSB nützlich als Spiegel für oft ernüchternde Realitäten.

Schade ist, dass diese Realitäten in dem Buch eher kurz kommen bzw. sich auf einer relativ hohen Abstraktionsebene bewegen. Insofern hätten dem Werk, um mit mehr Leben gefüllt zu werden, mehr Empirie, mehr Fallbeschreibungen und Rechtsprechung gutgetan. Doch auf der abstrakteren Ebene weist die Arbeit dafür eine sehr überzeugende und (fast) umfassende Behandlung der möglichen Konfliktlagen auf: Konflikte zwischen der Beratungs- und Kontrollaufgabe, zwischen der bDSB-Rolle und sonstigen für den Verantwortlichen wahrgenommenen Aufgaben, zwischen persönlicher Verbundenheit und formaler Treuepflicht werden im Detail erörtert und geben eine – im Sinne des Grundrechtsschutzes – datenschutzfreundliche Orientierung. Insofern eignet sich die Arbeit als qualifiziertes Nachschlagewerk, mit dem tatsächlich bestehende Konfliktlagen analysiert und bewertet werden können und ist damit viel mehr als eine juristische Fleißarbeit. Ein sehr detailliertes Inhaltsverzeichnis gibt eine gewisse Orientierung. Für eine praxisorientierte Nutzung der Arbeit wäre – was für Promotionen aber unüblich ist – ein Stichwortverzeichnis hilfreich gewesen.

Eine Stärke der Arbeit besteht darin, dass sie mögliche Interessenkonfliktlagen in den breiteren rechtlichen Rahmen, in dem sich die Tätigkeit eines bDSB abspielt, stellt und Ressourcen, Informationszugang, Ausbildungsfragen, Haftung, Kommunikationsstrukturen (z.B. zu Betroffenen), innerorganisatorische Fragen wie auch organisatorische Anbindung und Ausgestaltung thematisiert. Die Rolle des bDSB bei der Erfüllung der formellen Anforderungen des Verantwortlichen, etwa beim Aufbau eines Datenschutzmanagements oder der Durchführung einer Datenschutz-Folgenabschätzung werden ebenso behandelt wie das Verhältnis zwischen technischer und rechtlicher Expertise und entsprechenden Aufgaben. Nur am Rande behandelt wird die Beziehung zu Beschäftigtenvertretungen, etwa dem Betriebsrat. Dabei verblüfft angesichts der sonstigen Vollständigkeit der Arbeit, dass die spezifische Problematik der Kontrolle der Datenverarbeitung des Betriebsrats oder anderer spezifischer Geheimnisträger wie etwa des Betriebsarztes zu kurz kommt. Es mag sich mit dem Zeitpunkt des ersten Abschlusses der Arbeit erklären, dass die Regelung des 2021 verabschiedeten § 79a BetrVG, in der der spezifische Interessenkonflikt des bDSB zwischen Verantwortlichem und Betriebsrat adressiert wird, unberücksichtigt geblieben ist.

Die Arbeit wird abgeschlossen durch einige Vorschläge zur rechtlichen Weiterentwicklung des bDSB. Dabei werden neben überregulatorischen Vorschlägen erhöhte Anforderungen an die Qualifikation, eine verbesserte Absicherung der Vertraulichkeit und die Wiederein-

führung der Abberufungsmöglichkeit durch die Datenschutzaufsicht vorgeschlagen. Dem kann vom Rezensenten zugestimmt werden. Zwar hat die Stellung des bDSB schon eine lange Geschichte und eine intensive rechtliche Behandlung erfahren, doch zeigt sich, dass sich die Rolle des bDSB weiter in Entwicklung befindet. Die Arbeit von Grosmann gibt hierzu gute Anregungen. Sie hat aber auch praktischen Nutzen für Menschen, die ihre Arbeit als bDSB reflektieren wollen.



Denis Newiak, Janine Romppel, Alexander Martin (Hrsg.)
Digitale Bildung jetzt! – Innovative Konzepte zur Digitalisierung von Lernen und Lehre
Springer VS, Wiesbaden 2023,
134 Seiten, eBook,
ISBN 978-3-658-40845-9,
59,99 Euro

(hhs) Mit der Corona-Pandemie veränderte sich plötzlich die Lernlandschaft. Von der eigentlich verpflichtenden Präsenzschule, den Vorlesungen an Hochschulen und Kursen der Erwachsenenbildung war ganz plötzlich keine Rede mehr. Schule fand, wenn überhaupt, nun zu Hause statt. Schüler, aber auch Lehrer, wurden mit dieser Problemstellung vielfach alleine gelassen und es lag gerade an den Lehrkräften, wie sie dieses Problem auffingen. Dabei kam der Ruf nach Digitalisierung in einem besonderen Maße auf und fand seinen Höhepunkt in der Frage des Einsatzes von Videokonferenzsystemen, ja oder nein und wenn ja, welche? Damit hat die Schließung von Bildungseinrichtungen während der Corona-Pandemie die Probleme bei der technischen Modernisierung der Schulen offensichtlich werden lassen. Mit der Not entsteht auch die Chance Schulen neu zu denken – etwa durch innovative Konzepte für virtuelle Unterrichtsformate, den zielorientierten Einsatz von smarten Geräten im Präsenzunterricht und für eine Lehrkräfte-Ausbildung, die umfassend digital qualifiziert.

Das vorliegende Werk enthält mit seinen insgesamt acht unterschiedlichen Beiträgen sowohl eine Bestandsaufnahme, wie man mit der Lehre zu Hause und mit digitalen Lernmitteln während der Pandemie umgegangen ist, wie die Empfindungen der Schüler waren, es enthält aber auch einen Ausblick, was bei einer Digitalisierung der Zukunft zu beachten ist. Wie lassen sich neue digitale Medien für eine moderne Wissensvermittlung an Schulen und Hochschulen nutzen?

Die einzelnen Autoren stellen dabei in diesem Band ihre Studien und Erfahrungen, insbesondere aus dem Bereich der Pädagogik, der Medienwissenschaft und der Soziologie zusammen, entwickeln Vorschläge für den Einsatz digitaler Medien und Techniken für zeitgemäße Bildungs- und Lehrkonzepte und präsentieren ihre Best Practices.

Im Einzelnen handelt es sich um die folgenden Themenfelder, welche behandelt werden:

- Digitalisierung, digitale Lehre jetzt?!
- Digitale Bildung zwischen Ideal, Realisierung und Kritik: Der Versuch einer Kontextualisierung von Digitalität durch den Begriff der Bildung
- Digital gestützte Lernumgebungen aus ökologischer Perspektive analysieren und gestalten
- Binnendifferenzierung in der sprachlichen Grundbildung digital gestalten am Beispiel von KANSAS, einer innovativen Suchmaschine für authentische Lehr-/Lerntexte
- Reflexive Digitalisierung und kritische Digitalkompetenz
- Die Transformation der Schule in eine hybride Lernumgebung: Erste Erkenntnisse einer internationalen Interviewstudie
- Die Zukunft von wissenschaftlichen Bildungsvideos – nachhaltig gedacht und umgesetzt
- Belastungserleben als Herausforderung von Abiturient*innen im digital vermittelten Distanzunterricht.

Bei dem Werk, welches zur Rezension vorlag, handelte es sich um ein E-Book. Das Werk war also digital zu lesen. Den Rezensenten hat dabei gestört, dass Tabellen, wie in einem gedruckten Buch, hochkant abgebildet wurden. Ein gedrucktes Buch kann man einfach drehen, wenn ein Tablet zum Lesen zur Verfügung steht, dieses auch, aber bei einem Bildschirm bedarf es mehrerer Klicks, um die Seite lesbar zu machen. Dies natürlich auch, um das Seitenformat wieder in den Ausgangspunkt zu versetzen. Dies ist kein gutes Beispiel von gelungener Digitalisierung und würde digitale Schulbücher, welche vorliegend kein Thema sind, in keinem guten Licht oder digitaler Funktion dastehen lassen.

Insgesamt handelt es sich bei den Beiträgen, wie schon ausgeführt, um pädagogische, soziologische und sonstige Beiträge. Sie werfen aus dem Blickwinkel des Datenschutzes aber auch die Frage auf, wie dieser beachtet und angewendet wird. Die Forderung nach digitaler Kompetenz bedeutet jedoch auch bei Nutzung der selbigen, dass es zu einer Verhaltens- und Leistungskontrolle der Lehrkräfte, aber auch der Lernenden kommen kann. Wie soll damit umgegangen werden? Insgesamt: Wie wird das allgemeine Persönlichkeitsrecht und damit auch das Recht auf informationelle Selbstbestimmung geschützt? Hierzu findet man leider in den vorliegenden Beiträgen gar nichts.

Immerhin waren während der Pandemie die datenschutzrechtlichen Fragen nicht gerade gering (siehe nur Videokonferenzsysteme und Datenübermittlung in die USA). Hierfür gilt es für die Zukunft vorzusorgen. In dem Werk nicht erwähnt ist das Forschungsprojekt DIRECTIONS. Das Projekt ist durch Mittel des Bundesministeriums für Bildung und Forschung gefördert und hat zum Ziel, dass Lernanwendungen sowie Content-Plattformen, aber auch notwendige Lerninfrastrukturen wie virtuelle Klassenzimmer, Videokonferenzsysteme oder Systeme zur Unterstützung des Unterrichts auf ihre DSGVO-Konformität geprüft werden können – also datenschutzkonform sind bzw. werden (siehe dazu Hornung/Schindler, DIRECTIONS: Forschungsprojekt zur Zertifizierung schulischer Informationssysteme, ZD-Aktuell 2022, 01037). Auch dieser Themenkomplex sollte bei einem

Werk über digitale Bildung nicht außer Betracht bleiben. Dazu findet der geneigte Leser leider nichts.

Das vorliegende Werk, welches sich an den Bildungsbereich und die Kultusministerien wendet, kann diesen empfohlen werden. Datenschutzinteressierte erfahren leider nichts.

Claudia de Witt, Christina Gloerfeld, Silke Elisabeth Wrede
Künstliche Intelligenz in der Bildung
Springer VS, Wiesbaden 2023, 453 S.
ISBN 978-3-658-40079-8, 54,99 Euro

(hhs) Künstliche Intelligenz (KI) ist seit einiger Zeit ein Zauberwort und hat im letzten Jahr deutlich an Fahrt aufgenommen. Der vorliegende Band geht von einer bildungswissenschaftlichen Perspektive auf KI zu. Er enthält bildungstheoretische Standpunkte zum Einfluss von KI auf Bildung und stellt didaktische Positionen bzw. Gestaltungsansätze von KI in der Schule, der beruflichen (Weiter-)Bildung und der Hochschulbildung vor. Neben Ansätzen zur Kompetenzentwicklung mit KI in der Bildungspraxis hebt der Band zudem den erklärbaren, ethisch orientierten und souverän beherrschbaren Umgang mit KI hervor.

Die Ausführungen werden durch vier Oberkapitel geprägt, unter denen sich dann die einzelnen Beiträge befinden. Dabei geht es um:

Bildungstheoretische Positionen: Die Eigenlogiken von KI und ihr Einfluss auf Bildung

- Bildung durch Künstliche Intelligenz ermöglichen. Ein Beitrag aus bildungstheoretischer Perspektive
- Künstliche Intelligenz. Eine bildungstheoretische Annäherung aus Sicht kritisch-konstruktiver Didaktik
- KI und graue Intelligenz. Bildungstheoretische Perspektiven auf Lerntechnologie und ihre Akteure
- Zur (Un-)Berechenbarkeit der Künste. Wie algorithmische Strukturen die Bedingungen für Ästhetik und ästhetische Bildung verändern

Didaktische Positionen: Mit KI lehren und lernen

- Didaktische Impulse zum Lehren und Lernen mit und über Künstliche Intelligenz
- Lernpfade in adaptiven und künstlich-intelligenten Lernprogrammen. Eine kritische Analyse aus mediendidaktischer Sicht
- KI und Didaktik – Zur Qualität von Feedback durch Recommendersysteme
- Roboter in kollaborativen Lehr-Lernkontexten. Theoretische Reflexionen interaktiver Lehr-Lernformen mit sozialen Robotern
- Computational Thinking vermitteln. Wie Problemlösekompetenz als Bestandteil digitaler Souveränität erworben werden kann

Veränderungen in Bildungsinstitutionen: Chancen und Herausforderungen von KI für Schule, Hochschule und berufliche Bildung

- Künstliche Intelligenz und Schule. Aufgaben für Unterricht und die Organisation (von) Schule
- Künstliche Intelligenz in der Hochschulbildung. Bildungssoziologische Perspektiven und Herausforderungen
- Education 4.0. Smarte (IoT- und KI-gestützte) Hochschulbildung
- Akzeptanzforschung zum Einsatz Künstlicher Intelligenz in der Hochschulbildung. Eine kritische Bestandsaufnahme
- Aktanten als Grundlage und Analysegegenstand für KI in der Hochschulbildung
- Künstliche Intelligenz, Behinderung und Technoableism
- Fortgeschrittene Digitalisierung und Strategien für die berufliche (Weiter-) Bildung. Augmentation, Fusion Skills und Augmentationsstrategien

Bildungspraxis im Wandel: Kompetenzentwicklung mit KI

- Sprachenlernen per KI. Möglichkeiten und Grenzen in der Praxis
- KI-Unterstützung in der Kulturellen Bildung. Potenziale von Learning Analytics für Musiklernen am Beispiel automatisierter Auswertungen von Bildschirmaufzeichnungen
- Unter dem Zeichen Künstlicher Intelligenz. Berufe, Kompetenzen und Kompetenzvermittlung der Zukunft
- Umgang mit KI in der Bildung: erklärbar, ethisch orientiert und souverän beherrschbar
- Erklärbare Künstliche Intelligenz im Kontext von Bildung und Lernen
- Eine ethische Perspektive auf KI in der Bildung

Die einzelnen Beiträge haben durchaus einen eigenen Wert, welcher je nach Leser und Interesse unterschiedlich sein dürfte. Allen Beiträgen gemeinsam fehlt aber der rechtliche Bezug gerade auch im Hinblick auf personenbezogene Daten, welche bei KI eben auch verarbeitet werden können – sei dies bei KI-Anwendungen unter Verwendung von personenbezogenen Daten und damit der notwendigen Beachtung der DSGVO oder aber ein Ausblick auf die nun vor der Tür stehende EU-Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz. Sämtliche Beiträge sind leider rein aus der Bildungsperspektive ohne Einbeziehung der Daten der Betroffenen und des anstehenden Rechtsrahmens. Dies ist bei einem Werk dieses Umfangs sehr schade.

Daher kann das Werk im Ergebnis leider nur unter bildungswissenschaftlichen Gesichtspunkten empfohlen werden.

Schnabel, Christoph (Hrsg.)
Hamburgisches Datenschutzgesetz
Handkommentar; 1. Aufl.
Nomos Verlagsgesellschaft, Baden-Baden 2023, 482 S.
ISBN 978-3-8487-7126-4, 119,00 Euro

(hdn) Der Nomos Handkommentar zum Hamburgischen Datenschutzgesetz (HmbDSG) kommt recht genügsam daher. Sieben Autorinnen und Autoren kommentieren die 27 Paragraphen auf gut 480 Seiten. Vier Autoren stammen

aus Aufsichtsbehörden und zwei arbeiten als betriebliche Datenschutzbeauftragte. Die einzige Frau im Team ist Richterin und aktuell im Verbraucherschutz aktiv.

Nach den Kommentierungen der allgemeinen Vorschriften und den Grundsätzen der Verarbeitung personenbezogener Daten in den ersten zwei Abschnitten hebt der Kommentar verschiedene besondere Verarbeitungssituationen hervor: Videoüberwachung, Verarbeitung von Beschäftigtendaten sowie die Verarbeitung zum Zwecke wissenschaftlicher und historischer Forschung und künstlerischer Zwecke.

In einem speziellen Exkurs zu den besonderen Verarbeitungen werden das Hamburgische Pressegesetz und der Staatsvertrag über das Medienrecht in Hamburg und Schleswig-Holstein einbezogen. Hier wird auch auf die §§ 7-12 des Hamburgischen Krankenhausgesetzes eingegangen, die sich mit der Verarbeitung von Patientendaten befassen. Diese Kommentierungen haben die Richterin und der DSB der hiesigen Universitätsklinik übernommen.

Die außerhalb der DSGVO [Verordnung (EU) 2016/679] liegenden Verarbeitungen – das sind die zu Auszeichnungen, Ehrungen und Begnadigungen – werden in einem eigenen Abschnitt behandelt. Der fünfte Abschnitt, der sich mit den Betroffenenrechten befasst, kommentiert die Beschränkungen zur Informationspflicht, zum Auskunftsrecht, zur Löschungspflicht und zur Benachrichtigungspflicht. Es folgen die Abschnitte zum Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) sowie Kommentare zu Strafvorschriften und Ordnungswidrigkeiten.

Einigen Paragraphen, wie zum Beispiel denen zum Krankenhausgesetz oder zum HmbBfDI, sind erläuternde Vorbemerkungen vorgelagert, in denen besondere Gegebenheiten kommentiert werden. Auch auf die strittige Abgrenzung zwischen Verwaltungstätigkeiten und justiziellen Tätigkeiten in der Hansestadt wird sowohl von Seiten der Aufsicht als auch der Justizbehörde eingegangen. Zudem sind Verwaltungstätigkeiten der Bürgerschaft nach dem Hamburgischen Datenschutzrecht zu beurteilen; parlamentarische Tätigkeiten unterliegen der DSGVO und der Datenschutzordnung der Bürgerschaft.

Insgesamt ist der Handkommentar – auch wegen seiner guten Gliederung – ein wichtiges Nachschlagewerk.

Smoltczyk, Maja (Hrsg.)
Berliner Datenschutzgesetz
Handkommentar, 1. Aufl.
Nomos Verlagsgesellschaft, Baden-Baden 2023, 720 S.
ISBN 978-3-8487-8470-7, 119,00 Euro

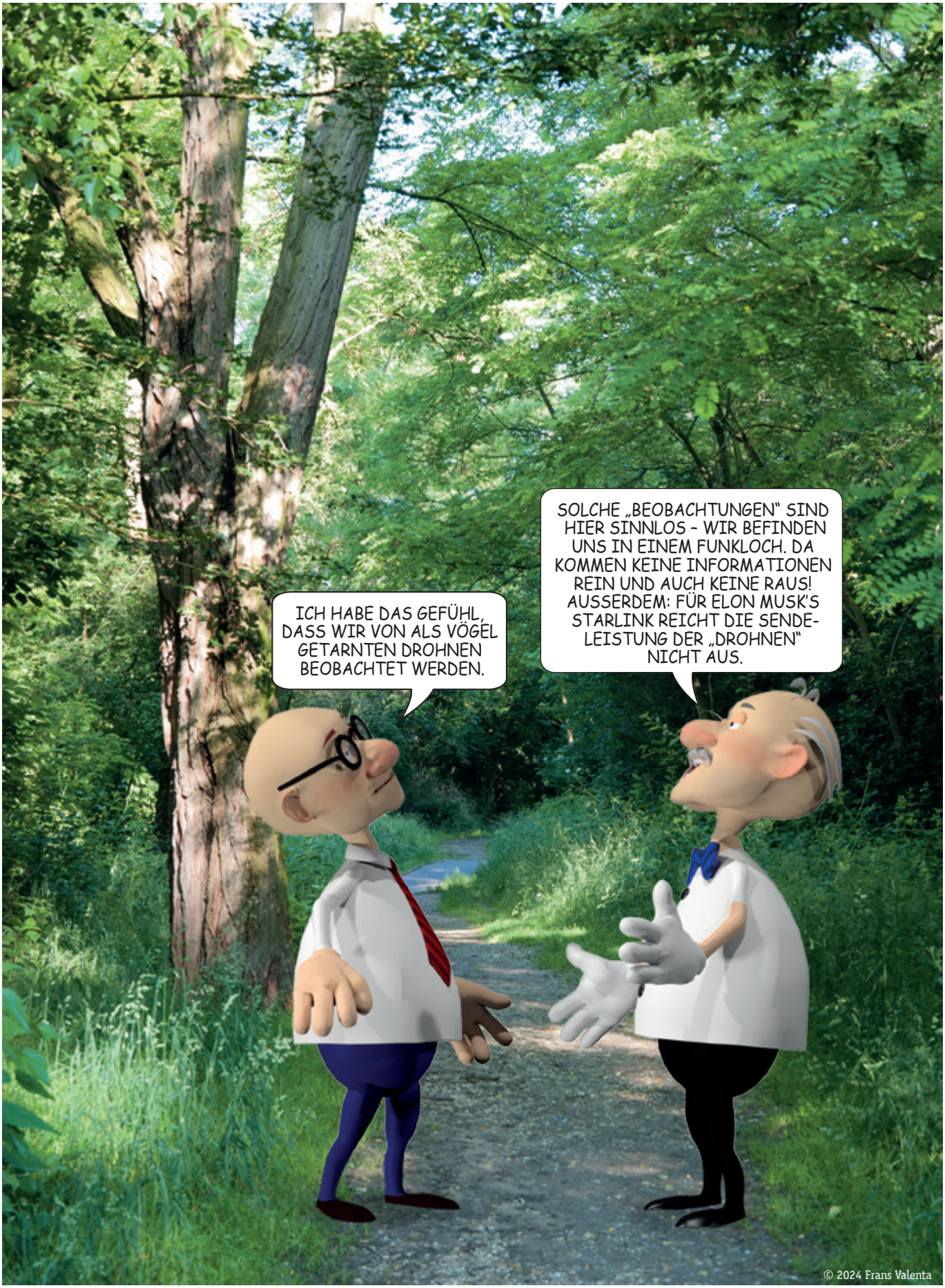
(hdn) Alle Autorinnen und Autoren dieses Handkommentars sind Mitarbeiterinnen und Mitarbeiter der Datenschutzaufsicht Berlin. Der Kommentar gibt also dogmatisch die Prüfersicht wieder.

Zunächst ist festzustellen, dass die 22 Fachleute die 72 Paragraphen in fünf Teile jeweils mit Kapiteln gegliedert haben. Die detaillierte Gliederung macht bereits

deutlich, dass in diesem Handbuch vertieft auf Verarbeitungstätigkeiten und deren juristische Einordnung eingegangen wird. So umfasst schon der Teil zu den Durchführungsbestimmungen für die EU-DSGVO 2016/679 über 200 Seiten zu den Themen Grundsätze, besondere Verarbeitungssituationen, Rechte der Betroffenen, Pflichten der Verantwortliche und Auftragsverarbeiter. Es wird ein umfassender Pflichtenkatalog aufgelistet, der technische und organisatorische Maßnahmen darstellt, ergänzt durch die Empfehlung der Datenschutzkonferenz (DSK) das Standard-Datenschutzmodell heranzuziehen.

Teil drei mit den Bestimmungen zur Verarbeitung personenbezogener Daten nach der EU-DSGVO 2016/680 umfasst im Kommentar 250 Seiten. Dabei werden die Rechtsgrundlagen ebenso gründlich wie die Betroffenenrechte und die Pflichten der Verantwortlichen und der Auftragsverarbeiter behandelt.

Die Autorinnen und Autoren heben in vielen Kapiteln hervor, welche Maßnahmen ergriffen werden müssen, um datenschutzkonform verarbeiten zu können. Daher ist dieser aus Prüfersicht verfasste Kommentar sehr hilfreich bei der Bewältigung datenschutzrechtlicher Problemstellungen.


ICH HABE DAS GEFÜHL, DASS WIR VON ALS VÖGEL GETARNTEN DROHNEN BEOBACHTET WERDEN.
SOLCHE „BEOBACHTUNGEN" SIND HIER SINNLOS - WIR BEFINDEN UNS IN EINEM FUNKLOCH. DA KOMMEN KEINE INFORMATIONEN REIN UND AUCH KEINE RAUS! AUSSERDEM: FÜR ELON MUSK'S STARLINK REICHT DIE SENDE-LEISTUNG DER „DROHNEN" NICHT AUS.
© 2024 Frans Valenta