3/2021

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

44. Jahrgang
ISSN 0137-7767
14,00 Euro

E-Government

■ Identitätsmanagement im E-Government ■ Online-Petitionen und der Datenschutz ■ Neuerungen beim Datenschutz in der Telekommunikation und bei den Telemedien ■ Unabhängige Datenschutzbeauftragte und deren Wirkmacht ■ E-Government – Daten und Studien ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

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

Inhalt

Termine

Foto: Pixabay.com

Mittwoch und Donnerstag, 27.10./28.10.2021 & Behördentag am Freitag, 29.10.2021
BvD-Herbstkonferenz
München (Hybrid-Veranstaltung)

Samstag, 01.11.2021
Redaktionsschluss DANA 4/2021
Schwerpunkt: ePrivacy-Verordnung, Veränderung des Datenschutzrechts

Donnerstag und Freitag, 18./19.11.2021
Forum Privatheit 2021: Auswirkungen der Künstlichen Intelligenz auf Demokratie & Privatheit
Landtag Wiesbaden (Hybrid-Veranstaltung)

Freitag, 28.01.2022
Europäischer Datenschutztag

Dienstag, 01.02.2022
Redaktionsschluss DANA 1/2022

DANA
Datenschutz Nachrichten
ISSN 0137-7767
44. Jahrgang, Heft 3

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)
Heinz Alenfelder, Dr. Susanne Holzgraefe
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 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen 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
Frans Jozef Valenta, Pixabay, shutterstock, iStock

Editorial

Bild: iStock.com/Bet_Noire

Auch die langfristige Planung von DANA-Themen ist in Zeiten der Pandemie nicht immer einfach. So hat diese Ausgabe gleich zwei wichtige Schwerpunkt-Beiträge: Einerseits haben wir mit dem Beitrag von Thomas Warnecke zu den Herausforderungen an das Identitätsmanagement auf kommunaler Ebene den geplanten Schwerpunkt „E-Government" beibehalten. Das Thema wird ergänzt durch eine Übersicht über die E-Petitionsportale in Bund und Ländern samt einer Betrachtung der privaten Plattform openPetition.

Andererseits stellt Werner Hülsmann ganz aktuell die „Neuerungen beim Datenschutz in den Telemedien und der Telekommunikation" vor. Für diesen Bereich treten am 1. Dezember dieses Jahres zwei im Juni veröffentlichte Gesetze in Kraft: das neue Telekommunikations-Gesetz und das Telekommunikation-Telemedien-Datenschutzgesetz.

Darüber hinaus betrachtet Thilo Weichert die Wirkmacht unabhängiger Datenschutzbeauftragter. Schließlich finden Sie wie gewohnt auch in diesem Heft eine umfassende Sammlung aktueller Datenschutz- und Technik-Nachrichten, Berichte über Urteile deutscher und internationaler Gerichte sowie einige Buchbesprechungen.

Wir wünschen Ihnen eine gute Lektüre!

Ihre DANA-Redaktion

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder, Vorstandsmitglied der DVD, alenfelder@datenschutzverein.de

Werner Hülsmann, Vorstandsmitglied der DVD, huelsmann@datenschutzverein.de

Dr. Thomas Warnecke, Stellvertretender behördlicher Datenschutzbeauftragter bei der Region Hannover

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

Dr. Thomas Warnecke[1]

Identitätsmanagement im E-Government – Aktuelle Herausforderungen bei der Umsetzung auf kommunaler Ebene

I. Einleitung

Mit dem Fortschreiten transaktionsbezogener E-Government-Angebote steigt auch die Notwendigkeit die Transaktionen rechtssicher zu gestalten und die Zurechnung zu beiden Kommunikationspartnern sicherzustellen. An die Transaktionen sind Rechtsfolgen für beide Seiten geknüpft. Bei Fehladressierungen greifen mittlerweile mit den Regelungen der DSGVO harte Meldepflichten für eine verantwortliche Stelle, so dass auch hieraus die grundsätzliche Verpflichtung erwächst elektronische Transaktionen rechtssicher zu gestalten. Für den Nutzer bedeutet dies, dass er die angebotenen Identitätsmanagement-Infrastrukturen mit unterschiedlichen nutzergesteuerten Gestaltungsmöglichkeiten nutzen kann und dabei aber auch entsprechende Sorgfaltsanforderungen erfüllen muss. Dieser Beitrag beleuchtet im Folgenden die aktuellen Entwicklungen im Bereich des Identitätsmanagements, um E-Government in Deutschland an der Schnittstelle zum Bürger weiter zu fördern und auch Abrufe von Behördenmitarbeitern in Registern im Verwaltungsalltag rechtssicher zu gestalten.

II. Identitätsmanagement für Transaktionsprozesse

Die Nutzung von E-Government-Angeboten erfordert vielfach vom Nutzer, dass er seine Identität offenlegt, ein Handeln unter Pseudonym ist nicht möglich[2]. Häufig findet der Begriff „digitale Identität" Verwendung[3]. Mit Blick auf die Verwendung als Tatbestandsmerkmal führt der Begriff aber nicht weiter. Im Rechtsverkehr kommt es auf die Zurechnung von Handlungen zu natürlichen Personen an. Zentral und damit wesentlich ist daher der Begriff der numerischen Identität natürlicher Personen, deren Merkmal es ist, dass bestimmte Daten eine Übereinstimmung mit einer einzigen Person haben[4]. So steht der Begriff im Zusammenhang mit Identifizierung und Identifizierbarkeit, was auch in der Definition für personenbezogene Daten in Art. 4 Nr. 1 DSGVO deutlich wird. Das ist auch wesentlicher Teil des Begriffs Identitätsmanagement[5]. Somit müssen Identitätsmanagement-Konzepte die Merkmale einer Person in den Blick nehmen, die sie einzigartig machen. Dies sind natürlich die Personalien, die in Transaktionsprozessen im Rahmen der Identifizierung abgeglichen werden müssen[6]. Die Personalien haben in Deutschland den Vorteil einer melderechtlichen Fundierung und Überprüfbarkeit, was bei Zweifelsfällen in der Verwaltungspraxis eine wichtige Rolle spielt.

III. Vermeidung von Datenschutzverletzungen im Sinne von Art. 33, 34 DSGVO bei Transaktionen im E-Government durch Identitätsmanagement

Seit Einführung der DSGVO sind die Vorgaben für Pannen bei elektronischer Kommunikation, die im Alltag der Verwaltungspraxis durchaus regelmäßig vorkommen, schärfer geworden. Die Pannen können durchaus in unterschiedlicher Art und Weise auftreten. Wird eine E-Government-Transaktion durch einen Dritten mittels Identitätsmissbrauch kompromittiert oder wird unwissentlich von der jeweiligen verantwortlichen Stelle aufgrund von Namensidentitäten über nicht gesicherte Infrastrukturen kommuniziert, dürfte in aller Regel ein meldepflichtiger Datenschutzverstoß i. S. d. Art. 33, 34 DSGVO zu prüfen und zu bejahen sein. Die Vertraulichkeit der Transaktion bzw. Kommunikation ist in diesem Fall mindestens verletzt, da eine andere Person mit einer anderen numerischen Identität im Rahmen der elektronischen Kommunikation adressiert wird. Je nach Kommunikationsinhalt und entsprechender Risikobewertung dürfte auch eine Meldepflicht an die eigentlich gemeinte natürliche betroffene Person gemäß Art. 34 Abs. 1 DSGVO bestehen. Fehladressierungen elektronischer Kommunikation finden sich somit regelmäßig als eine nach Art. 33 Abs. 1 DSGVO meldepflichtige Datenschutzverletzung in den Tätigkeitsberichten von Datenschutzaufsichtsbehörden wieder[7]. Diese Datenschutzverletzungen können insbesondere bei Kommunikation per einfacher E-Mail und ggf. bestehender Namensgleichheit oder einer Ähnlichkeit von Personen passieren. Trotz der im Folgenden darzustellenden jüngsten gesetzlichen Impulse für Identitätsmanagement passieren derartige Datenschutzverletzungen nach wie vor, da insbesondere nicht formgebundene Kommunikationsanlässe der Verwaltung nach wie vor massenhaft existieren. Die Verbreitung von identitätsgeschützten Kommunikationsmitteln wie De-Mail[8] ist in der Bevölkerung noch nicht so fortgeschritten, dass hierauf gesetzt werden kann. Insgesamt dient gesetzlich flankiertes Identitätsmanagement daher neben der Adressierung an die richtige natürliche Person im Rechtsverkehr gerade auch der Vermeidung meldepflichtiger Datenschutzverletzungen nach Art. 33, 34 DSGVO als einer Kernverpflichtung verantwortlicher Stellen nach der Datenschutzreform.

IV. Gesetzliche Vorgaben zur Förderung des E-Governments in Deutschland

Um die Entwicklung des E-Governments in Deutschland gezielt voranzutreiben hat zum einen der Bundesge-

setzgeber in jüngster Vergangenheit mit gesetzlichen Regelungen nachgesteuert, die auch gezielt Identitätsmanagement für den Bürger verbessern und rechtssichere Transaktionen ermöglichen sollen. Darüber hinaus gibt es deutschlandweit landesrechtliche Vorgaben im Bereich E-Government. Hier sollen im Folgenden gezielt einige der jüngsten Regelungen mit Relevanz bei der Umsetzung in der kommunalen Praxis beleuchtet werden.

1. Das Online-Zugangsgesetz (OZG)

Zur Förderung des bisher schleppenden E-Governments in Deutschland hat der Bundesgesetzgeber einen Impuls gesetzt und durch die Einführung des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) eine Zeitschiene zur verbindlichen Umsetzung der Digitalisierung von Verwaltungsleistungen bis Ende 2022 gesetzt[9]. Wesentlich ist der sog. Portalverbund[10] nach § 1 OZG, wonach – in Abgrenzung zum Begriff Verbundportal – bereits bestehende Verwaltungsportale lediglich zu einem gemeinsamen Verbund zusammengefasst werden sollen[11]. Aus Art. 91 c Abs. 5 GG ergibt sich eine Annexkompetenz für den Bund zur Regelung von Belangen der IT-Sicherheit und des Datenschutzes im Hinblick auf die Portalarchitektur, was eine fundamentale Bedeutung für die Funktionsfähigkeit des Portalverbundes hat[12] und auch für ein einheitlich funktionierendes Identitätsmanagement[13] wichtig ist.

a) Nutzerkonten nach § 3 Abs. 2 OZG

In § 3 Abs. 2 OZG sind daher Nutzerkonten vorgesehen, mit denen sich der Nutzer für die Verwaltungsleistungen von Bund und Ländern im Portalverbund einheitlich identifizieren und authentifizieren kann. Während es in E-Commerce-Anwendungen üblicherweise seit langem Nutzerkonten gibt, bestehen für E-Government-Anwendungen bisher nur Teillösungen ohne weitreichende Interoperabilität[14]. Teilweise sind die Identitätsmanagement-Infrastrukturen akzessorisch und flankierend zu stufenweisen Einführungsprojekten bereitgestellt worden[15]. Die Nutzerkonten des OZG eröffnen nun dem Nutzer die Möglichkeit die Nutzerkonten multifunktional einsetzen zu können. Die Leistungen, die für den Bürger erreichbar sein sollen, sollen aus Nutzerperspektive orientiert an Lebenslagen kategorisiert werden[16].

b) Once Only Prinzip

Die Identitätsdaten spielen bei der gesetzgeberischen Intention, das E-Government zu fördern und es dabei rechtssicher und gleichzeitig niedrigschwellig zu machen, eine große Rolle. Deutlich wird das an der Implementierung des sog. „Once only"-Prinzips. Hiernach soll es einmalig genügen die Identitätsdaten einzugeben und diese dann anlassbezogen der jeweiligen Behörde freizugeben anstatt sie neu hinterlegen zu müssen[17]. Hierfür sieht § 8 Abs. 5 S. 2 OZG eine ausdrückliche Einwilligung des Nutzers vor. Der Once only Grundsatz wird also unter dem Vorbehalt der Einwilligung des Nutzers implementiert[18]. Da es sich um hinterlegte personenbezogene Daten handelt, die nur zu bestimmten Anlässen benötigt werden, ist eine ausdrückliche Einwilligung des Nutzers folgerichtig, da die Kommunikationsanlässe gewissermaßen auch nutzergesteuert sind. Nach § 8 Abs. 5 S. 3 OZG ist eine selbstständige Löschungsmöglichkeit für den Nutzer zu gewährleisten, was im Sinne eines nutzergesteuerten Identitätsmanagements zu begrüßen ist.

c) Ermöglichung verschiedener Vertrauensniveaus

Die besonderen Anforderungen einzelner Verwaltungsleistungen an die Identifizierung und Authentifizierung ihrer Nutzer sind nach § 3 Abs. 2 S. 5 OZG zu berücksichtigen. Es gibt Verwaltungsdienstleistungen, die ein besonders hohes Vertrauensniveau erfordern und in gestufter Form müssen die Nutzerkonten des OZG neben dem niedrigschwelligen Zugang von Benutzername und Passwort auch die Verwendung der eID des Personalausweises, Softwarezertifikate wie das ELSTER-Zertifikat oder PIN/TAN-Verfahren ermöglichen können[19]. Insbesondere spezielle Anforderungen aus Fachverfahren können nach Einschätzung des Gesetzgebers gesteigerte Anforderungen an die Identifizierung stellen[20]. Der Gesetzgeber selbst nennt aber keine Identifizierungsverfahren oder klassifiziert diese in irgendeiner Form, sondern verweist lediglich auf die eIDAS-Verordnung (VO EU Nr. 919/2014, ABl EU L 257/73)[21]. Es liegt also an jedem Erbringer einer Verwaltungsleistung selbst, das Vertrauensniveau jeweils im konkreten Fachverfahren individuell selbst festzulegen[22]. Für die umsetzende kommunale Praxis bedeutet dies, dass sie im Rahmen der seitens der Länder zur Verfügung gestellten Komponenten schauen muss, welche Vertrauensniveaus hierbei unterstützt und dann von den kommunalen Behörden voreingestellt werden können[23].

d) Vorgaben aus § 8 OZG als gesetzlicher Tatbestand der Datenverarbeitung

In § 8 OZG ist der Annexkompetenz aus Art. 91 c Abs. 5 GG folgend eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten bei Identifizierungsprozessen geschaffen worden. Da es auf die numerische Identität im Rechtsverkehr ankommt, bezieht sich der gesetzliche Tatbestand auf die üblichen Stammdaten zu einer Person. Der Identifizierungsprozess mittels dieser Stammdaten ist neben der eigentlichen Verarbeitungstätigkeit in der Sache zur Erfüllung der Verwaltungsleistung eine weitere Verarbeitungstätigkeit im datenschutzrechtlichen Sinne, die zusätzlich in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO der jeweiligen verantwortlichen Stelle einzutragen wäre. Darüber hinaus kann der Nutzer gegen beide Verarbeitungstätigkeiten seine Betroffenenrechte aus Art. 12-22 DSGVO geltend machen.

e) Zwischenfazit

Insgesamt ist mit den skizzierten Regelungen des OZG zum Identitätsmanagement eine ganzheitliche Lösung gelungen, die es der Verwaltung insbesondere auch auf der kommunalen Ebene und dem Nutzer bei den OZG-Leistungen ermöglicht rechtssicher zu kommunizieren. Grundsätzlich bestehen auch

noch funktionale Ausbaumöglichkeiten der Servicekonten[24].

2. Das Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät

Der Bundesgesetzgeber hat sich ebenfalls auf die Fahnen geschrieben die eID-Funktion des Personalausweises nutzerfreundlicher zu machen und um die Nutzung auf mobilen Endgeräten zu erweitern. Das sog. Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät vom 5. Juli 2021 sieht Änderungen im Personalausweisgesetz (PAuswG) und dem eID-Karte-Gesetz vor[25]. Diese Nutzungsoption für den elektronischen Identitätsnachweis tritt neben die klassische Variante der eID-Nutzung mit Ausweiskarte und dem klassischen Lesegerät am heimischen PC[26]. Bisher war das Szenario durch Besitz der Ausweiskarte und Wissen der sechsstelligen Geheimnummer geprägt. Ab sofort soll es möglich sein, das Besitzelement mittels der AusweisApp2 und dem Smartphone zu erfüllen.

Nach dem neuen § 10 a PAuswG kann der Ausweisinhaber dann veranlassen, dass der Ausweishersteller die im Personalausweis hinterlegten Identitätsdaten über einen sicheren Übermittlungsweg an ein elektronisches Speicher- und Verarbeitungsmedium eines mobilen Endgerätes des Ausweisinhabers übermittelt. Der Ausweisinhaber ist dann auf seine besonderen Sorgfaltspflichten nach § 27 Abs. 2 PAuswG hinzuweisen, die auch bei der bisherigen Verfahrensweise bestehen. Der Nutzer muss ein kompatibles Smartphone mit eingebetteter Sicherheitsarchitektur auf hohem Niveau zur Verfügung haben[27]. Der Nutzer muss daher seine infrastrukturellen Voraussetzungen genau prüfen und sich im Klaren sein, dass sich mit der mobilen Nutzung der eID-Funktion seine Sorgfaltsanforderungen erweitern. Es bleibt abzuwarten, welche Nutzungsszenarien sich im E-Government für die mobile Variante entwickeln werden[28]. Aus kommunaler Umsetzungsperspektive ist interessant, in welchen Anwendungsfällen des E-Governments die mobile Variante der eID zum Einsatz kommen kann.

V. Identitätsmanagement bei Eingaben im Bereich der Betroffenenrechte der DSGVO

Neben den durch die E-Government-Gesetzgebung in jüngster Zeit fokussierten Verwaltungsleistungen ist ein weiterer Bereich in der kommunalen Praxis das Identitätsmanagement bei Eingaben im Bereich der Betroffenenrechte der DSGVO. Die Vorgaben in Art. 12 Abs. 1 DSGVO gehen davon aus, dass die verantwortliche Stelle dem Betroffenen alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache übermittelt. Die Übermittlung soll nach Art. 12 Abs. 1 S. 2 DSGVO schriftlich oder in anderer Form, ggf. auch elektronisch erfolgen. In der Konsequenz bedeutet dies in der kommunalen Praxis, dass die verantwortliche Stelle im Zuge der Informationspflichten nach Art. 13, 14 DSGVO eine einfache Funktionsmailadresse des behördlichen Datenschutzbeauftragten bereitstellt und benennt, an die Eingaben von Betroffenen gerichtet werden können. Hier tut sich dann das Spannungsfeld zwischen einer niedrigschwelligen Erreichbarkeit der Funktion des behördlichen Datenschutzbeauftragten und einem tragfähigen Identitätsmanagement auf. Bei Identitätszweifeln bezüglich des Betroffenen regelt die DSGVO in Art. 12 Abs. 6 DSGVO Mitwirkungspflichten der betroffenen Person. Diese bestehen in der Regel aus der Bereitstellung weiterer Identitätsdaten durch den Betroffenen[29]. Die Identifizierung des Betroffenen wird insoweit auch als arbeitsteiliges Pflichten- und Obliegenheitsprogramm bezeichnet[30]. Um die Intention der Betroffenenrechte nicht zu konterkarieren, dürfen Identitätsprüfungen nicht so aufwändig gestaltet sein, dass der Betroffene von der Geltendmachung seiner Betroffenenrechte absieht[31]. In der kommunalen Praxis empfiehlt es sich bei einer Kontaktaufnahme per einfacher E-Mail, in einer Eingangsbestätigung den Betroffenen auf die nicht identitätsgesicherte Kommunikation hinzuweisen und zunächst bei der verantwortlichen Organisationseinheit einen etwaigen Stammdatensatz zu dieser Person abzufragen und dann auf eine postalische Kommunikation an eine Meldeadresse umzuschwenken[32]. Sofern vorhanden können auch die gesetzlich flankierten Identitätsmanagement-Infrastrukturen wie De-Mail, die eID-Funktion des Personalausweises in allen Varianten und die qualifizierte elektronische Signatur für Eingaben von Betroffenen genutzt werden[33]. Das setzt selbstverständlich voraus, dass auf beiden Seiten diese infrastrukturellen Voraussetzungen vorhanden sind und eine Implementierung in vorhandene Arbeitsprozesse stattgefunden hat. Speziell bei der Kommunikation im Bereich der Betroffenenrechte liegt es an der verantwortlichen Stelle diese infrastrukturellen Voraussetzungen zu schaffen.

VI. Behördenübergreifende Abrufverfahren am Beispiel des Wettbewerbsregisters

Neben der Kommunikation der Verwaltung mit dem Bürger gewinnen auch Abrufverfahren von Behörde zu Behörde eine zunehmende Bedeutung. Auch hier ergibt sich die Notwendigkeit, die numerische Identität von Behördenmitarbeitern eindeutig festzustellen. Insoweit müssen diese Abrufverfahren auch ein tragfähiges Identitätsmanagement enthalten. Das Bundeskartellamt hat nun mit dem Wettbewerbsregister eine Anwendung bereitgestellt, bei der sich öffentliche Auftraggeber registrieren können. Dieses Register stellt öffentlichen Auftraggebern, Sektorenauftraggebern und Konzessionsgebern für Vergabeverfahren Informationen zur Verfügung, ob Unternehmen wegen begangener Wirtschaftsdelikte von Vergabeverfahren auszuschließen sind[34]. Für die Nutzung des Wettbewerbsregisters ist die Webanwendung SAFE Identitätsadministration vorgesehen, wonach es einen Zugangsadministrator, Identitätsadministratoren in den Behörden und dann registrierte abrufberechtigte Nutzer gibt[35]. Vorgesehen ist, dass die Identitätsadministratoren in den jeweiligen Behörden den Kreis der abrufberechtigten Behördenmitarbeiter administrieren. In der behördeninternen Sicht bedeutet dies, dass Beschäftigtendaten an eine externe Stelle übermittelt werden und dies innerhalb der jeweiligen Behörde mit internen Rechtsvorschriften geregelt werden muss[36].

VII. Fazit

Identitätsmanagement im E-Government hat aktuell in der kommunalen Praxis eine große Bedeutung bei den Verwaltungsleistungen an der Schnittstelle zum Bürger und ist maßgeblich beeinflusst durch die Umsetzungszeiträume im OZG. Daneben stellen aber auch weitere Kommunikationsanlässe der kommunalen Praxis wie der Bereich der Eingaben zu den Betroffenenrechten der DSGVO sowie auch fachspezifische Abrufverfahren wie das Wettbewerbsregister gewisse Anforderungen an ein tragfähiges und rechtssicheres Identitätsmanagement bei der Umsetzung.

1 Stellvertretender behördlicher Datenschutzbeauftragter bei der Region Hannover; der Beitrag gibt die persönliche Auffassung des Verfassers wieder.

2 Hansen/Meissner (Hrsg.), Verkettung digitaler Identitäten, 2007, S. 90; Roßnagel DuD 2002, 281 (282).

3 Vgl. hierzu Schulz G., DuD 2015, 466 (466); Müller/Redlich/Jeschke, DuD 2011, 465 (465); Brunst, DuD 2011, 618 (618).

4 Vgl. J. Meyer, Identität und virtuelle Identität natürlicher Personen im Internet, S. 25

5 Eine tragfähige Definition des Begriffs Identitätsmanagement bei Schulz S. E., in: Schliesky (Hrsg.) Technikgestütztes Identitätsmanagement, 51 (52 f.).

6 Federrath/Berthold, in: Bäumler (Hrsg.), E-Privacy, 189 (189).

7 Vgl. etwa 36. TB des ULD SH (2017), S. 41; abrufbar unter: https://www.datenschutzzentrum.de/tb/tb36/uld-36-taetigkeitsbericht-2017.pdf (letzter Abruf: 11.07.2021).

8 Vgl. zu De-Mail: Warnecke, Identitätsmanagement und Datenschutz, S. 80 ff.

9 Barthel/Schüler, DVP 2021, 85 (85).

10 Nach der Definition in § 2 Abs. 1 OZG ist der Portalverbund: …eine technische Verknüpfung der Verwaltungsportale von Bund und Ländern, über den der Zugang zu Verwaltungsleistungen auf unterschiedlichen Portalen angeboten wird.

11 Siegel, DÖV 2018, 185 (186).

12 Schliesky/Hoffmann, DÖV 2018, 193 (195).

13 Vgl. auch den Hinweis bei Rüdebusch, KommJur 2020, 41 (44).

14 Herrmann/Stöber, NVwZ 2017, 1401 (1405).

15 Zum Projekt iKfz vgl.: https://www.bmvi.de/SharedDocs/DE/Artikel/StV/Strassenverkehr/internetbasierte-fahrzeugzulassung.html (letzter Abruf: 17.07.2021).

16 Guckelberger, GewA 2019, 457 (458).

17 Schliesky/Hoffmann, DÖV 2018, 193 (196); das Spannungsfeld zwischen dem datenschutzrechtlichen Zweckbindungsgrundsatz und der Bürgerfreundlichkeit thematisieren Martini/Wenzel, DVBl. 2017, 749 ff.

18 Berger, KommJur 2018, 441 (443).

19 Herrmann/Stöber, NVwZ 2017, 1401 (1405).

20 BT-Drs. 18/11135 v. 13.2.2017, S. 92.

21 Denkhaus/Richter/Bostelmann, § 3 OZG, Rn. 10.

22 Herrmann/Stöber, NVwZ 2017, 1401 (1405).

23 Vgl. hierzu das NAVO-Portal in Niedersachsen unter: https://www.navo.niedersachsen.de/navo/portal?a=user&f=login (letzter Abruf: 17.07.2021).

24 Zu den Konfliktfeldern in diesem Kontext: Berger, KommJur 2018, 441 (443).

25 BGBl. I S. 2281.

26 Vgl. hierzu: Polenz, MMR 2010, 671 (673 ff.); Bender u. a., DuD 2010, 761 (761); Reisen, DuD 2008, 164 (164).

27 Derzeit gewährleisten das wohl nur bestimmte Smartphones: https://www.heise.de/news/Bundestag-bringt-Online-Ausweis-aufs-Handy-und-Passbilder-in-Zentralregister-6051520.html (letzter Abruf: 17.07.2021).

28 Zur Wirkung der verfügbaren relevanten Anwendungsfälle vgl. die Stellungnahme von VITAKO, S. 1.: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/entwurf-eines-gesetzes-zur-einfuehrung-eines-elektr-identitaetsnachweises-mit-mobilem-endgeraet/vitako.pdf?__blob=publicationFile&v=1 (letzter Abruf: 17.07.2021)

29 Müller/Sandvoß/Warnecke, DVP 2020, 351 (353).

30 Raji, ZD 2020, 279 (281).

31 Vgl. den Hinweis zu Vorgehensweisen bei Unternehmen: Buchmann/Eichhorn, DuD 2019, 65 (65).

32 Müller/Sandvoß/Warnecke, DVP 2020, 351 (354).

33 Petrlic, DuD 2019, 71 (73).

34 Vgl. hierzu: https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2021/25_03_2021_Betrieb_Wettbewerbsregister.html (letzter Abruf: 17.07.2021).

35 Vgl. Leitfaden SAFE Identitätsadministration, S. 3, abrufbar unter: https://www.justiz.bayern.de/media/images/behoerden-und-gerichte/ho-zenvg/leitfaden_identit_tsaministratoren.pdf (letzter Abruf: 17.07.2021).

36 Dienstanweisungen und ggf. Dienstvereinbarungen.

Bild: iStock.com/Andrey Suslov

Heinz Alenfelder

Online-Petitionen und der Datenschutz

Gerade in der Zeit der Pandemie-Lockdowns erhielt das Thema Petition großen Aufschwung. So erklärt beispielsweise der Landtag NRW auf seiner Webseite, dass im ersten Halbjahr 2020 3.300 Petitionen eingingen. Demgegenüber waren es im gesamten Vorjahr 5.300[1]. Im Internet gibt es zudem eine Reihe von Plattformen, auf denen „Petitionen" zu unterschiedlichsten Anliegen gestartet und elektronisch unterzeichnet werden können. Hier hängen die Regelungen stark vom Betreiber der Plattform ab und bereits 2015 kam es zu einem Skandal um die Praxis der Plattform change.org, der daraufhin in 2016 der Big Brother Award verliehen wurde.

Insgesamt scheint es also sinnvoll die Portale für Online-Petitionen unter Datenschutz-Aspekten genauer unter die Lupe zu nehmen. Dabei sollen zunächst die Möglichkeiten auf Europa-, Bundes- und Länderebene betrachtet werden und dann openPetition stellvertretend für die privaten „Petitions"-Plattformen. Abschließend wird in aller Kürze die Sicht der Wissenschaft einbezogen.

Grundlage des Petitionswesens

Petitionen sind Bitten oder Beschwerden, die an ein Parlament gerichtet werden. Der Weg dafür steht jeder und jedem offen und die schriftliche Eingabe kann formlos erfolgen. In Deutschland sind Petitionen im Grundgesetz (Art. 17), den Landesverfassungen (z. B. Art. 115 der Bayerischen Verfassung) und durch die Petitionsgesetze der Länder (z. B. Bayerisches Petitionsgesetz) geregelt. Dem Bund übergeordnet regelt der Vertrag über die Arbeitsweise der Europäischen Union (AEUV Art. 227) den Umgang mit Petitionen. Auf den Webseiten all dieser Ebenen gibt es mittlerweile Angebote, die die Eingabe von Petitionen online ohne Unterschrift ermöglichen. Die Institutionen kommen damit Forderungen nach, wie sie beispielsweise Rita Schuhmacher, Pressesprecherin von openPetition, 2018 in einer Analyse[2] für das Netzwerk Bürgerbeteiligung aufstellte: „Zukünftige Beteiligungswerkzeuge sollten […] internetgestützt agieren".

Im Folgenden werden Einzelheiten zum Datenschutz herausgearbeitet, die beim Besuch der Webseite der jeweiligen legislativen Ebene besonders auffallen.

Europaparlament

Das Europaparlament stellt in einer FAQ[3] klar, dass Petenten, die eine Petition eingereicht haben, lediglich erfahren, wieviele Personen ihre Petition unterstützen, nicht aber die Daten der Unterstützenden erhalten. Wenn Petitionen „sensible personenbezogene Daten" enthalten, kann beim Einreichen auch beantragt werden, dass die Identität der Petentin oder des Petenten nicht offengelegt wird. Außerdem behält sich der Petitionsausschuss selbst das Recht der Anonymisierung vor. Weitere detaillierte Regelungen enthält die Datenschutzerklärung[4]. Danach muss der Petent oder die Petentin auch bestätigen, dass übermittelte personenbezogene Daten Dritter „nach Maßgabe der geltenden innerstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten rechtmäßig erworben wurden." Im Bezug auf die Anonymisierung wird in der Datenschutzerklärung deutlich warnend darauf hingewiesen, „dass gemäß der Verordnung (EG) Nr.1049/2001 jeder Unionsbürger das Recht hat, die Offenlegung der einschlägigen personenbezogenen Daten zu beantragen" und das Europaparlament in diesem Fall gezwungen wäre, die personenbezogenen Daten mitzuteilen.

Deutscher Bundestag

Der Petitionsausschuss des Deutschen Bundestags hat schon 2005 ein eigenes Petitionsportal eingerichtet, das „System E-Petitionen"[5]. Dort wird explizit zum Einreichen von Petitionen jeder Art ermuntert, von persönlichen Bitten bis zu allgemein interessanten Anliegen. Ein Blick in die Datenschutzhinweise[6] zeigt auf, welche Daten verarbeitet werden und dass die Nutzung des „Systems E-Petitionen" für Mitunterzeichnung und Diskussion nach Registrierung auch mit einem Pseudonym möglich ist. Wenn kein Pseudonym gewählt wurde, erfolgt die Veröffentlichung der Beiträge mit einer „anonymen Nutzerkennung". Die E-Mail-Adresse wird nur sichtbar bei aktiv vorgenommener entsprechender Einstellung.

Generell heißt es für die Petitionen: „keine Veröffentlichung im Internet", es sei denn, beim Einreichen auf elektronischem Weg wird speziell „um Veröffentlichung" gebeten. In der „Richtlinie öffentliche Petitionen"[7] wird klargestellt, dass diese Petitionen über das allgemeine Petitionsrecht hinausgehen, um ein Forum „zu einer sachlichen Diskussion wichtiger allgemeiner Anliegen" zu schaffen. Es besteht allerdings kein Rechtsanspruch auf Annahme einer Petition als öffentliche Petition. Wer sich an einer öffentlichen Petition beteiligen möchte, muss über eine gültige E-Mail-Adresse verfügen. Analog zur Regelung des Europaparlaments wird auch hier geregelt: „Anliegen oder Teile eines Anliegens dürfen sich nicht erkennbar auf Personen beziehen." Petitionen, in denen beispielsweise eine Namensnennung erfolgt, werden nicht als öffentliche Petition genehmigt. In einer Gegenposition dazu fordert die Grünen-Bundestagsfraktion auf ihrer Webseite[8] die Abschaffung der Sonderkategorie öffentliche Petitionen: „alle Petitionen sind öffentlich, wenn der Petent dies will."

Länderregelungen – Vergleichende Betrachtung

Da mittlerweile alle Bundesländer Möglichkeiten zum Einreichen von Petitionen auf elektronischem Weg anbieten, lohnt sich ein Blick auf die

jeweiligen Webseiten. Dabei wird für jedes der 16 Petitionsportale geprüft, ob die dortigen Angebote aus Sicht des Datenschutzes geeignet sind Vertrauen zu schaffen. Vor allem die Erklärungen zum Verfahren der Behandlung von Petitionen durch den Petitionsausschuss und zum Umgang mit den Petitionsdaten sollen hier von Interesse sein. Immerhin musste im vergangenen Jahr der Europäische Gerichtshof (EuGH) erst feststellen, dass auch die Petitionsausschüsse der Länder der Datenschutz-Grundverordnung (DSGVO) unterliegen[9].

Außer in Thüringen, wo eine Registrierung für die Online-Petition erforderlich ist, erfolgt die Eingabe der Petitions-Daten per Formular. Als Protokoll wird HTTPS eingesetzt, da bei normaler E-Mail-Übertragung die Daten nicht verschlüsselt übertragen werden. Folgende Fragen stehen bei der Betrachtung der Webseiten der Länder (in alphabetischer Reihenfolge) im Vordergrund:

- Wird die erforderliche Unterschrift unter die Petition durch eine Bestätigung eines per E-Mail zugesendeten Links ersetzt oder erfolgt lediglich eine Empfangsbestätigung?
- Gibt es angepasste Datenschutzhinweise (bzw. einen Abschnitt über Online-Petitionen in den allgemeinen Datenschutzhinweisen des Landtags)?
- Gibt es genauere Hinweise zur Übermittlung der Daten an Behörden und die eventuelle Weiterleitung an andere Petitionsausschüsse?
- Gibt es eine Aussage, wann die im Zusammenhang mit der Petition verarbeiteten Daten gelöscht werden?

Baden-Württemberg: Zwar fehlt bei der Formulareingabe-Seite des Landtags[10] die spezielle Datenschutzerklärung, doch ist in den Erläuterungen hervorgehoben, dass jede Petition einem Abgeordneten zur Prüfung vorgelegt wird. Im Laufe des Ausfüllens des Formulars wird nicht nur die Einwilligung in die Verarbeitung eingeholt. Hervorgehoben ist die getrennt abgefragte Einwilligung zur Verarbeitung von Daten besonderer Kategorien, die einzeln aufgezählt werden. Die allgemeine Datenschutzerklärung[11] enthält nur einen kurzen, aber detaillierten Abschnitt zu den Formulardaten bei Online-Petitionen: „Die im Petitionsformular angegebenen Informationen werden aus Verarbeitungsgründen bis zu 72 Stunden bei einem externen Dienstleister (Firma Babiel) zwischengespeichert und dann wieder gelöscht." Über Löschfristen wird ansonsten nicht informiert.

Beim Bayerischen Landtag gibt es keine gesonderten „öffentlichen Petitionen", da jede Petition in öffentlicher Sitzung des Petitionsausschusses behandelt wird. Die Möglichkeit, eine Petition online einzureichen, wird über ein Formular[12] geboten, bei dem allgemeine Hinweise und eine Datenschutzerklärung[13] bestätigt werden müssen, die allerdings keine speziellen Datenschutzhinweise sind. Über den Verweis gelangen Interessierte lediglich auf die allgemeine Datenschutzerklärung des Landtages, so dass über Datenweitergabe und Löschung keine weiteren Informationen verfügbar sind.

Berlin: In den Verfahrenserklärungen[14] wird informiert, dass nach Einreichen der Petition (bei Online-Petition nach Bestätigen der E-Mail) noch eine Eingangsbestätigung per Post versendet wird. Die Behandlung der Petition findet in einer nichtöffentlichen Sitzung des Ausschusses statt. Zur Frage, was mit den Daten geschieht, heißt es lapidar: „Ihre personenbezogenen Daten werden unter Wahrung des Datenschutzes verarbeitet und nur für die Durchführung des Petitionsverfahrens genutzt. Soweit die jeweiligen Behörden vom Petitionsausschuss aufgefordert werden, zu Ihrer Petition ausführlich Stellung zu nehmen, erhalten diese Ihre Petition und Ihre Unterlagen in Kopie." Das Einverständnis für die Übermittlung dieser Daten wird vorausgesetzt. Interessanterweise muss beim Einreichen der Online-Petition[15] die Kenntnisnahme einer sehr viel älteren Erläuterung mit Stand von 2011[16] bestätigt werden. Statt der oben zitierten allgemeinen Erklärung „Durchführung des Petitionsverfahrens" wird dort spezieller beschrieben, dass die personenbezogenen Daten „für die Information der Mitglieder des Abgeordnetenhauses von Berlin genutzt" werden. Des weiteren ist in der zu bestätigenden älteren Erklärung nicht von Behörden, sondern von den „von Ihrer Petition betroffenen Stellen" die Rede, denen Petition und Unterlagen übermittelt werden. Auch hier wird das Einverständnis vorausgesetzt. Eine Löschung wird nicht erwähnt.

Brandenburg: In erfreulich klaren und präzise auf das Petitionsverfahren bezogenen Datenschutzhinweisen[17] wird über die Datenverarbeitung, -übermittlung und -löschung informiert. Auch die Möglichkeit, dass das Petitionsanliegen an ein anderes Länderparlament oder den Bundestag weitergegeben wird, ist im übersichtlichen Einreichungsverfahren erläutert.

Bremen hat ein Petitionssystem[18] mit speziellen Informationen über die Datenverarbeitung. Die Annahme der Petition unterliegt einer Prüfung durch den Petitionsausschuss. Die verlinkte Verfahrensordnung stellt klar, dass bei Veröffentlichungen der Name sichtbar ist (vorausgesetzt, die Einwilligung wurde erteilt). Weitere Daten, also die postalische Adresse und eine E-Mail-Adresse, die zur Identifikation dienen, werden nicht veröffentlicht. Die Mitzeichnenden werden nur zahlenmäßig erfasst. Eine Registrierung ist nötig für diejenigen, die in einem gesonderten Bereich, für den es auch eine eigene Datenschutzrichtlinie gibt, mitdiskutieren wollen. Die Datenschutzerklärung[19] erwähnt zwar die Weitergabe personenbezogener Daten zur Petitionsbearbeitung, unklar ist allerdings, wer das im folgenden Satz erwähnte Einsichtsrecht hat: „Die Petitionen sowie die dazu gehörigen Mitzeichnerlisten und Diskussionsbeiträge können während der jeweils laufenden Wahlperioden eingesehen werden." Das Löschen der Daten hängt von der Wahlperiode ab, nach deren Ende noch ein Jahr bis zur Löschung verstreicht.

Die Hamburgische Bürgerschaft hat einen Eingaben-Ausschuss[20], der auch Online-Petitionen entgegennimmt. Im Zusammenhang mit dem Formular erfolgen keinerlei Datenschutz- oder Verarbeitungs-Hinweise und selbst die E-Mail-Angabe ist freiwillig. Allerdings verpflichtet das zugrunde liegende „Gesetz über den Eingabenausschuss" in § 9 explizit „Mitglieder der Bürger-

schaft, deren Mitarbeiterinnen und Mitarbeiter, die Mitarbeiterinnen und Mitarbeiter der Fraktionen sowie Personen, die in amtlicher Tätigkeit Eingaben bearbeiten" zur Verschwiegenheit. Weitere Informationen – wie zum Beispiel zu Löschfristen – finden sich auch in der allgemeinen Datenschutzerklärung[21] der Bürgerschaft nicht.

Auf der Webseite des Hessischen Landtags wird unter „Service -> Petitionen" erklärt, was eine Petition ist und wie sie per Online-Formular eingereicht werden kann. Nach Richtlinien des Landtags sind die Petitionsakten geheim und nur den Ausschuss-Mitgliedern zugänglich. Gleich zu Beginn der Formulareingabe[22] wird die Möglichkeit geboten die Datenschutzhinweise zu lesen, allerdings sind dies die allgemeinen Hinweise, die alle Formulardaten betreffen, die „bei der Hessischen Zentrale für Datenverarbeitung gespeichert und nur für die Bearbeitung Ihres Anliegens von den fachlich zuständigen Personen verwendet" werden. In der Erklärung des Ablaufs einer Online-Petition wird dann unglücklicherweise in zwei jeweils mit „Datenschutzhinweise" überschriebenen, ansonsten fast gleichlautenden Abschnitten einmal auf Art. 13 und einmal auf Art. 14 der DSGVO verwiesen[23]. Einer Aussage der Datenschutzbeauftragten zufolge soll damit sowohl die persönliche Eingabe als auch die Eingabe für eine andere Person abgedeckt werden, ohne dass dies in der Überschrift und ohne Nachschlagen in der DSGVO erkennbar wäre. Am Ende der Formular-Eingabe muss dann eine Datenschutzerklärung bestätigt werden, die die Übermittlung an andere Behörden oder Petitionsausschüsse betrifft. Laut Angabe in den Datenschutzhinweisen beträgt die Löschfrist grundsätzlich fünf Jahre.

Mecklenburg-Vorpommern: Die Datenschutzerklärung[24] bei der Online-Petitionseingabe[25] per Formular ist sehr gut angepasst. Die einzelnen Hinweise zum weiteren Verfahren umfassen auch die verschiedenen Verschlüsselungen auf dem Webserver und den Transportwegen. Lediglich Löschfristen sind dort nicht zu finden.

In Niedersachsen besteht die Möglichkeit des Einreichens Öffentlicher Petitionen seit September 2017[26]. Gleich mit der Information über „Einzel(Individual)-Petitionen" wird zwar die Wahrung des Datenschutzes durch den Landtag zugesichert, im Zusammenhang mit der Eingabe per Formular gibt es dann aber keinerlei weitere Information darüber. Lediglich die Freischaltung durch Bestätigen der automatisch versendeten E-Mail wird erwähnt. In den allgemeinen Datenschutzhinweisen des Landtags[27] heißt es unter 4.4 Online-Petitionen, dass auf ein gesondertes Portal beim Innenministerium verlinkt wird. Die dort hinterlegten Nutzungsbedingungen[28] allerdings lassen jeden Hinweis auf Online-Petitionen vermissen und sind insofern nicht zielführend, als von Dienstleistern und von einer „Registrierung zur Bearbeitung von Anträgen" die Rede ist. Über Löschung der Daten wird nicht informiert.

Beim Landtag von Nordrhein-Westfalen enthält das Online-Formular[29] keine Datenschutzerklärung, aber in der allgemeinen Datenschutzerklärung des Landtags[30] findet sich ein gesonderter Abschnitt zu Petitionen, in dem die Grundlage der Datenverarbeitung ebenso genannt wird wie beispielhafte Empfänger von Daten im Petitionsverfahren. Die Daten werden zehn Jahre nach Abschluss des Petitionsverfahrens gelöscht.

Auf der Seite der Bürgerbeauftragten in Rheinland-Pfalz[31] werden Petitionen unter zwei Überschriften angeboten. „Einreichen einer Petition" führt direkt zu den Möglichkeiten und zu einem Link für das Online-Formular. Eine Datenschutzerklärung fehlt, statt dessen muss lediglich die Kenntnisnahme der allgemeinen Hinweise erklärt werden, ohne dass deutlich wird, welche Hinweise das sein sollen. Für öffentliche Petitionen wird weiterverwiesen auf eine andere Seite. Die dort verlinkte Datenschutzerklärung[32] ist speziell angepasst und umfangreich. Sie klärt auf, welche Daten zu welchem Zweck verarbeitet werden. Wenn teils auch Beispiele „ohne Anspruch auf Vollständigkeit" angegeben werden, ist die Löschung doch klar umrissen: „Nach Ablauf der Wahlperiode werden die Daten der abgelaufenen Wahlperiode noch ein Jahr aufbewahrt und danach gelöscht."

Saarland: Neben den Jahresberichten gibt es auf der Webseite des Landtages[33] nur eine äußerst knappe Information über die rechtlichen Grundlagen von Petitionen und dann zum Formular den Hinweis, dass eine Empfangsbestätigung versendet wird. Die allgemeine Datenschutzerklärung[34] sagt zu Online-Petitionen, dass die Weitergabe personenbezogener Daten einer besonderen Kategorie an Dritte nicht ohne Einwilligung erfolgt. Unklar und fragwürdig in Bezug auf die Löschung ist die Aussage: „Die vom Nutzer übermittelten Informationen werden nur so lange gespeichert, wie dies zur Erreichung des Verarbeitungs- und Speicherungszwecks erforderlich ist."

Im Online-Petitionsportal des Sächsischen Landtags[35] wird vor dem eigentlichen Formular empfohlen: „... lesen Sie bitte dringend die Hinweise unter Petitionshilfe". Vor dem Absenden des Formulars sind dann die Datenschutzhinweise für die Webseite des Landtags zu bestätigen. Diese enthalten auch einen Abschnitt zu Online-Petitionen, in dem die im Formular einzutragenden Datenarten nochmals aufgelistet werden. Zum Verfahren wird beschrieben, dass die Daten per E-Mail an den Ausschuss gesendet und gleichzeitig in einer Datenbank gespeichert werden. Nach Bestätigung des Links, der die Unterschrift ersetzt, wird dieser Datenbankeintrag gelöscht. Zu Löschfristen der Petitionsdaten allgemein findet sich kein Hinweis.

Auch in Sachsen-Anhalt erfolgt seit 2011 die Eingabe von Online-Petitionen ausschließlich per Formular[36] mit anschließender Bestätigung des per E-Mail zugesendeten Links. Die gesondert zu bestätigenden Hinweise zum Petitionsverfahren machen keine weiteren Aussagen über Speicherung und Löschung.

Die Webseite des Landtags Schleswig-Holstein[37] verlinkt auf einen Auszug aus der Datenschutzerklärung des Landtags[38], der das Petitionsverfahren betrifft, und dessen Kenntnisnahme bei Einreichen der Petition bestätigt werden muss. Dort wird auch informiert, „dass alle im Rahmen des Petitionsverfahrens Unterrichteten zur Vertraulichkeit verpflichtet sind". Die per Formular übertragenen Daten werden bei privaten Petitionen nach Übermittlung an den Petitionsausschuss auf dem Server

gelöscht. Bei öffentlichen Petitionen geschieht das analog, allerdings sind Daten der Mitzeichnenden bis zum Abschluss des Verfahrens abrufbar. Nach spätestens fünf Jahren werden die Daten von der Internetseite gelöscht.

Auf der Webseite des Thüringer Landtags[39] wird ausführlich über das Petitionsverfahren informiert. Demnach wird zwischen „veröffentlichten" und „nicht veröffentlichten" Petitionen unterschieden. Über die Veröffentlichung entscheidet der Petitionsausschuss abhängig vom allgemeinen Interesse und der Geeignetheit der Petition. Diese wird dann beim Erreichen eines Quorums von 1500 Unterschriften in einer öffentlichen Ausschusssitzung behandelt. Die Einreichung oder Mitzeichnung einer „veröffentlichten" Petition erfordert eine einmalige Registrierung für ein Benutzerkonto, zu der eine ausführliche Datenschutzerklärung existiert. Wird das Konto der/des Einreichenden wieder gelöscht, ändert sich der Status der eingereichten Petition automatisch auf „nicht veröffentlicht". Veröffentlichte Petitionen werden spätestens nach 10 Jahren gelöscht. Bezüglich der Weiterleitung der Unterlagen wird laut Verfahrensregelung das Einverständnis vorausgesetzt.

Die folgende Tabelle fasst die Ergebnisse der Petitionsportal-Analyse der 16 Bundesländer bezüglich der oben genannten Fragestellungen noch einmal zusammen.

Bei allen genannten Unterschieden und Unklarheiten ist die Möglichkeit der Online-Petitionseingabe also bundesweit grundsätzlich gegeben. Die Verfahren der staatlich betriebenen Petitionsportale sind durchaus vergleichbar und bei Erklärungslücken kann die Ähnlichkeit im Vorgehen unterstellt werden. Für den weitaus weniger übersichtlichen Bereich der privaten Petitionsportale soll jetzt zunächst die Daseinsberechtigung hinterfragt werden. Dann wird das Portal openPetition genauer untersucht.

Private Petitionsportale

Die Nutzung der Portale auf europäischer, Bundes- und Landes-Ebene hält sich zahlenmäßig in gewissen Grenzen. Private Portale sind teils sehr viel bekannter und haben einen hohen Zulauf, wenn sie mit dem Begriff der „Petition" für ein Anliegen eine breite Öffentlichkeit interessieren und mobilisieren wollen. Dr. Kathrin Voss hat jüngst in einer Studie[40] für die Friedrich-Ebert-Stiftung untersucht:

- Wer sind die Menschen, die sich im Netz politisch engagieren?
- Was sind ihre Anliegen und ihre Motivation?
- Welches Demokratie- und welches bürgerschaftliche Selbstverständnis vertreten sie?
- Und wie sind ihre digitalen Aktivitäten eingebunden in andere ‚klassische' Formen des Engagements?

Sie vergleicht dazu das Portal des Bundestags mit den privaten Plattformen change.org und openPetition und untersucht die Fragestellungen mithilfe von Interviews und einer Online-Befragung. Neben wenig überraschenden Ergebnissen – Alter meist Ü50, überwiegend akademischer Abschluss, Gender-Gap und „politisch aktiv" – findet die Studie auch heraus, dass mit der Petition oft eine rechtliche Regelung eines Problems erreicht werden soll, für das bereits ein Lösungsvorschlag unterbreitet wird. Statt also „Faulpelz-Aktivismus" zu betreiben sind diejenigen, die eine Petition einreichen, sehr aktiv in ihrem Themenbereich. Die Befragten verbinden allerdings „die Bundestagsplattform mit mehr Seriosität, mehr Datenschutz und mit einem direkten und verbindlichen Zugang zur Politik".

Zu dieser Einschätzung tragen sicher das Geschäftsgebaren und auch Skandale bei. So erhielt change.org 2016 den Big Brother Award, weil personenbezogene Daten an andere Unternehmen verkauft wurden (siehe DANA 2/2016, S. 88). Die Plattform WeAct von Campact musste im Juli 2019 mitteilen, dass personenbezogene Daten von zwei Millionen Unterstützenden nicht genügend vor Zugriff geschützt waren. Auch aktuell sind Angriffe auf Petitionsplattformen gang und gäbe. Bei den Datenpannen jüngeren Datums taucht etwa die Katholische Kirche auf. Die Webseite www.kath.ch wusste im Mai 2020 anhand der versehentlich veröffentlichten E-Mail-Adressen unter der Viganò-Petition[41] zu berichten, dass diese in der Schweiz von rund 260 Personen unterstützt wurde[42]. Aus Luxemburg wurde Ende Januar 2021 ein Hacker-Angriff auf ein Petitionsportal bekannt, als das „Tageblatt Lëtzebuerg" berichtete[43], ein externer Dienstleister, der die neue Internetseite für die Petitionen hostete, sei gehackt worden. Offenbar handelte es sich hier um eine DDoS-Attacke, die schnell abgewiesen werden konnte. Und im Februar 2021 wies ein Hacker nach[44], dass die rechtsgerichtete Schweizer Online-Petition lockdown-stop.ch in einfacher Weise manipulierbar und die Zahl von über 170.000 Unterschriften völlig unglaubwürdig war. Nicht einmal das automatisierte Unterzeichnen per Bot war abgefangen worden. Die für die

	E-Mail mit Link / Empfangsbestätigung	Hinweise angepasst / Teil der allgemeinen Hinweise	Infos zur Datenübermittlung	Info über Löschfristen
Baden-Württemberg	Link	kaum	unpräzise	-
Bayern	Link	-	-	-
Berlin	Link	zwei Versionen	ja	-
Brandenburg	Link	angepasst	ja	12 Jahre
Bremen	Bestätigung	angepasst	ja	max. 6 Jahre
Hamburg	-	-	-	-
Hessen	Link	unklar	ja	grds. 5 Jahre
Mecklenburg-Vorpommern	Link	angepasst	ja	-
Niedersachsen	Link	-	nein	-
Nordrhein-Westfalen	Bestätigung	allgemein	ja	10 Jahre
Rheinland-Pfalz	Bestätigung	angepasst	ja	max. 6 Jahre
Saarland	Bestätigung	-	kaum	fragwürdig
Sachsen	Link	allgemein	unpräzise	-
Sachsen-Anhalt	Link	-	-	-
Schleswig-Holstein	Link	angepasst	ja	5 Jahre
Thüringen	entfällt	angepasst	ja	10 Jahre


Bild: iStock.com/Vadim Sazhniev

Petition mitverantwortliche SVP sah – so zitiert das Nachrichtenportal watson.ch die SVP-Sprecherin – „ein Captcha für die Benutzer" als „eine weitere Hürde", so dass auf diese Maßnahme zunächst verzichtet worden war. Die Korrektheit der Unterschriften soll dennoch überprüft worden sein.

Nicht nur derartige „Datenpannen" lassen an der Effektivität privater Petitionsplattformen zweifeln, sondern auch aus den Parlamenten wird Kritik geäußert. Dr. Ute Bergner, Mitglied im Petitionsausschuss des Thüringer Landtags, stellt in einem Interview[45] fest: „Und wenn die Petition dann zuerst bei einer privaten Plattform veröffentlicht wurde, sind viele Mitzeichner der Meinung, dass sie ja bereits gezeichnet hätten und somit die eigentliche Mitzeichnung auf der Plattform des Landtages, die für einen Erfolg notwendig ist, nicht mehr nötig sei".

Nichtsdestotrotz haben private Petitionsportale allein durch ihren Bekanntheitsgrad eine gewisse Daseinsberechtigung. Hier soll openPetition als eines der Großen dieser Gattung näher betrachtet werden.

Das Beispiel openPetition

Jörg Mitzlaff, der Geschäftsführer der openPetition gGmbH, begründete die Notwendigkeit seines Portals 2019 in einem Interview mit Telepolis[46], indem er auf die Praxis des Bundestages hinwies: „Und da auch der Petitionsausschuss nach den Fraktionsstärken im Parlament besetzt wird, können allein die Abgeordneten des Regierungslagers alles ablehnen, was ihnen nicht genehm ist". Um dies zu umgehen, sammelt openPetition Unterschriften zu verschiedenen Anliegen und übernimmt dann selbst das Einreichen von Petitionen bei Parlamenten. In Einzelfällen – wie beim Bundestag, wo die von openPetition gesammelten Unterschriften nicht akzeptiert werden – sichert das Verfahren zumindest zu, dass die Petition vom Petitionsausschuss auf jeden Fall behandelt wird, da auch eine einzige Unterschrift bei der Einreichung genügt.

Das Thema Datenschutz behandelt openPetition unter anderem in einem Blogbeitrag auf der Webseite[47], in dem eine Reihe von Kritikpunkten genannt sind, die im Beitrag jeweils entkräftet werden. Es heißt dort, jede und jeder könne „selbstbestimmt darüber entscheiden, was mit seinen Daten passiert und ob er kontaktiert werden möchte." Eher befremdlich wirkt die Erweiterung der üblichen E-Mail-Unterschrift auf fünf Personen pro Adresse: „Eine Petition kann auch unterschrieben werden, wenn man jemanden kennt, der eine E-mail-Adresse hat und diese mitbenutzen darf." Positiv ist zu vermerken, dass bei openPetition eine Kommunikation mit PGP-Verschlüsselung möglich ist und der Empfang von Newslettern und Spendenaufrufen abgelehnt werden kann. Laut Datenschutzerklärung[48] vom November 2020 können Nutzende des Portals allerdings nicht unterbinden, dass openPetition ihnen Petitionsvorschläge aus den „zugeordneten Verwaltungsebenen" und „Petitionen mit ähnlichen Themen" zusendet. Auf die aus Datenschutzsicht äußerst kritisch zu betrachtende Zusammenarbeit mit Facebook, Twitter und Google wird hingewiesen.

Löschfristen (max. 5 Jahre für Unterschriften unter abgeschlossene Petitionen) werden in der Datenschutzerklärung ebenso angegeben wie die Aufforderung an die Petenten alle „Unterschriftendaten digital oder gedruckt zu vernichten". Was dies allerdings bei der Vielzahl verschiedener Themen bedeutet, die von unterschiedlichsten Petenten eingereicht werden, lässt sich nur vermuten. Insbesondere stellt sich die Frage, wie openPetition sicherstellen will, dass die an die Einreichenden übermittelten „Unterschriftendaten" nicht weitergegeben und nach Abschluss auf jeden Fall komplett vernichtet werden. Gerade bei Initiativen, in denen sich mehrere Personen engagieren, ist ein Verstoß gegen die Bedingungen wohl eher die Regel als die Ausnahme.

Insgesamt zeigt das Beispiel openPetition, dass die Verfahren und Praktiken der privaten Petitionsportale einer deutlich kritischeren Analyse zu unterwerfen sind, als die Portale der Petitionsausschüsse der Parlamente, die meist klaren, gesetzlichen Regelungen folgen. Dies wurde bisher von der Wissenschaft eher vernachlässigt, wie die abschließende Zusammenfassung zeigen soll.

Gutachten und Studien

Die Wissenschaftlichen Dienste des Bundestages (WD) hatten in 2015 die parlamentarischen mit den außerparlamentarischen Petitionsportalen verglichen[49]. Dabei wurde betont, das seit 2005 existierende E-Petitionsportal sei „das mit Abstand erfolgreichste Internet-Angebot des Deutschen Bundestages". Es wurde verglichen mit den privaten Plattformen openPetition, change.org, Avaaz.org und WeAct von Campact. Auch die Kategorie „Datenschutz" spielte eine Rolle. Die diesbezüglichen Fragen reichen von Nutzerdaten und Speicherdauer bis zu Nutzungsprofilen und Verkauf/Tausch der Daten. Bis auf Avaaz.org wurden laut des Vergleichs von 2015 „keine (personenbezogenen) Daten von Petenten und Mitzeichnern an andere Nutzer weitergegeben". Die damaligen Ergebnisse seien kurz zusammengefasst:

Portal	Profile	Datenweitergabe
openPetition	keine Profile, aber Google Analytics	keine
change.org	Profilbildung erfolgt	kein Tausch oder Verkauf
Avaaz.org	wahrscheinlich Profilbildung	Datenweitergabe vorbehalten
WeAct	Interessengebiete werden für E-Mails mit Werbung für andere Petitionen genutzt	keine

Carolin Kahlisch und Britta Oertel vom Büro für Technologiefolgen-Abschätzung beim Deutschen Bundestag (TAB) prüften 2020 in einer empirischen Studie[50] die Bekanntheit und Nutzung von Petitionen. Sie bezogen sich nicht nur auf eine Repräsentativbefragung sondern forderten auch die über drei Millionen Personen, die sich auf dem Petitionsportal des Bundestages registriert haben, zur Beteiligung auf. Dabei stellte sich wenig überraschend heraus, dass „die Nutzerschaft des Portals […] nicht den Durchschnitt der Bevölkerung" widerspiegelt. Während nach dieser Untersuchung den Petentinnen und Petenten, die sich auf dem klassischen Weg per Post einbringen, „außerparlamentarische Petitions- und Kampagnenportale" kaum bekannt sind, ist bei den im Portal registrierten Personen das Gegenteil der Fall. Allerdings ließ sich herauskristallisieren, dass die „ständige aktive Nutzung" des Bundestags-Portals die Ausnahme ist. Informationen über Petitionen beziehen die Befragten aus den klassischen Medien (25 %) und auch über die sozialen Medien (8 %). Mit der Studie wurde weiterhin festgestellt, dass die Überlappung der Nutzungsgruppen des Bundestag-Petitionsportals sowie der privaten Petitionsportale „mit ca. 40 % erstaunlich gering" ist. In Bezug auf den Datenschutz kritisiert die TAB-Studie, dass Portale wie change.org das Nutzungsverhalten protokollieren, zu Profilen zusammenfassen und für zielgerichtete Information über andere „Petitionen" nutzen.

In seinem Beitrag vom Oktober 2020 im KWI-Schriften-Band „Verwaltungsmodernisierung: Digitalisierung und Partizipation"[51] bezweifelt Michael Meier schließlich, „dass der Unterschied zwischen staatlichen und privaten Petitionsplattformen jedenfalls der breiten Öffentlichkeit" bewusst ist. Er unterscheidet bei seiner rechtswissenschaftlichen Prüfung zwischen echten und unechten Petitionen, um für erstere die Zulässigkeitsvoraussetzungen bei Online-Einreichung zu analysieren. Besondere Betrachtung findet das „Regelungsdickicht" für Online-Petitionen an den Bundestag. Insbesondere die „Einführung der sogenannten öffentlichen Petitionen" hätte nach Auffassung des Autors „einer gesetzlichen Grundlage bedurft." Die Wirksamkeit der erzwungenen Zustimmung zur „Netiquette" stellt er in Frage und fordert vor allem, „dass auch Einzelpetitionen mit gleicher Sorgfalt behandelt" und gegenüber öffentlichen Petitionen nicht vernachlässigt werden. Bei den unechten Petitionen der privaten Plattformen sagt Meier klar: „Allerdings birgt die Zwischenschaltung privater Intermediäre auch Risiken. Das betrifft etwa die Verwendung der angegebenen Daten." Als „Extrembeispiel" dafür nennt er den Fall change.org. Darüber hinaus sieht der Autor die Gefahr, dass private Plattformen falsche „Erwartungen an die staatliche Responsivität" wecken. Schlussendlich aber billigt er privaten Plattformen eine „Daseinsberechtigung" zu, denn sie seien „Forum für die […] öffentliche Meinungsbildung und gegebenenfalls […] Ausgangspunkt für eine spätere echte (Online-)Petition." Insgesamt sieht Meier „die Beteiligung an digitalen Partizipationsverfahren" nicht als einfachen „Sofa-Aktivismus", sondern als „zukunftsweisendes Format der Bürgerbeteiligung".

Zusammenfassung und Ausblick

Die Zusammenstellung der verschiedenen Verfahren zur elektronischen Eingabe von Petitionen auf europäischer, Bundes- und Landesebene lässt bisher kaum ein einheitliches Vorgehen erkennen. Nicht zuletzt darauf reagieren die privaten „Petitions"-Portale, die darüber hinaus einen weitaus größeren Bekanntheitsgrad haben. Die stellvertretend für viele Portale erfolgte Betrachtung von openPetition zeigt, dass trotz ausführlicher Information in Datenschutzerklärungen die Veröffentlichung und Weitergabe von Unterstützungslisten zu datenschutzrechtlichen Problemen führen kann. Inwieweit andere private Petitionsplattformen alternative Mechanismen verwenden oder noch größere Datenschutzverletzungen hinnehmen, bleibt einer weiteren detaillierten Analyse vorbehalten.

1 https://www.landtag.nrw.de/home/petitionen/sprechstunden-und-aktuelles.html

2 https://www.netzwerk-buergerbeteiligung.de/fileadmin/Inhalte/PDF-Dokumente/newsletter_beitraege/4_2018/nbb_beitrag_schuhmacher_181217.pdf

3 https://www.europarl.europa.eu/petitions/de/faq/pdf

4 https://www.europarl.europa.eu/petitions-content/docs/privacy_policy/PetitionPortal_PrivacyPolicy_de_v5.pdf

5 https://epetitionen.bundestag.de

6 https://epetitionen.bundestag.de/epet/service.$$$.rubrik.datenschutz.html#sicontent

7 https://www.bundestag.de/ausschuesse/a02/richtline-oep-532092

8 https://www.gruene-bundestag.de/themen/petitionen

9 https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200085de.pdf

10 https://www.landtag-bw.de/home/der-landtag/petitionen/online-petition.html

11 https://www.landtag-bw.de/datenschutz.html

12 https://www.bayern.landtag.de/petition-einreichen/petition-online-einreichen/

13 https://www.bayern.landtag.de/service/datenschutz/

14 https://www.parlament-berlin.de/de/Das-Parlament/Petitionen/Online-Petition/Petitionsverfahren-und-Datenschutz

15 https://www.parlament-berlin.de/de/Das-Parlament/Petitionen/Online-Petition-Formular

16 https://www.parlament-berlin.de/C1257B55002B290D/vwContentByKey/W29E8J9K530PARIDE/$File/Hinweise.pdf

17 https://www.landtag.brandenburg.de/de/mitgestalten/petitionen/datenschutzhinweise_zum_petitionsverfahren/979526

18 https://petition.bremische-buergerschaft.de

19 https://petition.bremische-buergerschaft.de/index.php?n=datenschutz_petition

20 https://www.buergerschaft-hh.de/eingaben

21 https://www.hamburgische-buergerschaft.de/datenschutz/

22 https://hessischer-landtag.de/content/formular-online-petition

23 https://hessischer-landtag.de/content/was-ist-beim-online-formular-zu-beachten

24 https://www.petition.landtag-mv.de/petition/elektronisch-uebermittelte-petition/datenschutzerklaerung

25 https://www.landtag-mv.de/petition

26 https://www.landtag-niedersachsen.de/mitgestalten/petitionen/online-petitionen-oeffentliche-petitionen/

27 https://www.landtag-niedersachsen.de/datenschutz/

28 https://www.navo.niedersachsen.de/navo2/portal/desktop/0/nutzungsbedingungen

29 https://www.landtag.nrw.de/portal/WWW/Navigation_R2010/050-Petitionen/Inhalt.jsp

30 https://www.landtag.nrw.de/home/datenschutz.html

31 https://formular.diebuergerbeauftragte.rlp.de/icc/assisto/nav/e9d/e9d60c14-a450-fa21-ccea-97c6fcb2c451&uTem=8721b524-4eb6-b21a-c31b-e220fcb2c451

32 https://formular.diebuergerbeauftragte.rlp.de/icc/assisto/nav/dd6/dd649126-5d0e-216c-be5c-810fcb2c4510&class=net.icteam.cms.utils.search.AttributeManager&class_uBasAttrDef=a001aaaa-aaaa-aaaa-eeee-000000000054.htm

33 https://www.landtag-saar.de/petitionen/online-petition/

34 https://www.landtag-saar.de/Datenschutz

35 https://www.landtag.sachsen.de/de/mitgestalten/petition/onlinepetition.cshtml

36 https://www.landtag.sachsen-anhalt.de/mitgestalten/petition/petition-einreichen

37 https://www.landtag.ltsh.de/petitionen/online-petition/index.html

38 https://www.landtag.ltsh.de/petitionen/datenschutzerklaerung/

39 https://petitionen.thueringer-landtag.de/infos

40 http://library.fes.de/pdf-files/dialog/17748-20210507.pdf

41 https://www.katholisch.de/artikel/25478-datenpanne-bei-vigano-petition-tausende-e-mail-adressen-oeffentlich

42 https://www.kath.ch/newsd/ueber-200-schweizer-von-datenleck-betroffen/

43 https://www.tageblatt.lu/non-classe/der-dienstleister-fuer-die-neue-petitionsinternetseite-wurde-gehackt/

44 https://www.watson.ch/digital/schweiz/445866038-fake-unterschriften-bei-lockdown-stop-ch-svp-verteidigt-online-petition

45 https://www.jenaer-nachrichten.de/stadtleben/15194-petitionen-auf-change-org-und-co-bewegen-nichts

46 https://www.heise.de/tp/features/Petitionen-sind-immer-Katalysatoren-fuer-Themen-4582174.html

47 https://www.openpetition.de/blog/presseabteilung/petitionsplattformen-16-kritikpunkte-beantwortet

48 https://www.openpetition.de/content/data_privacy

49 https://www.bundestag.de/resource/blob/420562/cae86703989754049a-2bee879797b2e7/WD-3-219-15-pdf-data.pdf

50 https://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Hintergrundpapier-hp025.pdf

51 https://publishup.uni-potsdam.de/frontdoor/index/index/docId/45910

Werner Hülsmann

Neuerungen beim Datenschutz in der Telekommunikation und bei den Telemedien

„Was lange währt wird endlich gut." Gilt dies auch für das am 01. Dezember 2021 in Kraft tretende „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien" (kurz: „Telekommunikation-Telemedien-Datenschutz-Gesetz" oder noch kürzer: TTDSG)? Entgegen den Behauptungen der Bundesregierung waren die 2009 erfolgten Änderungen der EG-ePrivacy-Richtlinie[1] (die Änderungsrichtlinie von 2009 wurde oft auch als Cookie-Richtlinie bezeichnet) bislang nicht vollständig in nationales Recht umgesetzt worden. Eine Umsetzung der Änderung von Art. 5 Abs. 3[2] der EG-ePrivacy-Richtlinie erfolgte gar nicht. Die Umsetzung der Änderung des Art. 13 der EG-ePrivacy-Richtlinie erfolgte beispielsweise in § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Andere Regelungen dieser Richtlinie wurden in den Datenschutzbestimmungen des Telekommunikationsgesetzes umgesetzt.

Schon lange wurde eine Umsetzung der EG-ePrivacy-Richtlinie an einer zentralen Stelle im nationalen Recht gefordert. Seit dem In-Kraft-Treten der DSGVO am 25. Mai 2016 wurden diese Forderungen verständlicherweise lauter, da mit dem Wirksamwerden der DSGVO nach der zweijährigen Umsetzungsphase am 25. Mai 2018 ein Teil der Regelungen im Telemediengesetz von der DSGVO verdrängt wurde. Auch von den Datenschutzregelungen des Telekommunikationsgesetzes (TKG) wurden die Regelungen, die nicht der Umsetzung der EG-ePrivacy-Richtlinie, sondern der alten EG-Datenschutzrichtlinie dienten, durch die DSGVO verdrängt. So machte sich eine gewisse Rechtsunsicherheit breit. Mit dem Inkrafttreten des TTDSG am 01. Dezember 2021 soll diese Rechtsunsicherheit der Vergangenheit angehören und eine vollumfängliche Umsetzung der EG-ePrivacy-Richtlinie erfolgen.

1. Einleitung

Am 28. Juni 2021 wurden im Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 35 zwei Gesetze verkündet.

Das ist zum einen das „Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz)". Dieses ist ein sogenanntes Artikelgesetz und enthält als Artikel 1 das neue, ab 01. Dezember 2021 geltende, Telekommunikationsgesetz (TKG-2021). Weitere Artikel dienen der Änderung, Einfügung und Aufhebung zahlreicher Paragraphen von 32 Gesetzen und 22 Rechtsverordnungen sowie der Aufhebung des bisherigen Telekommunikationsgesetzes (TKG-alt)[3]. Das TKG 2021 enthält erwartungsgemäß im Gegensatz zum TKG-alt keine Regelungen zum Datenschutz mehr, da diese im TTDSG enthalten sind.

Das zweite Gesetz ist das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien". Auch dieses ist ein Artikelgesetz und enthält als Artikel 1 das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutzgesetz - TTDSG)". Weitere Artikel führen zur Änderung der §§ 100g und 100j Strafprozessordnung, zur Aufhebung und Änderung verschiedener Paragraphen des Telemediengesetzes (TMG) sowie zur Änderung des § 307 Fünftes Buch Sozialgesetzbuch[4]. Die bisherigen Regelungen zum Datenschutz im TMG werden aufgehoben und durch die entsprechenden Regelungen im TTDSG ersetzt.

2. Das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)

2.1. Struktur des TTDSG

Das TTDSG gliedert sich in vier Teile. Die Teile 2 und 3 werden weiter in Kapitel untergliedert:

- Teil 1 – Allgemeine Vorschriften
- Teil 2 – Datenschutz und Schutz der Privatsphäre in der Telekommunikation
  - Kapitel 1 – Vertraulichkeit der Kommunikation
  - Kapitel 2 – Verkehrsdaten, Standortdaten
  - Kapitel 3 – Mitteilen ankommender Verbindungen, Rufnummernanzeige und -unterdrückung, automatische Anrufweiterschaltung
  - Kapitel 4 – Endnutzerverzeichnisse, Bereitstellen von Endnutzerdaten
- Teil 3 – Telemediendatenschutz, Endeinrichtungen
  - Kapitel 1 – Technische und organisatorische Vorkehrungen, Verarbeitung von Daten zum Zweck des Jugendschutzes und zur Auskunftserteilung
  - Kapitel 2 – Endeinrichtungen
- Teil 4 – Straf- und Bußgeldvorschriften und Aufsicht

Die beiden Paragraphen des Teil 1 enthalten den Anwendungsbereich und die Begriffsbestimmungen des Gesetzes. Die Inhalte der anderen Teile ergeben sich aus deren Überschriften und bei den Teilen 2 und 3 den Überschriften der enthaltenen Kapitel.

2.2. Ein erster Vergleich der Regelungen des TTDSG mit den bisherigen Regelungen des TKG-alt und des TMG

Durch die klare Strukturierung ist für die meisten Paragraphen des TTDSG eine direkte Gegenüberstellung mit den vergleichbaren bisher geltenden Paragraphen des TKG-alt und des TMG möglich.[5] Auf die Darstellung von Regelungen, die im wesentlichen redaktioneller Natur sind, wird im Folgenden verzichtet.

2.2.1. TTDSG Teil 1 – Allgemeine Vorschriften

Mit § 1 Abs. 3 TTDSG wird – vergleichbar wie in der DSGVO – das Marktortprinzip eingeführt: Dem TTDSG unterliegen demnach „alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen." Das Herkunftslandprinzip aus § 3 TMG bleibt allerdings unberührt.

2.2.2. TTDSG Teil 2 – Datenschutz und Schutz der Privatsphäre in der Telekommunikation

Im § 3 Abs. 1 TTDSG werden die zur Wahrung des Fernmeldegeheimnisses Verpflichteten konkreter benannt als dies im § 88 Abs. 1 TKG-alt der Fall war. Der neue § 4 TTDSG regelt, dass das Fernmeldegeheimnis der Wahrnehmung der Rechte eines Endnutzers durch dessen Erben oder durch andere berechtigte Personen, die zur Wahrnehmung der Rechte des Endnutzers befugt sind, nicht entgegensteht.

Im § 7 TTDSG (entspricht grundsätzlich § 95 TKG-alt) erlaubt ein neu eingefügter Absatz 2 für die Identifizierung der KundInnen nun die Nutzung der elektronischen ID-Funktionen, wie sie z.B. mit dem Personalausweis möglich sind. Im § 8 TTDSG (entspricht grundsätzlich § 90 TKG-alt) wird klargestellt, wann eine Telekommunikationsanlage als „zum unbemerkten Abhören oder Aufnehmen eines Bildes bestimmt" ist.

Im § 11 TTDSG, der die Regelungen zum Einzelverbindungsnachweis enthält (entspricht grundsätzlich § 99 TKG-alt), wurden mit den Absätzen 5 und 6 Regelungen eingeführt, die dazu führen, dass sich Anrufe zur anonymen Beratung bei entsprechenden Beratungsstellen nicht in Einzelverbindungsnachweisen erkennen lassen dürfen. Es wird hier auch geregelt, dass die Anschlüsse solcher Beratungsstellen von der Bundesnetzagentur in einer entsprechenden Liste aufzunehmen sind und die Dienstleister diese Liste quartalsweise abzurufen und in ihren Abrechnungsverfahren zu berücksichtigen haben.

2.2.3. TTDSG Teil 3 – Telemediendatenschutz, Endeinrichtungen

Für Teil 3 des TTDSG ist festzustellen, dass im Kapitel 1 vor allem Regelungen des TMG, die durch die DSGVO verdrängt wurden, nicht in das TTDSG übernommen wurden. Die umfangreichen und von DatenschützerInnen berechtigterweise kritisierten Regelungen zur Auskunftser-


Bild: iStock.com/ipopba

teilung an Sicherheitsbehörden des TMG wurden – bis auf wenige redaktionelle Änderungen – 1:1 in die Paragraphen 22 bis 24 des TTDSG übernommen.

Das Kapitel 2 dient nun endlich der Umsetzung der 2009 geänderten Fassung des Art. 5 Abs. 3 der EG-ePrivacy-Richtlinie. So regelt § 26 Abs. 1 TTDSG:

„Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679[6] zu erfolgen."

Abs. 2 enthält die Ausnahmen für technisch notwendige Cookies. § 27 TTDSG ermöglicht die Einführung von *„anerkannten Diensten zur Einwilligungsverwaltung"*. Für deren Anerkennung ist es erforderlich, dass diese Dienste:

„1. nutzerfreundliche und wettbewerbs-konforme Verfahren und technische Anwendungen zur Einholung und Verwaltung der Einwilligung haben,

2. kein wirtschaftliches Eigeninteresse an der Erteilung der Einwilligung und an den verwalteten Daten haben und unabhängig von Unternehmen sind, die ein solches Interesse haben können,

3. die personenbezogenen Daten und die Informationen über die Einwilligungsentscheidungen für keine anderen Zwecke als die Einwilligungsverwaltung verarbeiten und

4. ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglicht und aus dem sich ergibt, dass der Dienst sowohl technisch als auch organisatorisch die rechtlichen Anforderungen an den Datenschutz und die Datensicherheit, die sich insbesondere aus der Verordnung (EU) 2016/679 ergeben, erfüllt".

Die näheren Details für die Anerkennung dieser Dienste sollen in einer Rechtsverordnung, die der Zustimmung des Bundestages und des Bundesrates bedarf, festgelegt werden. Vielleicht weckt dies alte Erinnerungen an den am 22. Mai 2001 in Kraft getretenen damals neuen § 9a des BDSG-alt[7], mit dem ein Datenschutzaudit eingeführt wurde oder besser gesagt: eingeführt werden sollte. Falls nicht: Die Ausgestaltung des Datenschutzaudits sollte in einem gesonderten Gesetz erfolgen. Sie ahnen es vielleicht schon: Dieses besondere Gesetz hat es in den 17 Jahren und drei Tagen, die dieser „§ 9a Datenschutzaudit" galt, leider nie gegeben.

3. Fazit

Das TTDSG ist ein wichtiger und aus Sicht des Autors auch großer Schritt in die richtige Richtung, nicht nur um eine wesentliche, 2009 geänderte Regelung der EG-ePrivacy-Richtlinie endlich umzusetzen, sondern auch, um die bereits zum 25. Mai 2018 fällige Anpassung des TMG an die DSGVO vorzunehmen und auch die bislang manchmal etwas schwierige Abgrenzung, welche der Datenschutzregelungen eigentlich gilt (die DSGVO, die Datenschutzregelung aus dem TKG oder dem TMG als Umsetzung der EG-ePrivacy-Richtlinie) etwas zu vereinfachen.

Inwieweit das TTDSG die Anwendung des Datenschutzrechts im Bereich der Telekommunikation und der Telemedien wirklich erleichtert und ob das TTDSG zur gewünschten Erhöhung der Rechtssicherheit führt, bleibt abzuwarten und wird die Zukunft zeigen.

Zu hoffen ist, dass die Rechtsverordnung zur Einführung von „anerkannten Diensten zur Einwilligungsverwaltung" zeitnah – vielleicht sogar schon vor dem Inkrafttreten des TTDSG – verkündet wird.

1 Richtlinie 2002/58/EG des Europäischen Parlamentes und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation; ABl. L 201 vom 31.7.2002, S. 37) in der Fassung des Artikels 2 der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. L 337 vom 18.12.2009, S. 11)

2 Wortlaut des geänderten Art. 5 Abs. 3: „Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann."

3 Zum Gesetzgebungsverfahren vgl.: https://dip.bundestag.de/vorgang/.../272039 (die Punkte sind Bestandteil der URL)

4 Zum Gesetzgebungsverfahren vgl.: https://dip.bundestag.de/vorgang/.../273898 (die Punkte sind Bestandteil der URL)

5 Vgl.: Hülsmann: Eine Kommentierung des TTDSG mit einer Gegenüberstellung der bisherigen Regelungen aus TKG und TMG, EfWeHa-Verlag, August 2021 – https://efweha.de/TTDSG

6 Das ist die DSGVO

7 „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt." (BGBl 2001 I, Nr. 23, S. 904ff)

Dr. Thilo Weichert

Unabhängige Datenschutzbeauftragte und deren Wirkmacht

Das Rollenbild und die Einflussmöglichkeiten der Datenschutzbeauftragten des Bundes und der Länder haben sich im Laufe der Jahre verändert. Die DANA begleitet diese Veränderungen, ohne bisher ausführlicher und vertiefter den Bedeutungswandel dieser Institutionen und der diese repräsentierenden Personen nachvollzogen zu haben, dem Datenschutzbeauftragte in der sich digitalisierenden Gesellschaft unterworfen sind. Ich verfolge die Diskussion hierüber in Deutschland seit über 30 Jahren in unterschiedlichen Rollen: als Parlamentarier, als Vorsitzender einer NGO, als Publizist und Wissenschaftler, als Mitarbeiter und Leiter einer Aufsichtsbehörde und in jüngster Zeit auch als Unternehmensberater. Bei den Wechseln meiner Perspektive habe ich nie die Seiten gewechselt: Der digitale Grundrechtsschutz stand und steht für mich im Vordergrund.

Der Wandel der Informationstechnik und deren praktischer Einsatz in den letzten vier Jahrzehnten ließen den Grundrechtsschutz mit wachsen, wenn auch nicht in der gleichen Geschwindigkeit. Zwar hat der digitale Grundrechtsschutz seine Erscheinung und seine Wirkweisen verändert. Eine zentrale Institution blieben die unabhängigen Datenschutzbeauftragten, die inzwischen – in der Terminologie der europäischen Datenschutz-Grundverordnung – „Aufsichtsbehörden" (Art. 51 DSGVO) und die diese repräsentierenden Personen – wenig aussagekräftig und bürokratisch – „Mitglied der Aufsichtsbehörde" (Art. 52 Abs. 2, 3 DSGVO) genannt werden.

Gewaltenteilung

Vorab einige Grundsatzüberlegungen: Im 18. Jahrhundert neu war und heute noch richtig ist die Gewaltenteilung Montesquieus, die auf der Idee von „Checks and Balances" basiert. Diese Grundidee hat sich in unserer technisierten und arbeitsteiligen Welt weiter ausdifferenziert: Verwaltung, Justiz und Volksvertretung sind nicht mehr ausreichend, um sich mit ihren Gewalten gegenseitig unter Kontrolle zu halten. Im 19. Jahrhundert kam die unabhängige Presse als „vierte Gewalt" hinzu und hat bis heute ihre Funktion als zivilgesellschaftliches Korrektiv zu den drei staatlichen Gewalten ausgebaut.

Die Digitalisierung und Technisierung aller Bereiche unserer Gesellschaft und die damit verbundene Arbeitsteilung und Erhöhung von Komplexität eröffnen nun die Notwendigkeit einer weiter gehenden Kontrolle von Menschen und Organisationen bei ihrer Techniknutzung. In seinem weitsichtigen Volkszählungsurteil hat das deutsche Bundesverfassungsgericht (BVerfG) Ende 1983 festgestellt, dass die anerkannten Grund- und Freiheitsrechte nicht nur durch materielle, sondern auch durch informationelle Einflussnahme beeinträchtigt werden können und hat aus dem allgemeinen Persönlichkeitsrecht ein „Recht auf informationelle Selbstbestimmung" jedes Menschen abgeleitet. Dieses Recht ist heute als Ausfluss des Privatheitsschutzes in der Menschenrechtskonvention (Art. 8 EMRK) und als Grundrecht auf Datenschutz in der Grundrechtecharta der Europäischen Union (Art. 8 GRCh) in unserem Rechtskreis anerkannt. Im Urteil des BVerfG aus dem Jahr 1983 wird auch schon die Bedeutung unabhängiger Datenschutzbeauftragter für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung hervorgehoben.[1] Von „informationeller Gewaltenteilung" ist die Rede. Und in Art. 8 Abs. 3 Grundrechtecharta heißt es jetzt: „Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Das strukturell unlautere Interesse der Datenverarbeiter

Dahinter steckt folgende richtige Erwägung: Sowohl öffentliche wie private Datenverarbeiter, also Staat und Wirtschaftsunternehmen, nutzen die bei uns zum Einsatz kommenden Informations- und Kommunikationsmittel und bestimmen ihre Einrichtung und Verwendung. Waren dies zunächst Rechenzentren, wurden daraus vernetzte Personal Computer und schließlich eine digitale, internetbasierte Infrastruktur, die in der Praxis viele Gerätschaften des täglichen Lebens, Wirtschaftens und Verwaltens miteinander verbindet und betreibt.

Wer diese Infrastruktur kontrolliert, kontrolliert die Menschen, die an den digitalen Geräten hängen. Die Geräte, insbesondere das Smartphone, bestimmen das Denken und Tun der Menschen immer mehr. Zugleich verlieren die Menschen die Kontrolle über die Geräte und was diese tun. Aus Selbstbestimmung wird Fremdbestimmung. Und dieser Fremdbestimmung bedienen sich Staaten und Unternehmen. Die Volksrepublik China kontrolliert hierüber 1,4 Milliarden Menschen. Facebook kontrolliert 2,7 Mrd. Menschen, die jeden Monat die Dienste des Unternehmens nutzen. Google hat bei Suchmaschinen weltweit einen Marktanteil von über 90% und ist damit das Portal zum Internet für fast alle Menschen. Google dominiert zugleich viele weitere digitale Märkte, z.B. mit seinem Android-Betriebssystem die Nutzung von Smartphones.

Staaten und Wirtschaftsunternehmen haben so eine informationelle Macht erlangt, die sie nicht freiwillig zu teilen bereit sind. Der Einzelne ist hiergegen alleine machtlos. Dies macht unabhängige Datenschutzbeauftragte für den digitalen Grundrechtsschutz der Menschen so wichtig: Sie sollen ein Gegengewicht zur informationellen Macht der Verarbeiter sein, Partei und Sprachrohr der Bürgerinnen und Bürger. Ihre Unabhängigkeit muss doppelt sein, sowohl gegenüber der Regierung wie auch gegenüber der Wirtschaft.[2] Diese

haben in Sachen Datenschutz weitgehend gleichgelagerte Interessen: Sie wollen die Menschen kontrollieren und manipulieren. Sie praktizieren deshalb insofern ohne große Vorbehalte eine für beide Seiten nützliche Symbiose. So in China zwischen der Staatsregierung und Unternehmen wie Tencent, Alibaba oder Baidu oder in den USA zwischen dem Geheimdienst NSA und weiteren Sicherheitsbehörden auf der einen und Google, Amazon, Facebook, Microsoft oder Apple auf der anderen Seite.

Diese Symbiose funktioniert nicht nur in den USA und China, sondern auch in Europa, in Deutschland. Sie besteht zwischen den Großen auf globaler, europäischer und nationaler Ebene, aber auch im Kleinen, in Regionen, Kommunen und Betrieben.

Transparenz, wie sie das Datenschutzrecht einfordert, ist Gift für diese die Menschen kontrollierende Symbiose: Transparenz kann den Betroffenen ihre verlorene Selbstbestimmung zumindest kognitiv zurückgeben. Dafür benötigen sie externe Hilfe; hierin liegt eine Aufgabe der Datenschutzbeauftragten. Zur Selbstbestimmung gehört neben dem Wissen und Wissen-Können das Bestimmen oder zumindest das Mit-Bestimmen. Auch hierzu bedarf es der Unterstützung durch die Datenschutzbeauftragten. Der demokratische Staat ist von der Akzeptanz seiner Bürger abhängig ebenso wie die Wirtschaftsunternehmen von der Akzeptanz ihrer Kunden auf einem freien Markt. Die Datenschutzbeauftragten sollen dafür sorgen, dass das informationelle Machtungleichgewicht zugunsten der Menschen nivelliert wird. Sie sollen den Menschen ihre Selbstbestimmung zurückgeben. Sie sollen dabei zugleich für die in der Demokratie nötige Akzeptanz sorgen.

Soweit die Theorie. Die Praxis ist davon weit entfernt.

Unabhängigkeit und Qualifikation

Es beginnt mit der Auswahl der Datenschutzbeauftragten: Zwar verlangt in der EU die DSGVO, diese sollten „im Wege eines transparenten Verfahrens" ausgewählt werden (Art. 53 Abs. 1 DSGVO). Es ist aber weithin Praxis, dass die Amtsinhaber in den Hinterzimmern der Parlamentsfraktionen ausgeküngelt werden. Dabei war es bisher nicht ungewöhnlich, dass Politiker oder Ministerialbeamte zum Dank für ihre treuen Dienste vor dem Ruhestand mit diesem Prestigeposten belohnt wurden. Vorkenntnisse in Sachen Datenschutz waren keine Voraussetzung. So hatten wir z.B. von 2014 bis 2019 Andrea Voßhoff als Bundesdatenschutzbeauftragte, die kurz zuvor bei der Bundestagswahl als CDU-Kandidatin Frank-Walter Steinmeier (SPD) im Wahlkreis unterlegen war. Ich zitiere aus dem Wikipedia-Eintrag: „Von mehreren Seiten wurde gemutmaßt, dass Voßhoff nach ihrem verpassten Wiedereinzug in den Deutschen Bundestag versorgt werden sollte." Entsprechend war das Ergebnis: „Constanze Kurz, Sprecherin des Chaos Computer Club, bezeichnete die Bilanz … als ‚desaströs'"[3]. Eine Ausschreibung der Stelle der Datenschutzleitung und ein öffentliches Auswahlverfahren sind in Deutschland immer noch die Ausnahme.

Ungenügende Qualifikation sollte qua Gesetz in Zukunft ausgeschlossen sein. Zumindest verlangt die DSGVO seit 2018 „Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten" (Art. 53 Abs. 2 DSGVO).[4]

Wird der Posten von einem verdienten Ministerialbeamten besetzt, kennt dieser zumindest die Verwaltung. Leider ist oft festzustellen, dass die Loslösung von dieser alten Rolle und die Identifikation mit der neuen Aufgabe misslingen. Was Verwaltungsbeamten in Deutschland erfahrungsgemäß fehlt, von einem Datenschutzbeauftragten qua Rolle aber abverlangt wird, ist Konfliktbereitschaft, sowohl gegenüber der Regierung als auch, was angesichts der digitalen Marktmacht wichtig ist, gegenüber Unternehmen. Je mächtiger ein Digitalunternehmen, desto gewaltiger ist die Anwaltsphalanx, die gegenüber einer Datenschutzbehörde in Stellung gebracht wird. Zur Konflikt- muss Entscheidungsbereitschaft treten. So steht die bisherige Bereitschaft offensichtlich illegale Geschäftsmodelle z.B. im Internet zügig zu sanktionieren im umgekehrten Verhältnis zu den Profiten, die die Unternehmen damit erzielen. Zweifellos geht Gründlichkeit der Schnelligkeit bei der Datenschutzkontrolle vor. Es ist aber verblüffend, dass selbst nach drei Jahren DSGVO die vielen offensichtlich illegalen Geschäftsmodelle gerade von großen Unternehmen weitgehend unsanktioniert geblieben sind.

Dafür ist auch ein Webfehler im föderal strukturierten Datenschutz in Europa verantwortlich. In der deutschen Datenschutzkonferenz galt lange Zeit das Einstimmigkeitsprinzip, so zunächst auch in Europa in der Artikel-29-Arbeitsgruppe. Nun ist im Europäischen Datenschutzausschuss eine qualifizierte Mehrheit ausreichend, aber auch notwendig (Art. 65 DSGVO). Meine Erfahrung in 20 Jahren Datenschutzabstimmung in Deutschland war, dass es einigen Kollegen wichtiger war, ihre persönliche Unabhängigkeit zu wahren als den Datenschutz.

David gegen Goliath

Bei aller Unabhängigkeit und selbst bei Zivilcourage der Datenschutzbeauftragten bleibt deren Auseinandersetzung mit Datenverarbeitern in Regierung und Wirtschaft ein Kampf zwischen David und Goliath. Was für David die Steinschleuder war, kann für den Datenschutzbeauftragten kluge Öffentlichkeitsarbeit sein. In einer demokratischen Öffentlichkeit sollten schiere Größe und Geld weniger den Ausschlag geben als Fakten und gute Argumente. Medien sind gierig nach Auseinandersetzungen und dabei gerne bereit, dem David Gehör zu verschaffen. Zwar haben insbesondere Unternehmen immer wieder versucht Datenschutzbeauftragte mit juristischen Drohungen von der Öffentlichkeit fernzuhalten. Doch kann dies nur bedingt erfolgreich sein, wenn Zuständigkeit und Faktizität gewahrt bleiben. Juristische Abwehrkämpfe gegen Fakten werden – zumindest noch in Deutschland – eher zum Bumerang, der letztlich das Unternehmen trifft. In Deutschland gibt es eine detaillierte Rechtsprechung, die öffentliche Stellen wie Datenschutzaufsichtsbehörden dazu ermächtigt Warnungen auszusprechend und Öffentlichkeitsarbeit für die eigene Sache zu machen.[5] Die Gesetze, die Datenschutzbeauftragte zu medialen Interessenvertretern der Bürger machen, könnten aber noch verbessert werden.

Es gibt weitere Verbündete des Davids. Für digitale Bürgerrechte bringen

sich nicht nur amtliche Datenschützer in Stellung, sondern auch Bürgerrechtsorganisationen, Verbraucherschützer und Arbeitnehmervertretungen, also Gewerkschaften und Betriebsräte. Der Nachfolger von Andrea Voßhoff, Ulrich Kelber, diesmal ein einschlägig qualifizierter Informatiker, sucht regelmäßig den Dialog mit Nichtregierungsorganisationen (NGOs). Darüber können Argumente und evtl. auch Kräfte gebündelt werden, ohne dass damit die Unabhängigkeit verloren gehen muss.

Noch fruchtbarer erlebte ich persönlich als Aufsichtsbehörde die Kooperation mit den Verbraucherzentralen. Diese haben das Ohr nahe bei den Betroffenen. Und sie haben – jedenfalls in Deutschland – mit der Verbandsklagebefugnis eine Waffe gegen illegale Geschäftsmodelle im Köcher, die gerade gegen große Datenverarbeiter oft effektiver ist als das Aufsichtsinstrumentarium.[6]

Auch bei den Interessenvertretungen der Beschäftigten hat sich in den letzten Jahren ein starker Wandel vollzogen: Diese sind in Bezug auf Arbeitnehmerüberwachung zumeist stark sensibilisiert und nahe an der Praxis. Ihre Instrumente sind jedoch noch stumpf. Dies könnte sich mit einem Beschäftigtendatenschutzgesetz ändern, wozu in Deutschland gerade erneut eine Diskussion beginnt.[7]

Mehr Befugnisse, mehr Ressourcen, mehr Kontrolle

Vor 40 Jahren waren Datenschutzbeauftragte vor allem „Beauftragte". Eine billige und beliebte Polemik war es lange Zeit, sie als Teil des „Beauftragtenunwesens" zu diffamieren und sie mit den ebenso machtlosen Behinderten- und Gleichstellungsbeauftragten in eine Reihe zu stellen. Datenschutzrechtlich Betroffene sind aber keine diskriminierte Minderheit und kein diskriminiertes Geschlecht. Sie vertreten alle Betroffenen und damit die Gesamtheit.

Die Zeiten des reinen Mahnens über folgenlose Beanstandungen sollten spätestens mit der DSGVO zu Ende sein. Aufsichtsbehörden haben Untersagungs- und spürbare Sanktionsbefugnisse (Art. 58, 83 DSGVO), die sie auch – zunehmend – nutzen. Dabei müssen sie sich ihrer Parteilichkeit bewusst bleiben: Sie sind Partei der Menschen und damit strukturell geborene Gegner von Regierung und Unternehmen, wenn diese die digitalen Grundrechte der Menschen missachten.

Dabei darf der Datenschutz nicht mit kleiner Münze gehandelt werden. Es geht hier nicht nur um den Schutz einer engen Privatsphäre, sondern um Bürgerschutz, Verbraucherschutz, Arbeitnehmerschutz. Es ist in der DSGVO angelegt und sollte auch so praktiziert werden: Datenschutz erfasst als digitaler Grundrechtsschutz den Schutz vor Diskriminierung und den vieler weiterer informationeller Freiheiten. Er hat nicht nur eine individuelle, sondern auch eine kollektive Dimension. Er ist Demokratieschutz, Schutz eines freien Wettbewerbs, Schutz sozialer Rechte. Diese Erkenntnis ist aber leider noch nicht in allen Behördenstuben angekommen.

Für diese in einer digitalisierten Gesellschaft zentrale Aufgabe muss die Datenschutzaufsicht besser ausgestattet werden. Das gewaltige Vollzugsdefizit, mit dem wir auch nach drei Jahren der DSGVO-Geltung immer noch leben müssen, muss dadurch beseitigt werden, dass die Aufsichtsbehörden angemessen Personal und Ressourcen erhalten und nicht allein wegen ihrer Totalüberforderung nur als Feigenblatt fungieren können.

Datenschutzaufsicht als eigenständige Gewalt in einer digitalisierten Gesellschaft benötigt nicht nur Kontrollkompetenzen und Kontrollmacht, sondern muss selbst auch wirksam kontrolliert werden können. Dem dient einerseits die Bindung an Recht und Gesetz sowie die Möglichkeit, wegen Aktionen der Datenschutzaufsicht Rechtsschutz zu erlangen (Art. 78 DSGVO). Die parlamentarische Kontrolle ist zumeist beschränkt auf Informationsrechte sowie die Möglichkeit bei erheblichen Verstößen eine Amtsenthebung des „Mitglieds der Aufsichtsbehörde" zu bewirken (z.B. § 12 Abs. 2 BDSG). Angesichts dieser begrenzten Möglichkeiten ist es von Bedeutung, dass eine Kontrolle durch die Öffentlichkeit, also durch Medien, NGOs und kritische Bürger erfolgt. Insofern ist von Relevanz, dass die Aufsichtstätigkeit in den Anwendungsbereich der Transparenzpflichten gemäß den Informationsfreiheitsgesetzen fällt.

Die Versuchung zur Missachtung der Datenschutzrechte ist angesichts der Digitalisierung aller Lebensbereiche groß. Regierungen und Unternehmen haben ein institutionelles bzw. ein ökonomisches Interesse am Datenmissbrauch. Es ist die demokratische und rechtsstaatliche Aufgabe der Datenschutzaufsichtsbehörden sich dem entgegenzustellen. Die Datenschutzaufsicht gewinnt, wenn sie es schafft Regierung und Unternehmen davor zu bewahren, dass sie der latenten Versuchung zum Datenmissbrauch nachgeben.

1 BVerfG U. v. 15.12.1983 – 1 BvR 209/83 u.a., Rn. 103, 206, NJW 1984, 4422 f., 428.

2 EuGH U. v. 09.03.2010 – C-518/07, NJW 2010, 1266.

3 Dazu auch Appel DANA 1/2019, 27.

4 Zu den rechtlichen Schlussfolgerungen ausführlich Bernhardt/Ruhmann/Schuler/Weichert, Zum Auswahlprozess von Datenschutzbeauftragten als Leitung der Aufsichtsbehörden, 03.02.2017, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_auswahlblfdi6.pdf.

5 DSK AK Grundsatz, 09.11.2020, https://fragdenstaat.de/anfrage/zwischenbericht-des-ak-grundsatz-der-dsk-zu-den-rahmenbedingungen-fur-aufsichtsbehordliche-produktwarnungen/585048/anhang/BerichtAKGrundsatzRahmenbedingungenProduktwarnungen002.pdf; Weichert, DuD 2015, 323-327, 397-401.

6 Dazu ausführlich Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, UKlaG.

7 DANA 3/2020, 183; Schuler/Weichert, Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz, 18.12.2020, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020_beschdsg_final.pdf.

Heinz Alenfelder

E-Government – Daten und Studien

Bild: iStock.com/imaginima

Der Bereich des E-Government ist – so zeigten die Vorrecherchen für dieses Schwerpunktheft – unerwartet groß. Entsprechend ist die Einschränkung auf einschlägige Texte zum Datenschutz nicht einfach und kaum aus dem Stand heraus zu bewältigen. Was tun? Nun, eine Suchmaschine der Wahl (in diesem Fall www.metager.de) und passende Suchbegriffe helfen weiter. Die Ergebnisse kurz gesichtet ergaben dann die folgenden vier Empfehlungen zu Material, das bei der weiteren Beschäftigung mit dem Thema hilfreich sein kann.

- Bereits im Dezember 2018 gab die Bundesdruckerei in Berlin zusammen mit dem Think Tank iRights.Lab die Studie „Zukunft E-Government. Vorschläge für eine bürgerfreundliche und sichere Digitalisierung der Verwaltung" heraus. In dem frei verfügbaren PDF (https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie-Zukunft-E-Government.pdf) werden Umsetzung, Voraussetzungen und Risiken analysiert. Die Studie fordert Bürgerzentrierung; dabei seien „die Möglichkeit einer nachgelagerten Authentifizierung sowie das Prinzip des Single Sign-on von entscheidender Bedeutung".
- Den Stand und die Fortschritte bei der Digitalisierung der Verwaltung aus Sicht der Regierung beschreibt der „Monitor Digitale Verwaltung #5" des Nationalen Kontrollrats, der seinerseits beim Bundeskanzleramt als Beratungsgremium eingesetzt ist (https://www.normenkontrollrat.bund.de/nkr-de/digitalisierung).
- Aktuelle Daten zum Thema liefert die „Initiative D21" mit der seit 2011 jährlich aktualisierten Studie „eGovernment Monitor" (https://initiative21.de/app/uploads/2020/10/egovernment_monitor_2020_onlineausgabe.pdf). In der aktuellen Studie werden Nutzung und Akzeptanz staatlicher Digitalangebote in Deutschland, Österreich und der Schweiz untersucht. Beim Schwerpunkt Corona-Warnapp wird beispielsweise im Monitor für 2020 festgestellt, dass nur 40 % der Deutschen den Datenschutz bei dieser App als gesichert ansehen.
- Die vielfältigen Nutzungsmöglichkeiten der in Städten anfallenden Daten beleuchtet schließlich die im März 2021 vom Deutschen Städtetag veröffentlichte Studie zur kommunalen Datennutzung (https://www.staedtetag.de/files/dst/docs/Publikationen/Weitere-Publikationen/2021/stadt-der-Zukunft-mit-daten-gestalten-studie-2021.pdf). Anhand von Use-Cases (auch für städtische Datenplattformen) wird anschaulich vermittelt, was die Zukunft bringen kann und wie Städte mit Daten verfahren. Bei den Herausforderungen wird auch hier die Skepsis der Bürgerschaft erkannt: „Immer wieder zeigt sich jedoch, dass die Bürgerinnen und Bürger einer Verwendung dieser Daten durch die öffentliche Hand sehr kritisch gegenüberstehen." In diesem Zusammenhang wird auch das „Datenethikkonzept" der Stadt Ulm erwähnt. Vor Open-Data-Lösungen wird insofern gewarnt, als vielfach „Verwaltungsdaten aber aus datenschutzrechtlichen Gründen nicht veröffentlicht werden" können.

Presseerklärung der DVD Bonn, 14.06.2021

Datenschutzvereinigung fordert verlässliche Gütesiegel bei Gesundheitsanwendungen

Anlässlich der Verleihung des BigBrotherAwards 2021 am 11. Juni in der Kategorie „Gesundheit“ an den ärztlichen Terminvereinbarungsservice von Doctolib fordert die Deutsche Vereinigung für Datenschutz e.V. (DVD) eine umgehende Realisierung verlässlicher Datenschutzgütesiegel für Gesundheitsanwendungen. Das DVD-Vorstandsmitglied Thilo Weichert hat in seiner Laudatio wie in einem parallel dazu veröffentlichten Gutachten dargelegt, dass das Serviceangebot von Doctolib gegen grundlegende Datenschutzprinzipien – namentlich Erforderlichkeit, Zweckbindung und Transparenz – verstößt und dass durch dessen Einsatz Ärzte gegen ihre berufliche Schweigepflicht verstoßen. Zigtausende Ärztinnen und Ärzte nehmen das Terminvermittlungsangebot in Anspruch im falschen Vertrauen auf das Versprechen Doctolibs alle Gesetze zu beachten, und im Vertrauen auf die Rechtmäßigkeit bestätigenden Gütesiegel.

Hierzu erklärt der DVD-Vorsitzende Frank Spaeing: „Das Digitalisierungsangebot von Doctolib ist kein Einzelfall. Die Laudatio und das Gutachten von Weichert zeigen, dass Ärzten digitale Anwendungen angedient werden, die das Vertrauensverhältnis zu ihren Patientinnen und Patienten massiv beeinträchtigen. Der Ärzteschaft stehen keine Instrumente zur Verfügung, um die Zuverlässigkeit und Rechtmäßigkeit von durch sie genutzten Digitalangeboten glaubwürdig bestätigt zu bekommen. Der Ärzteschaft selbst fehlt zumeist die fachliche Kompetenz in Sachen Datenschutz. Der Fall Doctolib zeigt, dass es den derzeit angebotenen Gütesiegeln an Nachvollziehbarkeit, Transparenz, Unabhängigkeit und Qualität mangelt. Das Bundesgesundheitsministerium sollte in Kooperation mit der Konferenz der deutschen Datenschutzbeauftragten Kriterien für Digitalangebote bei der Verarbeitung von Gesundheitsdaten definieren, die als verlässlicher Beurteilungsrahmen solcher Angebote herangezogen werden können.“

Der stellvertretende Vorsitzende der DVD, Werner Hülsmann, ergänzt: „Wir haben in der neuen Datenschutz-Grundverordnung einen rechtlichen Rahmen für unabhängige, transparente und rechtskonforme Zertifizierungen. Es ist dringend an der Zeit, diesen Rahmen mit Leben zu füllen, um sicherzustellen, dass digitale Gesundheitsanwendungen den hohen Ansprüchen des Datenschutzes und des Medizinrechts genügen. Die Menschen haben einen Anspruch darauf, dass der Staat die Bedingungen dafür schafft, dass digitale Gesundheitsdienstleistungen die nötige Qualität und Vertraulichkeit aufweisen. Dies gilt sowohl für direkte Services des Staates, etwa bei der Impfterminvermittlung, die in Berlin durch die beim BBA prämierte Firma Doctolib durchgeführt wird, wie auch für entsprechende Services durch nichtstaatliche medizinische Leistungserbringer.“

Die Laudatio auf Doctolib können Sie abrufen unter https://bigbrotherawards.de/2021/gesundheit-doctolib

Das Gutachten zum Datenschutz von Docotlib finden Sie im Internet unter https://www.netzwerk-datenschutzexpertise.de/dokument/datenschutz-im-gesundheitsbereich

Offener Brief an die Deutsche Bundesregierung

Betreff: Cybersicherheitsstrategie für Deutschland 2021

24. Juni 2021

Sehr geehrte Damen und Herren,

die Bundesregierung plant wenige Monate vor der Bundestagswahl die Verabschiedung der „Cybersicherheitsstrategie für Deutschland 2021“. Diese Strategie ist von enormer Bedeutung, weil sie für Jahre die Weichen stellt, wie der Staat die Cybersicherheit in Deutschland gewährleistet, welche Verpflichtungen auf Unternehmen zukommen und welchen Schutz Bürger:innen erhalten.

Die Unterzeichnenden fordern die Bundesregierung dazu auf, die Verabschiedung der Cybersicherheitsstrategie auf die nächste Legislatur zu vertagen oder zumindest die Ausweitung der Befugnisse für die Sicherheitsbehörden ersatzlos zu streichen. Entscheidende Teile der Strategie sind bereits seit langem innerhalb der Bundesregierung hoch umstritten und erhalten massive Kritik durch Vertreter:innen der deutschen Industrie, Wissenschaft und der Zivilgesellschaft. Sollte die Strategie in ihrer jetzigen Form verabschiedet werden, würde dies auf Jahre eine Cybersicherheitspolitik zementieren, für die es keinen ausreichenden Rückhalt

in Wirtschaft und Gesellschaft gibt und deren Maßnahmen wenig Aussicht darauf haben, die IT- und Cybersicherheit in Deutschland zu verbessern. Die Grabenkämpfe um die Ausrichtung der nationalen Cybersicherheitspolitik würden so fortgeführt – zu Lasten der Sicherheit in Deutschland.

Im aktuellen Entwurf der Cybersicherheitsstrategie finden sich eine Reihe an Maßnahmen, die auf Kosten der IT-Sicherheit die Überwachung durch deutsche Sicherheitsbehörden vorantreiben. Dazu gehört zum Beispiel die „Entwicklung technischer und operativer Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation […]", die Umgehung von sicherer Implementierung starker Verschlüsselung (lies: Hintertüren). Es handelt sich hierbei um eine Maßnahme, gegen die sich die deutsche Industrie, Wissenschaft, Zivilgesellschaft und Politik bereits 2019 in einem Offenen Brief ausgesprochen hat, weil sie ausländischen Nachrichtendiensten und Cyberkriminellen mehr nutzen würde als unseren Sicherheitsbehörden. Hinzu kommen die internationale Signalwirkung und die Auswirkungen für besonders schutzbedürftige Bevölkerungsgruppen, die so ein Vorhaben hätte. Weiterhin fordert die Cybersicherheitsstrategie unter anderem Befugnisse zur Aktiven Cyberabwehr; eine Maßnahme, die so umstritten ist, dass sich sogar die aktuelle Bundesregierung selbst dagegen entschieden hat sie voranzutreiben. Es handelt sich hierbei nicht etwa um eine minimale Befugniserweiterung, sondern um ein Legislativvorhaben, welches sehr wahrscheinlich in einer Grundgesetzänderung münden wird. Es ist damit definitiv ein Vorhaben, über dessen Platz in einer Strategie eine neue Bundesregierung entscheiden sollte. Ein weiteres Problemfeld wird durch den geplanten Ausbau der Zentralstelle für Informationstechnik im Sicherheitsbereich (ZITiS) verdeutlicht: fehlende Kontroll-und Schutzmaßnahmen. Es gibt seit Jahren eine Kontroverse darüber, ob die „Hackerbehörde" aufgrund ihrer Aufgaben statt eines Ministererlasses mit einem Errichtungsgesetz auf solide rechtliche Grundlage gestellt werden sollte, auch wenn es rechtlich nicht zwingend notwendig ist. Hierzu findet sich in der Strategie kein Wort. Dieser Punkt zieht sich wie ein roter Faden durch die Strategie. Denn überhaupt fehlt der Strategie die im Koalitionsvertrag versprochene „gleichzeitige und entsprechende Ausweitung der parlamentarischen Kontrolle" sowie die wirksame juristische und administrative Kontrolle, bei Ausweitung der Befugnisse der Sicherheitsbehörden. Dass die Bundes- und Landesregierungen statt dem Ausbau der Überwachungsbefugnisse die Kontroll- und Schutzmaßnahmen stärken müssten, zeigte jüngst der Skandal um die Datensammlung von Politiker:innen durch den Verfassungsschutz in Sachsen. Dies stellt nur eine kleine Auswahl der problematischen Maßnahmen dar, die auf den über 120 Seiten, vor allem im Kapitel 8.3 der Strategie, genannt werden. Erschwerend kommt hinzu, dass die Bundesregierung erstmals Maßnahmen zum Controlling in eine Cybersicherheitsstrategie integrieren möchte. Was an sich eine begrüßenswerte Maßnahme ist, wird dadurch höchst problematisch, dass sich die aktuelle Bundesregierung daran nicht mehr halten muss, sondern es der kommenden Bundesregierung auferlegt. Ein Vertrag zu Lasten Dritter. Im Namen guter Regierungsführung und effektiver IT- und Cybersicherheitspolitik fordern die Unterzeichnenden die Bundesregierung dazu auf alle Maßnahmen, die den Ausbau von Überwachungsbefugnissen statt der Stärkung der IT-Sicherheit zum Ziel haben, ersatzlos zu streichen – im aktuellen Entwurf vom 9. Juni 2021 betrifft das mindestens die Maßnahmen 8.3.1, 8.3.7, 8.3.8, 8.3.9, 8.3.11, 8.3.12, 8.3.14, 8.4.7.

Unterzeichnende Industrie, Organisationen und Verbände: Adacor Hosting GmbH, AG KRITIS, Arbeitskreis Soziale Bewegungen und Polizei des Instituts für Protest-und Bewegungsforschung, AStA TU Berlin, Bits & Bäume Berlin, Boxcryptor, cnetz – Verein für Netzpolitik e.V., Chaos Computer Club e.V., Chaos Computer Club Darmstadt e.V., Cryptomator, D64 – Zentrum für digitalen Fortschritt e.V., Deutsche Vereinigung für Datenschutz e.V., Digitalcourage e.V., Digitale Gesellschaft e.V., eco Verband der Internetwirtschaft e.V., EnjoyVenture Management GmbH, European Society for Digital Sovereignty e.V., Feilner-IT, FlokiNET Ehf, Forschungsnetzwerk Sicherheit & Polizei, Forschungsverbund Naturwissenschaft, Abrüstung und internationale Sicherheit (FONAS) e.V., Forum Informatiker:innen für Frieden und gesellschaftliche Verantwortung e.V., Freiburger Institut für angewandte Sozialwissenschaft e.V., Gesellschaft für Informatik e.V., JP Berlin, Koordinierungskreis des Netzwerks für Gute Arbeit in der Wissenschaft, LOAD e.V. – Verein für liberale Netzpolitik, mail.de GmbH, mailbox.org, mediaTest digital GmbH, Netzwerk Datenschutzexpertise, Niedersachsen.digital e.V., Reporter ohne Grenzen e.V., SaveTheInternet, SerNet GmbH, Stiftung Neue Verantwortung e.V., Tutao GmbH, Unternehmerverbände Niedersachsen e.V., Wikimedia Deutschland e.V., sowie viele unterzeichenende Vertreter:innen aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft.

Pressemitteilung vom 30.06.2021 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)

Länderübergreifende Datenschutz-Prüfung von Medien-Webseiten: Nachbesserungen nötig

Zwischenergebnis der länderübergreifenden Datenschutz-Prüfung: Einwilligungen auf Webseiten von Medienunternehmen sind meist unwirksam – Nachbesserungen sind erforderlich.

Die Datenschutzaufsichtsbehörden mehrerer deutscher Länder haben die Webseiten von Medienunternehmen in Bezug auf den Einsatz von Cookies und die Einbindung von Drittdiensten untersucht. Insgesamt wurden auf Basis eines gemeinsamen Prüfkatalogs 49 Webangebote in 11 Ländern geprüft. Schwerpunkt dabei war das Nutzertracking zu Werbezwecken. Die meisten der geprüften Webseiten entsprechen nicht den rechtlichen Anforderungen für den Einsatz von Cookies und anderen Trackingtechniken. Die Medienunternehmen verstoßen damit gegen das Recht ihrer Nutzerinnen und Nutzer auf Schutz ihrer personenbezogenen Daten. Auch erste Anpassungen bei einigen Verantwortlichen konnten die rechtlichen Defizite bisher nicht vollständig beseitigen.

Für Nutzende besteht durch die Praxis der Medienunternehmen ein erhebliches Risiko. Die im Rahmen des Nutzertrackings erhobenen personenbezogenen Daten werden insbesondere zur Erstellung und Anreicherung umfassender und seitenübergreifender Persönlichkeitsprofile genutzt. Diese werden für das Onlinemarketing, insbesondere im Real Time Bidding-Verfahren (Echtzeitauktion von Werbeplätzen), eingesetzt.

Die beteiligten Landesdatenschutzbehörden wirken auf die Unternehmen in ihrem Zuständigkeitsbereich ein, um datenschutzkonforme Zustände herzustellen. Falls nötig, werden sie aufsichtsbehördliche Maßnahmen ergreifen.

Für die koordinierte Untersuchung verschickten die Behörden aus Baden-Württemberg, Brandenburg, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, dem Saarland, Sachsen und Schleswig-Holstein ab Mitte August 2020 einen gemeinsam erarbeiteten Fragebogen an Medienunternehmen in ihrer jeweiligen Zuständigkeit. Geprüft wurden nicht sämtliche Webseiten der Unternehmen, sondern deren reichweitenstärkste Angebote. Bereits vor Versendung der Fragebögen waren die ausgewählten Webseiten technisch gesichert und analysiert worden. So war ein Abgleich zwischen den Antworten der Medienunternehmen und der tatsächlichen technischen Ausgestaltung der Seiten möglich. Neben den bereits genannten Stellen beteiligte sich auch die Aufsichtsbehörde in Bayern an der inhaltlichen Auswertung der Untersuchungsergebnisse.

Auf den geprüften Medienwebseiten wird eine sehr hohe Anzahl von Cookies und Drittdiensten verwendet, die überwiegend dem Nutzertracking und der Werbefinanzierung dienen. Die Webseiten fragen zwar in der Regel differenzierte Einwilligungen der Nutzenden für die Verwendung von Cookies und Drittdiensten ab. In der Mehrheit der Fälle sind diese Einwilligungen allerdings nicht wirksam.

Im Rahmen der Prüfung wurden vor allem die folgenden Mängel festgestellt:

- Falsche Reihenfolge: Häufig werden einwilligungsbedürftige Drittdienste bereits beim Öffnen der Webseiten eingebunden und Cookies gesetzt – also noch vor der Einwilligungsabfrage.
- Fehlende Informationen: Auf der ersten Ebene der Einwilligungsbanner werden zudem nur unzureichende oder falsche Informationen über das Nutzertracking gegeben.
- Unzureichender Einwilligungsumfang: Selbst wenn Nutzende die Möglichkeit wahrnehmen, bereits auf der ersten Ebene des Einwilligungsbanners alles abzulehnen, bleiben zahlreiche Cookies und Drittdienste aktiv, die eine Einwilligung erfordern.
- Keine einfache Ablehnung: Während bei allen Einwilligungsbannern auf der ersten Ebene eine Schaltfläche vorhanden ist, mit der eine Zustimmung zu sämtlichen Cookies und Drittdiensten erteilt werden kann, fehlt auf dieser Ebene häufig eine ebenso einfache Möglichkeit, das einwilligungsbedürftige Nutzertracking in Gänze abzulehnen oder das Banner ohne Entscheidung schließen zu können.
- Manipulation der Nutzenden: Die Ausgestaltung der Einwilligungsbanner weist zahlreiche Formen des Nudging auf. Das bedeutet, Nutzende werden unterschwellig zur Abgabe einer Einwilligung gedrängt, indem die Schaltfläche für die Zustimmung beispielsweise durch eine farbliche Hervorhebung deutlich auffälliger gestaltet ist als die Schaltfläche zum Ablehnen oder indem die Verweigerung der Einwilligung unnötig verkompliziert wird.

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, sieht Nachbesserungsbedarf bei Webseiten-Angeboten und fordert datenschutzfreundliche Voreinstellungen ein: „Das Prinzip ‚Datenschutz by Default' kommt in unserer Online-Welt immer noch zu kurz. Weil neben den Smartphones künftig auch Haushaltsgeräte und Autos vernetzt sein werden und sich damit die Verarbeitung personenbezogener Daten auf immer mehr Lebensbereiche ausdehnt, ist ein Umdenken nötig: Wir brauchen ein Internet, das ohne ein Datensammeln zum Nutzertracking und zur Profilbildung auskommt."

Von den Jahren 2014 und 2015 sind noch alle Hefte in großer Anzahl verfügbar

Bestellbar für 4 Euro pro Jahrgang oder 6 Euro für beide Jahrgänge *

1/2014 Konzern-Datenschutz
2/2014 Das Internet der Dinge
3/2014 Datenschutz im Reiseverkehr
4/2014 Big Data

1/2015 Mobilität, Telematik und Datenschutz
2/2015 Datenerfassung und Flüchtlinge
3/2015 Rote Linien zur EU-DSGVO
4/2015 Sichere Häfen

* Nur solange der Vorrat reicht

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

BSI-Gesetzesnovelle in Kraft

Der Bundesrat hat am 07.05.2021 die seit Jahren umstrittene Reform des IT-Sicherheitsgesetzes gebilligt, so dass das Gesetz in Kraft treten kann. Damit soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu einer mächtigen Cyberbehörde mit Hackerbefugnissen aufgerüstet werden. Der Innenausschuss des Bundesrats hatte zwar empfohlen, den Vermittlungsausschuss mit dem Bundestag einzuberufen. Er sah die Länder nicht hinreichend in die Bemühungen zum Stärken der Sicherheit von IT-Systemen eingebunden. Im Plenum fand sich dafür aber keine Mehrheit.

Der Bundesrat war nicht zustimmungspflichtig. Über ein Vermittlungsverfahren hätte er das Vorhaben aber verzögern und möglicherweise vor den nahenden Bundestagswahlen noch zu Fall bringen können. Der Bundestag hatte zwei Wochen zuvor das Gesetz beschlossen. In einer Entschließung üben die Länder deutliche Kritik daran, dass der Bund ihrem Appell nach einer stärkeren Kooperation im gesamten Bundesgebiet nicht nachgekommen ist. Sie vermissen u.a. eine Unterrichtungspflicht über schwere Cybersicherheitsvorfälle. Der Bundesrat fordert die Bundesregierung daher auf, eine normative Grundlage zu schaffen, um die nach Landesrecht zuständigen Stellen unverzüglich mit relevanten Informationen zu versorgen. Nur so könnten diese rasch Gefahrenabwehrmaßnahmen ergreifen.

Das BSI soll mit dem Gesetz dank 799 neuer Stellen, die mit 74,24 Mio. € Personalkosten zu Buche schlagen, ein wesentlicher Akteur im Kampf gegen Bot-Netze, vernachlässigte Geräte im Internet der Dinge und Verbreiter von Schadsoftware werden. Es wird befugt Sicherheitslücken an den Schnittstellen von IT-Systemen zu öffentlichen Telekommunikationsnetzen mithilfe von Portscans zu detektieren. Ferner soll es Systeme und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden wie Honeypots und Sinkholes einsetzen dürfen.

Zur Abwehr konkreter erheblicher Gefahren für die IT-Sicherheit kann das BSI gegenüber einem Anbieter von Telekommunikationsdiensten mit mehr als 100.000 Kundinnen und Kunden anordnen, dass dieser „technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm“ an betroffene IT-Systeme verteilt. Die Behörde soll dabei technisch und organisatorisch sicherstellen, dass rechtswidrige Eingriffe in das Computer-Grundrecht unterbleiben.

„Protokolldaten“ einschließlich personenbeziehbarer Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes sowie Parlamentariern anfallen, darf das BSI künftig 12 bis 18 Monate lang speichern und auswerten. Dazu kommen interne „Protokollierungsdaten“ aus den Behörden, also Aufzeichnungen über die IT-Nutzungsform. Zum Schutz von Betroffenen und für Benachrichtigungen wird das Amt ermächtigt bei Anbietern von Telekommunikationsdiensten Bestandsdatenauskünfte einzuholen. Insgesamt soll es so weit verbreitete Trojaner wie Emotet sowie komplexe, oft von Geheimdiensten ausgehende Angriffe besser erkennen können.

Mit der Novelle verknüpft ist eine „Huawei-Klausel“, welche die Hürde für den Ausschluss einzelner Ausrüster vom Netzausbau, etwa für 5G, relativ hoch setzt. Die Bundesregierung soll damit den Einsatz „kritischer Komponenten“ bei „voraussichtlichen Beeinträchtigungen der öffentlichen Sicherheit und Ordnung“ untersagen können. Für solche Bestandteile kommt eine Zertifizierungspflicht, Hersteller müssen eine Garantieerklärung abgeben.

Das Bundesinnenministerium kann einen Bann verhängen. Es muss sich dazu aber „ins Benehmen“ setzen mit den jeweils betroffenen Ressorts wie dem Bundeswirtschaftsministerium und dem Auswärtigen Amt. Ins parallel reformierte Telekommunikationsgesetz hat der Gesetzgeber eine Zertifizierungspflicht für kritische Komponenten in Netzen eingefügt, wenn ein erhöhtes Gefährdungspotenzial besteht. Die für Betreiber kritischer Infrastrukturen (Kritis) geltenden Pflichten Sicherheitspannen zu melden und Mindestschutzstandards einzuhalten, werden auf Unternehmen ausgedehnt, die von besonderem öffentlichem Interesse sind.

Innenminister Horst Seehofer (CSU) sprach angesichts der Entscheidung der Länder von einem „guten Tag für die Cybersicherheit in Deutschland“. Experten hatten bei einer Anhörung dagegen kaum ein gutes Wort für die Initiative gefunden. Sie beanstandeten etwa, dass das BSI Sicherheitslücken offen lassen dürfe und so zum „Handlanger der Sicherheitsbehörden“ werde (Krempl, Bundesrat lässt IT-Sicherheitsgesetz 2.0 zähneknirschend passieren, www.heise.de 08.05.2021, Kurzlink: https://heise.de/-6041685).

Bund

Neue Ermittlungsbefugnisse in der StPO

Der Bundestag hat 11.06.2021 um 00:26 Uhr die Strafprozessordnung (StPO) um Ermittlungsmaßnahmen stark erweitert und den „Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften“ (vgl. DANA 1/2021, 33 f.) – in erweiterter Fassung – mit den Stimmen von CDU/CSU und SPD beschlossen. Die Linke und die Grünen

waren dagegen und forderten ein Moratorium, AfD und FDP enthielten sich.

- Die Cyberbunker-Klausel

So wurde eine sogenannte Cyberbunker-Klausel in das Gesetz eingefügt. Die Polizei darf damit künftig auch zur Nachtzeit Wohnungen, Geschäftsräume und Besitztümer durchsuchen, um Rechner und IT-Systeme im laufenden Zustand zu erwischen, um so unverschlüsselte Daten kopieren sowie beschlagnahmen zu können.

Der ergänzte § 104 StPO lässt fortan Durchsuchungen auch zwischen 21 und 6 Uhr zu, „wenn bestimmte Tatsachen den Verdacht begründen", dass während der Maßnahme „auf ein elektronisches Speichermedium zugegriffen werden wird, das als Beweismittel in Betracht kommt". Weitere Voraussetzung ist, dass andernfalls „die Auswertung des elektronischen Speichermediums, insbesondere in unverschlüsselter Form, aussichtslos oder wesentlich erschwert wäre". Bisher war eine solche Störung der Nachtruhe nur bei Gefahr im Verzug, zur „Verfolgung auf frischer Tat" sowie zum Ergreifen eines entwichenen Gefangenen erlaubt.

CDU/CSU und SPD begründeten ihre entsprechende Änderung am Regierungsentwurf wie folgt: „In Deliktsbereichen, die vorwiegend durch die Nutzung von Computern und Ähnlichem begangen werden, stehen die Ermittlungsbehörden vermehrt vor dem Problem, dass die Täter ihre Datenträger durch den Einsatz von Verschlüsselungstechnologien vor dem Zugriff durch die Strafverfolgungsbehörden schützen". Gelinge die Entschlüsselung nicht und zeige sich der Beschuldigte nicht kooperativ, werde eine „digital-forensische Auswertung" verhindert. Daher sei es von großer Bedeutung, Datenträger möglichst in unverschlüsseltem Zustand zu beschlagnahmen.

Schon jetzt hätten einige Gerichte zwar Beschlüsse für Durchsuchungen in den Nachtstunden erlassen, „weil bestimmte Tätergruppen als sehr nachtaktiv angesehen werden" und Beschuldigte in dieser Zeit am „offenen PC" angetroffen werden sollten. Eine einheitliche Rechtsprechung gebe es dazu aber nicht, sodass das Verfahren nun ausdrücklich geregelt werden solle. Der „besonderen Schutzwürdigkeit der Nachtruhe" werde Rechnung getragen: Die Umstände des Einzelfalls müssten geprüft werden. Zuvor hatte Rheinland-Pfalz sich im Bundesrat für eine solche Klausel starkgemacht. Der Justizminister des Landes, Herbert Mertin (FDP), begründete dies vor allem mit dem Cyberbunker-Verfahren und ähnlichen Situationen. Die Rechner müssten hier bei einem Zugriff laufen, was bei Internet-Kriminellen häufig nachts der Fall sei.

- Kfz-Kennzeichen-Scanning

Auch das Vorhaben der Bundesregierung eine einheitliche Rechtsgrundlage für das Kfz-Kennzeichen-Scanning in der Strafprozessordnung (StPO) zu schaffen, führte im Rechtsausschuss des Deutschen Bundestags zu einem Änderungsantrag von CDU/CSU und SPD. Der Entwurf sieht in § 163g unter anderem vor sogenannte automatisierte Kennzeichenlesesysteme (AKLS) im öffentlichen Verkehrsraum insbesondere zu Fahndungszwecken einzusetzen. Damit sollen „Regelungslücken im Bereich der strafprozessualen Ermittlungsbefugnisse behoben werden". Ohne das Wissen der betroffenen Personen dürfen Kfz-Kennzeichen sowie Ort, Datum, Uhrzeit und Fahrtrichtung automatisch erhoben werden, wenn Anhaltspunkte für eine Straftat von erheblicher Bedeutung vorliegen. Die Daten dürften danach nur vorübergehend und nicht flächendeckend erhoben werden.

Der Bundesrat bat um Prüfung, ob der AKLS-Einsatz auch auf weitere Ermittlungszwecke als die bisher vorgesehenen erweitert werden könne und ob Kfz-Kennzeichen vorübergehend auch ungefiltert gespeichert werden dürfen. Während Sachverständige aus „Sicht der staatsanwaltlichen Praxis" dafür plädiert hatten, empfahl der Rechtssauschuss den ausgeweiteten AKLS-Einsatz nicht, da dieser mit einem intensiven Eingriff in das Recht auf informationelle Selbstbestimmung sämtlicher Verkehrsteilnehmer verbunden wäre: „Ein derart eingriffsintensiver Einsatz von AKLS, der mit einer ungefilterten Speicherung von Kennzeichen sämtlicher Verkehrsteilnehmer verbunden ist", sei bislang im deutschen Recht nicht vorgesehen.

Der Ausschuss empfahl zunächst mit dem künftigen Kfz-Kennzeichenscanning Erfahrungen zu sammeln und diese auszuwerten. Dann könne weiter darüber entschieden werden den AKLS-Einsatz auszuweiten, denn eine „verfassungskonforme Ausgestaltung erscheint denkbar". Allerdings müsse vorher sorgfältig geprüft werden, unter welchen Anordnungs- und Verfahrensvoraussetzungen das passieren müsste, damit der Grundsatz der Verhältnismäßigkeit ausreichend gewahrt werde.

Für die Gefahrenabwehr werden Kfz-Kennzeichen schon seit vielen Jahren anlassbezogen polizeilich in zahlreichen Bundesländern gescannt. Strafprozessual konnte bisher höchstens mit Berufung auf § 100h StPO gescannt werden. Diese Regelung bestimmt aber nur allgemein, dass „auch ohne Wissen der betroffenen Personen außerhalb von Wohnungen Bildaufnahmen hergestellt werden dürfen", um den Aufenthaltsort eines Beschuldigten herauszufinden; damit wird gemäß der Bundesregierung nicht erlaubt Kennzeichen mit Datenbanken abzugleichen. Vor allem in Brandenburg gab und gibt es Widerstand gegen den AKLS-Einsatz. Dort wurden 40 Millionen Kennzeichen gespeichert; eine Verfassungsbeschwerde ist anhängig (DANA 2/2020, 119 f.). Mit dem neuen Gesetz könnte die brandenburgische Praxis legalisiert werden.

- Eingriffe in Kommunikation und Rechner

Mit § 95a StPO werden Ermittler zudem künftig vor allem auf elektronische Beweismittel wie beim Provider gespeicherte E-Mails oder Chats, Inhalte eines Nutzerkontos eines sozialen Netzwerks sowie Daten in der Cloud teils heimlich zugreifen dürfen. Es soll hier vor allem um die Strafverfolgung „in den Bereichen Kinderpornografie, Handel mit Waffen, Drogen, Hehlerware und sonstigen verbotenen Gegenständen sowohl im Internet als auch im sogenannten Darknet" gehen. Experten hatten hier vor einem Teich vol-

ler potenzieller Zufallsfunde und dem gläsernen Bürger gewarnt.

Mit der Novelle wird auch der bereits breite Straftatenkatalog für heimliche Online-Durchsuchungen mit Staatstrojanern und für den großen Lauschangriff weiter ausgedehnt. Entsprechende tiefe Eingriffe in IT-Systeme sind künftig auch bei Delikten aus dem Bereich des Menschenhandels, gewerbs- und bandenmäßigem Computerbetrugs sowie bei Tatbeständen aus dem Außenwirtschafts- und dem Neue-psychoaktive-Stoffe-Gesetz zulässig.

- Und Weiteres mehr

Die Regeln zur Postbeschlagnahme hat der Bundestag ebenfalls verschärft: Strafverfolger dürfen bald auch Auskunft von Postdienstleistern über Sendungen von oder an beschuldigte Personen verlangen können, die bereits ausgeliefert sind oder sich noch nicht beim Serviceanbieter befinden. Dies sei wichtig, „um eine effektive Strafverfolgung auch in Zeiten des vermehrten Online-Versandhandels zu gewährleisten". Gerade der zunehmende Versand krimineller Ware „über das besonders abgeschottete Darknet" könne so besser aufgeklärt werden. (Wilkens, Bundesweites Kfz-Kennzeichen-Scanning: „Verfassungskonforme Ausweitung denkbar", www.heise.de 08.06.2021, Kurzlink: https://heise.de/-6065479; Krempl, StPO: Bundestag erlaubt nächtliche Durchsuchungen und Kennzeichen-Überwachung, www.heise.de 11.06.2021, Kurzlink: https://heise.de/-6068277).

Bund

Gespaltenes Resümee zur Digitalisierung nach 4 Jahren

Die CDU/CSU-Bundestagsfraktion will mit den hierzulande gewachsenen Strukturen der unabhängigen Datenschutzbehörden von Bund und Ländern aufräumen. Die hiesige Organisation der Aufsicht mit 17 Datenschutzbeauftragten sei einer der größten Bremsklötze bei der Digitalisierung, befand der digitalpolitische Sprecher der Schwesternparteien, Tankred Schipanski, am 25.06.2021 im Bundestag während der letzten Plenardebatte vor der Sommerpause im Rahmen der Aussprache zur Digitalagenda der Bundesregierung. Damit einher gehe Innovationsfeindlichkeit. Der Christdemokrat betonte: „Das wird es in Zukunft mit der Union nicht mehr geben." Mit der aktuellen „Innovationsfeindlichkeit" beim Datenschutz werde die CDU/CSU-Fraktion Schluss machen. Das Recht auf informationelle Selbstbestimmung sei „kein Supergrundrecht". Schipanski forderte: „Wir brauchen realitätsnahe Entscheidungen." CDU/CSU drängten daher auf „mehr Zentralisierung" und Beratung sowie auf „verbindliche Auskünfte". Schon zu Beginn der Legislaturperiode hatte Digitalstaatsministerin Dorothee Bär (CSU) kritisiert, dass hierzulande „ein Datenschutz wie im 18. Jahrhundert" herrsche. Sie rieb sich damit vor allem an der „Tendenz zur Kleinstaaterei" bei der Aufsicht (DANA 2/2018, 102 f.). Zentralisierungspläne der Konservativen kamen seitdem aber nicht weit.

Bei der Debatte zog Bär nun ein positives Fazit der Umsetzungsstrategie für die digitale Agenda. Über 90% der angekündigten Schritte seien erledigt oder in Angriff genommen worden. Mit der Datenstrategie sei Schwarz-Rot sogar noch über den Koalitionsvertrag hinausgegangen. Über 300 Verwaltungsdienstleistungen seien mittlerweile digitalisiert, bei der digitalen Bildung „sind wir wahnsinnig weit vorangekommen". Das Cloud-Projekt Gaia-X könnte sich als Exportschlager entpuppen, digitale Identitäten mit einer E-Wallet als „Gamechanger". Die entsprechende Initiative kommt aber nicht aus Berlin, sondern von der EU-Kommission.

Die Opposition nutzte die Diskussion, um mit der Netzpolitik der Koalition abzurechnen. Die Grüne Tabea Rößner beklagte: „Es hakt überall." Die Infrastruktur sei desaströs, „das Ausland belächelt uns über die Funkloch-App". Das schwarz-rote Versagen müssten die Schüler während der Corona-Pandemie vor ihren Bildschirmen ausbaden. Statt die Datenschutz-Grundverordnung (DSGVO) „als Marke zu puschen, diffamieren Sie sie als Innovationsbremse". Die Datenstrategie sei „kalter Kaffee", Potenziale von Open Data blieben ungenutzt. Beim Verschlüsselungsstandort habe die Regierung „brillieren" wollen, gleichzeitig aber immer mehr Zugriffsrechte für die Sicherheitsbehörden geschaffen. Schwachstellen würden nicht geschlossen, Chancen für ökologisch-soziologische Innovationen nicht genutzt.

Die Linke Anke Domscheit-Berg schlug in die gleiche Kerbe: „Ein Überwachungsgesetz nach dem anderen wurde verabschiedet"; der Staatstrojaner sei jetzt auch für alle 19 Geheimdienste da. Viele dieser Initiativen seien wahrscheinlich verfassungswidrig. Zudem könne der Bund nur bei 45 der 575 Verwaltungsdienstleistungen sagen, dass diese wirklich Ende zu Ende online funktionierten. Zudem sei die Bundesrepublik „immer noch ein Land der Funklöcher und lahmen Netze".

Manuel Höferlin (FDP) urteilte, Schwarz-Rot habe „Schotterpisten hinterlassen", bei Breitband befinde sich das Land „immer noch auf dem langsamen Weg". Die Pandemie habe unfreiwillig mehr zur Digitalisierung beigetragen als der Staat, die digitale Verwaltung sei der Running Gag auf Familienfeiern. Ihr Ziel, die Bürgerrechte zu garantieren, habe die Koalition spätestens mit den jüngsten Staatstrojaner-Beschlüssen ad absurdum geführt.

Joana Cotar (AfD) monierte, nur bei der Zensur im Internet und der digitalen Überwachung der Bürger seien die Regierungsfraktionen von CDU/CSU und SPD „ganz groß". Selbst der Wissenschaftliche Beirat des Bundeswirtschaftsministeriums habe festgestellt, dass Deutschland beim Ausbau der digitalen Infrastruktur und Anwendungen hinter vielen anderen OECD-Ländern zurückgefallen sei.

Jens Zimmermann (SPD) hielt der Rechten entgegen: „Wenn ich vom Verfassungsschutz überwacht würde, hätte ich auch Angst davor, wenn der mehr Befugnisse bekommt." In jeder Ecke stünden Bagger und große Rollen mit orangen Kabeln. Es handle sich dabei um Glasfasern, „die überall im Land gerade verbaut werden". Es gebe gar nicht genügend Baukapazitäten, „um sie unter die Erde zu bringen". Die Koalition habe sich in der Tat „sehr viele Gedanken gemacht über Regeln im Internet" und den Kampf gegen Hass und Hetze. Diese dürfe nicht einfach so weiterlau-

fen: „Wir müssen vor allem auf der Seite der Opfer stehen."

Bundesforschungsministerin Anja Karliczek (CDU) erklärte, im Bereich IT-Sicherheit nähmen drei deutsche Kompetenzzentren internationale Spitzenpositionen ein. Die vermeintliche Strategie sei nur eine einfältige Auflistung diverser Vorhaben ohne messbare Erfolgskriterien, schimpfte dagegen Thomas Sattelberger (FDP). Auch bei der Strategie der Regierung für Künstliche Intelligenz (KI) sei „agiles Projektmanagement Fehlanzeige". Bisher gebe es nur für 15% aus den mit dieser Initiative verknüpften 5 Milliarden Verpflichtungen, sodass das Geld hier genauso träge tröpfele wie beim Digitalpakt Schule. Derweil lodere in der Wirtschaft schon der Dachstuhl, „weil eine riesige Expertenlücke klafft".

Die Linke Petra Sitte gab zu bedenken, dass der nötige Wandel nicht allein technologisch gemeistert werden könne. Innovationen müssten eingebettet sein in die Gesellschaft und mehr demokratische Mitsprache. Deutschland verliere mit der „in die Jahre gekommenen Hochglanzbroschüre" an Erneuerungskraft, ergänzte die Grüne Anna Christmann. Auch nachhaltige Sprunginnovationen warteten so trotz einer dafür mittlerweile eingerichteten Behörde wohl noch lange darauf „entfesselt zu werden". Deutschland zehre als Forschungs- und Industrienation von der Substanz, bedauerte Marc Jongen (AfD). Im Bildungsbereich bleibe Deutschland „unterbelichtet"; der Plan der Regierung für einen Ausbau des MINT-Sektors (Mathematik, Informatik, Naturwissenschaften und Technik) sei weitgehend verpufft (Krempl, CDU-Sprecher: Datenschutzstruktur als größte Bremse der Digitalisierung, www.heise.de 26.06.2021, Kurzlink: https://heise.de/-6120303).

Bund

Parlamentarisches Kontrollgremium legt Bericht für 2019 vor

2019 haben das Bundesamt für Verfassungsschutz (BfV), der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) mehr personenbezogene Daten bei Firmen nach dem Terrorismusbekämpfungsgesetz abgefragt als 2018. Dies geht aus dem am 28.06.2021 veröffentlichten Bericht des Parlamentarischen Kontrollgremiums des Bundestags (PKGr) hervor. In 22 Fällen setzten die Sicherheitsbehörden zudem IMSI-Catcher ein, um die Telekommunikation von Verdächtigen effektiver überwachen zu können. Gemäß dem Bericht verlangten die Geheimdienste des Bundes 2019 insgesamt 82-mal Auskunft insbesondere von Telekommunikations- und Telediensteanbietern sowie von Finanzdienstleistern und in geringerem Maße von Luftfahrtunternehmen. 2018 hatten sie in 78 Fällen Daten abgefragt. Der bisherige Höchststand lag hier 2016 bei 114 einschlägigen Ersuchen.

Die Anzahl der individuellen Überwachungsmaßnahmen ist zwar insgesamt von 110 in 2018 auf 104 in 2019 gesunken. Deutlich um gut 40% auf 279 gestiegen ist aber die Zahl der Personen, die 2019 von den Auskunftsverlangen sowie IMSI-Catcher-Einsätzen betroffen waren. 2018 waren es 199 Bürger gewesen. Bei 172 Personen handelte es sich 2019 um Hauptbetroffene, bei 107 um nebenbei erfasste wie Kontaktpersonen oder Angehörige.

Das Gros der Maßnahmen ging im Berichtszeitraum mit 88 auf das Konto des Staatsschutzes, der insgesamt 256 Personen ausspionierte. Der MAD überwachte 14 Personen mit 13 Aktionen, der BND setzte IMSI-Catcher gegen neun Betroffene ein. Schwerpunkt der Verfahren waren laut dem Bericht der „nachrichtendienstliche Bereich" sowie nachrangig die Bereiche Islamismus und Rechtsextremismus. IMSI-Catcher nutzten die Geheimdienste 2019 22-mal, während die Vergleichszahl 2018 mit 32 Einsätzen auf einem Rekordhoch war. Mit dem umstrittenen Instrument, das eine Mobilfunkzelle simuliert und stärker strahlt als Nachbarsender, lässt sich der Standort eines aktiv geschalteten Mobilfunkendgerätes oder die Geräte- und Kartennummer ermitteln und gegebenenfalls Kommunikation überwachen. Der Inlandsgeheimdienst ist auch hier mit 15 Anwendungen und 18 Betroffenen führend.

Zudem führten laut der Statistik 2019 neun der 16 Bundesländer insgesamt 27 Auskunftsersuchen durch, während im Jahr zuvor sechs Länder für 28 Verlangen zuständig waren. Mecklenburg-Vorpommern und Rheinland-Pfalz meldeten dem PKGr je fünf Maßnahmen, gefolgt von Hamburg mit vier und Baden-Württemberg sowie Nordrhein-Westfalen je mit drei. Der frühere Spitzenreiter Bayern kam auf zwei Ersuchen genauso wie Niedersachsen und Thüringen, Brandenburg auf ein Auskunftsverlangen.

Gesetzlich sind die Sicherheitsbehörden eigentlich prinzipiell verpflichtet, die Betroffenen im Nachgang über erfolgte Ausforschungen aufzuklären. Sie informierten 2019 aber nur 89 Personen in diesem Sinne darüber, während es im Jahr zuvor noch 218 waren. Bei 25 konnten sie dies „aus faktischen Gründen" nicht mehr tun, etwa weil der Betroffene verstorben, der Aufenthaltsort nicht bekannt war oder der Anschlussinhaber eine „Fiktivpersonalie ist" beziehungsweise nicht vollständig identifiziert werden konnte.

Bei 224 Personen sahen die Zuständigen von einer Mitteilung „vorerst oder weiterhin ab". Bei 7 Personen lautete der Beschluss von einer Bekanntgabe endgültig abzusehen. Beschwerden zu durchgeführten Maßnahmen gab es 2019 nicht. Ein Verfahren aus den Vorjahren gegen das BfV wurde im Sinne des Klägers vor Gericht entschieden und für erledigt erklärt, ein weiteres war gegen das Amt noch anhängig.

Der PKGr-Bericht zur „strategischen Fernmeldeaufklärung" des BND mit dem Datenstaubsauger für 2019 steht noch aus. Dabei geht es um eine spezielle Form der verdachtsunabhängigen Massenüberwachung, die der Bundestag nach einem einschlägigen Urteil des Bundesverfassungsgerichts im März 2021 erneut grundsätzlich legalisierte. Die zunächst temporär eingeführten Befugnisse aus dem Terrorismusbekämpfungsgesetz entfristete das Parlament im November 2020, um die Aufklärung schwerer Bedrohungen für den demokratischen Rechtsstaat dauerhaft zu gewährleisten (Krempl, Terrorbekämpfung: Deutlich mehr Personen von Geheimdiensten überwacht, www.heise.de 29.06.2021, Kurzlink: https://heise.de/-6122761).

Bund

Verfassungsschutz erhält Staatstrojaner

Das Bundesamt für Verfassungsschutz bekommt mit dem „Gesetz zur Anpassung des Verfassungsschutzrechts“ mehr Befugnisse bei der Kommunikationsüberwachung. Mit Stimmen von Union und SPD hat der Bundestag am 10.06.2021 die Gesetzesnovelle gebilligt. Die Opposition übte heftige Kritik am Einsatz sogenannter Staatstrojaner. Innerhalb der SPD, in der diese Form der Überwachung höchst umstritten ist, hatte die Zustimmung durch die Fraktion zu heftigen Verwerfungen geführt, die bis in die Parteispitze hineinreichten.

Mit den erweiterten Befugnissen will die Bundesregierung einerseits Konsequenzen aus den rechtsextremistisch motivierten Terroranschlägen in Halle und Hanau ziehen. Der Verfassungsschutz soll in die Lage versetzt werden auch verschlüsselte Kommunikation anzapfen zu können. Zudem werden die Hürden für die Beobachtung von Einzelpersonen durch den Verfassungsschutz gesenkt.

Der SPD-Innenpolitiker Uli Grötsch erklärte im Plenum, seine Fraktion habe sich entschieden, bei diesem Gesetz „mutig zu sein“, das Vertrauen in die Sicherheitsbehörden entstamme einem „positiven Staatsverständnis der Sozialdemokratie“. Der CDU-Abgeordnete Michael Brand argumentierte: Der Rechtsstaat müsse sich „angemessen und entschieden zur Wehr setzen, wenn er im Kern angegriffen wird“. Parteikollege Mathias Middelberg führte aus, dass es bei der Novelle um eine „Anpassung an die technischen Verhältnisse“ gehe, maximal wenige Dutzend Fälle der Überwachung im Jahr seien zu erwarten.

Dieser Darstellung widersprachen Politiker von FDP und Grünen. Stephan Thomae, Innenexperte der Liberalen, warf den Befürwortern vor Bürgerrechte „ohne Not preiszugeben“. Konstantin von Notz von den Grünen kritisierte, dass IT-Sicherheitslücken für die Überwachung genutzt würden, die für alle Bürger folgenschwer seien. Zudem äußerte er rechtliche Bedenken am Einsatz der Überwachungssoftware. André Hahn von der Linken nannte die Neuerungen verfassungswidrig. Die AfD stellte ihre Grundsatzkritik am Verfassungsschutz in den Vordergrund.

Die Reform war in der Koalition sehr umstritten. Ein erster Entwurf war den anderen Ministerien bereits im März 2019 zur Stellungnahme übersandt worden. Damals sah er für die Geheimdienste auch noch die Erlaubnis für „Online-Durchsuchungen“ vor, also den verdeckten Zugriff auf Computer, Smartphones und andere IT-Geräte, deren Daten dann ausgelesen werden können. Dieser Passus wurde auf Druck der SPD gestrichen.

Dennoch zog die Zustimmung zu der Reform schwere Konflikte in der Partei nach sich. Parteichefin Saskia Esken hatte sich bereits vor der Abstimmung im Bundestag von der Linie ihrer Fraktion distanziert: „Diese Form der Überwachung ist ein fundamentaler Eingriff in unsere Freiheitsrechte und dazu ein Sicherheitsrisiko für unsere Wirtschaft.“ Sie musste sich aus Teilen der Partei deutliche Kritik anhören, das Gesetzesvorhaben als Vorsitzende der SPD nicht gestoppt zu haben. Der Parteinachwuchs von den Jusos hatte die Abgeordneten aufgefordert, gegen das Gesetz zu stimmen. Mit „Entsetzen“ habe man zur Kenntnis genommen, dass sich die SPD mit der Union auf eine Einigung verständigt habe, heißt es in einem Schreiben aus dem Bundesvorstand. Die Innenexperten aus der Fraktion verteidigten ihrerseits in einem Schreiben an die Fraktionskollegen die Reformen. Die Sicherheitsbehörden müssten „online oder offline“ gegen Verfassungsfeinde vorgehen können. Sie sprachen von einem „schwierigen, aber aus unserer Sicht vertretbaren Kompromiss“. Im Plenum brachte die uneinheitliche Linie die SPD in eine schwierige Lage. Der FDP-Politiker Thomae provozierte die SPD-Abgeordneten mit der Aufforderung in diesem Streit doch lieber ihrer Parteivorsitzenden zu folgen. Die Grünen warfen den Sozialdemokraten vor „komplett umgefallen“ zu sein. Letztlich stimmten 123 der insgesamt 152 SPD-Abgeordneten für die neuen Rechte des Verfassungsschutzes. Esken hatte nicht an der Abstimmung teilgenommen, krankheitsbedingt, wie es aus der Fraktion hieß. Einen solch schweren Konflikt hatte die Partei seit Monaten nicht ausgetragen. Bundesfinanzminister Olaf Scholz hatte mit seiner Nominierung als Kanzlerkandidat der SPD Geschlossenheit eingefordert. Daran hatten sich bis dahin alle gehalten. Selbst die Jusos hatten Scholz ihre Unterstützung im Wahlkampf zugesagt.

Die FDP-Bundestagsabgeordneten Marco Buschmann, Stephan Thomae und Konstantin Kuhle kündigten umgehend an gegen die Zulassung der Staatstrojaner beim Verfassungsschutz Verfassungsbeschwerde zu erheben. Im Vorfeld einer konkreten Gefahr agierende Dienste sollten derart „schwerwiegende und risikoreiche“ Befugnisse nicht erhalten. Der Staatstrojanereinsatz könne zudem „nur funktionieren, wenn Sicherheitslücken auf den digitalen Endgeräten aller Bürgerinnen und Bürger offen gelassen werden. Dies lade auch „Kriminelle und fremde Mächte zu Cyberangriffen, Datenklau, Ransomware-Attacken und Spionage ein“. Die Beschwerdevertretung übernimmt Nikolaos Gazeas, ein Experte für Straf- und Geheimdienstrecht (Szymanski, Die Staatstrojaner kommen, SZ 11.06.2021, 7; Klage gegen Staatstrojaner, Der Spiegel Nr. 26 26.06.2021, 9).

Bund

Fluggastdatenerhebung trotz Pandemie massiv ausgeweitet

Obwohl der Flugverkehr im Corona-Jahr 2020 deutlich abnahm und die Zahl der Passagiere hierzulande laut dem Statistischen Bundesamt um 75% gegenüber 2019 sank, hat das Bundeskriminalamt (BKA) im Jahr 2020 deutlich mehr Fluggastdaten gesammelt. Die zuständige Fluggastdatenzentralstelle beim BKA erfasste insgesamt rund 105 Mio. Datensätze über Passagiere, die in Deutschland starten oder landen. Im Vorjahr waren es circa 78 Mio. gewesen, also rund 35% weniger.

Die unbereinigte Zahl der betroffenen Fluggäste gab das Bundesinnenministerium (BMI) in einer Antwort auf eine Anfrage des Bundestagsabgeordneten Andrej Hunko (Die Linke) für 2020 mit knapp 31 Millionen an, während es 2019 rund 24 Millionen waren. Darin seien

auch Personen enthalten, die mehrfach geflogen sind. Passagiere, die Hin- und Rückflüge oder auch mehrfach Flugreisen unternommen haben, würden auch mehrfach gezählt. Insgesamt starteten oder landeten 2020 auf den 24 größten deutschen Verkehrsflughäfen rund 58 Millionen Fluggäste.

Eindeutige Rückschlüsse auf die Anzahl der betroffenen Einzelpersonen seien, so das BMI, „systembedingt nicht möglich". Dies liege daran, dass Luftfahrtunternehmen pro Flugverbindung und befördertem Gast unterschiedlich viele Passagierdatensätze lieferten und sich aus dieser Gesamtzahl keine genaue Personenstatistik ermitteln lasse. Im ersten Quartal 2020 hatte die BKA-Zentralstelle laut einer anderen Antwort der Bundesregierung auf Anfrage des Abgeordneten Alexander Ulrich knapp 43 Mio. der sogenannten Passenger Name Records (PNR) über gut 12 Millionen Fluggäste erfasst. Sie begründete den Anstieg gegenüber dem Vergleichszeitraum 2019 damals „durch den sukzessiven Aufwuchs des PNR-Systems durch Anbindung weiterer Luftfahrtunternehmen und Flugverbindungen".

Ziel der Rasterfahndung am Himmel ist es gesuchte Straftäter und Verdächtige, insbesondere terroristische Gefährder, zu identifizieren. Nach einem Abgleich mit dem polizeilichen Fahndungsbestand blieben so im Jahr 2020 78.179 „Personenvorgänge" im Filter hängen. Die Zahl der „ausgeleiteten fachlich positiven Personenfahndungstreffer" gibt das BMI mit 5.347 an. Das sind 0,2 Promille der erfassten unbereinigten Passagierzahl. 2019 hatte diese Erfolgsquote nur bei 0,082 Promille gelegen, die Zahl der Vorgänge nach dem Abgleich lag bei 111.588.

Die 5.347 „fachlich positiv" überprüften Treffer habe das BKA, so eine Antwort des Innenministeriums auf eine Anfrage des linken Bundestagsabgeordneten Thomas Nord, an die Bundeszollverwaltung beziehungsweise die Bundespolizei „zur weiteren Bearbeitung" übergeben. Von diesen hätten die zuständigen Sicherheitsbehörden den entsprechenden Fluggast in 3.593 Fällen antreffen können. Auch diese angeblich erhärteten Verdachtsmeldungen sind oft falsch: 2018 und 2019 entpuppten sich fast alle vermeintlichen Treffer letztlich als Irrtümer, nachdem die Beamten die Ergebnisse händisch überprüft hatten.

Die Einreise verweigerten die Ordnungshüter 2020 nur in drei Fällen. 2.352-mal ging es um Aufenthaltsermittlungen. Gegen 460 Personen lag ein Ersuchen zur Festnahme vor. Etwa ebenso viele ausfindig gemachte Personen (457) waren in den Polizeisystemen zur polizeilichen Beobachtung für „verdeckte Kontrollen" ausgeschrieben. Die fahndende Behörde wird dabei heimlich über den Reiseweg und potenzielle Begleiter von Gesuchten informiert. Rund 10% (321) der fachlichen Treffer führten zu gezielten offenen Kontrollen und gegebenenfalls Durchsuchungen.

Gemäß einer Antwort des BMI auf eine Anfrage der Linken-Abgeordneten Ingrid Remmers wurden 2020 zudem 348 Ersuchen von Fluggastdatenzentralstellen anderer EU-Mitgliedstaaten an das deutsche Pendant beim BKA gerichtet. Im gleichen Zeitraum habe die hiesige Zentralstelle insgesamt 277 Anfragen an den EU-Verbund gestellt. Im Jahr 2020 hatte es ferner 1.720 inländische Rechercheersuchen gegeben.

Zu den PNR gehört eine Vielzahl sensibler Informationen, die vom Geburtsdatum über die Namen der Begleitpersonen, E-Mail-Adressen, eventuelle Vielfliegernummern und die zum Kauf des Fluges verwendeten Zahlungsmittel bis hin zu einem nicht näher definierten Freitextfeld reichen. Hierzulande laufen diverse Klagen gegen die damit durchgeführte Rasterfahndung, mit denen sich inzwischen der Europäische Gerichtshof beschäftigt. Mit den Antworten sieht Hunko die Kritik der Linken an der „EU-Vorratsdatenspeicherung der Fluggastdaten" bestätigt: Nach und nach würden mehr Fluglinien an das System angeschlossen. Das erklärte die Zunahme von Passagieren, die ins Raster gerieten – „obwohl die Flüge im Corona-Jahr drastisch heruntergefahren wurden". Dass im Jahr 2020 weniger „Personenvorgänge nach Abgleich mit polizeilichem Fahndungsbestand" übrig geblieben seien, könnte laut dem Abgeordneten daran liegen, „dass das BKA endlich gelernt hat das Programm richtig einzustellen". Denkbar sei auch, dass „die Airlines und Reisebüros die Rechtschreibung der Namen besser einhalten". Ausschlaggebend sei aber die Zahl derer, die dann polizeilich überprüft werden – „und die ist trotz brachliegender ziviler Luftfahrt in 2020 auffällig hoch". Er gehe deshalb davon aus, „dass es sich bei einer Vielzahl davon um falsche Treffer handelt" (Krempl, Trotz Lockdown: Bundeskriminalamt hat 2020 deutlich mehr Fluggastdaten erfasst, www.heise.de 13.06.2021, Kurzlink: https://heise.de/-6069495)

Bund

Kelber an Regierung: Facebook-Fanpages abschalten

Der Bundesdatenschutzbeauftragte Ulrich Kelber hat Ende Juni 2021 in einem Brief die Bundesregierung und die obersten Bundesbehörden aufgefordert, ihre Facebook-Seiten bis Ende des Jahres abzuschalten. Ein datenschutzkonformer Betrieb einer „Facebook-Fanpage" sei nicht möglich. Nur neue Zugeständnisse von Facebook könnten den Weiterbetrieb ermöglichen.

Der Datenschützer hatte zuvor im Mai die Forderung nach einer Schließung der Facebook-Seiten in einem Rundschreiben an denselben Verteiler begründet. Danach hatte das Presse- und Informationsamt der Bundesregierung mit Facebook über die Datenschutzbedenken der Behörde gesprochen. Kelber schrieb nun, Facebook habe leider auch dem Presseamt nur das öffentlich bekannte „Addendum" von Oktober 2019 übersandt. Diese Vereinbarung, das „Page Controller Addendum" sieht vor, dass sich Seitenbetreiber und Facebook die Verantwortung der Seiten teilen. Alle relevanten Pflichten für den eingeforderten Datenschutz lägen demnach bei Facebook. Kelber hält das „Addendum" für unzureichend, um die Datenschutz-Bestimmungen zu erfüllen: „Dies zeigt aus meiner Sicht, dass Facebook zu keinen Änderungen an seiner Datenverarbeitung bereit ist." Die grüne Bundestagsfraktion hat vor dem Landgericht Hamburg eine Klage wegen des rechtlich unzureichenden Addendums eingereicht.

Die Ressorts und deren Geschäftsbereiche, die eigene Facebook-Seiten betreiben, können, so Kelber, ihrer Re-

chenschaftspflicht gemäß der europäischen Datenschutz-Grundverordnung (DSGVO) nicht nachkommen. „Ein längeres Abwarten ist mir angesichts der fortdauernden Verletzung des Schutzes personenbezogener Daten der Nutzerinnen und Nutzer nicht möglich. Sofern Sie eine Fanpage betreiben, empfehle ich Ihnen daher nachdrücklich, diese bis Ende diesen Jahres abzuschalten."

Mit einem Abschalten der Facebook-Seiten könnte die Bundesregierung erheblich an Reichweite verlieren. Die zentrale Seite der Bundesregierung hat auf Facebook 870.000 Fans und über eine Million Abonnenten. Ohne eigene Seiten können Ministerien und Behörden auch kaum auf kritische Bemerkungen reagieren, die auf der Plattform verbreitet werden (Behörden sollen Facebook verlassen, www.tagesschau.de 28.06.2021).

Bund

BfDI prüft Stasi-Unterlagenherausgabe zu Journalisten an die Presse

Die Behörde des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) Ulrich Kelber hat ein Verfahren gegen die dann noch existierende Behörde des Bundesbeauftragten für die Stasi-Unterlagen (BStU) wegen der Herausgabe von tausenden Seiten mit Stasi-Informationen über Journalisten und Gewerkschafter eröffnet. Gemäß Presserecherchen sollen Mitarbeiter der Stasi-Unterlagenbehörde Redaktionen dabei geholfen haben Mitglieder und Funktionäre der größten deutschen Journalisten-Gewerkschaft, des Deutsche Journalisten-Verbands (DJV), „auszuforschen". Zu diesem Ergebnis war eine interne Prüfung der Stasi-Unterlagenbehörde selbst gekommen. Nach kurzfristiger Zusendung eines Fragenkatalogs antwortete Jahn und bestätigte die Vorwürfe und Recherchen, was den BfDI aber offenbar nicht zufriedenstellte.

Eine Sprecherin Kelbers erklärte, dass die Behörde von Roland Jahn um Übermittlung ergänzender Unterlagen gebeten wurde, „um sich selbst ein Bild vom Antragsgegenstand und den durchgeführten Recherchen machen zu können. Im Anschluss hieran wird zu prüfen sein, ob die bisher durch BStU getroffenen Maßnahmen ausreichend sind, oder weiterer Handlungsbedarf besteht, der erforderlichenfalls auch mit aufsichtsrechtlichen Maßnahmen durchzusetzen wäre." Dem BfDI stünden in diesem Falle umfangreiche Mittel zur Verfügung. Neben Anweisungen kann er auch Beanstandungen oder Verwarnungen aussprechen und sogar Geldbußen verhängen – auch gegen andere Behörden.

Grundlage für die eingeleitete Prüfung waren Hinweise darauf, dass Medienanträge einiger weniger Redaktionen in der Stasi-Unterlagenbehörde auch dann bearbeitet wurden, wenn sie erkennbar unzulässig waren. In einem konkreten Fall war demnach ein unzulässiger Medienantrag der „Bild"-Zeitung wie ein zulässiger Antrag behandelt worden. Er hatte zunächst 20 Personen umfasst, war allerdings immer und immer wieder erweitert worden, sogar durch den Sachbearbeiter der Behörde selbst, so dass er am Ende 164 Personen umfasst habe, zu denen in der Behörde dann Unterlagen durchforstet wurden, darunter solche zu Ehepartnern, Eltern oder Kindern.

Am Ende seien rund 1.000 Seiten Unterlagen mit teils privaten Informationen aus der Stasi-Unterlagenbehörde herausgegeben worden. Auch zur Zusammenarbeit der Behörde mit einer Reporterin des rbb stehen Vorwürfe im Raum. Darüber hinaus wurde offenbar eine Rede, die der Vorsitzende des DJV Berlin 2015 auf einem Verbandstag gehalten hatte, in der BStU als Tonaufzeichnung und Teil-Abschrift gespeichert und ausgewertet; die Rede war nicht öffentlich und hätte nicht aufgezeichnet werden dürfen. Als der Betroffene Auskunft darüber erhalten wollte, wer Unterlagen über ihn abgefragt bzw. erhalten hat, hatte sich der Bundesbeauftragte Roland Jahn persönlich von einer privaten Mailadresse eingeschaltet, um dies zu verhindern. Verwaltungsrechtler Cord Heinichen, der den Betroffenen vertritt, kritisierte: „Es ist nicht die Aufgabe der Behörde, rechtswidrig zustande gekommene Tonaufnahmen in den Datenbestand aufzunehmen. Das ist ja Stasi 2.0".

Unmittelbar nachdem die Vorwürfe veröffentlicht worden waren, erklärte die Stasi-Unterlagenbehörde gegenüber „Bild", die Herausgabe der mehr als 1.000 Seiten sei „rechtskonform" gewesen und widersprach damit ihrem eigenen internen Gutachten. Zahlreiche journalistische Nachfragen wurden danach durch die Behörde nicht mehr beantwortet, die Pressesprecherin war telefonisch nicht erreichbar, Rückrufbitten blieben unbeantwortet.

Die Sprecherin Kelbers teilte mit, dass in der BStU-Stellungnahme erklärt werde, die Vorgänge seien Gegenstand einer internen Prüfung gewesen, die zu dem Ergebnis gekommen sei, dass sowohl der Antrag als auch die Bearbeitung in der Behörde rechtswidrig gewesen seien und der Vorgang „damit eine unzulässige Gruppenabfrage darstellte". Von einer Rückforderung der Unterlagen von dem Antragsteller sei damals abgesehen worden. Innerhalb der BStU habe man jetzt jedoch „aufgrund der aktuellen Debatte" nochmals auf die geltenden Richtlinien und Anforderungen des Datenschutzes hingewiesen.

Der Deutsche Journalistenverband (DJV) schaltete sich ein, nachdem die Vorgänge bekannt wurden. Der Bundesvorsitzende Frank Überall schrieb am 24.04.2021 an Kulturstaatsministerin Monika Grütters, die die Dienstaufsicht über die Stasi-Unterlagenbehörde innehat, sprach von einer „Aktenaffäre" und einem „Generalverdacht" gegen DJV-Mitglieder und forderte umfassende Aufklärung. Auf Nachfrage wurde mitgeteilt, Grütters habe das Schreiben zur Beantwortung an Roland Jahn weitergegeben.

In einem offenen Brief an den DJV Berlin JVBB, dem viele Betroffenen angehören oder angehörten, kritisieren diese den Landesverband scharf, weil der sich, anders als der Bundesvorstand, bislang öffentlich nicht zu den Ausforschungen seiner Mitglieder geäußert habe: „Wir erwarten vom Vorstand Maßnahmen zu ergreifen die Rechte seiner Mitglieder durchzusetzen. Dazu gehören Beschwerden beim Landesdatenschutzbeauftragten Berlin und beim Kultursenator, ebenso bei der Intendanz und Chefredaktion des rbb sowie bei der Verlagsgeschäftsführung des Springer-Verlags und der Chefredaktion der Bild-Zeitung." Sie forderten persönlichen Rechtsschutz ein.

Der Chefredakteur des rbb, David Biesinger, wies die Vorwürfe, dass der Sender fast 50 Funktionäre des damaligen DJV Berlin abgefragt habe, zurück und erklärte, dass die interne Prüfung in der Stasi-Unterlagenbehörde keine Anträge des rbb zum Gegenstand gehabt habe. Es habe sich für den rbb um eine „eine rechtmäßige und gerechtfertigte Recherche" gehandelt.

Die Auseinandersetzung überschattet das Ende der Amtszeit von Roland Jahn, der Mitte Juni 2021 nach mehr als zehn Jahren in den Ruhestand ging (DANA 2/2021, 107 ff.). Den Bundesbeauftragten für die Stasi-Unterlagen löst ein Bundesbeauftragter für die Opfer der SED-Diktatur beim Deutschen Bundestag ab. Die Stasi-Unterlagenbehörde wird ins Bundesarchiv überführt. Rund 900 Mitarbeiter arbeiten im Bundesarchiv, rund 1.300 in der Stasi-Unterlagenbehörde (Engert, Nach „Ausforschung" von Journalisten: Datenschutz-Verfahren gegen Stasi-Unterlagenbehörde, uebermedien.de/59691/ 13.05.2021).

Baden-Württemberg

Brink gegen Microsoft 365 in Schulen

Das Programmpaket Microsoft 365 sollte nach Ansicht des dortigen Landesbeauftragten für den Datenschutz (LfDI) Stefan Brink nicht an Schulen in Baden-Württemberg verwendet werden. Es gebe inakzeptabel hohe datenschutzrechtliche Risiken.

Das baden-württembergische Kultusministerium wollte Microsoft 365 als Teil der Bildungsplattform für Schulen in einer speziell konfigurierten Version zur Verfügung stellen. Vorher sollte Brink in einem Pilotprojekt, das an einigen Schulen stattfand, von Mitte Januar bis Ende März 2021 beratend tätig werden; dafür unterzog er die Software einem Praxistest in einem eigens vom Parlament finanzierten Prüflabor. Brinks Behörde stellte dabei fest, dass die Schulen keine vollständige Kontrolle über das Gesamtsystem und den Auftragsverarbeiter in den USA haben. Sie könnten nicht ausreichend nachvollziehen, welche personenbezogenen Daten wie und zu welchen Zwecken verarbeitet werden. Auch könnten sie nicht nachweisen, dass die Verarbeitung auf das notwendige Minimum reduziert ist: „All das müssten sie aber, um ihrer Rechenschaftspflicht aus Artikel 5 Absatz 2 DSGVO gerecht zu werden."

Für Übermittlungen persönlicher Daten an Microsoft, die teilweise auch in Regionen außerhalb der EU gehen, ist nach Ansicht des LfDI keine Rechtsgrundlage erkennbar: „Das gilt insbesondere auch für internationale Datenflüsse im Lichte des Schrems-II-Urteils des Europäischen Gerichtshofs aus dem Jahr 2020." Brink hat nach eigenen Angaben geprüft, ob die Minimierung der Risiken der Microsoft-Software, die das Kultusministerium in der Datenschutz-Folgenabschätzung im Oktober 2020 vorschlug, umgesetzt wurde und ausreichend ist. Auch schaute der Datenschützer nach, welche Datenflüsse im Pilotbetrieb messbar stattfanden. Dabei ging es besonders darum, ob unerwünschte oder nicht angeforderte Datenverarbeitungen – beispielsweise von Telemetrie- oder Diagnosedaten – erkennbar waren und ob Microsoft personenbezogene Daten von Lehrern und Schülern verarbeitet. Wichtig war Brink dabei auch, ob Daten in Drittstaaten außerhalb des Geltungsbereichs der DSGVO fließen und ob der Zugriff durch eine sichere verschlüsselte Kommunikation eingeschränkt werden konnte.

Brink: „Wenngleich die Prüfungen aufgrund des Umfangs und Weiterentwicklung der Dienste nicht abschließend sein konnten, so waren deren Ergebnisse doch hinreichend klar, um eine Empfehlung an das Kultusministerium zu richten." Der Staat habe eine Garantenstellung für die in der Regel minderjährigen Schülerinnen und Schüler. Diese unterlägen zudem der staatlichen Schulpflicht und könnten daher der Verwendung ihrer persönlichen Daten nicht ausweichen. Es könne nicht komplett ausgeschlossen werden, dass Microsoft 365 in anderer Modifikation in Schulen rechtskonform einsetzbar sei. Es sei „in den vergangenen Monaten auch nach intensiver Zusammenarbeit und mit hohem Personaleinsatz aber nicht gelungen, eine solche Lösung zu finden". Daher erscheine es mehr als fraglich, ob es den für die Datenverarbeitungen verantwortlichen Schulen und dem Kultusministerium gelingen kann die getesteten Produkte rechtssicher zu nutzen.

Eine Bildungsplattform hat für Brink durchaus weiter Zukunft. Sie könne beispielsweise aus unterschiedlichen Tools wie zum Beispiel Big Blue Button und Moodle bestehen, die schon intensiv von den Schulen in Baden-Württemberg genutzt würden. Diese würden vom Land selbst betrieben; daher lägen hier nicht die Risiken vor, die sich im Test mit Microsoft 365 ergeben hätten (Wilkens, Microsoft 365 an Schulen: Baden-Württembergs Datenschutzbeauftragter rät ab, www.heise.de 07.05.2021, Kurzlink: https://heise.de/-6041379).

Bayern

Opposition hält überarbeiteten Polizeigesetzentwurf für verfassungswidrig

Das Polizeiaufgabengesetz (PAG) ist wohl das umstrittenste bayerische Gesetz im vergangenen Jahrzehnt; es hatte 2018 viel Protest ausgelöst (DANA 1/2018, 11 ff., 39. 3/2018, 149 f., 4/2018, 198 f.); eine geplante Novelle löst das Problem offenbar nur begrenzt. Zehntausende hatten sich im Frühjahr 2018 landesweit an Protesten gegen das Gesetz beteiligt. Sie argumentierten u.a., dass durch das PAG und neue Befugnisse der Polizei die Freiheit der Bürger beschränkt werde – vor allem durch den Begriff der „drohenden Gefahr" und Regeln zu einem präventiven Gewahrsam.

Ministerpräsident Markus Söder und seine CSU hatten sich – mit Blick auf die Landtagswahl im Herbst 2018 und aus Furcht vor einem Erfolg der AfD – auch in der Migrationspolitik schärfer positioniert. Aus den Bewegungen „No PAG" und „Ausgehetzt" entstand eine brisante Melange. Schnell erkannte Söder, dass er an das Gesetz noch mal ran muss, und berief eine Kommission, deren Ergebnisse mit der aktuellen Novelle jetzt konkret Gesetz werden sollen. Am 24.02.2021 brachten die Regierungsfraktionen eine PAG-Reform in erster Lesung in den Landtag ein als „entschärftes und dennoch schlagkräftiges Gesetz". Am Ende werden Gerichte darüber entscheiden müssen, da mehrere Klagen dazu laufen.

Die Kommission bestätigte die grundsätzliche Verfassungsmäßigkeit des Gesetzes. Sie bot allerdings ein Bündel an Änderungsvorschlägen auf. Den Vorsitz führte Karl Huber, ehemaliger Präsident des Bayerischen Verfassungsgerichtshofs. Ihr gehörten u.a. auch der Landesdatenschutzbeauftragte Thomas Petri sowie Professoren an. Auf Basis dieser Ergebnisse haben CSU und Freie Wähler ihren Entwurf erarbeitet und im Dezember 2020 erstmals präsentiert.

Mit der Novelle will Innenminister Joachim Herrmann (CSU) „die Bürgerrechte stärken" durch „noch mehr Transparenz". Gleichzeitig sei sichergestellt, dass die Polizei weiterhin „hocheffektiv eingreifen" könne, um die Bürger vor Gefahren zu schützen. Kernpunkte der Reform: Die Dauer des Präventivgewahrsams wird auf maximal einen Monat verkürzt, kann dann erneut einmal verlängert werden; bei längerem Gewahrsam wird ein Anwalt von Amts wegen beigeordnet. Bei der Vorbeugehaft im gültigen Gesetz fehlen Rechte, die konkret Tatverdächtige oder Angeklagte automatisch haben. Daten aus dem Ministerium zeigen, dass die Maßnahme bisher in einigen Dutzend Fällen angewendet wurde, in der Regel bei Personen, die eine Gefahr für Leib und Leben darstellten. So hatte ein Mann angekündigt im Fall der Ablehnung seines Asylantrages seine Familie zu töten. Exakte Zahlen fehlen, das Ministerium verfügt über keine automatische Erfassung.

An vielen Stellen des PAG soll ein Richtervorbehalt eingebaut werden, etwa bei gewissen DNA-Analysen oder beim Einsatz von „Bodycams" in Wohnungen. Der Begriff der drohenden Gefahr, bei der die Polizei quasi schon mit vollem Programm handeln darf und der zu einer Herabsetzung der Eingriffsschwelle führt, wird präziser definiert. Sie soll nur noch bei Gefahr für Leib und Leben gelten. Im Regelfall ist die „konkrete Gefahr" Anlass von Einsätzen: also konkrete Tatsachen, die befürchten lassen, dass „ein geschütztes Rechtsgut zu Schaden kommt". Freie-Wähler-Fraktionschef Florian Streibl meinte bei der Präsentation des Entwurfs, dadurch eröffne sich eine „Spielwiese für Juristen".

Der Richtervorbehalt, der in der Novelle so häufig auftaucht, gilt auch für das Gesetz selbst. Das Bündnis „No PAG" teilte mit, es halte an seiner Klage beim Bundesverfassungsgericht fest. „Unverhältnismäßige und weit ins Gefahrenvorfeld reichende Befugnisse" blieben bestehen. Die SPD-Fraktion klagt ebenfalls in Karlsruhe und hält eine Normenkontrollklage am Verfassungsgerichtshof aufrecht. SPD-Fraktionschef Horst Arnold sieht die Novelle als „Kosmetik", ein „verfehlter Begriff wie jener der drohenden Gefahr werde nicht besser, wenn man ihn einfach neu definiert". Das Gesetz sei über die Jahre zu einer „unrühmlichen Never-ending-Story" geworden. Der aktuelle Entwurf sei „abermals missglückt". Der Begriff der „drohenden Gefahr" ist für Arnold „ein Affront gegen unbescholtene Bürgerinnen und Bürger". Arnold beruft sich bei seiner Beurteilung auch auf Ergebnisse einer Expertenanhörung im Landtag. Ebenso wenig ist eine Klage der Grünen vom Tisch. Fraktionschefin Katharina Schulze sagte: „Die Entschärfungen sind leider nicht der Einsicht der Staatsregierung geschuldet, sondern auf konstante Kritik durch uns, Kommission und Zivilgesellschaft zurückzuführen." Es bleibe „der Webfehler des Gesetzes": die niedrige Eingriffsschwelle, die drohende Gefahr. Die CSU könne nun im Gesetzgebungsverfahren gerne „konstruktive Kritik" aufnehmen (SPD: Polizeigesetz ist verfassungswidrig, SZ 28.05.2021, 28; Osel, Entschärft, aber weiter umstritten, www.sueddeutsche.de 24.02.2021).

Berlin

Massenhafte Zugriffsmöglichkeit auf gesperrte Meldedaten

Bei der Aufklärung der Serie von 72 rechtsextremen Straftaten kommt die Polizei kaum weiter. Externe Sonderermittler durchforsteten die Akten von Staatsanwaltschaft, Polizei und Verfassungsschutz nach Hinweisen auf rechtsextreme Netzwerke in der Berliner Polizei. Sie wollten auch wissen, ob aus rechtsextremen Motiven heraus Ermittlungen behindert wurden. Für beides fanden sie keine Belege. Zu klären war auch, ob aus Berliner Polizeicomputern – teils gesperrte – Meldeadressen von Opfern abgefragt und an Neonazis gegeben wurden. Auch hier fanden sich keine Hinweise.

Dafür kamen die Ermittler zu einer anderen Erkenntnis: Außerhalb der Polizei können etwa eintausend Mitarbeiter der anderen Verwaltungen auf Adressen des Einwohnerwesens beim Landesamt für Bürger- und Ordnungsangelegenheiten zugreifen, u.a. auch auf Adressen, die gesperrt sind, etwa weil die Personen bedroht werden. Für SPD-Innensenator Andreas Geisel, der die Aufsicht über die Verwaltungsorganisation und das Melderecht hat, war dieses Ausmaß gemäß eigenen Angaben bisher nicht bekannt. Auch die Datenschutzbeauftragte des Landes hatte dieses Problem nicht allzu sehr beschäftigt. Routinemäßige Kontrollen zu solchen Abfragen führt sie laut Sonderermittlern nur bei der Polizei durch.

Anfang Mai 2021 wurde der mutmaßliche Schreiber der „NSU 2.0"-Drohbriefe in Berlin verhaftet. Die Strafverfolger rätselten, ob er Helfer bei der Polizei hatte, die ihn mit den teils gesperrten Privatadressen seiner Adressaten versorgten. Viel wahrscheinlicher ist, dass seine Helfer an einem der unzähligen Verwaltungscomputer saßen. Spekuliert wird darüber, dass auch andere Extremisten und wohl auch Kriminelle aus Berlins Verwaltung mit sensiblen Daten versorgt werden – vielleicht aus Geschäftszimmern der Justiz, Bürger- oder Jugendämter (Kopietz, 1000 Mitarbeiter in Berlins Behörden kommen an gesperrte Adressen - ein Skandal, www.berliner-zeitung.de 31.05.2021).

Berlin

Mitarbeiterbeschwerde gegen TikTok

Teile der Belegschaft der Digitalplattform TikTok in Deutschland haben sich mit einer Datenschutzbeschwerde an die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) gewendet. Sie wurden demnach im Homeoffice angehalten Firmen-Apps mit weit reichenden Zugriffsrechten auf ihre privaten Handys zu laden. Die BlnBDI Maja Smolczyk erklärte dazu: „Für

die datenschutzkonforme Nutzung privater Endgeräte zu beruflichen Zwecken gelten hohe technische und rechtliche Hürden.“ TikTok erklärte, man „setze sich sehr für den Datenschutz unserer Mitarbeiter ein“. Das „derzeitige Verfahren“ sehe „nicht vor, dass Apps auf die persönlichen Mobiltelefone der Mitarbeiter heruntergeladen werden.“ Die BlnBDI prüft, ob der Vorgang eine internationale Dimension hat. Die Europazentrale des chinesischen TikTok-Mutterkonzerns sitzt in Dublin/Irland. Sollte sich diese im Verfahren als verantwortlich erweisen, werde man den Fall an die irische Datenschutzbehörde weitergeben (s.u. S. 195; Beschwerde gegen TikTok, Der Spiegel Nr. 30, 24.07.2021, 62).

Bremen

Sensitive Daten nicht per Fax verschicken

Gemäß der Landesbeauftragten für Datenschutz in Bremen Imke Sommer ist das klassische Telefax nicht mehr datenschutzkonform, wenn sensitive Daten übermittelt werden sollen. Art. 9 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) verbiete dies. Grund dafür seien in den vergangenen Jahren vollzogene technische Änderungen in den Telefonnetzen. Waren Faxe früher noch Ende-zu-Ende-Telefonleitungen vorbehalten, würden sie mittlerweile über das Internet verschickt. Weiterhin stehe am anderen Ende der Faxübertragung häufig kein zweites Faxgerät mehr. Die Telefaxe würden meist von Systemen empfangen, die das eingehende Fax automatisch in eine E-Mail umwandeln. Durch diese technischen Änderungen habe ein Telefax mittlerweile das gleiche Sicherheitsniveau wie eine unverschlüsselte E-Mail.

Laut der Datenschutzbeauftragten verfügen Fax-Dienste über keinerlei Sicherungsmaßnahmen für vertrauliche Daten. Aus diesem Grund seien sie für die Übermittlung personenbezogener Daten ungeeignet. Als Alternativen zum Telefax müssten Nutzer Dienste wie etwa Ende-zu-Ende verschlüsselte E-Mails oder auch die herkömmliche Briefpost in Betracht ziehen. Die Datenschutzbeauftragten anderer Bundesländer haben sich zu dem Thema noch nicht geäußert (Bergert, Datenschutz: Fax ist nicht DSGVO-konform, www.pcwelt.de 11.05.2021).

Hessen

Ausweisbehörden verweigern biometriefreien Personalausweis

Da ab dem 02.08.2021 Personalausweise in Deutschland nur noch mit den elektronisch erfassten Fingerabdrücken des linken und des rechten Zeigefingers ausgegeben werden, beantragte ein Bürger aus Hessen bei seinem Einwohnermeldeamt noch im Juli einen neuen Ausweis – ohne Fingerabdrücke, obwohl sein alter Ausweis noch sechs Jahre gültig ist. Ihm wurde daraufhin mitgeteilt, es sei gesetzlich verboten, ohne Not, also Verlust oder Diebstahl, einen Ausweis vorzeitig zu beantragen. Dies ist natürlich Unsinn; ein solches Verbot existiert nicht. Nach Rücksprache im Hessischen Ministerium des Innern und für Sport, bekräftigte die freundliche Mitarbeiterin des Amtes aber die behördliche Verweigerungshaltung und bestätigte die ministerielle Anweisung als verbindliche Vorgabe „von Oben“ (eigene Recherche).

Hessen

Polizeireformkommission fordert u.a. besseren Datenschutz

Eine unabhängige Expertenkommission zu rechtsextremen Äußerungen und Fehlverhalten bei der hessischen Polizei hat zu unverzüglichen Reformen aufgerufen. Die Vorsitzende des Gremiums, Angelika Nußberger, erklärte am 12.07.2021 in Wiesbaden: „Für die Polizei in Hessen ist ein kritischer Moment erreicht.“ In ihrem 128-seitigen Abschlussbericht empfahl die Kommission unter anderem Verbesserungen beim Datenschutz, eine wirksamere interne Fehlerkultur sowie mehr Augenmerk auf Aus- und Fortbildung der Beamtinnen und Beamten. Nußberger war bis 2020 Vizepräsidentin des Europäischen Gerichtshofs für Menschenrechte. Innenminister Peter Beuth hatte die Kommission im August 2020 eingesetzt, nachdem Ermittlungen zu rechtsradikalen Drohmails gegen die Anwältin Seda Başay-Yildiz, die Kabarettistin Idil Baydar und die nunmehrige Linken-Bundeschefin Janine Wissler Verstöße zutage gebracht hatten.

Die vielen empörenden und aufsehenerregenden Vorfälle der Vergangenheit hätten zu einem deutlichen Vertrauensverlust der Polizei in der Bevölkerung geführt. Deshalb sei es nötig, Reformen bei der Polizei anzugehen. Das müsse so schnell und so nachhaltig getan werden, dass der Neuanfang für alle unmittelbar sichtbar sei: „Hessen muss ein Exempel statuieren und zeigen, dass es den Ehrgeiz hat im Kampf gegen Rechtsextremismus deutschlandweit eine Vorreiterrolle einzunehmen.“

Der Vizevorsitzende der Kommission, der Grünenpolitiker Jerzy Montag, sagte, der wachsende Rechtsextremismus bei Polizei, Spezialeinsatzkommandos, Bundeswehr und Berufsfeuerwehren sei eine große Bedrohung der Sicherheit und der Demokratie: „Noch sind es Einzelne und organisierte Minderheiten, aber es gilt den Anfängen zu wehren.“ Bund und Länder seien hier immer noch nicht ausreichend abwehrbereit.

Konkret empfahl die Kommission in 58 Einzelempfehlungen unter anderem, Polizeianwärter sollten vom Verfassungsschutz über Regelanfragen auf ihre Treue zur freiheitlich-demokratischen Grundordnung überprüft werden. Im polizeilichen Alltag müsse stärker gegen Rechtsextremismus sensibilisiert werden. Aus- und Fortbildung seien der „Dreh- und Angelpunkt zum Aufbau und zur Stärkung einer resilienten, lernenden Organisation“. Whistleblower sollten ermutigt, ein Polizeibeauftragter eingerichtet werden.

Die Kommission kritisierte den internen Umgang mit Fehlverhalten: „Die Ahndung von auch grobem Fehlverhalten von Polizeiangehörigen bleibt wegen der Parallelität von Straf- und Disziplinarverfahren langwierig und schwierig und entfaltet oftmals auch nicht in ausreichendem Umfang eine generalpräventive Wirkung.“ Zur Verbesserung des Datenschutzes regte die Kommission an, für alle Beamtinnen und Beamten eine eindeutige Identifizierung für das Polizeiauskunftssystem einzuführen, etwa über biometrische Daten.

Auch bei der Öffentlichkeitsarbeit gebe es Nachholbedarf. Oft werde „das Richtige gemacht, aber falsch kommuniziert", etwa beim Umgang mit den Betroffenen der Drohschreiben. Die beanstandeten Chats mit extremistischen Inhalten negieren nach Auffassung der Kommission die freiheitlich-demokratische Grundordnung und erforderten „eine konsequente und eindeutige Antwort" im Sinne eines „Nicht weiter so!". Betroffen waren 47 Chatgruppen, an denen 136 Polizeibeamte beteiligt waren. Es sei „besorgniserregend", dass Fälle von gruppenbezogener Menschenfeindlichkeit und Rechtsextremismus intern – auch durch Vorgesetzte – relativiert wurden.

Die Kommission hatte gemäß eigenen Angaben interne polizeiliche Dokumente analysiert und mehr als 70 Menschen befragt. Darunter waren neben Empfängern von Drohschreiben auch Journalistinnen, Rechtsextremismusexperten und angehende Polizisten. Die Kommission, die den Bericht vorlegte, war gebildet worden, nachdem unter anderem unerlaubte polizeiliche Datenabfragen im zeitlichen Zusammenhang mit rechtsextremen Drohschreiben an Politikerinnen und andere Personen des öffentlichen Lebens bekannt wurden. Die Adressen der Betroffenen, an welche die Schreiben mit der Signatur „NSU 2.0" geschickt wurden, waren zuvor an Polizeicomputern abgefragt worden (DANA 1/2019, 38 f., 4/2019, 222f.). Außerdem ermittelt die Staatsanwaltschaft wegen Chats von Polizisten mit rechtsextremen Inhalten. Anfang Mai 2021 war in Berlin der mutmaßliche Verfasser der Drohschreiben festgenommen worden. Wer die Daten an den Polizeicomputern abgerufen hat, ist nicht ermittelt (s.o. S. 177; Kommission dringt auf Reformen bei hessischer Polizei, www.zeit.de 12.07.2021; Bielicki, Braucht Hessens Polizei Reformen? SZ 13.07.2021, 5).

Hessen u.a.

NSU 2.0-Täter kommt per Social Engineering an Polizeidaten?

Anfang Mai 2021 waren die Ermittler der Staatsanwaltschaft Frankfurt am Main erfolgreich bei der Überführung des mutmaßlichen Täters Alexander M. aus Berlin, der unter dem Kürzel „NSU 2.0" Menschen wohl mit mehr als 100 Drohschreiben und Drohanrufe adressierte und dabei polizeiliches Insiderwissen über seine Opfer verwendete. Lange Zeit ermittelten sie in Polizeikreisen. Nun zeigte sich, dass dem Verdächtigen keine direkten Verbindungen zur Polizei nachgewiesen werden können. Die Staatsanwaltschaft vermutet, dass die privaten Daten der Opfer durch „social engineering" beschafft wurden, dass der Täter sich gegenüber der Polizei am Telefon als Kollege ausgegeben hat und so die Daten aus der hessischen Polizeidatenbank Polas erlangt hat.

Dass im Umgang mit Polizeidaten Probleme bestehen, erwies sich schon im Juli 2018, als die Schlagersängerin Helene Fischer im Frankfurter Waldstadion vor 40.000 Zuschauern auftrat und an diesem Abend ganze 83 Mal ihre privaten Daten im System POLAS abgefragt wurden. Hessens Polizeipräsident hatte damals gegenüber dem Innenausschuss in Wiesbaden erklärt, es sei „wohl relativ unwahrscheinlich", dass es dafür triftige Gründe gab. Er zählte pro Monat mehr als 1.000 missbräuchliche Suchanfragen.

Ans Licht kamen die Fischer-Abfragen wegen mehrerer missbräuchlicher Datenabfragen mit rechtsextremem Hintergrund. Einmal gab ein hessischer Polizist Daten an eine Neonazi-Kameradschaft weiter. In einem anderen Fall war die Frankfurter Rechtsanwältin Seda Başay-Yildiz von „NSU 2.0" bedroht worden. In einem Fax, das sie am 02.08.2018 erhielt, standen private Daten, die nur anderthalb Stunden zuvor an einem Polizeicomputer in Frankfurt abgerufen worden waren: „Verpiss dich lieber, solange du hier noch lebend rauskommst, die Schwein!". Der Absender drohte auch, ihre Tochter zu „schlachten" (DANA 1/2019, 38 f.).

- Die Bedrohung eines Rechtsanwalts aus Würzburg

Alexander M. hatte auch den Rechtsanwalt Can-jo Jun aus Würzburg seit Februar 2017 bedroht: Er wisse, wo er wohne und dass er zwei Kinder habe. Wenn er mit der Sache nicht aufhöre, werde es „Leichen" geben: „Sieg Heil". Die „Sache", das waren Prozesse, die der Fachanwalt für IT-Recht insbesondere gegen den Internet-Giganten Facebook führte, um diesen dazu zu bringen, stärker gegen rassistische Hasspostings vorzugehen. Schon 2017 hatte die Würzburger Polizei Alexander M. als möglichen Täter ermittelt, da die Verbindungsdaten mit unterdrückter Nummer zu einem Festnetzanschluss in einem Mietshaus in Berlin-Gesundbrunnen führten. Doch war der Anschluss auf einen Dirk Heist angemeldet, den es in Berlin nicht gab. Bei der Überprüfung des Mietshauses stellte die Polizei damals fest, dass dort ein Alexander M. wohnte, der seine Telekom-Rechnung bar bezahlte und der im Polizeicomputer vermerkt war wegen 95 Fällen zu Betrugsdelikten, Köperverletzungen, Kinderpornografiebesitz und Beleidigungen sowie auch einer Bedrohung mit unterdrückter Nummer. Die Polizei wollte den genauen Anschlussinhaber von der Telekom genannt bekommen, doch die verweigerte sich, da sie nach dem Telekommunikationsgesetz nur zur Auskunft über die Adresse verpflichtet und berechtigt sei, und nicht zur präzisen Lokalisierung des Anschlusses in einem großen Mietshaus. Ohne den eindeutigen Beweis der Herkunft der Bedrohung ließ das Amtsgericht Würzburg damals die Anklage gegen Alexander M. mangels „hinreichendem Tatverdacht" nicht zu. Alexander M. triumphierte und schrieb in Briefen, die Anklage sei „lächerlich" und „sachfremd", eine einzige „Unverschämtheit"; der Oberstaatsanwalt müsse sich „die Frage gefallen lassen, was er mit einem solchen Quatsch eigentlich bezweckt". Wenige Tage nach der Entscheidung der Beschwerdeinstanz ging bei der Rechtsanwältin Başay-Yildiz das erste mit „NSU 2.0" gezeichnete Drohfax ein.

- Unberechtigte Datenabfragen

Das Problem unberechtigter Datenabrufe in Polizeirechnern besteht auch in anderen Bundesländern. In Berlin nutzte gemäß dem Bericht der Berliner Datenschutzbeauftragten für 2020 eine Polizistin die interne Datenbank Poliks, „um die Ex-Freundinnen des neuen Lebensgefährten ausfindig zu machen und sie anschließend zu Gesprächen aufzusuchen". 2018 hatte ein Berliner Polizist Daten über Angehörige der linken

Szene genutzt, um ihnen Drohbriefe zu schreiben.

Oft bleibt ein solches Vorgehen unentdeckt. Die hessische Polizeidatenbank POLAS wird täglich mehr als 40.000 Mal abgefragt. Das Schengener Informationssystem verzeichnet 220 Abfragen pro Sekunde. Im Jahr 2019 mussten hessische Beamte nur bei jeder 200. Abfrage des Informationssystems überhaupt den Grund eingeben („stichprobenartig"). In einem Fall, beklagte der Landespolizeipräsident, schrieb ein Beamter einfach „Mickey Mouse".

Die Staatsanwaltschaft Frankfurt am Main vermutet, der mutmaßliche Täter hinter „NSU 2.0" könnte sich dies zunutze gemacht haben. Er könnte im Innenstadtrevier der Frankfurter Polizei angerufen haben. Die Beamtin, an deren Rechner die Daten von Seda Başay-Yildiz abgerufen wurden, Miriam D., beteuerte, sie erinnere sich an nichts. Daten würden dort jeden Tag massenhaft abgefragt. Sie habe ihr Passwort immer offen herumliegen lassen, damit Kollegen schnell die Datenbank nutzen können.

Als „NSU 2.0-Verdächtiger" sitzt seit dem 04.05.2021 ein 53jähriger arbeitsloser und mehrfach vorbestrafter EDV-Techniker Alexander M. in Untersuchungshaft. Mehr als 30 Menschen waren von ihm in den vorangegangenen drei Jahren unter dem Kürzel „NSU 2.0" bedroht worden. Die Festplatten, die in seiner vermüllten Einzimmerwohnung beschlagnahmt und von Forensikern analysiert wurden, bestätigten seine Zuordnung zu dem Pseudonym. Die Daten zu Anwalt Chan-jo Jun wurden von M. offenbar durch eine komplexe Recherche im Internet herausgefunden. Bei den privaten Angaben zur Kabarettistin Idil Baydar hatte es dagegen offenbar Abfragen über Polizeicomputer am 04.03.2019 auf dem 4. Revier in Wiesbaden gegeben. Einen Tag später gab es solche Abfragen auch in Berlin auf Revieren in den Stadtteilen Spandau und Neukölln. Auch im Fall von Janine Wissler, der hessischen neuen Bundesvorsitzenden der Linkspartei hatte es wenige Tage vor ihrer Bedrohung am 10.02.2020 eine Polizeiabfrage aus dem 3. Revier Wiesbaden gegeben.

Die Vorschriften für den Datenschutz wurden danach in Hessen und in anderen Bundesländern verschärft; jetzt müssen öfter Passwörter und Abfragegründe eingegeben werden. In den 90er Jahren war es einem Mitarbeiter eines Antifa-Archivs in Nordrhein-Westfalen gelungen, in der Parteizentrale der Republikaner anzurufen, sich als Parteichef Franz Schönhuber auszugeben und sich die komplette Liste der Parteimitglieder faxen zu lassen. Niemand weiß, wie oft der mutmaßliche „NSU 2.0"-Täter den Trick bei Polizeidienststellen versucht haben könnte (Steinke, Sogar nach Helene Fischer wurde gefragt, SZ 07.05.2021, 6; Bartsch/Diehl/Lehberger/Röbel, Kein Anschluss in Berlin, Der Spiegel Nr. 19 v. 08.05.2021, 42 f.; Flade/Steinke, Bösartige Recherche, SZ 14.05.2021, 7).

Nordrhein-Westfalen

Corona-Schnelltestregistrierungen von Medican waren online zugänglich

Gegen den privaten Corona-Schnelltestanbieter Medican, der auch wegen undurchsichtiger Abrechnungspraktiken in der Kritik steht, wird der Vorwurf erhoben, die Daten der Getesteten nicht ausreichend gesichert zu haben. Gemäß Zerforschung, einer Gruppe von IT-Experten, konnten Zehntausende Schnelltestregistrierungen von Unbefugten eingesehen werden.

Auf den ersten Blick wirkte das System von Medican sicher: Zwar war für das Login kein Passwort notwendig, Getestete mussten aber ihre Personalausweisnummer kennen, um zu ihrem Profil und ihren Ergebnissen weitergeleitet zu werden. Wer jedoch erkannte, nach welchem System die Links zu den Webseiten aufgebaut waren, konnte ohne Ausweisnummer eine Datei mit den persönlichen Daten der Getesteten abrufen. Sichtbar waren so Vornamen, Nachnamen, Geburtsdaten und E-Mail-Adressen. Zwei Wege, die zu den Registrierungsdaten führten, sind Zerforschung zufolge besonders problematisch: Zum einen war ein Programm in einigen Fällen in der Lage, eine von zwei persönlichen Identifikationsnummern zu erraten, weil diese vergleichsweise kurz und simpel aufgebaut waren. Die andere Identifikationsnummer bestand lediglich aus dem kodierten Registrierungszeitpunkt eines Getesteten: Wer auf die Sekunde genau den Registrierungszeitpunkt einer Person kannte oder erriet, konnte weitere Daten einsehen. Zerforschung gelang dies bei mehr als jedem zehnten Versuch. Wie viele Personen von der Lücke betroffen waren, ist unklar. Von Zehntausenden Fällen ist auszugehen.

Medican hat in der Zwischenzeit auch das letzte seiner über 50 Testzentren geschlossen, Verantwortliche wurden wegen des Vorwurfs der Falschabrechnung festgenommen, online war das Unternehmen nicht mehr erreichbar. Reinhard Peters, der Verteidiger eines der beiden Beschuldigten im Fall Medican, bestätigte die Datenlücke: „Darum ist die Webseite ja auch abgeschaltet worden." Auch rückwirkend dürfte damit kein Zugriff auf Registrierungsdaten mehr möglich sein.

Zerforschung hatte die Sicherheitslücke an die Datenschutzbehörde in Nordrhein-Westfalen und an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet. Das BSI hat nach eigenen Angaben den Betreiber aufgefordert die Sicherheitslücke zu beheben. Über Hinweise auf Missbrauch der Daten ist dem BSI bislang nichts bekannt.

Der Fall Medican ist nur einer von zahlreichen Datenschutzpannen durch mangelhafte IT-Infrastruktur bei Schnelltestanbietern. Zerforschung hatte bereits Sicherheitslücken bei der Software Medicus AI und zwei weiteren Testanbietern publik gemacht. Dass im Rahmen der Pandemie oftmals Web-Anwendungen ohne grundlegende Sicherheitsmaßnahmen online gegangen sind, kritisiert auch BSI-Sprecher Joachim Wagner: „In den Fällen, die uns bekannt sind, waren die Sicherheitslücken trivial auszunutzen, wären aber auch trivial zu vermeiden gewesen."

Anbieter von Schnelltests stehen in einer besonderen Verantwortung Daten zu sichern: Zwar konnten im Fall von Medican nur Registrierungen für Covid-Tests abgerufen werden, Medican und andere Anbieter sind aber auch für die Sicherung sensiblerer medizinischer Daten verantwortlich, die gemäß der Datenschutz-Grundverordnung besonders schutzbedürftig sind. Sowohl das BSI als auch einige Landesbehörden für Datenschutz informieren deshalb über

Mindestanforderungen an die Datensicherung von Testzentren. So dürfte der Zugang zu Daten der Behörde aus Baden-Württemberg zufolge nicht – wie in diesem Fall – „einfach erratbar sein". Auch sollten Systeme professionelle Sicherheits-Prüfungen durchlaufen. Dass das bei Medican der Fall war, bezweifeln die Mitglieder von Zerforschung: „Solche Fehler würden sonst innerhalb kürzester Zeit gefunden werden" (Kruse, Zutritt für Unbefugte, SZ 15.06.2021, 5).

Nordrhein-Westfalen u.a.

Coronapoint-Testzentren mit großem Daten-Leak

Das IT-Sicherheitskollektiv „Zerforschung" publizierte eine weitere von ihr entdeckte Lücke in der Datensicherheit von Corona-Testzentren. Der Fall Coronapoint ist wohl der bisher gravierendste in einer Reihe von Datenpannen. Das Unternehmen betreibt über 30 Testzentren, vorrangig in Nordrhein-Westfalen: Knapp 174.000 Buchungsbestätigungen von Zehntausenden Betroffenen waren teils mit Testergebnissen abrufbar. Die Aktivisten haben die zuständigen Behörden und den Betreiber informiert, der die Datenlücke erst nach mehreren Hinweisen schloss. Der SPD-Gesundheitsexperte Karl Lauterbach hatte kurz zuvor ein Testzentrum des Betreibers Coronapoint besucht und erklärt: „Ich habe mich sehr geärgert, dass ein paar wenige Zentren den Ruf dieser wichtigen Branche beschädigt haben." Dass Coronapoint kurz darauf auch zur Rufschädigung beitragen würde, wusste er zu diesem Zeitpunkt nicht; das Unternehmen war jedoch schon über die Mängel in der Software informiert.

Von dem Leak betroffen waren neben sensiblen Gesundheitsdaten auch Ausweisnummern. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wies auf die damit verbundene Gefahr hin: „Kriminelle können damit erheblichen finanziellen Schaden verursachen." Auch der Landesbeauftragte für Datenschutz in Baden-Württemberg, Stefan Brink, sieht im Identitätsdiebstahl ein großes Risiko, was Testzentren zu einem lohnenden Ziel für Hacker macht. Ob es in diesem Fall unerlaubte Zugriffe gab, ist nicht klar.

Der Schutz der sensiblen Daten wird in den Testverordnungen von Bund und Ländern schlicht nicht berücksichtigt. Auch werden die zuständigen Behörden von der Eröffnung von Testzentren nicht benachrichtigt. Sonst, so Brink, könnten sie zumindest Hinweise zur Datensicherung geben. Schon die Erhebung von Ausweisdaten, wenn sie nicht notwendig ist, bezeichnete Brink als „klaren datenschutzrechtlichen Verstoß" und „unverhältnismäßiges Risiko". Auch das Bundesgesundheitsministerium sprach von einem „Verstoß gegen das Gebot der Datenminimierung". Das Missbrauchsrisiko ist in diesem Bereich hoch, weil die IT-Systeme oft laienhaft geschützt sind. Systematische Kontrollen gibt es keine, weil Ressourcen fehlen. Die Behörden sind auf das Engagement von Aktivisten angewiesen.

Was mit Millionen sensibler Daten passiert, wenn sich die betreffenden Unternehmen auflösen, ist unklar. Gefährliche Szenarien reichen von der unsachgemäßen Entsorgung von Speichergeräten bis zur gezielten Veräußerung der Daten, so Brink: „Wer von der Insolvenz bedroht ist, für den kann das lukrativ sein." Datenschützer zeigen sich ob dieser Gefahren alarmiert, politisch fehlt aber eine klare Zuständigkeit. Das Gesundheitsministerium verweist bei Fragen auf das BSI; die NRW-Datenschutzbehörde sieht die Verantwortung bei den Unternehmen. Karl Lauterbach erklärte auf Anfrage, er gehe weiter davon aus, dass überwiegend ehrlich gearbeitet werde, zeigte sich jedoch entsetzt: „Wenn ich von den Verdächtigungen gewusst hätte, hätte ich auf keinen Fall dieses Unternehmen besucht" (Kruse, Sicherheitslücken bei Corona-Tests, SZ 23.05.2021, 1).

Sachsen

Verfassungsschutz sammelt Daten über Abgeordnete und Regierungsmitglied

Das sächsische Landesamt für Verfassungsschutz (LfV) hat Informationen über den eigenen Wirtschaftsminister und stellvertretenden Ministerpräsidenten Martin Dulig (SPD) gesammelt. Dulig hatte ein Auskunftsersuchen gestellt und erhielt sechs Seiten mit Informationen, wie Aussagen und Facebook-Einträge. „Das ist ein ungeheuerlicher Vorgang. Mir fehlen dafür die Worte." Auslöser für Duligs Anfrage war ein Auskunftsersuchen des Linken-Fraktionschefs Rico Gebhardt. Ihm war mitgeteilt worden, dass Daten von ihm gesammelt wurden. So wurde unter anderem eine Teilnahme an einer Demonstration vermerkt, an der auch Dulig, der Landesvorsitzender der SPD ist, selbst teilnahm. Daraufhin stellte auch das Regierungsmitglied ein Auskunftsersuchen und bekam jene sechs Seiten mit Informationen, die über ihn gesammelt wurden. Duligs Kommentar: „Das war belangloses Zeug. Und ist eher peinlich für die Agenten."

Die für die Geheimdienstaufsicht zuständige Parlamentarische Kontrollkommission (PKK) des Landtags bewertete eine Beobachtung von Landtagsabgeordneten in einem veröffentlichten Bericht als „klar rechtswidrig". Der Bericht wurde am 08.06.2021 vom Sächsischen Landtag als Nachbericht „zur Sammlung und Speicherung von Abgeordnetendaten durch das Landesamt für Verfassungsschutz Sachsen" herausgegeben. Demnach speicherte der Geheimdienst kritische Äußerungen Duligs zum Umgang der sächsischen CDU mit dem Thema Rechtsextremismus. Die CDU habe das Problem 25 Jahre lang verharmlost, soll der SPD-Politiker in einer Studie des Göttinger Instituts für Demokratieforschung geschrieben haben. Genauer taucht Dulig mit der Äußerung auf, dass „die CDU eine Verantwortung dafür trägt, welche Zustände heute in Sachsen hinsichtlich Rechtsextremismus und Rassismus herrschen". Zudem, so heißt es in dem PKK-Bericht, habe der Verfassungsschutz die Kritik von Dulig dokumentiert, wonach die CDU denen mit Misstrauen begegne, die sich stets gegen Rechtsextremismus und Rassismus engagiert haben.

Die gespeicherten Informationen seien, so der PKK-Bericht, weder dazu geeignet „im Rahmen einer Prüf- oder Verdachtsfallbearbeitung den Nachweis zu führen, dass sich die betroffene Person einer Bestrebung gegen die freiheitliche demokratische Grundordnung

angeschlossen hat oder für eine fremde Macht geheimdienstlich tätig ist". Noch seien diese Informationen im Rahmen einer Sicherheitsüberprüfung der Betroffenen erhoben worden. Hintergrund des Berichts sind Untersuchungen der PKK zur Sammlung und Speicherung von Daten sächsischer AfD-Abgeordneter. Daraufhin richteten zahlreiche Landtagsabgeordnete verschiedener Fraktionen Auskunftsersuchen an das LfV. Sachsens Innenminister Roland Wöller (CDU) und der neue Verfassungsschutzchef Dirk-Martin Christian halten die Datenspeicherung auch für rechtswidrig und verwiesen auf den Schutz des freien Abgeordnetenmandats durch das Grundgesetz.

Durch den PKK-Bericht wurde bekannt, dass neben den Äußerungen von Dulig auch Aussagen des Linken-Abgeordneten Rico Gebhardt festgehalten wurden. So habe Gebhardt Ministerpräsident Michael Kretschmer (CDU) vorgeworfen, dieser habe sich als „Verlautbarungsorgan des Militärs" betätigt. Ebenfalls in dem Bericht namentlich erwähnt sind Valentin Lippmann und Christin Melcher (beide Grüne) sowie Marco Böhme (Linke). Zu Lippmann etwa heißt es: „Im Nachgang an die ‚Querdenken-Demo' in Leipzig äußerten Sie sich in der dpa am 08.11.2020 kritisch über die Planungen zur Demonstration, das Versammlungsgeschehen und die Angriffe auf Gegenproteste, Journalisten und die Polizei." Grundsätzlich genießen Abgeordnete besonderen Schutz vor Geheimdienstbeobachtung: Alles, was mit ihrer Abgeordnetentätigkeit in Zusammenhang steht, darf nicht gesammelt oder gespeichert werden.

Der aktuelle Verfassungsschutzchef Dirk-Martin Christian räumte Fehler bei der Speicherung von Abgeordnetendaten ein und teilte mit, es seien inzwischen eine Reihe von rechtlichen und organisatorischen Maßnahmen auf den Weg gebracht worden, „die künftig eine rechtssichere Vorgehensweise sicherstellen". Die Praxis der Erfassung von Abgeordnetendaten habe mit der Einführung einer elektronischen Datenverarbeitung beim Verfassungsschutz zu tun: Jegliches Schriftgut werde nach Eingang automatisch erfasst. Erst später werde geprüft, ob die Informationen überhaupt eine Relevanz für die Geheimdienstarbeit hätten. Diese Prüfung „erfolgte bis Mitte 2020 nicht fristgemäß". Die Abgeordnetendaten hätten bei korrekter Arbeitsweise „bereits unverzüglich mit Posteingang gelöscht werden müssen, weil sie überhaupt keinen nachrichtendienstlichen Mehrwert besitzen und auch nicht zur Aufgabenerfüllung des LfV erforderlich sind".

Die Sammlung war in der Amtszeit des umstrittenen seit 2012 im Amt befindlichen Verfassungsschutzpräsidenten Gordian Meyer-Plath erfolgt. Er war 2020 abgelöst worden durch Dirk-Martin Christian. Meyer-Plath wurde von Kritikern vorgeworfen, zu wenig gegen rechtsextreme Netzwerke vorzugehen.

Dulig kritisierte, der Umstand, dass sogar über ihn eine Sammlung existiert habe, zeige, welcher Geist seinerzeit im Landesamt für Verfassungsschutz geherrscht habe; so was gebe es nur in Sachsen. Dinge wie ein Angriff auf sein Bürgerbüro, also konkrete Bedrohungen, seien dagegen nicht aufgeführt worden. 2015 waren Pflastersteine in Duligs Bürgerbüro in Radebeul geworfen worden. Die gesammelten Daten über ihn würden gelöscht, da „es illegal war".

Meyer-Plath war für eine Stellungnahme nicht zu erreichen. In Verfassungsschutzkreisen hieß es, Dulig sei niemals überwacht worden. Der Dienst habe Äußerungen festgehalten, in denen es darum ging, wie Politiker aktuell Extremismus bewerten. Das sei eine der Arbeitsgrundlagen des Verfassungsschutzes. Außerdem müsse damit gerechnet werden, dass Extremisten auf die Äußerungen von Politikern reagieren.

Der SPD-Generalsekretär auf Bundesebene, Lars Klingbeil, erklärte: „Martin Dulig ist ein aufrechter Sozialdemokrat und ganz sicher kein Fall für den Verfassungsschutz. Dass politische Bewertungen und Statements von ihm, die sich unter anderem gegen die CDU richteten, gesammelt wurden, entbehrt jeder Grundlage." Es sei gut, dass diese illegalen Aktionen aufgedeckt wurden und dass beim Verfassungsschutz in Sachsen aufgeräumt werde: „Unsere Sicherheitsbehörden müssen unsere Demokratie schützen und sie gegen Feinde abwehren, vor allem von rechts. Darauf muss der Fokus liegen."

Der Fall reiht sich ein in die seit Jahren anhaltenden Debatten, ob der Verfassungsschutz ausreichend politisch neutral ist und das linksextreme wie das rechtsextreme Lager gleichermaßen im Blick hat. Die SPD im Bund war auch einer der Treiber für die Entlassung des Verfassungsschutzpräsidenten Hans-Georg Maaßen. Dieser hatte nach der Tötung eines Deutschen mit kubanischen Wurzeln und den anschließenden Auseinandersetzungen im sächsischen Chemnitz trotz eines entsprechenden Videos den Eindruck zurückgewiesen, dass es dort rechtsextreme Hetzjagden gegeben habe. Maaßen kandidiert für die CDU in Südthüringen, um dort am 26.09.2021 ein Direktmandat für den Bundestag zu erobern. Der Chef des thüringischen Verfassungsschutzes, Stephan Kramer, erklärte, Maaßen sei in Thüringen derzeit aktiv und falle somit auch in dessen Zuständigkeitsbereich. Maaßen benutze „klassische antisemitische Stereotype", verwende „doppeldeutige Begriffe". Derlei sei bereits bekannt vom Thüringer AfD-Chef Björn Höcke oder vom AfD-Bundestagsfraktionschef Alexander Gauland und „eine beliebte Methode der Neuen Rechten". Das wiederum brachte ihm von CDU und AfD den Vorwurf der fehlenden politischen Neutralität ein, weshalb es Entlassungsforderungen gegen ihn gibt (Ismar, Sächsischer Verfassungsschutz sammelte illegal Material über Vize-Regierungschef, www.tagesspiegel.de 08.06.2021; Landesverfassungsschutz sammelte „klar rechtswidrig" Abgeordnetendaten, www.zeit.de 08.06.2021).

Datenschutznachrichten aus dem Ausland

Weltweit

„Pegasus-Projekt“ legt Überwachung von Journalisten, Oppositionellen und Politikern durch NSO-Software offen

Ein internationales Journalistenkonsortium hat neue Vorwürfe gegen den israelischen Überwachungssoftware-Anbieter NSO Group veröffentlicht. IT-Experten fanden den Berichten zufolge auf 37 Smartphones von Journalisten, Menschenrechtlern, Politikern, deren Familienangehörigen und Geschäftsleuten Spuren von Angriffen mit der Pegasus-Software des Unternehmens. Die Nummern seien Teil eines Datensatzes von mehr als 50.000 Telefonnummern, den die Journalisten gemeinsam mit den Organisationen Forbidden Stories und Amnesty International auswerteten. Die Nummern waren gemäß den Berichten von NSO-Kunden als potenzielle Ausspähziele ausgewählt worden. NSO wies die Vorwürfe vehement zurück.

Gemäß der Darstellung des Journalistenkonsortiums, an dem von deutscher Seite die Süddeutsche Zeitung, NDR, WDR und die Zeit beteiligt sind, legen die Recherchen des „Pegasus-Projekts“ nahe, dass Hunderte Journalisten, Menschenrechtler, Oppositionelle und Politiker ausgewählt wurden, um mit der Spionagesoftware überwacht zu werden. Bei monatelangen Recherchen war es gelungen Tausende der Nummern Personen zuzuordnen. Die Nummern von mehr als 180 Journalistinnen und Journalisten aus verschiedenen Ländern stünden auf der Liste. Nummern deutscher Journalisten seien nicht darunter.

Insgesamt finden sich im Leak des Pegasus-Projekts die Telefonnnummern von 14 Staats- und Regierungschefs, die während ihrer Amtszeit Opfer des Handy-Spions Pegasus geworden sein könnten. Betroffen sind etwa der jemenitische Premier Amed Obeid bon Daghr, Saad Hariri aus Libanon, Ruhakana Rugunda aus Uganda, Mustafa Madbuli aus Ägypten und Imran Khan, der Regierungschef Pakistans. Insgesamt konnte das Pegasus-Projekt die Nummern aus mehr als 20 Ländern sowie von Hunderten Regierungsbeamten aus mehr als 30 Ländern identifizieren. Betroffen sind auch der französische Regierungschef Emmanuel Macron mit einer Nummer, die er seit 2017 verwendet, sowie der frühere Premierminister Édouard Philippe sowie etliche Ministerinnen und Ministern seiner im ersten Halbjahr 2019 amtierenden Regierung. Auch die Mobilnummer von Charles Michel, damals Belgiens Premierminister und heute Präsident des Europäischen Rates, war offenbar ein potenzielles Ziel marokkanischer Behörden. Der ehemalige EU-Kommissionspräsident Romano Prodi geriet den Recherchen zufolge ebenso ins Visier marokkanischer Behörden.

Der ehemalige mexikanische Präsident Felipe Calderón wiederum wurde offenbar von Stellen seines eigenen Landes ins Visier genommen, allerdings nach seiner Amtszeit. Sogar eine Nummer, die nach den Projekt-Pegasus-Recherchen dem marokkanischen König Mohammed VI. selbst zuzuordnen ist, findet sich auf der Liste der 50.000 potenziellen Ausspähziele.

Auch globale Organisationen sind demnach potenzielle Ziele staatlicher Überwachung. Die Handynummer des Äthiopiers Tedros Adhanom Ghebreyesus, Generaldirektor der Weltgesundheitsorganisation WHO, ist im Leak ebenso gelistet wie die verschiedener UN-Botschafter und anderer Diplomaten. Auch zu diesem Namen nahm die NSO Stellung: Ghebreyesus sei weder jetzt noch früher Ziel oder mögliches Ziel eines NSO-Kunden. Ghebreyesus scheint nach den Pegasus-Projekt-Recherchen ebenso wie die französischen und algerischen Ziele von marokkanischen Behörden ins Visier genommen worden zu sein, Pakistans Regierungschef Imran Khan von indischen Behörden. Saad Hariri (Libanon) und Barham Salih (Irak) scheinen das Interesse sowohl von Saudi-Arabien als auch der Vereinigten Arabischen Emirate geweckt zu haben, Ägyptens Premier sollen allein die Saudis, den jemenitischen Regierungschef hingegen nur die Emirate auf dem Radar haben. Der Präsident von Südafrika und der damalige Premierminister von Uganda wurden den Recherchen zufolge von entsprechenden Stellen in Ruanda anvisiert – allerdings bestreitet Ruanda Pegasus überhaupt zu nutzen. Die Regierungen von Saudi-Arabien und den Vereinigten Arabischen Emiraten ließen Anfragen zur Nutzung von NSO-Software unbeantwortet. Aus Indien kam die Erklärung, die indischen Behörden würden nach Recht und Gesetz operieren.

Wie die Liste zu Forbidden Stories und Amnesty International kam, die sie dann mit den Medien teilten, bleibt in den Berichten offen; es wurde auf den Quellenschutz verwiesen. Forensische Untersuchungen bestätigten in vielen Fällen Infektionen mit der Software.

In Ungarn waren Medienmanager, Rechtsanwälte und Oppositionelle sowie sogar ein Ex-Minister betroffen. Die Regierung in Budapest teilte auf Anfrage mit, diese „angebliche Datensammlung“ sei dort „nicht bekannt“. In Ungarn herrsche Rechtsstaatlichkeit, weshalb „staatliche Stellen, die das Recht haben, heimliche Methoden einzusetzen, regelmäßig von Regierungs- und Nichtregierungsinstitutionen kontrolliert“ würden. Bei den Recherchen konnten neben Ungarn mindestens neun Länder identifiziert werden, die mit Pegasus politisch unliebsame, aber unbescholtene Personen ins Visier nehmen: Aserbaidschan, Saudi-Arabien, Bahrein, Kasachstan, die Vereinigten Arabischen Emirate, Marokko, Ruanda, Indien und Mexiko.

NSO wird vorgeworfen, seine Überwachungssoftware habe bei der Ermordung des saudischen Dissidenten Jamal Khashoggi eine Rolle gespielt. Demnach gehörten zwei der Smartphones, auf denen IT-Experten von Amnesty International Spuren von Pegasus-Angriffen gefunden hätten, Frauen, die Khashoggi nahestanden: Kashoggis Ex-Frau und dessen Verlobte. Die Telefonnummern aus dem Umfeld des Washington-Post-Kolumnisten, der im Oktober 2018 im saudischen Konsulat in Istambul er-

mordet wurde, weisen darauf hin. Die Recherchen legen zudem nahe, dass mutmaßliche saudische Behörden – anders als bislang bekannt – nicht nur vor dem Mord das Umfeld des Dissidenten, sondern auch danach die türkischen Ermittler ins Visier genommen haben. Die Nummer des türkischen Chef-Ermittlers wurde zumindest als potenzielles Ziel geführt. Eine Anfrage dazu ließ die saudi-arabische Regierung unbeantwortet.

„Pegasus" infiltriert Smartphones, späht persönliche Daten aus und kann auch Kamera und Mikrofon des Handys aktivieren. Im Fall von Journalisten können Hacker so die Kommunikation mit Quellen verfolgen.

NSO Group war bereits in der Vergangenheit vorgeworfen worden mit der Software Pegasus totalitären Regierungen bei der Ausspähung von Journalisten und Dissidenten geholfen zu haben. Facebook hatte NSO 2019 in den USA verklagt. Der Vorwurf in der Klage lautet, NSO habe versucht sich über eine später geschlossene Sicherheitslücke bei WhatsApp Zugriff auf Hunderte Smartphones zu verschaffen. Unter den Zielpersonen seien Journalisten, Anwälte, Dissidenten, Menschenrechtsaktivisten, Diplomaten und Regierungsbeamte gewesen.

Die NSO ist ein weltweit führender Anbieter von Überwachungssoftware und vergibt Pegasus-Lizenzen nach eigenen Angaben nur an staatliche Stellen. In Deutschland soll die Firma ihre Software dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst und einigen Bundesländern angeboten haben – offenbar ohne Erfolg. Gemäß einer Abfrage unter den Innenministerien der Länder kam es zu keinen Geschäftsabschlüssen mit NSO. Das große Leistungsspektrum von Pegasus sei nicht mit den Gesetzen vereinbar, die Abhörmaßnahmen hierzulande erlauben. Für ihre Verfassungsschutzämter gaben Berlin, Rheinland-Pfalz und Nordrhein-Westfalen an, Pegasus nicht zu besitzen; die anderen machten keine Angaben.

- Die Reaktion von NSO und von „Täterstaaten"

Das israelische Unternehmen sprach mit Blick auf den Forbidden-Stories-Bericht von „falschen Vorwürfen und irreführenden Behauptungen". Deren Quellen hätten sie mit Informationen versorgt, die keine Faktenbasis hätten: „Die Vorwürfe sind so empörend und weit von der Realität entfernt, dass NSO eine Verleumdungsklage erwägt."

NSO bekräftigte, seine Technologie stehe „in keiner Weise mit dem abscheulichen Mord an Jamal Khashoggi in Verbindung". Die Technologie werde „ausschließlich an Strafverfolgungsbehörden und Geheimdienste von geprüften Regierungen verkauft, mit dem alleinigen Ziel durch Verhinderung von Verbrechen und Terrorakten Menschenleben zu retten". Die NSO teilte mit, der marokkanische Monarch sei nie Ziel oder mögliches Ziel eines ihrer Kunden gewesen.

Die marokkanische Botschaft in Paris erklärte, es handele sich um „unbegründete Anschuldigungen", die man schon in der Vergangenheit „kategorisch zurückgewiesen" habe. Die Regierung des Königreichs und ihre Behörden hätten „niemals Computersoftware erworben", um „Kommunikationsgeräte zu infiltrieren, noch haben die marokkanischen Behörden jemals auf solche Handlungen zurückgegriffen".

- Reaktion von Journalisten

Nach den Berichten forderten deutsche Journalisten-Verbände Aufklärung und Gegenmaßnahmen. Der Vorsitzende des Deutschen Journalisten-Verbandes, Frank Überall, sprach von einem „nie da gewesenen Überwachungsskandal". Geheimdienste und Sicherheitsbehörden müssten Auskunft darüber geben, ob die berüchtigte Software auch gegen deutsche Journalisten eingesetzt worden sei.

Die Vorsitzende der Deutschen Journalistinnen- und Journalisten-Union (dju), Monique Hofmann, forderte Einschränkungen für den Export von Überwachungstechnologie: „Autoritäre Staaten nutzen ‚Pegasus', um kritische und oppositionelle Stimmen zum Schweigen zu bringen. Ausspäh-Software darf nicht an Staaten geliefert werden, in denen immer wieder Menschenrechte verletzt werden." Erst in diesem Jahr habe die Europäische Union mit der Reform der Dual-Use-Verordnung die Chance auf eine solche starke Regulierung verpasst.

- Politische Reaktionen

Der frühere UN-Sonderberichterstatter David Kaye meinte: „Die Überwachungsindustrie ist außer Kontrolle." Er fordert ein weltweites Exportverbot für Spähsoftware. EU-Kommissionschefin Ursula von der Leyen forderte eine Überprüfung der Enthüllungen über die weltweite Ausspähung von Journalisten, Aktivisten und Oppositionellen: „Wenn es stimmt, dann ist es komplett inakzeptabel. Eine freie Presse ist einer der Grundpfeiler der Europäischen Union."

Auch die stellvertretende Sprecherin der Bundesregierung, Martina Fietz, betonte die Bedeutung der Pressefreiheit. Eine freie Presse und ein freier Rundfunk seien „von besonderer Bedeutung für das Funktionieren eines demokratischen Staates und einer demokratischen Gesellschaft". Ein Sprecher des Bundesinnenministeriums sagte, in Deutschland gälten Recht und Gesetz, „und sämtliche Maßnahmen der Ermittlungsbehörden müssen sich genau danach richten". Er verwies zudem darauf, dass für besondere Ermittlungsmaßnahmen, etwa eine Telekommunikationsüberwachung, ein Richtervorbehalt gelte.

Der stellvertretende Fraktionschef der Grünen im Bundestag, Konstantin von Notz, sprach von einem „ultimativen Spionageangriff" und „massiven Verstößen gegen die Rechtsstaatlichkeit". Er nannte das „einen ernsten und problematischen Vorgang. Wenn Unrechtsstaaten diese Technik einsetzen, um Oppositionelle und Journalisten auszuforschen und gegebenenfalls am Ende in die Folterkeller zu führen, dann sieht man, wie groß das Problem ist und wie schlimm diese Technik missbraucht werden kann." Man müsse dann genauso über mögliche Konsequenzen diskutieren, wie wenn EU-Staaten wie Ungarn solche Software einsetzten. Von Notz forderte eine strenge Regulierung des Umgangs mit Spionageprogrammen – etwa durch internationale Abkommen oder Exportverbote.

Frankreichs Regierungssprecher Gabriel Attal reagierte erstaunt und entrüstet auf die Enthüllungen: „Das ist natürlich ein äußerst schockierender Sachverhalt." Er kündigte – nicht näher detaillierte – Untersuchungen an. „Wir hängen sehr an der Pressefreiheit."

Forderungen nach einer Untersuchung kommen auch aus Ungarn, wo Journalisten und Oppositionelle mit der Software bespitzelt wurden. Drei Mitglieder des Parlamentsausschusses für nationale Sicherheit beantragten eine Sondersitzung, um Regierungsbehörden zu ihrer möglichen Verwicklung in die Überwachungstätigkeiten zu befragen. Der Vorsitzende des Ausschusses, János Stummer, ein Abgeordneter der rechtsgerichteten Oppositionspartei Jobbik, erklärte, eine Überwachung wie von den Journalisten aufgedeckt, sei in einem Rechtsstaat nicht legal. Der Ausschuss wolle Sicherheitsbehörden und Geheimdienste zu den Vorwürfen befragen. Stummer verwies jedoch darauf, dass eine Mehrheit der Ausschussmitglieder Abgeordnete der Regierungspartei seien, die mit einem Boykott eine Untersuchung verhindern könnten. „Unsere Sichtweise ist, dass ein Schweigen im Wesentlichen ein Eingeständnis wäre, dass die Regierung tatsächlich in diese Sache verwickelt ist“ (Obermaier/Obermayer/Wiegand, Spähangriff auf Staatsspitzen, SZ 21.07.2021, 1; Obermaier/Obermayer/Wiegand, Cyberangriff auf die Demokratie, SZ 19.07.2021, 1; Scharfe Kritik an Überwachungssoftware, www.tagesschau.de 19.07.2021; Spyware: Neue Überwachungsvorwürfe gegen israelischen Software-Anbieter NSO, www.heise.de 19.07.2021, Kurzlink: https://heise.de/-6141286).

Weltweit

Globale Initiative gegen biometrische Erkennung im öffentlichen Raum

175 zivilgesellschaftliche Organisationen, Aktivisten und Forscher aus der ganzen Welt fordern ein Verbot des Einsatzes biometrischer Überwachungstechnik. Instrumente zur Identifizierung von Menschen aus der Ferne wie Videoüberwachung mit automatisierter Gesichtserkennung sind in der Lage die Betroffenen auf Schritt und Tritt zu verfolgen und auszusondern sowie Profile über sie zu erstellen. Sie untergraben gemäß dieser Initiative so die Menschenrechte und bürgerlichen Freiheiten, weshalb in einem offenen Brief an die Gesetzgeber ein globaler Bann biometrischer Überwachungstechnik im öffentlichen Raum gefordert wird.

Das Verbot müsse für Regierungen, Strafverfolgungsbehörden und private Akteure gelten. Das Bündnis will einen Schlussstrich unter die Entwicklung einschlägiger Instrumente für eine massenhafte oder diskriminierende gezielte Überwachung gezogen wissen. Diese stellten einen Angriff auf die Privatsphäre und den Datenschutz dar, „verschärfen Ungleichheit sowie Diskriminierung und haben das Potenzial die Meinungs- und Versammlungsfreiheit mundtot zu machen“. So werde es noch einfacher legitimen Protest zu kriminalisieren.

Auf die Beine gestellt haben die Allianz Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, die Internet Freedom Foundation (IFF) und die brasilianische Verbraucherschutzorganisation Instituto Brasileiro de Defesa do Consumidor (IDEC). Zu den Erstunterzeichnern gehören auch Institutionen wie AlgorithmWatch, der Chaos Computer Club Luxemburg, Digitalcourage, Digitale Gesellschaft, Electronic Privacy Information Center, Epicenter.works, La Quadrature du Net, Privacy International und Statewatch. Die Kampagne steht für weitere Unterstützer offen.

Die Beteiligten wollen erreichen, dass alle öffentlichen Investitionen in biometrische Techniken zur massenhaften oder gezielten Überwachung gestoppt werden. Weder öffentliche Einrichtungen noch private Unternehmen dürften sie nutzen oder vorantreiben. An Investoren richtet sich der Appell die von ihnen finanzierten Firmen aufzurufen entsprechende Entwicklungen oder den Vertrieb solcher Werkzeuge einzustellen.

US-Konzerne wie Amazon, Microsoft und IBM haben den Verkauf von Programmen zur Gesichtserkennung an die Polizei bereits dauerhaft oder vorübergehend gestoppt. Offenbar seien ihnen die problematischen Auswirkungen bewusst, heißt es von dem Bündnis. Der folgerichtige zweite Schritt wäre es aber, die Finger ganz von solchen Instrumenten zu lassen.

Daniel Leufer, Analyst für Europapolitik bei Access Now, meint: „Gesichtserkennung und verwandte biometrische Erkennungstechnologien haben keinen Platz in der Öffentlichkeit.“ Sie schafften gefährliche Anreize für Diskriminierung und eine unverhältnismäßige Anwendung, sodass sie „hier und jetzt verboten werden müssen“. Leufers für Lateinamerika zuständige Kollegin Verónica Arroyo ergänzte, viele Regierungen beriefen sich auf die öffentliche Sicherheit und behaupteten, „dass sie rechtliche Schutzmaßnahmen ergreifen“. Die Erfahrung zeige, dass damit die schädlichen Folgen der Technik nur verschleiert würden.

Die EU-Kommission will mit ihrem Gesetzespaket für Künstliche Intelligenz (KI) Echtzeit-Gesichtserkennung weitgehend untersagen. Damit blieben aber Ausnahmen möglich für die Verfolgung besonders schwerer Verbrechen. Bürgerrechtsgruppen drängen mit der Europäischen Bürgerrechtsinitiative „Reclaim Your Face“ dagegen auch auf dem alten Kontinent schon seit ein paar Monaten für ein komplettes Verbot biometrischer Massenüberwachung (Krempl, Gesichtserkennung: Globaler Appell zum Verbot biometrischer Überwachung, www.heise.de 08.06.2021, Kurzlink: https://heise.de/-6064806).

Weltweit

Erpressungsangriff mit Kaseya-Software

Bei einer Attacke mit Erpressungssoftware haben Hacker auf einen Schlag hunderte Unternehmen ins Visier genommen. Sie nutzten eine Schwachstelle beim US-amerikanischen IT-Dienstleister Kaseya mit Sitz in Miami/Florida, um dessen Kunden mit einem Programm zu attackieren, das Daten verschlüsselt und Lösegeld verlangt. Folgen waren bis nach Schweden zu spüren, wo die Supermarkt-Kette Coop fast alle Läden schließen musste. Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) meldete sich auch ein betroffener IT-Dienstleister aus Deutschland. Dessen Kunden seien in Mitleidenschaft gezogen worden, sagte ein BSI-Sprecher.

Es handele sich um einige Tausend Computer bei mehreren Unternehmen.

US-Präsident Joe Biden ordnete eine Untersuchung des Angriffs durch die Geheimdienste an: „Der erste Eindruck war, dass die russische Regierung nicht dahintersteckt, aber wir sind uns noch nicht sicher." IT-Sicherheitsexperten hatten die Attacke anhand des Software-Codes der Hackergruppe REvil zugeordnet, die in Russland verortet wird. REvil steckte wenige Wochen zuvor bereits hinter dem Angriff auf den weltgrößten Fleischkonzern JBS, der als Folge für mehrere Tage Werke unter anderem in den USA schließen musste. Biden hatte den russischen Präsidenten Wladimir Putin bei deren Treffen in Genf im Juni 2021 aufgefordert auch keine Aktivitäten von Hackergruppen zu tolerieren und mit Konsequenzen bei weiteren Attacken gedroht.

Kaseya, ein mit zwei Milliarden Dollar bewertetes Unternehmen, teilte mit, nach ersten Erkenntnissen seien weniger als 40 Kunden betroffen. Die Angreifer haben die Software bei IT-Dienstleistern manipuliert, die eigentlich Systeme sicherer machen sollen. Kleine und mittlere Firmen haben oft nicht das Personal und die Kompetenz ihre IT selbst zu warten und vor Angriffen zu schützen und engagieren hierfür Dienstleister, sog. Managed Service Provider (MSP). Diese übernehmen es z.B. Software-Updates einzuspielen. Dafür nutzten sie die VSA-Software von Kaseya. So entstand eine Art Domino-Effekt. Auf diesem Wege traf es auch über mehrere Stufen die schwedische Coop-Kette, bei der die Kassensysteme nicht mehr funktionierten. Nur 5 der gut 800 Märkte und der Online-Shop blieben geöffnet.

Der Schaden hätte auf jeden Fall weit größer sein können: Kaseya hat insgesamt mehr als 36.000 Kunden. Mithilfe des Kaseya-Programms VSA verwalten Unternehmen Software-Updates in Computer-Systemen. Ein Eindringen in die VSA-Software kann den Angreifern also viele Türen auf einmal öffnen. Die IT-Sicherheitsfirma Huntress sprach von mehr als 1.000 Unternehmen, bei denen Systeme verschlüsselt worden seien.

Kaseya stoppte am 02.07.2021 seinen Cloud-Service und warnte die Kunden, sie sollten sofort auch ihre lokal laufenden VSA-Systeme ausschalten. Nach Angaben des Unternehmens waren Kunden des Cloud-Dienstes zu keinem Zeitpunkt in Gefahr – und alle betroffenen Firmen griffen auf lokale VSA-Installationen zurück. Kaseya zeigte sich zuversichtlich die Schwachstelle gefunden zu haben, wolle sie demnächst schließen und die Systeme nach einem Sicherheitstest wieder hochfahren. Am 03.07.2021 kam noch ein Kunde zur Liste der Opfer dazu, der sein lokal laufendes VSA-System nicht abgeschaltet hatte.

Die betroffenen Firmen wurden vor die Wahl gestellt entweder Lösegeld zu bezahlen und dadurch die Chance zu erhöhen, dass ihre Systeme bald wieder laufen, oder diese Systeme neu aufzusetzen. Das kann dauern und ist teuer, weshalb viele Firmen zähneknirschend bezahlen. Sicherheitsbehörden sehen dies nicht gerne. Zum einen ist nicht sicher, ob das Entsperren der Systeme wirklich klappt. Zum anderen gibt es auch keine Sicherheit, ob die Angreifer nicht noch eine weitere Schadsoftware eingeschleust haben. Zudem machen die Hackergruppen mit ihrer Erpressersoftware, der sog. Ransomware, ein großes Geschäft.

Kaseya hat am 26.07.2021 Spekulationen zurückgewiesen, es könnte Lösegeld für den Generalschlüssel zur Freischaltung der betroffenen Computer seiner Kunden gezahlt haben. Weder direkt noch über andere sei Geld an die Angreifer gegangen. Die Hacker hatten für ein solches Entschlüsselungswerkzeug 70 Mio. US-$ gefordert. Da Kaseya keine Angaben zur Herkunft seines Generalschlüssels machte, wurde zum Teil auch spekuliert, das Unternehmen könne ihn bei den Hackern gekauft haben. Die US-Firma betonte jedoch, dass man sich dafür entschieden habe nicht mit den Angreifern zu verhandeln. Die Herkunft des Generalschlüssels blieb unklar. Kaseya versicherte, dass damit zu 100% bei der Attacke verschlüsselte Dateien gerettet werden könnten (Martin-Jung, Angriff mit Kettenreaktion, SZ 05.2021, 15; Hacker-Angriff über IT-Dienstleister Kaseya trifft Hunderte Unternehmen, www.heise.de 05.07.2021, Kurzlink: https://heise.de/-6128388; Kaseya: Kein Lösegeld an Hacker für Generalschlüssel bezahlt, www.heise.de 27.07.2021, Kurzlink: https://heise.de/-6148327).

EU

Kommission beschließt Datenschutzangemessenheit von Großbritannien

Die Europäische Kommission hat am 28.06.2021 den grenzüberschreitenden Export von Daten nach Großbritannien im Rahmen eines Angemessenheitsbeschlusses genehmigt. Damit bescheinigt die Kommission dem aus der EU ausgeschiedenen Land ein Datenschutzniveau, das im Wesentlichen dem in der EU entspricht. Also dürften personenbezogene Daten ungehindert über den Ärmelkanal exportiert werden.

Die Kommission stellt sich damit explizit gegen das EU-Parlament, das sich aus Sorge um zu viel Überwachung gegen den Beschluss ausgesprochen hatte. Das Parlament hatte mit Beschluss Ende Mai 2021 die Behörde Ursula von der Leyens aufgefordert das Vorhaben zu überarbeiten. Vorher müssten unbedingt die britischen Praktiken bei der Massenüberwachung sowie bei der Weitergabe von Daten auf Basis internationaler Abkommen geklärt werden. Diese Bitte berücksichtigte die Kommission explizit nicht.

Konkret hat die EU-Kommission zwei Angemessenheitsbeschlüsse getroffen, einen im Rahmen der Datenschutz-Grundverordnung (DSGVO) und einen im Rahmen der Richtlinie zum Datenschutz bei der Strafverfolgung (DSRl-JI). Angemessenheitsbeschlüsse gibt es beispielsweise auch für die Schweiz, Kanada oder Israel. Ausgenommen sind von der Datenfreizügigkeit lediglich Übermittlungen für die in Großbritannien praktizierte Einwanderungskontrolle. Neu bei derartigen Entscheidungen ist, dass beide Angemessenheitsbeschlüsse auf vier Jahre begrenzt sind.

Auf Seiten der EU führte die Kommissions-Vizepräsidentin für Werte und Transparenz, Věra Jourová, die Verhandlungen, die bereits für den vom Europäischen Gerichtshof für ungültig erklärten Privacy Shield verantwortlich zeichnete. Sie habe die Bedenken von Parlament, den Mitgliedstaaten und vom Europäischen Datenschutzausschuss „aufmerksam zur Kenntnis genom-

men". Falls sich in Großbritannien die rechtlichen Gegebenheiten änderten, werde sie „sofort eingreifen". Datenerhebungen durch britische Nachrichtendienste unterlägen der vorherigen Genehmigung durch ein unabhängiges Rechtsorgan. Wer sich unrechtmäßiger Überwachungsmaßnahmen ausgesetzt sehe, könne dagegen Klage beim Investigatory Powers Tribunal (Gericht für Ermittlungsbefugnisse) einreichen. Kurz vor Abschluss steht auch ein Verfahren zur Annahme der Angemessenheitsentscheidung für Südkorea. Das Verfahren wurde Mitte Juni 2021 eingeleitet (Heidrich, EU-Kommission bewilligt Datenexport nach Großbritannien, www.heise.de 28.06.2021, Kurzlink: https://heise.de/-6121458).

EU

Vorgaben für elektronische Identitäten werden verfeinert

Die Europäische Union (EU) will allen Bürgerinnen und Bürgern das Recht auf eine elektronische Identität (eID) verschaffen. Alle EU-Staaten müssen diesen und Unternehmen künftig digitale Brieftaschen zur Verfügung stellen. In diesen „E-Wallets" sollen diese ihre nationale elektronische Identität (eID) mit anderen Dokumenten wie Führerschein, Abschlusszeugnissen, Geburts- oder Heiratsurkunden und ärztlichen Rezepten hinterlegen können, um sie auf Wunsch vorzeigen zu können. Dies sieht der Verordnungsentwurf für eine europäische digitale Identität (EUid) vor, den die EU-Kommission am 03.06.2021 vorgestellt hat.

Gemäß der Kommission erhalten die Bürger mehr „Souveränität" über ihre Daten und werden „in der Lage sein, mit einem Klick auf ihrem Handy ihre Identität nachzuweisen und Dokumente in elektronischer Form aus ihren EUid-Brieftaschen weiterzugeben". Der Online-Ausweis müsse künftig von jedem Mitgliedsstaat ausgegeben und anerkannt werden. Auch „sehr große Plattformen" wie Facebook, Google & Co. sowie Dienstleister wie Banken sollen verpflichtet werden, den Einsatz der EUid-Wallets auf Verlangen des Nutzers etwa zum Nachweis seines Alters jenseits eigener Login-Dienste zu akzeptieren.

Die europäische „digitale Identität" ist eine Schnittstelle für die vorrangig nationalen digitalen Dokumente, die parallel entwickelt werden. So wird derzeit in Deutschland ein Pilotprojekt für einen digitalen Ausweis auf dem Smartphone durchgeführt. Das Bundeswirtschaftsministerium fördert zudem mit 50 Mio. € drei „Schaufensterregionen", in denen Unternehmen, Banken und Behörden lokale Tauschsysteme für elektronische Dokumente etablieren wollen. Diese sollen sich nach Abschluss des Projekts miteinander zu einem bundesweiten System verbinden, das über die „europäische digitale Identität" wiederum an die anderen EU-Länder angeschlossen wird.

Die für Digitales zuständige Kommissionsvizepräsidentin Margrethe Vestager sprach von einem wichtigen Schritt, „um unser Alltagsleben zu vereinfachen und sich zwischen den Mitgliedsstaaten zu bewegen". Nutzer der EUid könnten künftig in jedem Mitgliedstaat ohne zusätzliche Kosten und mit weniger Hürden dasselbe tun wie zuhause, also etwa außerhalb ihres Heimatlandes eine Wohnung mieten oder ein Bankkonto eröffnen. Der „endlose Kampf" Dokumente hin- und her zu senden, sowie Wartestunden in den Bürgerämtern entfielen.

Mit der Initiative strebe die Kommission eine sichere und transparente Lösung auf Basis der bestehenden eIDAS-Verordnung an. Vestager: „Es geht um unsere Identität und die damit verknüpften Daten." Jeder könne selbst entscheiden, wie viel er über sich preisgeben wolle etwa für einen Login-Prozess. Es müssten nicht mehr persönliche Informationen geteilt werden als heute im analogen Verfahren. Der Einsatz der EUid sei freiwillig. Bisher hätten aber erst 14 der 27 Mitgliedsstaaten einen Online-Ausweis ausgegeben, noch weniger erlaubten damit eine grenzüberschreitende Identifizierung. Es gelte daher eine übergreifende Infrastruktur zu schaffen.

Binnenmarktkommissar Thierry Breton versprach, dass das EUid-Wallet den Zugriff von Hackern auf sehr sensible persönliche Daten nicht vereinfachen werde. Dank „Security by Design" werde die Brieftasche eher einem „digitalen Safe" ähneln, „der unsere Identität schützt". Die Schutzvorkehrungen seien höher als bei vergleichbaren bereits auf dem Markt verfügbaren Lösungen. Entscheidend für das Projekt sei eine „ultrasichere Verschlüsselung". Dabei müsse sich die EU etwa schon auf die Post-Quanten-Kryptografie ausrichten. Mit bestehenden Single-Sign-on-Diensten nutzten private Anbieter wie Facebook und Google oft ihre Position aus, da sie bereits große Datenmengen über die User gesammelt hätten, monierte der Franzose. Diese privaten Anbieter seien so eher Rivalen für die Souveränität der Mitgliedsstaaten. Es gehe darum, dass die Bürger ihre Daten besser kontrollieren könnten. Die Verordnung dürfte laut Breton eine ähnliche Wirkung entfalten wie der Wegfall der Roaming-Gebühren.

Die Kommission will auf Basis einer Empfehlung mit den EU-Staaten und dem Privatsektor bereits vor dem Beschluss der Verordnung durch das Parlament und den Ministerrat zusammenarbeiten, um die Technik sowie den weiteren erforderlichen Rahmen etwa in Form von Normen für die EUid vorzubereiten. Sie strebt an, dass das entsprechende Instrumentarium bis September 2022 steht. Danach soll der Werkzeugkasten in Pilotprojekten getestet werden. Anwendbar sein wird die Verordnung laut dem Plan ein Jahr nach ihrer Verabschiedung. Ausgeben können die virtuelle Brieftasche staatliche und private Stellen.

Der Bundestag hatte im Mai 2021 bereits ein Gesetz beschlossen, wonach die Bundesbürger von September 2021 an die mit dem Personalausweis verknüpfte eID direkt in ihrem Smartphone oder Tablet speichern können. Ein entsprechendes Mobilgerät benötigt dafür aber eine eingebettete Sicherheitsarchitektur auf hohem Niveau. Momentan leisten dies nur Samsung-Geräte der Reihe Galaxy S20. Auch diese verdanken dies nur dem staatlich geförderten Projekt Optimos 2.0.

Das Bundeswirtschaftsministerium fördert aktuell bis zu vier weitere große IT-Projekte im „Schaufenster Sichere Digitale Identitäten" mit gut 50 Mio €, um die Möglichkeiten einer digitalen Ausweisfunktion auf Mobiltelefonen neuerer Generationen zu demonstrieren. Die eID

auf dem elektronischen Personalausweis kommt bisher nicht vom Fleck: Laut dem E-Government-Monitor 2020 haben erst sechs Prozent der Befragten die Online-Ausweisfunktion schon einmal genutzt – genauso viele wie 2019. Dabei ist ein spezielles Lesegerät nicht mehr nötig, wenn ein Handy über einen NFC-Chip zur Nahfeldkommunikation verfügt.

Der IT-Verband Bitkom begrüßte den Ansatz der Kommission: Die geplante Verordnung biete die Chance Vertrauensdienste und digitale Identitäten „fest im europäischen Wirtschaftsraum zu verankern". Das Vorhaben sollte als „wichtiger Beitrag für mehr Daten- und Verbraucherschutz in Deutschland verstanden und gefördert werden". Auch der eco-Verband der Internetwirtschaft lobte, dass sich die Kommission „nun endlich für eine weitere Stärkung von Vertrauensdiensten einsetzt". Dies „löst uns aus der Abhängigkeit von einzelnen monopolierten Anbietern" (Bovermann, Die EU als Login-Anbieter, SZ 05./06.06.2021, 23; Krempl, EUid: Online-Ausweise kommen EU-weit, Facebook & Co. müssen sie anerkennen, www.heise.de 03.06.2021, Kurzlink: https://heise.de/-6061860).

EU

EDSA hebt Hamburgs Eilentscheidung gegen WhatsApp auf

Der Europäische Datenschutzausschuss (EDSA) als übergeordnetes Gremium aller einschlägigen Aufsichtsbehörden der EU hat in einer verbindlichen Eilentscheidung des kürzlich ausgeschiedenen Hamburgischen Datenschutzbeauftragten Johannes Caspar eine im Dringlichkeitsverfahren erlassene Anordnung gegen Facebook nicht gebilligt. Caspar hatte es der Facebook Ireland Ltd. im April 2021 untersagt Daten deutscher Nutzer der Konzerntochter WhatsApp mit eigenen Informationsbeständen zusammenzuführen.

Stein des Anstoßes sind die Änderungen der Nutzungsbedingungen und der Datenschutzbestimmungen, die für europäische Nutzer von WhatsApp gelten sollen. Caspar, dessen Amtszeit Ende Juni nach zwei Perioden endete, sah Grund zu der Annahme, dass die neuen Vorgaben zum Teilen der Daten zwischen WhatsApp und Facebook „mangels Freiwilligkeit und Informiertheit der Einwilligung unzulässig durchgesetzt werden sollen". Um einen möglichen „rechtswidrigen massenhaften Datenaustausch" zu verhindern, hatte er daher im Frühjahr das dringliche Verwaltungsverfahren auf Basis von Art. 66 der Datenschutz-Grundverordnung (DSGVO) eingeleitet.

Für Facebook ist in der EU generell die irische Datenschutzbehörde, die Data Protection Commission (DPC), am Sitz der europäischen Tochterfirma in Dublin zuständig. Die deutsche Niederlassung des Internetkonzerns ist in Hamburg, weshalb hierzulande der dortige Datenschutzbeauftragte das Sagen hat. Der EDSA hat nun beschlossen, dass in dem Hamburger Fall „die Voraussetzungen für den Nachweis des Vorliegens einer Zuwiderhandlung und einer Dringlichkeit nicht erfüllt sind". Er verfügte daher, dass die DPC „keine endgültigen Maßnahmen" gegen Facebook ergreifen müsse.

Der EDSA begründete seine Entscheidung damit, dass die Facebook Ltd. als Verantwortliche bereits Nutzerdaten von WhatsApp „für den gemeinsamen Zweck der Sicherheit und Integrität" des Messenger-Dienstes und anderer Facebook-Unternehmen verarbeite. Dies geschehe offenbar auch bereits für den Zweck Produkte aus dem Konzernkonglomerat zu verbessern. Zugleich verweist der EDSA aber auf „verschiedene Widersprüche, Unklarheiten und Unsicherheiten", die er in den nutzerorientierten Informationen von WhatsApp sowie Stellungnahmen des Chat-Betreibers und „in einigen schriftlichen Verpflichtungserklärungen von Facebook" festgestellt habe. Man sei daher nicht in der Lage gewesen „mit Sicherheit festzustellen, welche Verarbeitungen tatsächlich durchgeführt werden und in welcher Eigenschaft".

Ferner moniert das Gremium, es lägen nicht einmal genügend Informationen vor, um mit Sicherheit feststellen zu können, ob Facebook mit dem Zusammenführen von Nutzerdaten bereits begonnen habe. Diese Verweise auf eine große Intransparenz bei dem Konzernverbund führen zunächst aber zu keinen direkten Konsequenzen. Die Hamburgische Datenschutzbehörde hat laut dem EDSA-Beschluss nicht nachweisen können, dass die DPC es versäumt habe, Informationen im Rahmen eines förmlichen Amtshilfeersuchens gemäß Art. 61 DSGVO bereitzustellen. Ferner entschied der Ausschuss, dass die Annahme der aktualisierten WhatsApp-Geschäftsbedingungen allein keine Dringlichkeit begründeten, da sie „ähnliche problematische Elemente wie die vorherige Version enthalten".

Auch der EDSA geht aber von einer „hohen Wahrscheinlichkeit von Verstößen" gegen die DSGVO angesichts der Aktivitäten von Facebook und WhatsApp aus. Er forderte die DPC daher auf den Fall und die Rolle der beteiligten Unternehmen weiter in einem geregelten Verfahren zu untersuchen. Dabei gelte es vor allem zu prüfen, ob die Facebook-Unternehmen in der Praxis Verarbeitungen durchführen, die eine Kombination oder einen Abgleich der Nutzerdaten von WhatsApp mit anderen Datensätzen beinhalten. Dies könnte etwa durch den Einsatz eindeutiger Kennungen erleichtert werden.

Aktivisten und Datenschützer, v.a. aus Deutschland und Österreich, werfen der irischen Behörde schon seit Langem vor, die zahlreichen Beschwerden gegen die in Irland mit ihren EU-Zentralen ansässigen Internetriesen nicht ernsthaft und zeitnah abzuarbeiten.

WhatsApp hatte den Start der neuen Nutzungsbedingungen mehrfach verschoben und besonders kritische Passagen noch gestrichen. Ende Mai 2021 hieß es nach dem Inkrafttreten, dass es für Nutzer vorerst keine negativen Folgen haben werde, wenn sie den neuen Datenschutz-Bestimmungen des Chatdienstes nicht zustimmen. Es gebe aktuell keine Pläne den Funktionsumfang für sie einzuschränken oder Konten zu löschen. Ein Konzernsprecher hatte erklärt, die Anordnung Caspars beruhe auf einem fundamentalen Missverständnis in Bezug auf die Absicht und den Effekt des rechtlichen Updates und habe keine zulässige Grundlage.

Der bisher stellvertretende und nun kommissarisch tätige Hamburgische Datenschutzbeauftragte Ulrich Kühn bezeichnete die EDSA-Entscheidung als enttäuschend: „Das Gremium, das geschaffen wurde, um die einheitliche

Anwendung der DSGVO in der gesamten EU sicherzustellen, verpasst damit die Chance sich klar für den Schutz der Rechte und Freiheiten von Millionen Betroffenen in Europa einzusetzen." Die DPC sei „trotz unserer über mehr als zwei Jahre hinweg wiederholten Aufforderung, die Frage des Datenaustausches zwischen WhatsApp und Facebook zu untersuchen und gegebenenfalls zu sanktionieren, in dieser Hinsicht nicht tätig geworden". Dass sie jetzt zu einer Prüfung gedrängt werde, sei zumindest „ein Erfolg unserer langjährigen Bemühungen". Allerdings werde diese unverbindliche Maßnahme der Bedeutung der Thematik nicht gerecht. Der EDSA beraube sich damit ferner „perspektivisch eines entscheidenden Instruments, um die DSGVO europaweit durchzusetzen. Dies ist keine gute Nachricht für die Betroffenen und den Datenschutz in Europa insgesamt."

Caspar selbst sieht den Beschluss mit großer Sorge. Inhaltlich stütze der EDSA zwar seine Auffassung. Die auch von den früheren Kollegen angenommene „hohe Wahrscheinlichkeit, dass es derzeit zu einer unrechtmäßigen Datenverarbeitung durch Facebook kommt, zeigt, dass unser Verfahren eben nicht auf einem ‚Missverständnis' aufbaut". Höchst widersprüchlich und „völlig mutlos" sei aber, dass der Ausschuss trotzdem keine Dringlichkeit sehe. Wenn aufgrund klarer Indizien von einer unrechtmäßigen Datenverarbeitung durch Facebook und vermutlich von mehreren 100 Millionen Betroffenen in der EU auszugehen sei, widerspreche dies der Gewährleistungsverantwortung aus der EU-Grundrechtecharta. Es sei zu prüfen, ob in der Sache nicht der Europäische Gerichtshof das letzte Wort haben sollte (Krempl, EU-Datenschützer tragen deutsche Eilanordnung gegen WhatsApp nicht mit, www.heise.de 15.07.2021, Kurzlink: https://heise.de/-6139592).

Österreich

Neues Anti-Terror-Gesetz erlaubt elektronische Fußfessel für Islamisten

Acht Monate nach einem islamistischen Anschlag in Wien verschärfte Österreich seine Anti-Terror-Gesetze. Der Nationalrat beschloss das Gesetzespaket am 07.07.2021. Die neuen Regelungen ermöglichen es den Behörden unter anderem elektronische Fußfesseln für bedingt entlassene Straftäter anzuordnen, die auf der Grundlage von Terrorparagrafen verurteilt wurden. Generell soll die Überwachung terroristischer Straftäter während des Vollzugs und nach Entlassung auf Bewährung verstärkt werden.

Am 02.11.2020 hatte ein Anhänger der Terrormiliz „Islamischer Staat", der auf Bewährung aus der Haft entlassen worden war, in der Wiener Innenstadt vier Menschen erschossen, bevor er selbst von der Polizei getötet wurde. Die deutsche Bundesanwaltschaft teilte nun mit, dass zwei junge Islamisten aus Osnabrück und Kassel ihren Ermittlungen zufolge vorab von dem Anschlag in Wien gewusst haben. Die Bundesanwaltschaft verdächtigt die Männer demnach der Nichtanzeige geplanter Straftaten und ließ am Morgen ihre Wohnungen durchsuchen.

Täter können nun zu einer Distanzierung von dem sozialen Umfeld angehalten werden, das zu ihrer Radikalisierung beigetragen hat – etwa radikal-salafistische Bewegungen und religiöse Einrichtungen. Menschen, die nach einem der Terrorparagrafen des Strafgesetzbuchs verurteilt werden, droht künftig auch der Entzug der Staatsbürgerschaft, sofern sie Doppelstaatsbürger sind. Zudem können sie den Führerschein verlieren. Außerdem werden bestimmte politische Zeichen auch der rechtsextremen Szene verboten. Dabei wehrte sich die rechte FPÖ im Parlament vehement gegen das Verbot der Symbole der rechtsextremen Identitären. Fraktions- und Parteichef Herbert Kickl bezeichnete die Identitären erneut als rechte Nicht-Regierungsorganisation (NGO).

Die Schaffung eines Straftatbestands für „religiös motivierte" Verbrechen wurde von Opposition und Justiz-Vertretern heftig kritisiert. Die Präsidentin der österreichischen Richtervereinigung, Sabine Matejka, nannte es im besten Fall unnötig die „religiöse Motivation" hinter einer Straftat hervorzuheben. Es sei besorgniserregend, dass andere Motivationen, etwa rassistische, in dem Straftatbestand nicht genannt würden. Kritik an der neuen Gesetzgebung kam auch von Islamverbänden. Sie werden in der neuen Gesetzgebung dazu verpflichtet eine Art Imame-Verzeichnis zu führen. Auch Kirchenvertreter hatten diese Maßnahme verurteilt (Österreich verabschiedet umstrittenes Anti-Terror-Gesetz, www.spiegel.de 07.07.2021; Neue Anti-Terror-Gesetze, SZ 08.07.2021, 7).

Frankreich

Versicherungskonzern erhält Millionen-Bußgeld-Bescheid

Die französische Datenschutzaufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) hat ein Bußgeld in Höhe von 1,75 Mio. € gegen den französischen Versicherungskonzern AG2R La Mondiale verhängt. Sie begründet ihre Millionenstrafe für AG2R La Mondiale damit, dass der vor allem im Bereich Altersvorsorge, Renten- und Krankenversicherung tätige Konzern die Daten von Millionen von Personen „über einen übermäßig langen Zeitraum aufbewahrt" sowie Informationspflichten bei Telefon-Marketingkampagnen nicht nachgekommen sei. Das Unternehmen habe die monierten Praktiken inzwischen abgestellt.

AG2R La Mondiale hatte laut der CNIL in seinen Kundendatenbanken keine Löschfristen implementiert. Der im Sportsponsoring sehr aktive Konzern habe teils sensible Informationen aus den Bereichen Gesundheit und Finanzen von mehr als zwei Mio. Kundinnen und Kunden über das Vertragsende hinaus gespeichert. Zudem seien Daten von knapp 2.000 Interessenten archiviert worden, obwohl diese seit mehr als drei bis fünf Jahren keinen Kontakt mehr zu dem Unternehmen gehabt hätten.

Die CNIL wirft dem Versicherer ferner vor, es seien Telefongespräche von Subunternehmern mitgeschnitten worden, ohne dass die kontaktierte Person über das Prinzip der Aufzeichnung oder über ihr Einspruchsrecht im Sinne der Datenschutz-Grundverordnung (DSGVO) aufgeklärt worden sei. Wegen ähnlicher Verstöße hatten die französischen Kontrolleure zuvor bereits den Handelsriesen Carrefour (vgl. DANA 1/2021, 52 f.) und

den Schuhversand Spartoo sanktioniert (Krempl, EU-Datenschutzstrafen für TikTok und französische Versicherungsgruppe, www.heise.de 23.07.2021, Kurzlink: https://heise.de/-6146707).

Italien

DSGVO-Verhaltensregeln für Bonitätsbewertungen

In Italien wurde ein Genehmigungsverfahren von Verhaltensregeln im Sinne des Art. 40 DSGVO abgeschlossen. Die Regelungen traten umgehend nach Veröffentlichung im offiziellen Gesetzesblatt in Kraft. Damit schließt das am 12.06.2019 begonnene Aufstellungsverfahren mit der Akkreditierung der Kontrollinstanz ab. Die „Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito“ (ANCIC) als Vereinigung einzelner Wirtschaftsunternehmen aus dem Bonitäts-Analysebereich hatte zuvor mit juristischer Unterstützung der Rechtsanwaltskanzlei Panetta&Associati die Verhaltensregeln für seine Mitgliedsunternehmen ausgearbeitet.

Ziel des neuen „Codice di condotta“ ist es Rechtssicherheit für italienische Unternehmen, die in der Bonitätsanalyse tätig sind, zu schaffen, so die Präambel: „In den vorliegenden Verhaltensregeln sind angemessene Sicherheiten und Durchführungsbestimmungen in Bezug auf die Verarbeitung personenbezogener Daten zum Schutz von Betroffenenrechten festgelegt, die im Rahmen der Ausübung der Verarbeitung von geschäftlichen Informationen beachtet werden müssen, um einerseits die Klarheit und Transparenz in Geschäftsbeziehungen, sowie angemessene Kenntnisse und Verbreitung solcher Informationen, und andererseits die Qualität, die Bedeutung, die Richtigkeit und die Aktualität der verarbeiteten personenbezogenen Daten zu garantieren.“

„Informazione commerciale“, geschäftliche Information, ist nach der Definition in Art. 2 Nr. 2 lit. a Codice jedes Datum, auch lediglich bewertend, das sich auf vermögensrechtliche, wirtschaftliche, finanzielle, kreditbezogene, unternehmensbezogene, industrielle, organisatorische, produktive, unternehmerische oder auch berufliche Aspekte einer natürlichen Person bezieht. „Um Geschäftsinformationen verarbeiten zu können, kann der Anbieter personenbezogene Daten beim Betroffenen selbst, bei öffentlich oder allgemein zugänglichen Quellen oder bei anderen vom Gesetz autorisierten Institutionen erheben“ (Art. 4 Abs. 1 Codice).

Unter öffentlichen Quellen („fonti pubbliche“) werden öffentliche Register wie das Handelsregister verstanden, während allgemein zugängliche Quellen („fonti pubblicamente e generalmente accessibili da chiunque“) Zeitungen oder auch frei zugängliche Internetseiten sein können.

Informationen, die aus öffentlich oder allgemein zugänglichen Quellen stammen, haben grundsätzlich gem. Art. 14 DSGVO die Informationspflicht des Betroffenen zur Folge. Deren Umsetzung werden durch die neuen Verhaltensregeln vereinfacht. Den einzelnen Unternehmen wird es ermöglicht, die Informationspflichten über ein neu geschaffenes Internetportal der ANCIC vorzunehmen, die somit als Repräsentant der jeweiligen Unternehmen auftritt (Art. 5 Abs. 1 Codice). Dort werden auch die Pflichtangaben des Art. 14 Abs. 1, 2 DSGVO aufgeführt. Eine Ausnahme wird kleineren Unternehmen gewährt, die einen Jahresumsatz unter 300.000 € aufweisen. Diese dürfen auf ihrer eigenen Website über die Verarbeitung von personenbezogenen Daten aufklären (Art. 5 Abs. 3 Codice).

Art. 6 Abs. 1 Codice regelt: „Die Verarbeitung von Geschäftsinformationen von personenbezogenen Daten aus Quellen wie in Art. 4 (...) benötigt keine Einwilligung des Betroffenen.“ Das berechtigte Interesse des Verarbeiters (Art. 6 Abs. 1 S. 1 lit. f DSGVO) zielt auf einen fairen Wettbewerb und ein funktionierendes Marktgeschehen ab. Die Verarbeitung von Daten im Sinne des Art. 9 DSGVO wird ausgeschlossen (Art. 3 Abs. 1 Codice). Die Datenerhebung aus Berichten über „negative Ereignisse“ wie Insolvenzen o.ä. ist eingeschränkt (Art. 8 Codice). Zudem werden eigene Maßstäbe an die IT-Sicherheit gesetzt (Art. 11 Codice). Die Rechte und Interessen der betroffenen Dritten werden für die Interessensabwägung nach Art. 6 Abs. 1 S. 1 lit. f DSGVO präzisiert.

Auf die Betroffenenrechte (Art. 15 ff. DSGVO) wird in Art. 10 Codice hingewiesen. Die Betroffenen können ihre Rechte direkt bei der ANCIC bzw. auf deren neu geschaffenen Seite wahrnehmen, nachdem sie herausgefunden haben, ob und inwieweit sie tatsächlich selbst betroffen sind. Die Überwachung und Einhaltung der Verhaltensregeln gem. Art. 41 DSGVO erfolgt durch den „Organismo di Monitoraggio“, der unabhängig von der ANCIC agiert und aus bis zu fünf Mitgliedern bestehen soll. Neben genauen Abläufen bei Beschwerden und Überprüfungen hat man auch genaue Vorstellungen von den Merkmalen dieser Kontrollinstanz: Deren notwendiges Fachwissen (Art. 41 Abs. 2 lit. a) DSGVO) wird wie folgt beschrieben: „(...) es ist essentiell, dass jeder Angehörige der Kontrollinstanz ein angemessenes Kompetenzniveau garantiert, das als Zusammenspiel von Wissen, Erfahrung und den nötigen Mitteln für eine effiziente Ausübung der übertragenen Aufgaben zu verstehen ist. Dafür müssen die Angehörigen der Kontrollinstanz, sowohl individuell als auch universell als Einrichtung, über ein vertieftes Wissen und Verständnis um die Materie der geschäftlichen Informationen, mit besonderem Blick für die Probleme des Datenschutzes personenbezogener Daten verfügen“ (Art. 12 Abs. 3 lit. d Codice). Zu möglichen Interessenskonflikten heißt es: „Jedes Mitglied der Einrichtung muss dauerhaft absolute Unparteilichkeit und Unabhängigkeit garantieren und dabei jeden Interessenskonflikt vermeiden, ob real oder potenziell, ob für sich selbst oder einen Verwandten bis einschließlich dritten Grades, Ehegatten oder Lebenspartner“ (Art. 12 Abs. 3 lit. c Codice).

Die Verhaltensregeln können ein Beispiel für andere sein. Wenige Tage nach der Veröffentlichung durch die italienische Datenschutz-Aufsicht wurde auch der erste Verhaltenskodex auf europäischer Ebene unter Federführung der belgischen Datenschutz-Aufsicht zum Thema Cloud Services genehmigt (Wehowsky, DSGVO-Verhaltensregeln in Italien: Code-of-Conduct zur Bonitätsauskunft von Betroffenen, www.iitr.de 20.05.2021).

Niederlande

Bußgeld gegen TikTok

Die niederländische Aufsichtsbehörde, die Autoriteit Persoonsgegevens (AP) hat ein Bußgeld in Höhe von 750.000 € gegen TikTok verhängt. Sie sanktionierte damit den Betreiber der Video-App, der zum chinesischen Konzern ByteDance gehört. Die AP wirft TikTok vor die Privatsphäre vor allem von Kindern verletzt zu haben. Die Informationen, die niederländische Nutzer bei der Installation und Nutzung der App erhielten, seien lange Zeit nur auf Englisch und daher schwer verständlich gewesen. Indem der Betreiber seine Datenschutzerklärung nicht auf Niederländisch angeboten habe, sei gerade den zahlreichen jüngeren Anwendern nicht ausreichend klar geworden, „wie die App personenbezogene Daten erhebt, verarbeitet und weiter nutzt". Dies sei mit der Datenschutz-Grundverordnung (DSGVO) unvereinbar.

Die niederländischen Kontrolleure hatten ihre Untersuchung 2020 gestartet, da sie Bedenken hatten, dass TikTok die Privatsphäre der besonders gefährdeten Gruppe der Kinder nicht hinreichend schützt. Damals hatte das Unternehmen noch keinen Hauptsitz in der EU angemeldet. Daher war es Aufsichtsbehörden in allen Mitgliedsstaaten möglich die Praktiken von TikTok unter die Lupe zu nehmen. Inzwischen hat der App-Anbieter angegeben sich dauerhaft in Irland niedergelassen zu haben. Hauptsächlich für ihn zuständig ist so die irische Data Protection Commission (DPC), die allerdings bereits mit vielen anderen Internetgrößen wie Google, Facebook und Twitter in ihrem Aufgabengebiet übermäßig beschäftigt ist. Die AP war daher nur noch befugt über die Datenschutzerklärung zu entscheiden, da TikTok hier mittlerweile nachgebessert hatte und der Fall damit geschlossen war.

Gemäß der AP-Vizepräsidentin Monique Verdier werden die weiteren Ergebnisse der Untersuchung nun an die DPC übermittelt. Es liege dann an dieser ein endgültiges Urteil über sämtliche ins Spiel gebrachten Datenschutzverletzungen zu fällen. Ein heikler Punkt bleibe etwa, dass es für Kinder immer noch möglich sei bei der Registrierung ein höheres Alter einzutragen, sich damit als älter auszugeben und mehr Risiken einzugehen.

Verdier betonte, es gebe auch Menschen mit bösen Absichten auf TikTok: „Sie verwenden die Aufnahmen für eine unerwünschte Verbreitung, Mobbing oder Cyber-Grooming". TikTok habe zwar verschiedene Änderungen versprochen und umgesetzt, um die App für Nutzer unter 16 Jahren sicherer zu machen. Eltern können die Privatsphäre-Einstellungen der Konten ihrer Kinder etwa nun von ihren eigenen Smartphones aus verwalten. Dies reiche aber noch nicht. Die italienische Datenschutzbehörde hatte bereits im Januar 2021 verfügt, dass TikTok keine Daten mehr von europäischen Nutzern verarbeiten darf, „deren Alter nicht mit voller Sicherheit festgestellt werden konnte".

TikTok hat laut der AP Einspruch gegen den Bußgeldbescheid eingelegt. Das Unternehmen verweist darauf, dass die Datenschutzerklärung und eine besonders leicht verständliche, gekürzte Version für jüngere Anwender bereits seit Juli 2020 auf Niederländisch zur Verfügung stünden. Insgesamt haben in Holland 3,5 Mio. Nutzende von Mobiltelefonen die App installiert (Krempl, EU-Datenschutzstrafen für TikTok und französische Versicherungsgruppe, www.heise.de 23.07.2021, Kurzlink: https://heise.de/-6146707).

Schweiz

Volksabstimmung bestätigt Anti-Terror-Gesetz

56,6% der abstimmenden Schweizerinnen und Schweizer haben am 13.06.2021 für ein neues Anti-Terrorgesetz gestimmt, mit dem der Bundesrat und das Parlament der Schweiz eine rechtliche Grundlage dafür schaffen, dass die Polizei im Gefahrenvorfeld eingreifen kann. Gemäß der Begründung der Initiative kann die Polizei bisher in der Regel erst einschreiten, wenn eine Person eine Straftat begangen hat. Um das zu ändern, hatte das Parlament im Sommer 2020 das „Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus" (PMT) beschlossen.

Gegen das Gesetz hatte sich ein Komitee gebildet, das u.a. von der aus Bosnien-Herzegowina stammenden Juristin Sanija Ameti gegründet worden war. Zusammen mit ihrer Partei, den Grünliberalen, wurden über 50.000 Unterschriften gesammelt, so dass eine Volksinitiative zustande kam. Schon bei der Gesetzgebung war das Gesetzesvorhaben massiv kritisiert worden, was aber weder die Regierung noch das Parlament beeindruckte. Justizministerin Keller-Sutter verwies vielmehr bei jeder sich bietenden Gelegenheit auf die angeblich europaweit gestiegene Terrorismusgefahr. Die Kritik in einem offenen Brief von Dutzenden namhafter Schweizer Juristen an der geplanten Terrorismus-Definition konterte sie mit der Bemerkung: „Bei Rechtfragen gibt es immer verschiedene Meinungen."

Die Polizei soll gemäß dem nun gebilligten Gesetz einschreiten können, wenn „konkrete und aktuelle Anhaltspunkte vorliegen, dass von einer Person eine terroristische Gefahr ausgeht". Solche Gefährder können auf Antrag eines Kantons, des Geheimdienstes NDB oder einer Gemeinde zu Ansprachen eingeladen und verpflichtet werden sich regelmäßig bei der Polizei zu melden. Außerdem sieht das Gesetz ein Kontakt- und Ausreiseverbot vor und auch eine Abschiebehaft.

Als terroristische Gefährder gelten gemäß der Vorlage Personen, wenn wegen „konkreter und aktueller Anhaltspunkte davon ausgegangen werden muss, dass sie oder er eine terroristische Aktivität ausüben wird". Als terroristische Aktivität gelten Bestrebungen zur Beeinflussung oder Veränderung der staatlichen Ordnung, die durch die Begehung oder Androhung von schweren Straftaten oder mit der Verbreitung von Furcht und Schrecken verwirklicht oder begünstigt werden sollen.

Mit diesen Definitionen könnten präventive und Zwangsmaßnahmen alle treffen, die aus politischen Gründen „Furcht und Schrecken" verbreiteten, kritisierte vor der Abstimmung der UN-Sonderberichterstatter für Folter, Nils Melzer. Das könnten Rechtspopulisten sein, die vor Überfremdung warnen, genauso wie Klimaaktivisten, die vor der Klimakrise warnen, – oder auch er selbst. Auch die Menschenrechtskommissarin

des Europarates, Dunja Mijatović, findet die Definitionen zu vage; sie hatte die Schweizer Gesetzgebenden aufgefordert das Gesetz daraufhin zu überprüfen, ob es mit den Menschenrechtsverpflichtungen vereinbar ist.

Die Schweizer Regierung hatte argumentiert, das neue Gesetz enthalte Bestimmungen, mit denen eine willkürliche und unverhältnismäßige Anwendung verhindert werden solle. Jede Sanktion sei auf einen Einzelfall bezogen und zeitlich befristet, gegen sie könne beim Bundesverwaltungsgericht Beschwerde eingereicht werden (Pfaff, Sanija Ameti, Die Schweizerin bekämpft das neue Anti-Terror-Gesetz, SZ 07.06.2021, 4; Wilkens, Schweizer stimmen für Anti-Terrorgesetz, www.heise.de 14.06.2021, Kurzlink: https://heise.de/-6069991).

Schweiz

Sprachanalyse für Datenschützer

Die Geschäftsstelle der Deutschen Vereinigung für Datenschutz e.V. (DVD) erhielt mit Datum vom 19.04.2021 per Mail eine Einladung der Schweizer Firma Spitch AG zu einem „Webinar über Speech Analytics - Automatische Digitalisierung und Analyse des Telefonverkehrs am Beispiel einer Schweizer Bank“ am 05.05.2021 mit folgendem Werbetext:

Sprachcomputer entlasten nicht nur die Call Center, sondern erlauben den Unternehmen auch die Analyse von Telefongesprächen in einem nie zuvor gekannten Ausmaß. Dazu lädt der Schweizer Sprachsystemspezialist Spitch AG zu einem Webinar über professionelle Gesprächsanalyse unter Einhaltung des Datenschutzes ein. ... Die für den deutschsprachigen Raum zuständige Marketingchefin Carmen Keller erläutert: „Mit Speech Analytics kann man jedes einzelne Wort und jeden Satz, der im Unternehmen am Telefon gesprochen wird, analysieren und für die Verbesserung der Gesprächsziele einsetzen. Das Potenzial zur Verbesserung der Kundenzufriedenheit bei gleichzeitiger Steigerung der Effizienz in den betrieblichen Abläufen ist enorm.“

Durch die automatische Digitalisierung und Analyse lassen sich Umsatzpotenziale für Up- und Cross-Selling erkennen, Möglichkeiten finden den Kundenservice zu verbessern, die Qualitätskontrollkosten senken, unzufriedene Kunden frühzeitig erkennen und Rückgewinnungs-Maßnahmen einleiten sowie Risiken durch die automatische Erkennung von Betrugsversuchen (Fraud Detection) reduzieren. Speech Analytics erschließt somit weitere Automatisierungspotenziale und prüft kontinuierlich deren Weiterentwicklung. Dazu Carmen Keller: „Bei konsequentem Einsatz der zahlreichen Features erweist sich eine effiziente Sprachanalyse als nachhaltiger Wettbewerbsvorteil.“

Das Schweizer Unternehmen Spitch gehört zu den technologisch führenden Entwicklern und Anbietern von Sprachsystemen für Unternehmen und Behörden. Spitch-Systeme verstehen nicht nur Wörter und Sätze, sondern insbesondere auch den Sinn des Gesagten. Hierzu setzt Spitch auf durchgängig eigenentwickelte Software, die Natural Language Processing (NLP), Artificial Intelligence (AI) und Machine Learning (ML) kombiniert. Die Systeme von Spitch können in der Cloud oder im Rechenzentrum des Kunden zum Einsatz kommen. Sie sind heute schon in allen wesentlichen Branchen in Verwendung, in denen sich Sprachtechnologien besonders anbieten. Dazu gehören Call- und Contact-Center, Banken und Versicherungen, Telekommunikationsfirmen, die Automobil- und Transportbranche, das Gesundheitswesen sowie der öffentliche Dienst. Der Einsatz professioneller Sprachsysteme ermöglicht Kosteneinsparungen bis zu 80 Prozent und führt mit immer besserer Technologie zu einer Steigerung der Kundenzufriedenheit. Auf der Kundenliste von Spitch stehen bspw. die Schweizer Bundesbahnen SBB, Swisscom, Swisscard und Amag, der größte Automobilhändler in der Schweiz.

Die DVD hat an dem Webinar nicht teilgenommen. Das Angebot der Firma ist für Datenschützer interessant, weil hier offenbar – vorrangig wohl in der Schweiz – ein Sprachanalyseprodukt als datenschutzkonform beworben wird, das wie beschrieben gar nicht datenschutzkonform eingesetzt werden kann.

Sollte eine DANA-Leserin oder ein -Leser davon Kenntnis erlangen, dass das Produkt dieser Firma in Deutschland zum Einsatz kommt, so sind wir von der DVD über eine entsprechende Information dankbar: Wir würden uns das dann genauer anschauen.

Schweiz

Regierung vergibt Cloud-Aufträge an Alibaba und US-Unternehmen

Eine 110 Millionen Franken (ca. 100 Mio. €) schwere Ausschreibung konnten sich Alibaba, AWS, Microsoft, IBM und Oracle sichern. Sie sichern künftig staatliche Daten der Schweiz. Der chinesische Cloud-Provider hat neben den US-Anbietern die Ausschreibung gewonnen. Schweizer oder europäische Cloud-Provider wurden nicht berücksichtigt. Besonders wichtig war bei der Ausschreibung der Preis, denn die Kosten wurden in den Vergabekriterien mit 30% gewichtet. Gerade hier konnte Alibaba punkten.

Rechenzentren in der Schweiz betreiben Microsoft und Amazon. Dieser Faktor spielte allerdings bloß zu 10% eine Rolle. Eine Vergabebedingung war dagegen, dass die Bewerber Rechenzentren auf mindestens drei Kontinenten haben und ihre Dienstleistungen einer internationalen Kundschaft zur Verfügung stellen. Entsprechend gering wurde gewichtet, dass Alibaba weder einen Cloud-Standort noch einen juristischen Ableger in der Schweiz hat – eine Tochterfirma in London ist hingegen der Vertragspartner des Bundes. Welche Daten genau ausgelagert werden sollen, ist nicht bekannt.

Der Auftrag unterstreicht die derzeitige Dominanz weniger Cloud-Provider: Alibaba investiert kräftig in sein Cloud-Geschäft und ist bereits Marktführer in Asien. Hauptkonkurrenten aus den USA um das weltweite Geschäft sind Microsoft und Amazon. In Europa soll nun Gaia-X zur Alternative reifen, mit Werten wie Datenschutz, digitale Souveränität, Vertrauen, Transparenz und Offenheit. Dass mittlerweile auch Provider aus den USA und China bei Gaia-X mit an Bord sind, hat allerdings für Erstaunen und

Kritik gesorgt. Geheimdienste in den USA und China sind berüchtigt für ihren Datenhunger und haben über nationale Gesetze, z.B. den US-amerikanischen Cloud Act, Zugang zu den von nationalen Firmen verarbeiteten Daten. Jens Klessmann, Leiter des Bereichs Digital Public Services am Fraunhofer-Institut für Offene Kommunikationssysteme, hielt die Schweizer Entscheidung für bemerkenswert und aus deutscher Sicht für „etwas Neues“: „Beim Cloud-Computing muss man tatsächlich von einem Management der Abhängigkeiten sprechen“. Wie sicher Schweizer Daten bei den ausgewählten Anbietern sind, hänge von der Art der Daten und ihrer Form ab: „Man kann beispielsweise Daten an Alibaba weitergeben, die ohnehin öffentlich sind. Und sensiblere Informationen können ja vorab verschlüsselt werden.“

Die Schweizer Bundesverwaltung hat im Dezember 2020 ihre Cloud-Strategie veröffentlicht. Darin steht unter anderem, dass „in einem ersten Schritt“ dort nur solche Informationen landen sollen, die nicht als „vertraulich“ oder „geheim“ klassifiziert sind. Aber: „Basierend auf den Erfahrungen und weiteren rechtlichen Klärungen wird die Empfehlung künftig angepasst.“ Grundsätzlich liege es in der Verantwortung der Schweizer Bundesministerien zu entscheiden, an welchen Stellen sie Cloud-Dienste in Anspruch nehmen wollen. Diese Entscheidung müssen sie „basierend auf einer Risikobeurteilung und Prüfung der Rechtskonformität“ treffen (Pfaff, Die Schweiz und die Cloud, SZ 02.07.2021, 9; Förster, Schweizer Daten werden nach China und in die USA ausgelagert, www.heise.de 30.06.2021; Kurzlink: https://heise.de/-6124333).

China

Tencent erzwingt biometrische Alterserkennung zwecks Spielzeitbeschränkung

Der Spielehersteller Tencent aus dem südchinesischen Shenzhen hat auf drastische Weise seine Jugendschutzmaßnahmen verschärft, um Kindern die Spielzeit am Computer, insbesondere zur Nachtzeit, zu begrenzen. Dafür setzt das Unternehmen auf Gesichtserkennung. Ein eingebautes Programm, eine Art digitale Nachtwache, scannt dafür das Gesicht des Spielers, um herauszufinden, ob das Kind nicht schon längst ins Bett gehört und am Daddeln gehindert werden muss. Bei der Bettzeit orientiert sich der Spielehersteller an der staatlich verordneten Sperrstunde für jugendliche Spieler im Land. Diese liegt zwischen 22 Uhr abends und 8 Uhr morgens. Bei mehr als 60 seiner Videospiele ist die Schutzfunktion bereits aktiv. Darunter auch bei dem Rollenspiel „Honor of Kings“, das zu den erfolgreichsten Handyspielen der Welt gehört. Bis zu 100 Mio. Chinesinnen und Chinesen zocken das Fantasy-Spiel pro Tag. Wie die Technologie genau funktioniert, ob die Software das Alter anhand von Gesichtsmerkmalen berechnet oder mit Gesichtsdaten abgleicht, die es womöglich aus staatlichen Datenbanken bezieht, ist nicht bekannt.

China ist der größte Markt für Computer- und Videospiele, eine globale Gaming-Hochburg. Mehr als jeder Dritte spielt regelmäßig. Die Videospiel-Industrie ist ein Milliardengeschäft und wichtiger Wirtschaftszweig; Hersteller wie Tencent sind globale Schwergewichte. Gleichzeitig bereitet die unkontrollierte Spiellust den Behörden seit Jahren Sorgen; Staatsmedien sprechen von einem Gift. Viele Games seien zu gewalttätig, zu freizügig, zu süchtig machend. Gerade junge Spielende seien gefährdet der Spielsucht zu verfallen. Chinesische Kinder haben in der Regel nur wenig Freizeit neben der Schule. Nur wenige haben ein Hobby oder sind Mitglied in einer Sportmannschaft. Zocken ist für viele die einzige Rückzugsmöglichkeit, auch um Stress abzubauen.

Seit Jahren erlassen die Behörden deshalb immer striktere Vorgaben, um die Spielzeit von Schülerinnen und Schülern zu reduzieren. Sie sollen lieber fürs echte Leben lernen als sich durch Fantasiewelten zu schlagen. Bereits seit 2019 ist ihre Spielzeit monatlich begrenzt, an Werktagen dürfen sie maximal 90 Minuten spielen. Gedeckelt ist auch, wie viel sie für Onlinespiele und neue Spielfunktionen ausgeben können. Die Vorgaben müssen nicht von den Eltern durchgeboxt werden. Vielmehr stehen die Entwickler unter Druck sich eine Lösung für die Durchsetzung auszudenken. Sonst drohen ihnen Strafen oder die Abschaltung.

Vor diesen neuen Schutzmaßnahmen sind auch Erwachsene nicht gefeit. Wenn der digitale Nachtdienst einen Spieler bei einer Kontrolle für jünger als 18 Jahre hält, fliegt er raus. Protest ist laut Tencent zwecklos. Fälschlicherweise als zu jung identifizierte Erwachsene können es am nächsten Abend wieder probieren. Und solange erst mal ins Bett gehen (Sahay, Digitale Nachtwache, SZ 22.07.2021, 1).

Technik-Nachrichten

noyb gegen Google-Werbe-ID auf Android

Die Datenschutzaktivisten von noyb (European Center for Digital Rights) wollen Google zwingen transparenter mit den Datenspuren auf Androidhandys umzugehen. Der österreichische Datenschützer Max Schrems und seine NGO haben in Frankreich eine Datenschutzbeschwerde eingereicht. Sie fordern eine Prüfung, ob die derzeit gängige Praxis von Google legal ist Informationen aus verschiedenen Apps umfangreich zusammenzuführen.

Im Zentrum der Beschwerde steht Android-Advertising-ID (AAID) – ein Code, der den Besitzer eines Smartphones gegenüber den Apps eindeutig identifiziert. Indem die Betreiber verschiedener Apps und Google selbst auf diesen Code zugreifen können, lässt sich das Onlineverhalten konkret einer Identität zuordnen. „Die versteckte ID ermög-

licht es Google und allen Apps auf dem Telefon Nutzer:innen zu verfolgen und Informationen über das Online- und Offlineverhalten zu kombinieren."

Android ist der Marktführer unter den Betriebssystemen für Smartphones. Auch Einstiegsmodelle etwa für Kinder laufen unter Android. Während der oft lebenslangen Partnerschaft zahlen die Kunden für das vermeintlich kostenlose Betriebssystem mit ihren Daten: Viele der Apps können ihre Erkenntnisse über die Nutzer mit der Identifikationsnummer verbinden. Damit vermitteln sie ein umfassendes Bild von deren Verhalten.

Wer also etwa auf Datingplattformen wie Tinder oder Grindr seine sexuellen Vorlieben eingibt, teilt sie unwissentlich mit Google und seinen Werbepartnern. Aber auch Spiele für Kinder sind immer wieder in Verdacht geraten Daten mit der AAID zu verbinden. Dazu gehörten beispielsweise „Princess Salon", das einen Schönheitssalon für Prinzessinnen simuliert, oder eine App zum Ausmalen von 3D-Figuren. Diese Anwendungen musste Google nach Beschwerden von Datenschützern aus dem App-Store nehmen. Die Aktivisten wollen zu einem Zustand zurück, wo Smartphone-Anwender wählen können, welche Informationen sie mit Werbetreibenden teilen und welche nicht. Im Prinzip sehen die Datenschutzregeln das für EU-Bürger bereits vor. Google hält sich nach Ansicht von noyb nicht daran. Der große Konkurrent Apple, auf den fast der gesamte Rest der Handy-Betriebssysteme entfällt, macht es besser. Seit Februar 2021 müssen die Kunden ausdrücklich zustimmen, bevor das Handy mit der Datensammelei beginnt (Datenschutzbeschwerde gegen Google: Angriff auf Schnüffelapps, www.taz.de 15.04.2021, https://taz.de/!5761123/).

„Technological Solutionism" bei Coronabekämpfung in der Kritik

Die gemeinnützige Organisation AlgorithmWatch und die Bertelsmann Stiftung ließen eine Studie „Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective" erstellen, in der der Nutzen von Contact-Tracing-Apps und Gesichtserkennung bei der Eindämmung untersucht wird, die Zweifel am Nutzen der Technik äußert und vor ihren Folgen warnt.

Im Königreich Bahrain zum Beispiel sollen sich Menschen, die die staatliche Contact-Tracing-App BeAware Bahrain herunterladen, mit ihrer nationalen Identifikationsnummer registrieren und zustimmen, dass der Standort auf ihrem Handy verwendet werden darf. Damit können die Wege jeder Person genau nachverfolgt werden. Amnesty International bezeichnete die App als „höchst invasives Überwachungswerkzeug". Bahrains App wurde dem Report zufolge auch als Grundlage für eine Fernsehsendung namens „Are you at home?" (Sind Sie zu Hause?) verwendet. Der Inhalt: Über die Kontaktdaten aus der App rief man wahllos Menschen an und prüfte während des Ramadans, ob sie zu Hause waren – ob sie wollten oder nicht. Wer brav zu Hause geblieben war, erhielt einen Preis. Erst später änderte man die App dahingehend, dass jeder und jede über die Teilnahme selbst bestimmen konnte.

Durch die Corona-Krise sind Technologien, die in die Privatsphäre von Menschen eingreifen, in vielen Ländern alltäglich geworden – teils auch in der Europäischen Union. Eine Erkenntnis des veröffentlichten Reports ist, dass einige der untersuchten Technologien auch innerhalb der EU verwendet werden, obwohl ihr Nutzen zweifelhaft ist. Für den Report wurden unter anderem Zeitungsbeiträge, wissenschaftliche Studien und Regierungsinformationen ausgewertet.

Grundsätzlich ist der technische Aktionismus vieler Staaten nachvollziehbar: Als sich im Frühjahr 2020 das Coronavirus Sars-CoV-2 in der ganzen Welt ausbreitete, war noch wenig über den Erreger bekannt, einen erprobten Impfstoff gab es nicht. Viele Länder verhängten zunächst Ausgangs- und Kontaktsperren, um die Ausbreitung des Virus einzudämmen. Einen neuerlichen Lockdown hätten Politik und Wissenschaft für die Zukunft verhindern wollen, heißt es in dem Report: Man habe „intelligente" Lösungen gesucht, um Virusträgerinnen und Virusträger schnell aufzuspüren und ihre Kontakte in den jeweils vergangenen zwei Wochen zuverlässig zu rekonstruieren.

Das blinde Grundvertrauen in Technologie beschreiben die Studienautorinnen und -autoren als „technological solutionism". Den Begriff hat der Publizist Evgeny Morozov geprägt; er beschreibt damit den Glauben, dass es für jedes gesellschaftliche Problem eine technische Lösung gibt. Dabei können solche technischen Systeme ebenso in Grundrechte eingreifen wie eine Kontaktsperre – ohne, dass die Wirkung der digitalen Hilfsmittel wirklich sicher wäre, so der Studienverantwortliche Fabio Chiusi: „Man opfert Grundrechte und weiß nicht, was man dafür bekommt."

Die Europäische Union (EU) und die Weltgesundheitsorganisation (WHO) haben früh dafür geworben, solche digitalen Systeme nur unter Berücksichtigung von Grundrechten wie der Privatsphäre einzusetzen. Weiter hieß es, eine Freiwilligkeit müsse vorausgesetzt werden. Dem Report zufolge haben sich viele europäische Länder daran auch orientiert. Als positive Beispiele werden Italien, Dänemark, Estland, die Schweiz und auch Deutschland genannt: Sie haben Contact-Tracing-Apps gebaut, die via Bluetooth auf dem Smartphone funktionieren und pseudonymisiert Kurzschlüssel austauschen. Sie werden bis zur Meldung einer Infektion mit dem Coronavirus nicht auf einem Server gespeichert, sondern lokal auf dem Smartphone. Über die App ist so nicht nachvollziehbar, wer wann wo mit wem Kontakt hatte.

Allerdings gibt es auch europäische Länder, die dem Report zufolge sehr stark in die Privatsphäre ihrer Bürgerinnen und Bürger eindringen. In Polen verfolgt der Staat mit einer App, ob sich Menschen an ihre Quarantäne halten. Die App fordert Nutzerinnen und Nutzer routinemäßig auf ihren Standort anzugeben und Fotos von sich aufzunehmen. Die Daten müssen dann mit dem GPS-Standort und dem Bild des jeweiligen Nutzerkontos übereinstimmen. Der Download der App war verpflichtend. In Norwegen stellte man eine über GPS funktionierende Contact-Tracing-App ein, da man darüber in Echtzeit Nutzerinnen und Nutzer hätte überwachen können. Und eine App in Litauen war der lokalen Datenschutzbehörde zufolge nicht mit der Datenschutz-Grundverordnung vereinbar.

Ob diese technischen Mittel wirklich dabei helfen die Pandemie einzudämmen oder die Gesundheitsdaten einer Person zu erfassen, ist bei vielen technologischen Lösungen dem Report zufolge nicht klar. Die American Civil Liberties Union (ACLU) stellte in einer Analyse fest, dass GPS-Signale nicht genau genug sind, um zu erfassen, wie nah jemand einer Person gekommen ist. Ob man eineinhalb Meter entfernt stehe oder 20 Meter, sei nicht mit Sicherheit zu erkennen. Die Stärke des Bluetooth-Signals, auf das auch die deutsche Corona-Warn-App zurückgreift, kann einer Studie zufolge variieren, etwa wenn das Smartphone in einer Handtasche steckt. Ähnlich hatte sich vor der Veröffentlichung der deutschen Corona-Warn-App auch der Informatiker und D64-Vorsitzende Henning Tillmann geäußert. Auch Gesichtserkennungssysteme können stark daneben liegen – besonders im Zeitalter des Maskentragens.

Selbst der Effekt von Contact-Tracing-Apps ist nicht gut belegt. Forscherinnen und Forscher aus London haben in einer Übersichtsstudie andere Untersuchungen zu automatisierten und teilautomatisierten Anwendungen ausgewertet (The Lancet, Braithwaite, 2020) mit dem ernüchternden Fazit: „Es wurden keine empirischen Belege für die Wirksamkeit der automatisierten Ermittlung von Kontaktpersonen (in Bezug auf die ermittelten Kontakte oder die Reduzierung der Übertragung) gefunden."

Über die deutsche Corona-Warn-App meinte Studienautor Fabio Chiusi, selbst wenn die App nicht wirken sollte, richtet sie zumindest auch keinen Schaden an. Er sieht aber ein ernsthaftes Risiko darin, dass teils invasive Technologien, deren Wirkung noch nicht ausreichend bewiesen sei, in der Fläche ausgerollt werden: Der Einsatz sei nicht nur ungesund für Individuen, sondern auch für Demokratien, denn dadurch normalisiere man totalitäre Methoden wie Überwachung: Auch wenn der soziotechnische Apparat aus einer Gesundheitsnotlage heraus entstanden sei, würden Beispiele zeigen, „dass er gekommen sei, um zu bleiben". In der chinesischen Stadt Hangzhou sollen etwa Gesundheitstracker, die zu Corona-Zeiten eingeführt wurden, nun dauerhaft weiter in Betrieb bleiben.

Gemäß der Studie sind Contact-Tracing-Apps aber nicht alle automatisch sinnlos. Selbst die Studienautorinnen und Studienautoren des Lancet-Berichts meinen, es müsse weitere Forschung geben (Hegemann, Weitreichende Überwachung, wenig Wirkung, www.zeit.de 01.09.2020).

Kurzzeitiges Datenleck bei Klarna

Beim schwedischen Bezahldienstleister Klarna ist es am Vormittag des 27.05.2021 aufgrund „technischer Probleme" zu einem schweren Datenleck gekommen. Nutzende der App berichteten, dass sie die Daten und Transaktionen verschiedener anderer Personen einsehen konnten. Klarna bestätigte das und nahm die App nach eigenen Angaben sofort offline. Kurz danach wurde zumindest der Login über die Website wieder zur Verfügung gestellt. Betroffene berichteten, dass sie bei einem Reload immer andere Konten von Dritten einsehen konnten. Dabei seien Bankverbindungen, Bestellungen, offene Rechnungsbeträge, Namen, Adressen und Telefonnummern sichtbar gewesen.

Klarna bestätigt den Vorfall. Während rund einer halben Stunde seien Nutzerinnen und Nutzern zufällige Benutzerdaten Dritter angezeigt wurden. Davon seien rund 90.000 der insgesamt 90 Millionen aktiven Kunden betroffen gewesen: „Es ist uns äußerst wichtig zu betonen, dass der Zugriff auf die Daten vollkommen willkürlich war und keinerlei Karten- oder Bankdaten angezeigt wurden." Betroffen seien Name, Adressen, Telefonnummern, verifizierte E-Mail-Adressen und Bilder von Bestellungen. „Bankdaten von Kunden, die Steuernummer und Kartendetails waren nicht sichtbar." Klarna räumte ein, das „verschleierte Daten" sichtbar gewesen seien – also die maskierten Karten- und Kontonummern.

Gemessen am DSGVO-Standard sind gemäß der Sprecherin nur nicht-sensible Daten offengelegt worden: „Wir erkennen jedoch an, dass das, was als nicht sensibel gilt, sehr individuell empfunden wird und wir setzen unsere eigenen Standards stets höher als die gesetzlichen Regelungen wie die der DSGVO." Ein interner Fehler habe den Vorfall verursacht; es habe sich „nicht um externen Eingriff in unsere Systeme" gehandelt. Nach einem menschlichen Bedienungsfehler sei ein fehlerhaftes Softwareupdate ins Live-System eingespielt worden. Nachdem der Fehler entdeckt und die Ursache identifiziert wurde, sei die App sofort offline genommen worden.

Der Zahlungsdienstleister hat die zuständigen Behörden über den Vorfall informiert. Er ermittelt, welche Nutzer betroffen waren und in welchem Umfang. Darüber hinaus sollen interne Prozesse überprüft werden, damit sich so eine Panne nicht wiederholt: „Wir möchten uns aufrichtig für jegliche Unannehmlichkeiten entschuldigen."

Der Zahlungsdienstleister Klarna ist spätestens seit der Übernahme der Sofort AG im Jahre 2013 kein Unbekannter mehr in Deutschland. Das Unternehmen bietet für Händler und Kunden verschiedene Zahlungsweisen an, darunter Sofortüberweisung oder Rechnungskauf. Klarna baut sein Produktangebot aus. Seit Anfang des Jahres bietet Klarna auch in Deutschland ein Konto an. Zuletzt hat das Unternehmen eine Milliarde US-Dollar bei Investoren eingesammelt (Briegleb, Datenleck beim Zahlungsdienstleister Klarna: Fremde Konten sichtbar, www.heise.de 27.05.2021, Kurzlink: https://heise.de/-6056032).

Bild: iStock.com/AndreyPopov

Rechtsprechung

EGMR

Großbritannien und Schweden wegen Massenüberwachung verurteilt

Der Europäische Gerichtshof für Menschenrechte (EGMR) erklärte mit Urteilen vom 25.05.2021 britische und schwedische Geheimdienstgesetze für weitgehend illegal (ECHR 165 - 2021, ECHR 164 - 2021). In beiden Fällen erkannten die Richter eine Verletzung der Grundrechte der Europäischen Menschenrechtskonvention (EMRK). Allerdings erklärte eine Mehrheit der Richter es für rechtens, dass die Briten Daten von befreundeten Geheimdiensten erhalten.

Die 2000 im Regulation of Investigatory Powers Act (RIPA) regulierte massenhafte Ausspähung von Kommunikationsdaten verletzt das Grundrecht auf Familienleben und Privatsphäre (Art. 8 EMRK). Das Gesetz erlaubte etwa das Abgreifen der Datenströme an den Seekabeln und wurde durch die Enthüllungen Edward Snowdens als Tempora-Programm bekannt. Ebenso verurteilten die Richter den Erwerb von Daten über Internet-Provider. Außerdem würden durch RIPA, das 2016 durch den Investigatory Powers Act (IPA) abgelöst wurde, die in Art. 10 der Konvention garantierten Rechte einer freien Presse beschnitten.

Zwar sei das präventive Abhören durch die Geheimdienste nicht per se grundrechtlich unzulässig. Doch fehlten entscheidende Kontrollmaßnahmen. Die Grundrechtseingriffe erforderten eine Art „Ende-zu-Ende-Aufsicht". Eine von der Exekutive unabhängige Stelle habe vorab über das Anzapfen der Daten zu entscheiden. Ferner seien Suchbegriffe, die sogenannten Selektoren, zu prüfen und es müsse eine effektive Nachkontrolle stattfinden. Geklagt hatten im britischen Verfahren die Londoner Organisation Privacy International zusammen mit Bürgerrechts- und Journalistenorganisationen aus drei Kontinenten. Eine der Klägerinnen ist CCC-Sprecherin Constanze Kurz.

Privacy International sieht sich durch das erstrittene Urteil bestätigt. Vor allem die geforderten Anforderungen an die Aufsicht über die Geheimdienstaktivitäten seien im Vergleich zum ersten Urteil des Gerichts ausgeweitet, schreibt die Organisation. Die Forderung nach der „Ende-zu-Ende-Aufsicht" bei der geheimdienstlichen Überwachung ist laut Privacy International von entscheidender Bedeutung, nicht nur für den britischen Gesetzgeber. Auch gegen das Nachfolgegesetze IPA klagt die Organisation.

Nicht gefolgt ist die Mehrheit der Richter allerdings dem Ansinnen der Bürgerrechtler auch die zwischen den Five-Eye-Staaten (die Geheimdienstallianz von USA, Großbritannien, Kanada, Australien und Neuseeland) und darüber hinaus üblichen Abkommen als Verletzung der Grundrechte zu sehen. Hier entschied die Kammer mit 12 gegen 5 Stimmen, dass ausreichend klare Regeln für die Übernahme von Daten von anderen Diensten bestehen. Die Richter hoben dabei unter anderem die Rolle des Interception of Communications Commissioner und des Investigatory Powers Tribunal hervor. 12 der 17 Richter waren überzeugt, dass missbräuchliche Anfragen und die Umgehung eigener Gesetze so vermieden werden können. Fünf Kammermitglieder widersprachen in einem Sondervotum und mahnten, die Festlegung von Regeln allein sei nicht ausreichend, auch hier bedürfe es klarer Mechanismen zur Kontrolle des möglichen Missbrauchs.

Noch länger als die britischen Kläger und ihre internationalen Partner hatte das schwedische Centrum für Rättvisa auf das Urteil in seinem Fall warten müssen. Die Bürgerrechtsorganisation legte ihre Klage gegen den Signals Intelligence Act bereits am 14.07.2008 direkt in Straßburg ein. Auch im Fall des schwedischen Signal Intelligence Act bemängelten die Richter vor allem das Fehlen einer effektiven Kontrolle der durch die Überwachungsmaßnahmen entstehenden massiven Grundrechtseingriffe. Nicht nur die Technik der Überwacher, auch die Mittel der Aufsicht müssen den durch neue Technologie entstehenden Möglichkeiten angepasst werden, mahnten sie.

Im Kern fehle es an Löschroutinen für die abgefischten Massendaten sowie an Kontrollen für die Weitergabe der Daten durch den schwedischen Geheimdienst FRA an ausländische Dienste. Auch die nachlaufende generelle Kontrolle der Überwachung ist laut dem Urteil grundrechtswidrig. Das Centrum für Rättvisa erklärte, das in über einem Jahrzehnt erstrittene Urteil sei ein Signal nicht nur für den eigenen Gesetzgeber, sondern auch für die Anforderungen an die Geheimdienstkontrolle in ganz Europa. Zu spät kommt das Signal für den deutschen Gesetzgeber, der gerade die vom Verfassungsgericht gekippte BND-Kontrolle neu geregelt hat, und zwar gemäß der Ansicht von Kritikern unzureichend (Ermert, Überwachungsgesetze: EU-Gerichtshof verurteilt Schweden und Großbritannien, www.heise.de 26.05.2021, Kurzlink: https://heise.de/-6054035).

Britisches IPT

Vorratsdatenspeicherung verstieß gegen EU-Recht

Das britische Investigatory Powers Tribunal (IPT) hat am 22.07.2021 geurteilt, dass ein lange gültiges Gesetz zum massenhaften Sammeln von Nutzerspuren mit EU-Recht unvereinbar war (IPT/15/110/CH). Das Urteil des für die Sicherheitsbehörden zuständigen Gerichts erging auf Klage der Bürgerrechtsorganisation Privacy International (PI). Demgemäß war die Befugnis für die Polizei und Geheimdienste zum anlasslosen massenhaften Erheben und Aufbewahren von Verbindungs- und Standortdaten im Telecommunications

Act von 1984 nicht vereinbar mit dem EU-Recht.

Das IPT vollzieht mit dem Beschluss ein Urteil des Europäischen Gerichtshofs (EuGH) vom 06.10.2020 nach. Dieser hatte damals zum wiederholten Mal festgestellt, dass das flächendeckende und pauschale Protokollieren elektronischer Nutzerspuren in der EU nicht zulässig ist (DANA 4/2020, 263 ff.). Ein solches tief in die Grundrechte einschneidendes Instrument beiße sich mit der Richtlinie zum Datenschutz in der elektronischen Kommunikation (E-Privacy). Die britischen Richter hatten den Fall zuvor dem EuGH vorgelegt.

Für das Tribunal sei das EuGH-Urteil auch nach dem Brexit bindend, heißt es in dem aktuellen Londoner Richterspruch. Die Entscheidung der Luxemburger Kollegen sei während der Übergangsperiode ergangen. Das Austrittsabkommen mit der EU sehe vor Urteile aus diesem Zeitraum anzuerkennen. Man setze so auch den Willen des britischen Parlaments um.

Das IPT verweist in seinen Ausführungen auf die Hinweise des Klägers, dass der Wortlaut des einschlägigen Abschnitts 94 des britischen Telekommunikationsgesetzes „außergewöhnlich weit gefasst" gewesen sei: „Er erlaubte es Anordnungen zu treffen, die eine allgemeine und unterschiedslose Übermittlung von Kommunikationsdaten vorsahen." Das Gesetz habe weder die materiellen noch die verfahrensrechtlichen Voraussetzungen für die Verwendung massenhaft erhobener Nutzerspuren festgelegt.

Der Gesetzgeber hat laut dem Gericht auch keine „objektiven Kriterien" festgelegt, um die Umstände und Bedingungen zu definieren, unter denen Sicherheits- und Nachrichtendiensten Zugang zu diesen Daten gewährt werden solle. Es habe daher nicht nachgewiesen werden können, dass Abschnitt 94 „unbedingt erforderlich" gewesen sei. Zum maßgeblichen Zeitpunkt habe zudem eine Genehmigung der zuständigen Staatsministerin ausgereicht. Die Richter monieren: Offensichtlich habe diese „nicht als unabhängig von der anfragenden Behörde bezeichnet werden" können.

Das Urteil erklärt: „Wir möchten betonen, dass wir heute nicht entschieden haben, welche Folgen diese Erklärung hat. Dies ist nach wie vor eine Streitfrage zwischen den Parteien und wird zu einem späteren Zeitpunkt geprüft werden." Dies wird der Fall sein, wenn es um die allgemeinere Frage der Rechtsmittel geht. Eine Berufung sei nur möglich, wenn noch eine wichtige Grundsatz- oder Praxisfrage zu behandeln wäre.

Wie es mit der Vorratsdatenspeicherung in Großbritannien generell weitergeht, ist ebenfalls noch offen. Die relevanten Bestimmungen sind bereits durch das Überwachungsgesetz Investigatory Powers Act von 2016 mit Wirkung zum 22.02.2019 aufgehoben worden. Damit hat der Gesetzgeber den Sicherheitsbehörden unter anderem die Lizenz erteilt selbst zu Hackern zu werden und wiederum massenhaft Überwachungsdaten zu sammeln. Provider müssen damit auch technische Schutzmaßnahmen beseitigen, wenn staatliche Stellen Zugriff auf Inhalte verlangen.

Das oberste Berufungsgericht, der High Court, hatte 2018 bereits eine Klausel zur Vorratsdatenspeicherung im Notstandsgesetz DRIPA (Data Retention and Investigatory Powers Act) gekippt. Die britische Regierung verwies in ihrer Eingabe vor dem IPT aber zugleich darauf, dass der EuGH in seinen jüngsten Urteilen zum verdachtsunabhängigen Protokollieren von Nutzerspuren auch in Belgien und in Frankreich den Einsatz des Werkzeugs in Ausnahmefällen erstmals für möglich erachtet. Dies gelte etwa, wenn sich ein Staat einer ernsthaften Bedrohung seiner nationalen Sicherheit gegenübersieht, die sich als tatsächlich und gegenwärtig oder vorhersehbar erweist.

Trotz der verbliebenen Fragezeichen begrüßt PI den Beschluss: Für die Bürgerrechtler ist das wichtigste Ergebnis des Urteils, „dass eine jahrzehntelange geheime Datenerfassung für unrechtmäßig erklärt wurde". Sechs Jahre nach dem Einleiten der ursprünglichen Klage herrsche in diesem Punkt zumindest Rechtssicherheit. Auch nach dem erreichten „Meilenstein" ist die Auseinandersetzung für PI nicht vorbei. Man habe das IPT bereits gebeten den Fall im Lichte neuer Erkenntnisse über Geheimdienstaktivitäten im Graubereich weiter zu verfolgen. Parallel hat die Organisation beantragt die zunächst geheim gehaltenen abweichenden Meinungen zweier Richter zu veröffentlichen (Krempl, Britisches Gericht erklärt Vorratsdatenspeicherung für rechtswidrig, www.heise.de 25.07.2021, Kurzlink: https://heise.de/-6147032).

EuGH

Ausnahmen vom One-Stop-Shop zwecks Grundrechtseffektivierung

Gemäß einem Urteil des Europäischen Gerichtshofs (EuGH) vom 15.06.2021 können nationale Datenschutzbehörden in Ausnahmefällen gegen DSGVO-Verstöße vorgehen, auch wenn eigentlich Irland zuständig wäre (C-645/19). Gemäß der Datenschutz-Grundverordnung (DSGVO) ist die nationale Datenschutzbehörde zuständig, wo die Firma ihren Hauptsitz in Europa hat. Im Fall der meisten großen Tech-Unternehmen ist dies die irische Behörde, so für Google, Tiktok oder Apple. Das Urteil konkret trifft Facebook. Die belgische Datenschutzbehörde hatte eine Unterlassungsverfügung gegen Facebook erlassen, in der es um Verstöße gegen die Datenschutzvorschriften ging. Der EuGH bestätigte, dass sie das Recht dazu hatte: „Unter bestimmten Voraussetzungen kann eine nationale Aufsichtsbehörde ihre Befugnis, vermeintliche Verstöße gegen die DSGVO vor einem Gericht eines Mitgliedstaats geltend zu machen, ausüben, auch wenn sie in Bezug auf diese Verarbeitung nicht die federführende Behörde ist."

Die Facebook Ireland, Facebook Inc und Facebook Belgium gemachten Vorwürfe betreffen die Sammlung und Verarbeitung von Daten belgischer Internetnutzerinnen und -nutzer, von denen nicht alle ein Facebook-Konto haben, mittels Cookies, Social Plugins oder per Pixel. 2015 hatte sie der Präsident des belgischen Ausschusses für den „Schutz des Privatlebens" eingereicht – also noch vor Inkrafttreten der DSGVO. Ein in Belgien zuständiges Gericht entschied, dass Facebook nicht alle Menschen ausreichend über den Umgang mit ihren Daten informiert sowie dass die Einwilligung gefehlt habe (DANA 1/2018, 46). Gegen dieses Urteil aus dem Jahr 2018 legte Facebook Berufung ein.

Das zuständige belgische Gericht wollte daraufhin wissen, ob es handeln darf und leitete diese Frage an den EuGH weiter. Grundsätzlich wäre Daten verarbeitende Instanz Facebook Ireland und damit auch die irische Datenschutzbehörde zuständig. Dort liegen bereits ähnliche Verfahren, die federführend der Datenaktivist Max Schrems führt, gegen Facebook vor, die allerdings wegen einiger Nebenschauplätze nur langsam voranschreiten. Kritiker werfen der irischen Behörde vor absichtlich Entscheidungen zu verschleppen (DANA 2/2021, 126 f.).

Der EuGH bestätigte nun, dass entgegen dem Grundprinzip der DSGVO des „One-Stop-Shop" nationale Behörden reagieren dürfen, wenn dabei die „Zusammenarbeit und Kohärenz" beachtet werden. Ziel der DSGVO sei der Schutz der Grundrechte der EU-Bürger. Wenn eine federführende Behörde diesen Schutz nicht sicherstelle, aus welchen Gründen auch immer, hätten die nationalen Behörden das Recht dies selbst zu tun. Sonst bestehe die Gefahr, dass sich Unternehmen dort niederlassen, wo sie am wenigsten zu befürchten haben. Allerdings gälten für diese Fälle klare Regeln. So können nationale Behörden dies in den meisten Fällen nur im Rahmen eines Dringlichkeitsverfahrens tun, dessen Ergebnis nur für drei Monate gilt. Danach müsse der Europäische Datenschutzausschuss (EDSA) ein verbindliches Urteil fällen. Im EDSA sind die nationalen Datenschutzbehörden vertreten; dort hat die irische Behörde nur noch einfaches Stimmrecht.

Die federführende Behörde muss reagieren, wenn eine andere Aufsichtsbehörde dies verlangt. Auch dass die ursprüngliche Klage vor dem Wirksamwerden der DSGVO eingereicht wurde, stellt kein Hindernis dar. Zuvor hatte es bereits eine öffentliche Empfehlung des EuGH-Generalanwalts Michal Bobek gegeben, der schrieb: „Die anderen betroffenen nationalen Datenschutzbehörden seien gleichwohl befugt, in Situationen, in denen es ihnen die Datenschutz-Grundverordnung spezifisch gestattet derartige Verfahren in ihren jeweiligen Mitgliedsstaaten einzuleiten."

Auch Datenschutzbeauftragte aus Deutschland können nun entsprechend gegen Aktivitäten von Facebook oder etwa Google vorgehen. Mit der Entscheidung rechtfertigte u.a. der Hamburger Datenschutzbeauftragte Johannes Caspar seine Anordnung gegen Facebooks Tochterunternehmen WhatsApp, die dem Konzern die Daten-Weitergabe untersagte. Der EDSA entschied jedoch, dass die Grundlagen hier nicht gegeben seien (s.o. S. 192). Dass es jetzt zu massenhaften dringlichen Entscheidungen gegen Facebook kommen wird, glaubt Caspar nicht: „Dennoch dürfte das Instrument, das bislang in der Praxis kaum Anwendung gefunden hat, durch das Urteil aufgewertet werden, um die Rechte und Freiheiten Betroffener zu schützen". Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber, begrüßte die EuGH-Entscheidung: „Wir dürfen nicht tolerieren, dass Unternehmen sich eine federführende Aufsichtsbehörde suchen, die ihrer Verpflichtung zum Schutz dieser Grundrechte nicht entschieden nachkommt." Er finde es deshalb gut, dass es Ausnahmen von der federführenden Zuständigkeit geben kann. Seine Behörde werde „sehr genau prüfen, wann sich diese Möglichkeiten zukünftig ergeben". Facebook nahm wie folgt Stellung: „Wir freuen uns, dass der EuGH den Wert und die Grundsätze des One-Stop-Shop-Mechanismus bestätigt und seine Bedeutung für eine effiziente und einheitliche Anwendung der DSGVO in der gesamten EU hervorgehoben hat" (Muth, Direkter Zugriff auf Facebook, SZ 17.06.2021, Weiß, EuGH: Nationale Datenschutzbehörden haben DSGVO-Befugnisse in Irland, www.heise.de 15.06.2021, Kurzlink: https://heise.de/-6071490).

Österreichischer OGH

Vorlage beim EuGH wegen Facebook-Einwilligungen

Der österreichische Oberste Gerichtshof (OGH) hat mit Entscheidung vom 23.06.2021 im Streit zwischen Max Schrems und Facebook vier Fragen an den Europäischen Gerichtshof (EuGH) weitergeleitet (6 Ob 56/21k). Dabei geht es um nichts Geringeres als die grundsätzliche Frage, und das bereits seit 2018, ob Facebook durch seinen Umgang mit den Nutzerdaten gegen die DSGVO verstößt.

Schrems ist außerdem ein symbolischer Schadenersatz in Höhe von 500 € zugesprochen worden. Diesen bekommt er, weil das soziale Netzwerk seiner Auskunftspflicht nicht ausreichend nachkommt. Der Datenschutzaktivist hatte alle Informationen über sich angefordert, wie es die DSGVO vorsieht, aber nur solche als PDF bekommen, die Facebook für relevant hielt. Zudem teilte das Unternehmen mit, welche Auskunfts- und Downloadmöglichkeiten es gäbe, über die der Suchende selbst alles finden könne. Das hält der OGH für nicht ausreichend. Dies hätte von Schrems erfordert, mit den Werkzeugen in „mindestens 60 Datenkategorien mit Hunderten, wenn nicht Tausenden von Datenpunkten" zu suchen. Der OGH soll das als „Ostereiersuche" bezeichnet haben.

Weiterhin entschied der OGH, Facebook müsse beweisen, dass die Daten vollständig seien. Facebook behauptete zuvor, der Gegenbeweis dazu sei Aufgabe des Suchenden.

Die an den EuGH weitergeleiteten Fragen betreffen vor allem die Einwilligung. Vor Wirksamwerden der DSGVO 2018 hatte Facebook schlicht eine generelle Zustimmung der Nutzenden in die Verarbeitung verlangt. Danach deutete Facebook laut dem Verein noyb (None of your Business) die Zustimmung in einen Vertrag um, durch den die Menschen personalisierte Werbung quasi bestellen würden. Eine Einwilligung ist notwendig, sobald es nicht ausschließlich um eine Verarbeitung geht, die für die Funktionsfähigkeit des Dienstes nötig ist. noyb befürchtet: „Die Erfordernisse einer ‚freien', ‚spezifischen' oder ‚informierten' Einwilligung würden nicht mehr gelten, sobald die Einwilligung als 'Vertrag' angesehen wird."

Der EuGH wird auch gefragt, ob Facebook gegen den Grundsatz der Datenminimierung verstößt, etwa durch die Zusammenführung von Daten von Like-Buttons und Pixel auf anderen Seiten, sowie ob es Kategorien gibt, die gar nicht für Werbezwecke genutzt werden dürfen – das sind z.B. die politische Meinung und sexuelle Orientierung.

noyb bezeichnete die Weiterleitung an den EuGH auf seiner Webseite als „Breaking", so Schrems: „Verliert Face-

book vor dem EuGH, müssten sie nicht nur damit aufhören Daten zu missbrauchen und illegal gesammelte Daten löschen, sondern auch Millionen von Nutzern Schadenersatz zahlen. Wir sind über die Vorlage daher sehr glücklich" (Weiß, Schrems versus Facebook: Österreichischer OGH leitet Fragen an EuGH weiter, www.heise.de 20.07.2021, Kurzlink: https://heise.de/-6142701).

Oberster Gerichtshof Italien

Datenschutz-Einwilligung setzt Transparenz voraus

Der italienische oberste Gerichtshof in Rom, der „Corte di Cassazione", hat mit Urteil vom 25.05.2021 festgestellt: „Im Bereich der Verarbeitung personenbezogener Daten ist eine Einwilligung nur dann wirksam erteilt, wenn sie freiwillig und ausdrücklich für die eindeutig festgestellte Verarbeitungsart abgegeben wurde" (sentenza numero 14381).

Die italienische Datenschutzaufsichtsbehörde, die „Garante per la protezione dei dati personali" (GPDP), hatte dem Unternehmen Mevaluate Onlus 2016 die Verarbeitung personenbezogener Daten verboten. Das Unternehmen berechnet auf Grundlage von erstellten und angelegten Profilen natürlicher oder juristischer Personen die Reputation und Glaubwürdigkeit dieser für Dritte. Dagegen ist das Unternehmen im November 2016 gerichtlich vorgegangen.

Nachdem diese Klage in erster Instanz beim Tribunale di Roma noch Erfolg hatte, wurde dies jetzt durch den „Corte di Cassazione" revidiert. Die Begründung der ersten Instanz aus Rücksicht vor privatautonomen Entscheidungen sei für einen funktionierenden Markt zu sorgen, überzeugte die Richter des obersten italienischen Gerichtshofs nicht: „Dieser Begründung kann aus Sicht des Gerichts nicht zugestimmt werden, denn das Problem beruht nicht auf einer Bedrohung für den ‚Markt' (…). Das Problem einer rechtmäßigen Verarbeitung liegt vielmehr auf einer wirksamen Einwilligung, die im Moment des Beitritts abgegeben wird. Und logischerweise kann man nicht argumentieren, dass der Beitritt zu einer Plattform eine Einwilligung in eine auf einem Algorithmus basierende, automatisierte Verarbeitung darstellt, die für eine objektive Auswertung personenbezogener Daten – wobei weder die Ausführungsmechanismen des Algorithmus noch die berücksichtigten Elemente klar werden – ausreicht."

Eine Einwilligung seitens eines Betroffenen kann also nicht wirksam erteilt werden, wenn die Funktionsweise der automatisierten, technischen Verarbeitung nicht verständlich erläutert wird. Den Verantwortlichen kommt insofern eine präventive Aufklärungspflicht zu. Wie genau diese ausgestaltet sein soll, lässt die Entscheidung aber offen. Die Richter argumentieren im Sinne der DSGVO, wonach gewährleistet sein muss, dass für Betroffene nachvollziehbar wird, was genau mit ihren personenbezogenen Daten passiert, wo und wie genau diese verarbeitet werden (Art. 5 Abs. 1 lit. a DSGVO).

Im italienischen „Codice per la protezione dei dati personali" (kurz: „Codice Privacy"), der nach Einführung der DSGVO weitgehend abgeschafft wurde, fanden sich in Art. 23 grundsätzliche Anforderungen an eine Einwilligung („Consenso"). Diese sind aus Sicht der italienischen Aufsichtsbehörde nahezu komplett in der DSGVO aufgegangen, so dass auch weiterhin gilt, dass eine Einwilligung in jedem Fall „frei, spezifisch, unmissverständlich" und vor allem „informiert" sein muss.

Zudem besagt Art. 22 Abs. 1 DSGVO, dass Betroffene grundsätzlich nicht einer lediglich automatisierten Entscheidung unterworfen sein dürfen. Entscheidungen, die eine Person bewerten und einordnen, sollen nicht einer rein automatisierten Verarbeitung – also einem Algorithmus – allein, sondern vorrangig menschlicher Beurteilung überlassen werden. Die Ausnahme einer „ausdrücklichen Einwilligung" setzt ein beim Betroffenen geschaffenes Verständnis für die angedachten Verarbeitungsmechanismen voraus. Gemäß dieser nationalen Entscheidung müssen Anbieter gewährleisten, dass ihre Verarbeitungstätigkeit transparent verständlich ist, wenn sie auf eine Einwilligung gestützt werden soll. Dies scheitert im Bereich der Tracking-Maßnahmen auf Webseiten häufig daran, dass der Webseiten-Anbieter selbst häufig keinen detaillierten Einblick in die genaue Funktionsweise der eingesetzten Tracking-Algorithmen hat, um deren Zustimmung durch die Webseitenbesucher erbittet (Wehowsky, Oberster Gerichtshof Italien: Datenschutz-Einwilligung nur bei transparenter Verarbeitung, www.iitr.de 31.05.2021).

BVerfG

Staatliches Ausnutzen von Sicherheitslücken eingeschränkt

Mit Beschluss vom 08.062021 wies das Bundesverfassungsgerichts (BVerfG) eine Verfassungsbeschwerde zurück, die sich gegen § 54 des baden-württembergischen Polizeigesetzes zur „präventiv-polizeilichen" Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) richtete (1 BvR 2771/18). Die Klage sei unzulässig, weil die Beschwerdeführenden nicht hinreichend dargelegt hätten, dass sie von der Klausel und der damit verknüpften Option zum Einsatz von Staatstrojanern betroffen seien.

Die Beschwerde gegen die Gesetzesnovelle von 2017 hatte die Gesellschaft für Freiheitsrechte (GFF) zusammen mit Unterstützern vom Chaos Computer Club Stuttgart, zwei Anwälten und Journalisten, einem Onlinehändler und einer Einkaufsgesellschaft für Internetprovider Ende 2018 eingelegt. Die Kläger monierten, dass für die erlaubte Quellen-TKÜ zum Abhören verschlüsselter Kommunikation, etwa über WhatsApp, Signal und Threema, IT-Sicherheitslücken womöglich durch Zero-Day-Exploits ausgenutzt werden müssten.

Die Ermittler haben, so die Beschwerde, kein Interesse daran, dass die Schwachstellen von den Herstellern geschlossen würden. Existierende Sicherheitslücken lieferten den Behörden Fehlanreize. Auch Cyberkriminelle könnten auf die Lücken zugreifen. Das sei unvereinbar mit dem Schutzauftrag des Staates gegenüber den Bürgern und dem vom Bundesverfassungsgericht selbst aufgestellten Grundrecht auf Vertraulichkeit und Integrität von IT-Systemen.

Das BVerfG bestätigte in dem Beschluss, dass eine „grundrechtliche Schutzpflicht" besteht. Betroffen sei-

en das Fernmeldegeheimnis und das sogenannte Computer-Grundrecht. Behörden müssten zum Schutz „informationstechnischer Systeme vor Angriffen Dritter auf diese Systeme beitragen". Prinzipiell sei die informationelle Selbstbestimmung von Nutzenden bedroht, weil sich mit dem Zugang zu deren Daten „weitgehende Kenntnisse über persönlichkeitsrelevante Informationen gewinnen lassen". Zudem hätten Sicherheitslücken „ein über die Offenbarung persönlichkeitsrelevanter Informationen weit hinaus gehendes Schädigungspotenzial": Dritte könnten darüber in Systeme eindringen, diese manipulieren und Abläufe zum Schaden der Betroffenen stören. „Mit dem Risiko der Infiltration durch Dritte ist so auch eine besondere Erpressungsgefahr verbunden." Die staatliche Schutzpflicht schließe daher eine Auflage für den Gesetzgeber ein „den Umgang der Polizeibehörden mit solchen IT-Sicherheitslücken zu regeln" etwa über ein Schwachstellen-Management, auch wenn das Instrument der Quellen-TKÜ „für sich genommen nicht von vornherein verfassungsrechtlich unzulässig" sei. Auch jede Lücke müsse nicht „sofort und unbedingt dem Hersteller" gemeldet, der „Zielkonflikt" aber grundrechtskonform aufgelöst werden.

Die Beschwerdeführenden haben, so der Senat des BVerfG, jedoch nicht in der erforderlichen Weise begründet, dass der festgestellte Schutzauftrag bei ihnen tatsächlich verletzt sein könnte. Sie hätten die einschlägigen gesetzlichen Regeln zum Schutz von IT-Systemen „weder in ihren Grundzügen dargestellt noch ausgeführt", aus welchen konkreten Gründen die Bestimmungen „auch in ihrer Zusammenschau erheblich hinter dem Schutzziel zurückbleiben". Zudem wären die Kläger gehalten gewesen sich zunächst an die Verwaltungsgerichte zu wenden, um von diesen verschiedene Bestimmungen „des Polizei-, des Datenschutz-, des Cybersicherheits- und des IT-Sicherheitsrechts" auslegen zu lassen.

Trotz der formell-juristischen Schlappe sieht der GFF-Vorsitzende Ulf Buermeyer in der Entscheidung einen „großen Erfolg für die IT-Sicherheit". In der Begründung hätten die Richter den Klägern und dem Prozessbevollmächtigter Tobias Singelnstein „in weiten Teilen Recht" gegeben. So müsse die Polizei künftig „bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke" die damit verknüpften Gefahren ermitteln, den „Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ" bestimmen und beides zueinander ins Verhältnis setzen. Die Schwachstelle sei an den Hersteller zu melden, wenn nicht das Interesse an ihrem Offenhalten überwiege.

Zahlreiche weitere Verfassungsbeschwerden gegen Staatstrojaner sind noch anhängig. Allein die GFF ist in Karlsruhe gegen sieben andere entsprechende Gesetze vorgegangen. Sie plant weitere Klagen, etwa gegen die neue Befugnis für alle Geheimdienste, wo die FDP bereits vorgeprescht ist (s.o. S. 177; Janisch, Nützliche Sicherheitslücke, SZ 22.07.2021, 5; Krempl, Bundesverfassungsgericht weist Klage gegen Staatstrojaner zurück, www.heise.de 21.07.2021, Kurzlink: https://heise.de/-6144044)

BVerfG

Bestandsdatenauskunft in Schleswig-Holstein ist verfassungskonform

Die 3. Kammer des Ersten Senats des Bundesverfassungsgerichts (BVerfG) hat mit Beschluss vom 19.04.2021 eine Verfassungsbeschwerde aus der Piratenpartei nicht angenommen, in der es um den Abruf von Bestandsdaten und Passwörtern ging (Az.: 1 BvR 1732/14). Die Klage des Aktivisten Patrick Breyer und fünf seiner früheren Landtagsfraktionskollegen von der Piratenpartei in Schleswig-Holstein richtete sich gegen Vorschriften des Bundes und des schleswig-holsteinischen Landesrechts zur manuellen Auskunft über Bestands- und Nutzungsdaten bei Telekommunikations- und Telemediendiensteanbietern.

Die Polizei und das Landesamt für Verfassungsschutz in Schleswig-Holstein dürfen seit einer 2013 erfolgten Novelle ausdrücklich auf Bestandsdaten wie E-Mail-Adressen und Anschriften sowie Passwörter von Nutzern sozialer Netzwerke wie Facebook, Twitter oder YouTube zugreifen. Die Sicherheitsbehörden benötigen dafür eine richterliche Genehmigung. Betroffene müssen sie nachträglich über entsprechende Maßnahmen benachrichtigen.

Breyer, mittlerweile Abgeordneter im EU-Parlament, und seine Mitstreiter griffen in ihrer Beschwerde zugleich § 15 und einen zugehörigen Verweis auf § 14 Telemediengesetz (TMG) des Bundes an. Damit werden Diensteanbieter von Telemedien zur Erteilung einer Nutzungsdatenauskunft für bestimmte, vorwiegend behördliche Zwecke berechtigt. Ermöglicht wird aber auch eine Abfrage von Bestandsdaten, „soweit dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist".

Die in Frage gestellten Vorschriften des Landes Schleswig-Holstein zum Abruf von Bestandsdaten bei Telekommunikationsanbietern durch Polizei und Verfassungsschutzbehörde genügen laut dem Beschluss vollständig den Maßgaben aus den einschlägigen Urteilen des Bundesverfassungsgerichts von 2012 und 2020. Entsprechende Vorschriften seien verhältnismäßig, wenn sie im präventiven Bereich „an das Bestehen einer konkreten Gefahr geknüpft sind" und für geheimdienstliche Zwecke vorsähen, „dass die Auskunft im Einzelfall zur Aufklärung einer beobachtungsbedürftigen Aktion oder Gruppierung geboten sein muss".

Regeln zur Bestandsdatenauskunft bei Telekommunikationsdienstleistern anhand dynamischer IP-Adressen müssten aufgrund ihres gesteigerten Eingriffsgewichts zumindest dem Schutz von Rechtsgütern von hervorgehobenem Gewicht dienen. Ferner sei eine Dokumentation der Entscheidungsgrundlagen nötig. Dem genügten die schleswig-holsteinischen Vorschriften.

Der Teil der Beschwerde, der sich auf Auskunftsersuchen bei Telemediendiensteanbietern bezieht, wurde als unzulässig zurückgewiesen. Die Kläger hätten nur das Online-Angebot eines Magazins als genutzten Dienst benannt und nicht näher dargelegt, dass sie damit mit einiger Wahrscheinlichkeit von einschlägigen Maßnahmen betroffen sein könnten. Die Beschwerde gegen die TMG-Paragrafen und eine entsprechende Passage des Landesverfassungsschutzgesetzes sei zudem zu spät er-

hoben worden, die entsprechende Einspruchsfrist sei schon abgelaufen. Die am 02.04.2021 in Kraft getretene bundesrechtliche Neufassung der Bestands- und Nutzungsdatenauskunft zur Anpassung der entsprechenden Gesetze an die jüngsten Vorgaben aus Karlsruhe prüften die Richter nicht. Sie waren nicht Gegenstand des Verfahrens (Krempl, Bundesverfassungsgericht weist Beschwerde gegen Bestandsdatenauskunft ab, www.heise.de 19.05.2021, Kurzlink: https://heise.de/-6049630).

BGH

Voraussetzungen für Strafbarkeit von Computersabotage geklärt

Der Bundesgerichtshof (BGH) präzisierte mit einem Urteil vom 08.04.2021 die Voraussetzungen für eine Beihilfe zu versuchter und vollendeter banden- und gewerbsmäßiger Erpressung und zu Computersabotage und hob zugleich eine Entscheidung des Landgerichts (LG) Stuttgart auf (Az. I StR 78/21). Das LG hatte am 06.11.2020 einen 36-jährigen Mann zu einer Freiheitsstrafe von vier Jahren und sechs Monaten wegen Beihilfe in mehreren hundert Fällen verurteilt (Az. 14 KLs 251 Js 48346/14). Der Verurteilte war nach der Entscheidung der Stuttgarter Richter verantwortlich für die Betreuung von Servern, die eine Gruppierung aus mindestens drei Personen für ihre Erpressungen benutzt haben.

Die Täter schleusten Schadsoftware über Werbeanzeigen, die von den Opfern angeklickt wurden, auf deren Computer. Durch die Schadsoftware wurden die Rechner mit der Meldung gesperrt, dass auf dem Computer strafrechtlich relevantes Material wie Kinderpornografie gefunden worden sei. Um die Hardware wieder freizugeben und ein Strafverfahren abzuwenden, sollten die Opfer 100 € über ein elektronisches Zahlungssystem überweisen.

Der BGH bestätigte die Strafbarkeit wegen Beihilfe zur Erpressung und Computersabotage und sorgte gerade im Bereich der Strafbarkeit von unerwünschter Datenverarbeitung für mehr Klarheit. Eine strafbare Computersabotage gem. § 303b StGB beinhaltet eine wesentliche Störung in der Datenverarbeitung wie zum Beispiel das Löschen oder Verändern von Informationen.

Der BGH bestätigte das LG Stuttgart, dass eine Veränderung in der Registry-Datenbank eine strafbare Datenveränderung darstellen kann. Die Täter hatten durch die Schadsoftware einen Sperrbildschirm ausgelöst und dadurch den Zugriff auf den Computer unmöglich gemacht. Dies erreichten sie, indem sie Einträge in der Windows-Registry-Datei hinzufügten, sodass sich beim nächsten Hochfahren des Computers automatisch Dateien veränderten.

Ein weiterer zu klärender Punkt war, ab wann der Störung durch die Veränderung von Daten eine wesentliche strafrechtliche Bedeutung zukommt. Problematisch war hier, dass bei jeder einzelnen Infektion von Rechnern durch die Malware festgestellt werden müsste, ob es tatsächlich zu einer Sperrung der Computer durch die Schadsoftware gekommen ist. Um dies zu umgehen, ging der BGH davon aus, dass eine wesentliche Störung auch vermutet werden kann. Als Begründung führte er aus, dass in vielen Fällen die Erpressung erfolgreich war und das Betriebssystem, unter Verlust sämtlicher Daten, neu installiert werden musste. Deswegen kann auch angenommen werden, dass es auch in allen anderen Fällen zu einer wesentlichen Störung der Computer gekommen ist.

Der BGH stellte klar, dass in den Fällen, in denen es zur massenhaften Infizierung von Rechnern durch eine Schadsoftware kam, keine gerichtliche Feststellung in jedem Einzelfall vonnöten ist. Es ist also unerheblich, wie stark es jeden Einzelnen getroffen hat. Allein die Tatsache, dass es bei den meisten Opfern zu einer Blockierung des Systems kam, lässt die Vermutung zu, dass dies bei allen anderen auch der Fall gewesen ist.

Abweichend vom LG Stuttgart bewertete der BGH den Beitrag des Täters als technischer Berater und Administrator für die Server als nicht ganz so gravierend für die Tatbestände der Erpressung und der Computersabotage, weswegen die Revision zumindest teilweise Erfolg hatte und das Strafmaß gekürzt werden muss. Das Landgericht muss unter Berücksichtigung dieser höchstrichterlichen Vorgaben seine Entscheidung noch einmal neu formulieren (Meier, BGH hebt Verurteilung des Mitgliedes einer Trojaner-Bande teilweise auf, www.heise.de 20.07.2021, Kurzlink: https://heise.de/-6142431).

LG Erfurt

Arbeitgeber ist bei TK-Privatnutzung nicht Diensteanbieter

Mit Urteil vom 28.04.2021 erklärte das Landgericht (LG) Erfurt, dass die private Nutzung betrieblicher E-Mail-Accounts den Arbeitgeber nicht zum Diensteanbieter i.S.d. Telekommunikationsgesetzes (TKG) werden lasse und ein Zugriff auf die E-Mails daher unter besonderen Voraussetzungen auch ohne Einwilligung des Betroffenen zulässig sei (1 HK O 43/20). Es geht um die umstrittene Frage, ob ein Arbeitgeber als Diensteanbieter gem. § 3 Nr. 6 TKG zu werten ist, wenn er seinen Beschäftigten die private Nutzung betrieblicher E-Mail-Accounts ermöglicht. Wäre dies der Fall, dürfte der Arbeitgeber nur mit expliziter Zustimmung auf die E-Mails des Arbeitnehmers zugreifen.

Dies lehnte das LG Erfurt ab. Sollte daher der Arbeitgeber auf den E-Mail-Account seines Arbeitnehmers zugreifen, so stehen dem Arbeitnehmer nach Ansicht des LG keine Schadensersatz- oder Unterlassungsansprüche nach §§ 44, 88 TKG zu. Aus Sicht des Gerichts ist dem Arbeitgeber also gestattet in besonderen Ausnahmefällen auch ohne Einwilligung des Arbeitnehmers auf das Postfach zuzugreifen. Besondere Ausnahmefälle ergeben sich für Accounts von Beschäftigten danach grundsätzlich aus § 26 Abs. 1 BDSG. Dem Arbeitgeber soll es so möglich sein bei Abwesenheit des Arbeitnehmers oder bei Verdacht auf Straftaten auf die E-Mail-Accounts zuzugreifen.

Ein solcher Eingriff des Arbeitgebers müsste stets dem Grundsatz der Verhältnismäßigkeit entsprechen. Das schutzwürdige Interesse des Betroffenen dürfe nicht überwiegen. Dabei sei insbesondere auf den Grundsatz der

Datenminimierung zu achten (Art. 5 Abs. 1 lit. c DSGVO). Es seien z.B. nur diejenigen Daten zu überprüfen, die erforderlich sind, um den Verdacht der etwaigen Pflichtverletzung aufzuklären. Außerdem sei das Persönlichkeitsrecht des Beschäftigten zu berücksichtigen, welches stärker gelte, wenn eine private Nutzung des E-Mail-Accounts erlaubt wird. Andernfalls überwiege in der Regel die unternehmerische Freiheit des Arbeitgebers.

Geschäftsführer und Vorstände fallen gemäß dem LG mangels Beschäftigteneigenschaft hinsichtlich der Bestimmungen in § 26 Abs. 8 BDSG nicht unter den Tatbestand des § 26 Abs. 1 BDSG. Für sie stelle vielmehr Art. 6 Abs. 1 S. 1 lit. f DSGVO die Rechtsgrundlage dar, die ein überwiegendes Interesse des Arbeitgebers verlangt. Dabei sind im Rahmen der Interessensabwägung die jeweiligen berechtigten Interessen wie bei Beschäftigten zu beachten und zu werten. Einem solchen Zugriff könne der Betroffene nach Art. 21 DSGVO widersprechen.

Auch andere Gerichte (u.a. LAG Berlin-Brandenburg v. 14.01.2016 – 5 Sa 657/15 und v. 16.02.2011 – 4 Sa 2132/10; VG Karlsruhe v. 27.05.2013 – 2 K 3249/12; LAG Hamm v. 10.07.2012 – 14 Sa 1711/10; LAG Niedersachsen v. 31.05.2010 – 12 Sa 875/09; VGH Hessen v. 19.05.2009 – 6 A 2672/08.Z; ArbG Düsseldorf v. 29.10.2007 – 3 Ca 1455/07) hatten zuvor die Auffassung des LG Erfurt vertreten. Eine höchstrichterliche Klärung steht bisher aus.

Die Datenschutz-Aufsichtsbehörden gehen dagegen von der Diensteanbietereigenschaft des Arbeitgebers aus. In der „Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ heißt es: „Ist die private E-Mail-Nutzung erlaubt (…), ist der Arbeitgeber gegenüber den Beschäftigten und ihren Kommunikationspartnern zur Einhaltung des Fernmeldegeheimnisses verpflichtet. (…) Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber grundsätzlich nur mit Einwilligung der betreffenden Beschäftigten erlaubt.“

Der Bundestag hat am 19.05.2021 dem Telekommunikation-Telemedien-Datenschutz-Gesetz zugestimmt, das die Datenschutzbestimmungen des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) zusammenführt. Darin wird die Anwendbarkeit des Fernmeldegeheimnisses in dem neu geschaffenen § 3 Abs. 2 inhaltlich aber nicht geändert (Wehowsky, Datenschutz und Privatnutzung betrieblicher E-Mail-Accounts, www.iitr.de 14.05.2021).

VG Berlin

Handydatenanalyse bei Asylsuchenden nur im begründeten Verdachtsfall

Das Verwaltungsgericht (VG) Berlin hat mit Urteil vom 01.06.2021 die Erhebung der Daten aus Smartphones auf Vorrat, also ohne unmittelbaren gerichtlichen Verwendungszweck, für rechtswidrig erklärt (VG 9 K 135/20 A). Das Bundesamt für Migration und Flüchtlinge (BAMF) liest seit einer Änderung des Asylgesetzes im Jahr 2017 Smartphones Geflüchteter zu Beginn des Asylverfahrens aus. Ländervorwahlen eingehender Anrufe, der Dialekt, in dem der Besitzer Nachrichten schreibt, Logins für Dating-Apps – all das sind Informationen, die das BAMF aus den Geräten von Neuankömmlingen bisher ohne begründeten Verdacht auf Falschaussagen bezüglich ihrer Herkunft und Identität ausliest, um Aussagen zu verifizieren.

Geklagt hatten die Gesellschaft für Freiheitsrechte (GFF) und der Rechtsanwalt Matthias Lehnert im Namen einer 44-Jährigen aus Afghanistan, die im Prozess erklärte: „Auf meinem Handy sind private Nachrichten mit meiner Familie. Ich hatte keine andere Wahl, als der Auswertung zuzustimmen und wusste gar nicht, was mit meinen Daten genau passiert“.

Kristina Banasch, Sprecherin des BAMF, erläuterte: „Bei Personen ohne Pass- oder Ausweisdokumente kann das Mobiltelefon die einzige Quelle für die Feststellung der Identität sein.“ Bisher waren Auswertungen von Handydaten möglich, wenn Geflüchtete keinen Pass vorlegten – auch wenn es keinen begründeten Verdacht gab, dass sie lügen. Das Handy von Geflüchteten muss zur Erhebung der Informationen von ihnen entsperrt werden. Dann schließen Beamte es an einen Computer an, der bis zu 45 Minuten lang die Daten ausliest. Im Anschluss bekommt das BAMF einen „Ergebnisreport“. Banasch betont, dass die individuelle Anhörung von Geflüchteten dadurch nicht ersetzt werde. Die Auswertung erfolge zudem immer durch einen Volljuristen, der prüfe, ob der Bericht im Einzelfall für die Klärung der Identität notwendig sei. Einer GFF-Studie zufolge geht allerdings gerade einmal in 2% der Fälle, in denen Handydaten ausgewertet werden, aus diesen ein Widerspruch zu den getätigten Aussagen der Geflüchteten hervor (DANA 2/2020, 108 f.).

Vor der Auswertung unterschreiben Geflüchtete eine Einverständniserklärung. Die Juristin Lea Beckmann von der GFF relativiert: „Da steht nichts Genaues drauf, was bei der Analyse passiert.“ Die Mitwirkungspflicht der Geflüchteten ist gesetzlich verankert; weigern sie sich, befürchten viele Betroffene schwerwiegende Konsequenzen für ihren Asylantrag. Nicht zu wissen, was genau im eigenen Handy untersucht wird, ist gemäß Beckmann belastend: „Sie wissen nicht, was da passiert, geben ihr Handy ab, beschreiben ein Gefühl von Hilfslosigkeit und Ausgeliefertsein.“

Die Beamten wollen Dinge herausfinden, die normalerweise auf einem Pass stehen würden – durch die Analyse von Kontakten, ein- und ausgehenden Anrufen, Nachrichten, Browserverläufen, Geodaten aus Fotos, sowie Login-Daten für Apps. Beckmann: „Wir wissen nicht, bei welchen Apps genau Login-Daten im Klartext erfasst werden – in den Schulungsunterlagen werden aber auch beispielsweise Dating-Apps genannt.“

Apps geben mehr preis als nur vermeintliche Informationen über Identität und Herkunft der Geflüchteten. Als besonders heikel beschreibt Beckmann die Analyse von Textnachrichten: Linguistinnen und Linguisten hätten große Bedenken geäußert, ob die automatisierte Erkennung von Sprachen gut genug funktioniere, um Aussagen über die Herkunft Geflüchteter zu treffen. Unklar sei, auf welchen Trainingsdaten

die Spracherkennung programmiert sei, und für welche Sprachen und Dialekte sie wie gut funktioniere.

Auch die Herkunft aus ein- und ausgehenden Anrufen abzuleiten, steht in der Kritik. Gerade bei Geflüchteten, die schon länger auf der Flucht sind und deren Verwandte sich vielleicht ebenfalls außerhalb der Heimat aufhalten, sind die Vorwahlen von ein- und ausgehenden Anrufen nur bedingt aussagekräftig.

Die Analyse birgt Missbrauchspotenzial: Login-Daten können Auskunft über die Auffindbarkeit der Geflüchteten auf Social Media geben, deren Verwendung als Anhaltspunkt für weitere Recherchen durch Beamte unzulässig wäre. Geodaten können auch Informationen über die Fluchtroute der Betroffenen geben. Entscheider im BAMF sehen diese Informationen, sind aber dazu angehalten, sie zu ignorieren, wenn es im Verfahren um die Angaben über die Fluchtgeschichte der Personen geht. Das umzusetzen, dürfte in der Praxis aber kaum möglich sein.

Für das BAMF ist die Überprüfung der Identität wichtig, weil sie Grundlage von Entscheidungen im Asylverfahren sein kann. Das Auslesen mobiler Datenträger kann die Aussagen zur Identität der Geflüchteten auch bestätigen, und das könne laut Amtssprecherin Banasch ja ebenfalls relevant für das Verfahren sein. Das Gericht entschied jetzt, dass diese Handydatenauswertungen nur dann möglich sind, wenn keine milderen Mittel vorliegen. Als mildere Maßnahmen, um Herkunft und Identität von Geflüchteten zu prüfen, könnten zum Beispiel weitere Dokumente angefordert werden oder Sprachanalysen durch Dolmetscher angefertigt werden (Kruse, Flüchtlingspolitik: Besserer Schutz für Handydaten von Geflüchteten, www.sueddeutsche.de 02.06.2021).

VG Berlin

Airbnb muss im Verdachtsfall Vermieterdaten rausgeben

Das Ferienwohnungsportal Airbnb muss nach einem Urteil des Berliner Verwaltungsgerichts (VG) vom 23.06.2021 die Daten privater Vermieterinnen und Vermieter an Behörden herausgeben, wenn es den Anfangsverdacht einer Zweckentfremdung gibt (Az. 6 K 90/20). Das VG Berlin wies die Klage des irischen Unternehmens dagegen zurück und ließ wegen der grundsätzlichen Bedeutung des Falls die Berufung beim Oberverwaltungsgericht Berlin-Brandenburg zu.

Airbnb betreibt eine Internetplattform, auf der Ferienwohnungen zur Miete angeboten werden. Im Dezember 2019 hatte das Berliner Bezirksamt Tempelhof-Schöneberg das Unternehmen verpflichtet Namen und Anschriften zahlreicher Anbieterinnen und Anbieter und die genaue Lage der von ihnen angebotenen Ferienwohnungen zu übermitteln. Die Vermieter und Vermieterinnen waren in Onlinelisten aufgeführt worden. Das Bezirksamt hatte laut Gericht den Verdacht, dass gegen das Berliner Zweckentfremdungsverbot von Wohnungen verstoßen wurde, weil die Inserate keine oder falsche Registriernummern hatten oder die Geschäftsdaten gewerblicher Vermieter nicht zu erkennen waren. Da die Angebote bei Airbnb anonym geschaltet waren, bestand ein Anlass die Auskünfte einzuholen, um mögliche Zweckentfremdungen zu unterbinden. Zur Aufdeckung von Verstößen gegen das Zweckentfremdungsverbot von Wohnraum dürfen die zuständigen Behörden nicht nur bei den Bewohner der Wohnungen bzw. beim jeweiligen Vermieter/Eigentümer ermitteln, sondern auch Auskünfte bei Dritten einholen, auch wenn diese im Ausland sind.

Das VG stellte fest, dass die Registriernummer gerade wegen des zunehmenden anonymen Angebots von Ferienwohnungen im Internet gesetzlich eingeführt worden ist. Sie gilt in der Regel für Vermieterinnen, die ihre Wohnung kurzzeitig als Ferienwohnung anbieten. Die Nummer soll im Internet der Nachweis für ein legales Angebot sein. Wer in Berlin seine Wohnung an Feriengäste vermieten will, braucht dafür seit 2014 eine Genehmigung.

Airbnb hatte argumentiert, der Bescheid des Bezirksamts sei rechtswidrig, die geforderte Auskunft sei verfassungswidrig. Zudem werde verlangt, gegen irisches Datenschutzrecht zu verstoßen. Das VG hatte dagegen keine verfassungsrechtlichen Bedenken. Zwar werde in das Grundrecht auf informationelle Selbstbestimmung eingegriffen, der Eingriff sei jedoch verhältnismäßig, gesetzlich hinreichend bestimmt und normenklar. Auf irisches Datenschutzrecht könne sich Airbnb trotz Unternehmenssitz in Dublin nicht berufen. Das sogenannte Herkunftslandprinzip sei hier nicht anwendbar.

Das Musterverfahren des Wohnungsamts Tempelhof-Schöneberg wurde in Zusammenarbeit mit der Senatsverwaltung für Stadtentwicklung und Wohnen geführt. Berlins Stadtentwicklungssenator Sebastian Scheel (Linke) meinte, die Entscheidung des VG sei „von größter Bedeutung – für unsere Stadt, aber auch über Berlins Grenzen hinaus“. Nur mit Transparenz und der Möglichkeit der Datenabfrage ließen sich legale von illegalen Ferienwohnungsangeboten unterscheiden.

Das Gesetz für die Registrierung von Ferienwohnungen wurde inzwischen weiter verschärft, wegen knappen Wohnraums sollen die Regelungen noch strenger werden. Nach einer Umfrage von Anfang April 2021 haben Berliner Bezirke gegen Anbieter ungenehmigter Ferienwohnungen seit 2018 Bußgelder in Millionenhöhe verhängt. Allein in sieben Bezirken belief sich die Summe auf 3,4 Millionen € (Airbnb muss im Verdachtsfall Vermieterdaten herausgeben, www.zeit.de 24.06.2021; Dligatch, Verwaltungsgericht Berlin verurteilt Airbnb zur Herausgabe von Daten bei Verdacht auf Zweckentfremdung, www.anwalt.de 23.06.2021).

Buchbesprechungen

Rolf Gössner
Datenkraken im Öffentlichen Dienst „Laudatio" auf den präventiven Sicherheits- und Überwachungsstaat
2021, PapyRossa Verlag Köln, 366 S., broschiert
ISBN 978-3-89438-753-2, 19,90 €

(tw) Bei der Verleihung der BigBrotherAwards (BBA) 2021 am 11.06.2021 in Bielefeld gab Rolf Gössner seinen Abschied und zog in seiner Rede Bilanz über seine 20jährige Jurytätigkeit für den von DigitalCourage organisierten BBA. Dabei zeichnete er die Sicherheitsbestrebungen in unserer Gesellschaft und unserer Politik nach, vor allem die mit Terrorismusbekämpfung legitimierte staatliche Überwachungspolitik. Gössners Resümee kann nun auch – ausführlicher und mit allen nötigen Informationen und Nachweisen versehen – in dem hier rezensierten Buch nachgelesen werden.

Rolf Gössner weiß, worüber er schreibt und urteilt: Seit Jahrzehnten befasst er sich kritisch und kompetent mit dem Überwachungsstaat. Dabei wurde er über Jahrzehnte hinweg vom beamteten Verfassungsschutz beobachtet. Dass dies illegal war, wurde ihm jüngst letztinstanzlich vom Bundesverwaltungsgericht bestätigt (DANA 1/2021, 60). Auch wenn er seine BBA-Jurymitgliedschaft aufgibt, so nicht sein Engagement für Bürgerrechte und Datenschutz. Insofern wird das Buch nicht seine letzte Äußerung sein. Wohl aber ist es ein umfassender Rückblick, eine detaillierte Analyse und ein politisches Resümee. Der Rückblick besteht insbesondere aus den von Gössner von 2000 bis 2020 präsentierten BBA-Laudationes, in denen die Vergeheimdienstlichung und Militarisierung der sich technisierenden Sicherheitspolitik in Gesetzgebung und Praxis angeprangert werden. Ergänzt werden diese historischen Beiträge durch Wortmeldungen von Gerhard Baum, Sabine Leutheusser-Schnarrenberger und Heribert Prantl, die diese im Rahmen der BBA-Events vorgetragen haben.

Diese Beiträge sind repräsentativ; es geht um Verfassungsschutzbehörden, Polizei, Bundesnachrichtendienst, NSA, Terrorabwehrzentrum; es geht um Drohneneinsatz, Telefonüberwachung, elektronische Fußfessel oder Racial Profiling; es geht um Protagonisten der sog. inneren Sicherheit, etwa um Werthebach, Schily, Harms, Schünemann, Friedrich oder Schäuble. Die Beiträge sind aber nicht umfassend. Insofern wird das Buch bereichert durch einen zweiten Teil, in dem nicht exemplarisch, sondern strukturiert der Weg in einen präventiv-autoritären Überwachungsstaat beschrieben wird. Dabei liegt Gössners Schwerpunkt auf der Innenpolitik; diese ergänzt er aber mit einer aktuellen interessanten Analyse der Corona-Abwehrpolitik, wobei er Parallelen zwischen der Polizei-/Geheimdienst-/Militärpolitik und der staatlichen Reaktion auf das Coronavirus aufzeigt. Gössner nimmt dabei immer eine klare, strenge bürgerrechtliche Position ein, ohne dabei andere Belange, also etwa die der Sicherheit oder der Gesundheit auszublenden. Er beschreibt zugleich auch die Mittel, mit denen Sicherheit im Interesse des Gemeinwohls ohne übermäßige Überwachung realisiert werden können/müssen. Dies sind demokratische Transparenz, soziale Prävention und rechtsstaatliche Kontrolle.

Ebenso wie der BBA ein Instrument der bürgerrechtlichen Öffentlichkeitsarbeit ist, ist es auch dieses Buch. Ihm geht es nicht darum, auch die Vertreter der Gegenseite zu Wort kommen zu lassen, die ohnehin in den Medien sehr präsent sind. Insofern ist dieses Buch parteiisch. Es ist auch für schon engagierte Bürgerrechtler:innen eine Fundgrube von Fakten und Argumenten. Und nicht nur das: Wer kurzweilige unterhaltsame Texte vor dem Einschlafen lesen oder auch einfach nur etwas – mit Gewinn – schmökern möchte, auch der oder dem sei dieses Buch empfohlen.

Roßnagel, Alexander (Hrsg.)
Hessisches Datenschutz- und InformationsfreiheitsG – HDSIG – Handkommentar
2021, Nomos-Verlag, 836 S. gebunden, 98,00 €
ISBN 978-3-8487-6808-0

(tw) Alexander Roßnagel ist seit März 2021 „Der Hessische Beauftragte für Datenschutz und Informationsfreiheit" (HBDI). Er war zuvor als Universitätsprofessor einer der Wissenschaftler, die das deutsche Datenschutzrecht maßgeblich beeinflusst haben. Mit der Herausgabe seines Kommentars zum HDSIG vollzieht Roßnagel sozusagen im Vorweg den Spagat zwischen Wissenschaft und Praxis, indem er sich und seinem Bundesland den Maßstab vorgibt, nach dem das seine Behörde bestimmende Gesetz zu messen und anzuwenden ist.

Der Datenschutz in Hessen hat eine lange Geschichte; 1970 setzte dieses Bundesland das weltweit erste Daten-

schutzgesetz überhaupt in Kraft. Unter Spiros Simitis, der von 1975 bis 1991 die hessische Datenschutzbehörde leitete, blieb das Bundesland bestimmend für die Datenschutzdiskussion, nicht zuletzt, weil Simitis auch den führenden Kommentar zum damaligen Bundesdatenschutzgesetz herausgab. Auf seine Person war auch die hessische Professorenlösung ausgerichtet, wonach der Leiter der Datenschutzbehörde zugleich Universitätsprofessor sein musste. Angesichts des Aufgabenzuwachses bei der Datenschutzaufsicht war dies nicht immer die beste Lösung. Mit Roßnagel kehrt Hessen „back to the roots", also zu einer qualifizierten Kombi von Wissenschaft und Verwaltungspraxis.

Dies ist auch nötig. Hessen war schon lange nicht mehr im Datenschutz innovativ; einige der von der schwarz-grünen Regierung verabschiedeten Gesetze zeichnen sich durch Überwachungsstaatlichkeit aus, nicht durch starke Bürgerrechte. Hessen war denn auch das viertletzte Schlusslicht bei der Verabschiedung eines Anspruchs auf Informationszugang zu Behördenunterlagen – vulgo auf Informationsfreiheit.

Diese Informationsfreiheit wird nun – und das ist nun wieder einzigartig und zugleich richtungsweisend – gemeinsam mit dem Datenschutz, der an die Datenschutz-Grundverordnung (DSGVO) angepasst werden musste, im HDSIG geregelt. Auch wenn jetzt im Datenschutz die europäische DSGVO bestimmend ist, so bleibt noch genügend Regelungsbedarf auf Bundeslandsebene, insbesondere was den öffentlichen Bereich im Bundesland, dort insbesondere den Polizei- und Justizbereich, und generell die Aufsicht, betrifft.

Der Kommentar wird von Alexander Roßnagel nicht nur herausgegeben, sondern inhaltlich auch weitgehend verantwortet. Er verfolgt eine einheitliche datenschutz- und informationsfreiheitsfreundliche Linie. Ein Meinungsstreit unter den Autoren ist mir nur aufgefallen zwischen Roßnagel und Armin Herb, der den öffentlich-rechtlichen Rundfunk kommentiert und dabei dessen Beitragsservice – fälschlich – der Meinungsfreiheit zuschlägt. Der Kommentar ersetzt den von Hans-Hermann Schild herausgegebenen Kommentar zum alten Hessischen Datenschutzgesetz. Die Koautorinnen und -autoren kommen aus der Behörde selbst, aus der Wissenschaft (weitgehend aus „Roßnagels Stall") und aus der Aufsichtsbehörde von Rheinland-Pfalz – durchgängig bestens ausgewiesen und qualifiziert – was sich auf die Qualität des Werks auswirkt. Auch der Vorgänger von Roßnagel, Prof. Michael Ronellenfitsch, kommt zur „Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften" zu Wort.

Der Kommentar ist einerseits knapp und übersichtlich, zugleich aber für die praktischen und wissenschaftlichen Bedürfnisse mit seinen über 800 Seiten ausführlich genug. Das Verständnis für die Landesnormen wird dadurch erhöht, dass deren Geschichte erzählt wird und zugleich die Bezüge zur DSGVO oder zu anderen Regelungen hergestellt werden. Die aktuelle Literatur wird rezipiert und zitiert. Er ist insofern auch geeignet, bei der Auslegung des Rechts zu Datenschutz und Informationsfreiheit generell zu helfen. Da aber im öffentlichen und vor allem im privaten Bereich die DSGVO Vorrang hat, genügt der Kommentar in den vielen Fällen, wenn es um den Datenschutz – auch in Hessen – geht, nicht, weshalb dann auf die – äußerst umfangreiche – Literatur zur DSGVO zurückgegriffen werden muss.

Partsch, Christoph J. (Hrsg.)
Bundesarchivgesetz - Handkommentar
Nomos Baden-Baden, 2. Aufl. 2021
ISBN 978-3-84876931-5, 635 S., 88,00 €

(tw) Es ist noch nicht lange her, dass in der DANA die erste Auflage dieses Handkommentars rezensiert wurde (Heft 4/2019, 241 f.). Darin wurde moniert, dass das Archivwesen kaum eine Rolle in der Datenschutzliteratur spielt. Eine breitere Diskussion zwischen Archiv- und Datenschutzrechtlern wurde eingefordert. Die unberechtigte Beschuldigung gegenüber dem Datenschutz, den archivrechtlichen Informationszugang allzu sehr zu beschränken, wurde zurückgewiesen.

Seit der Erstauflage des Kommentars hat sich Einiges getan: Es gibt neue Literatur, die sich eingehend mit dem Verhältnis von Datenschutz und Archivrecht befasst. Dies gilt insbesondere für die hervorragende Promotion von Hannes Berger „Öffentliche Archive und staatliches Wissen", in der dieser nicht nur das Archivrecht mit der europäischen Datenschutz-Grundverordnung (DSGVO) zusammenbringt, sondern auch die Defizite des bisherigen Archivrechts aufzeigt und Lösungsvorschläge zu deren Behebung macht (vgl. die Rezension in DANA 2/2020, 133 f.). Dabei liegen die Anliegen von H. Berger und der Autoren des hier besprochenen Kommentars – neben dem Herausgeber Christoph J. Partsch der BMI-Referatsleiter Sven Berger und die Anwälte Norman Koschmieder und Axel Mütze – nahe beieinander: Das Archivrecht aus seinem Dornröschenschlaf zu holen und in eine Zukunft zu führen, in der das historische Archivwissen für die aktuellen politischen Diskussionen und für die Forschung nutzbar gemacht wird.

Leider werden aber die bestehenden Diskussionsstränge unzureichend zusammengefügt, so dass die beiden Rechtsgebiete Datenschutz- und Archivrecht weiterhin mehr oder weniger unvermittelt nebeneinander her bestehen. Zweifellos ist dies hier weniger der Fall als in der ersten Auflage, doch so richtig gelungen ist das Zusammenfügen – bei den Einzelautoren in unterschiedlichem Maße – noch nicht: Die Existenz des Europarechts wird zur Kenntnis genommen. Doch schon der Umstand, dass die DSGVO eine äußerst archivfreundliche Grundtendenz verfolgt, dass das Europarecht positiv zu Informationszugängen steht, wird kaum nutzbar gemacht. Die DSGVO könnte mobilisiert werden das 2017 zwar überholte, aber nicht generalüberholte, deutsche Archivrecht endlich auf einen modernen Stand zu bringen. Der Bedarf ist groß und geht weit über das klassische Bereitstellen von staatlichen Informationen auf An-

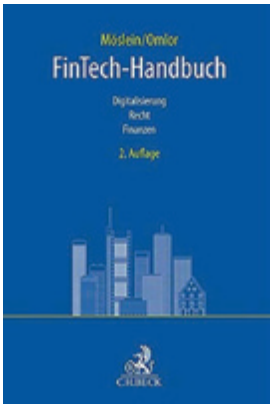
frage in Archiven hinaus. Er erstreckt sich auch auf das Informationsfreiheits- und auf das Forschungsrecht (dazu Weichert, DVBl. 2020, 19-26).

Die anstehende neue Legislaturperiode mit einer voraussichtlich anderen Regierungszusammensetzung bietet in Deutschland die Gelegenheit für eine grundlegende Reform. Bisher fehlt es am Druck dafür, dass die Politik aktiv wird. Politische Widerstände gegen eine Modernisierung sind wenig zu erwarten – würden doch praktisch alle relevanten Player davon profitieren – insbesondere auch die demokratische Öffentlichkeit und die Wirtschaft.

In den zwei Jahren seit dem Ersterscheinen des Kommentars hat sich auch eine für das Archivrecht markante Entwicklung ergeben: die Integration der Stasi-Unterlagenbehörde in das Bundesarchiv (DANA 2/2021, 107 ff.). Dies wird in der Neuauflage zwar durch den Abdruck des neuen § 3b BArchivG zur Kenntnis genommen, doch praktisch nicht kommentiert und schon gar nicht gewürdigt. Es gibt zwar die – weiterhin gültigen – Kommentierungen zum Stasi-Unterlagengesetz (StUG), doch könnte gerade diese Änderung zu frischem Wind führen, der das Bundesarchiv insgesamt aufwertet. Die Befürchtung vieler DDR-Bürgerrechtler, mit der Integration der Stasi-Unterlagen in das Bundesarchiv würden deren Errungenschaften beerdigt, müssen nicht Wirklichkeit werden. Umgekehrt könnte die Zusammenführung zu einer Aufwertung des Bundesarchivs führen.

Trotz der hier geäußerten Kritik dürfen die äußerst positiven Seiten des Kommentars nicht verdrängt werden: Archivrechtlich haben die Ausführungen ein hohes Niveau und berücksichtigen umfassend die wenige vorhandene Rechtsprechung. Insofern geht der Kommentar über eine „Hand"-Reichung hinaus und genügt wissenschaftlichen Bedürfnissen. Die Ausführungen zum Informationszugangsrecht sind hilfreich – von den insofern bestehenden Einzelgesetzen bis hin zur Darstellung der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte. Wertvoll ist der Dokumententeil am Ende, in dem das StUG sowie die Landesarchivgesetze sowie Nutzungsverordnungen abgedruckt sind. Ergänzt wird der Anhang durch das Sicherheitsüberprüfungsgesetz, die Verschlusssachenanweisung und die Hausanordnung des Bundesinnenministeriums zur Schriftgutverwaltung.

Nützlich, aber leider aus Datenschutzsicht wenig ergiebig sind das Stichwort- und die Literaturverzeichnisse. Anders als in Einzelkommentierungen wurde dort z.B. vergessen das grundlegende Werk von Hannes Berger aufzuführen. Es besteht also nach wie vor Luft nach oben für eine weitere Neuauflage – gerade und weiterhin beim Datenschutz. Es besteht zweifellos ein gewaltiger Bedarf schon am vorhandenen Text, aber auch an dessen Weiterentwicklung. Dabei sollte dann weniger auf eine Seitenbegrenzung geachtet werden als auf eine umfassende Einarbeitung der Verschränkung des Archivrechts mit dem Datenschutzrecht.



Möslein, Florian/Omlor, Sebastian (Hrsg.)
FinTech-Handbuch
Digitalisierung – Recht - Finanzen
C.H.Beck-Verlag München, 2. Aufl. 2021
ISBN 978-3-406-75449-4, 1132 S.,
219,00 €

(tw) FinTechs sind in unsere Finanzaktivitäten eingedrungen und machen sich immer weiter breit. Deren Entwicklung ist rasant. Es werden viele Milliarden € oder $ hierüber umgesetzt und viele Milliarden damit verdient. Wie das funktioniert und ob und inwieweit das alles mit rechten Dingen zugeht, entzieht sich dem „Normalbürger". Aber auch die spezialisierte Juristin ist schnell ratlos. Es ist daher kein Wunder, dass es die trotz Milliarden-Kapitaldeckung sich oft noch als Start-Ups gerierenden FinTechs mit Compliance oft nicht so genau nehmen.

Insofern ist es ein gewaltiger Verdienst der Herausgeber Möslein und Omlor zwischen zwei Bucheinwänden 37 Autoren und 5 Autorinnen versammelt zu haben die Ökonomie, Technik und Recht von FinTechs umfassend darzustellen versuchen. Dass dies nur ein Versuch bleiben kann, ergibt sich durch die Schnelllebigkeit der FinTechs selbst wie der durch diese ausgelösten Regulierungen, die sich oft noch im Experimentierstadium befinden. Die technische Schnelllebigkeit wird gekennzeichnet durch Distributed Ledger-Technologien (Blockchain), durch algorithmenbasierte Entscheidungen und sog. Künstliche Intelligenz, durch Transnationalisierung von Daten, Dokumenten, Finanzen, Märkten, durch Crowdfunding, Crowdlending, Bitcoins, Robo-Advices…

Das systematisch aufgebaute Handbuch hat drei Teile. In einem ersten allgemeinen Teil werden übergreifende Grundlagen thematisiert, so die wirtschaftliche Marktentwicklung, die institutionelle, auch bankpraktische Einbettung der FinTech-Akteure, die technologischen Grundlagen sowie die damit verbundenen Rechtsfragen, insbesondere die Einbettung der FinTechs in das etablierte Finanzwesenrecht und dessen Digitalisierung – einschließlich internationalem Privatrecht, Datenschutz, geistigem Eigentum, IT-Sicherheit und Geldwäscheprävention.

In einem zweiten besonderen Teil werden einzelne von FinTechs wahrgenommene Bankgeschäfte abgehandelt, etwa zum Zahlungsverkehr, zur Beteiligungsfinanzierung, zu Effektengeschäften, zur Vermögensanlage und zu Versicherungen. Im dritten Teil wird die internationale Dimension technologiegestützter Finanzdienstleistungen behandelt und ein Blick über die Grenzen nach England, Österreich, die Schweiz, Holland, Italien und Irland vorgenommen.

Sämtliche Texte sind, soweit das bei einer derart fachspezifischen Thematik überhaupt möglich ist, verständlich verfasst, regelmäßig in Deutsch, einige wenige in Englisch. Es erfolgen Verweise auf die einschlägige Literatur, wobei die inhaltliche Tiefe und Durchdringung je nach Autorenschaft mal größer und mal geringer ist. So sind die Ausführungen zum Datenschutz sehr allgemein gehalten und ermöglichen zumindest in dem

diesem Thema hauptsächlich gewidmeten Kapitel keine direkten Rückschlüsse auf die konkrete FinTech-Praxis. So wird z.B. das Wechselspiel zwischen Finanz- und Datenschutzrecht nicht wirklich dargestellt und aufgelöst, etwa das Verhältnis der Datenschutz-Grundverordnung zur PSD-II-Richtlinie und zum Finanzdienstleistungsaufsichtsgesetz, zu der Regulierung der Geldwäschebekämpfung oder zu den Regelungen des Verbraucherschutzes im Finanzwesen. Dies mag dem Umstand zuzuschreiben sein, dass dieser Sektor augenscheinlich bisher völlig an den Aufsichtsbehörden, aber auch an den Betroffenen und den Gerichten vorbeigegangen ist und so eher die unternehmerische Blickweise im Fokus steht. Demgemäß sind es eben auch vor allem Anwälte und Professoren, die FinTechs und Banken beraten, die in dem Sammelwerk zu Wort kommen.

Für Datenschützer, die sich FinTechs annehmen wollen, ist das Handbuch von großem Wert, da die praktischen und rechtlichen Seiten der FinTechs sehr qualifiziert dargestellt werden und so eine Wissensgrundlage geschaffen wird, auf der dann datenschutzrechtliche Expertise aufsetzen kann. Das nicht gerade kostengünstige Buch ist nicht nur für Datenschützer, sondern generell sich mit FinTech-Recht befassenden Expertinnen und Experten eine Fundgrube und in mancher Hinsicht ein Wegweiser. Für den Laien und nicht vorbelasteten Leser ist es dagegen eher als schwere Kost nicht zu empfehlen. Es schafft etwas Transparenz in einem absolut undurchsichtigen und sich schnell entwickelnden Wirtschaftssegment. Die Aufgabe, hier wirklich gesellschaftliche Transparenz herzustellen, müsste die Politik und die staatliche Finanzaufsicht schaffen, die sich angesichts der hier abgespielten Skandale – von Cum-Ex bis Wirecard – damit noch sehr schwer tun.

Prof. Dr. Gernot Sydow, M.A. (Hrsg)
Kirchliches Datenschutzrecht – Datenschutzbestimmungen der katholischen Kirche – Handkommentar,
1. Auflage 2021, 597 Seiten,
ISBN 978-3-8487-6255-2, 128,00 €

(wh) Eine Anmerkung vorab: Der Titel „Kirchliches Datenschutzrecht" verspricht deutlich mehr, als der Inhalt bietet. Behandelt wird nur das Datenschutzrecht der römisch-katholischen Kirche, so dass auch der Untertitel als unvollständig zu bezeichnen ist. Zu dem Datenschutzrecht der katholischen Kirche gehört zumindest auch noch die „Bischöfliche Verordnung über den kirchlichen Datenschutz (KDO) im Katholischen Bistum der Alt-Katholiken in Deutschland" vom 24. Mai 2018. Sehen wir mal über den Absolutheitsanspruch des Titels hinweg und nehmen das Werk als das, was es ist: Ein umfassender Handkommentar zum römisch-katholischen Datenschutzrecht in Deutschland.

Neben dem röm.-kath. „Gesetz über den kirchlichen Datenschutz" (KDG) werden auch die „Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz" (KDG-DVO) sowie die „Kirchliche Datenschutzgerichtsordnung (KDSGO)" und die „Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG") in diesem werk erörtert.

In der Einführung zum KDG wird dargelegt, warum das Datenschutzrecht der Kirchen zum Gültigwerden der DSGVO neu geordnet werden musste. So erlaubt Art. 91 Abs. 1 DSGVO die Beibehaltung kirchlichen Datenschutzrechts anstelle des staatlichen Datenschutzrechts. Dies gilt allerdings nur unter der Bedingung, dass die kirchlichen Regelungen mit der DSGVO in Einklang stehen. In der Einführung wird auch dargestellt, welche der behandelten Rechtsnormen durch welche Institution in Kraft gesetzt wurde. So ist das KDG diözesanes Recht, das wortgleich in allen röm.-kath. Diözesen verabschiedet wurde. Gleiches gilt für die KDG-DVO. Die KDR-OG ist dagegen nur ein Mustertext, der durch die einzelnen Ordensleitungen für die jeweilige Ordensgemeinschaft in Kraft gesetzt werden muss. Nur die KDSGO liegt in der Gesetzgebungskompetenz der röm.-kath. Deutschen Bischofskonferenz.

Der Schwerpunkt des Handkommentars liegt laut Verlag auf den Abweichungen des kirchlichen Datenschutzrechts gegenüber der DSGVO bzw. dem BDSG. NutzerInnen sollen so auf den ersten Blick erkennen, welche Regelungen auch im röm.-kath. Bereich gelten, wie die röm.-kath. Eigenregelungen zu interpretieren sind und welche röm.-kath. Institutionen mit Datenschutzaufgaben betraut sind.

Durch die durchweg durchgehaltene Strukturierung der Kommentierungen der einzelnen Paragraphen der Normen in „A. Gesamtverständnis und Zweck der Norm", „B. Verhältnis zur DSGVO und zum BDSG" und dem Abschnitt C mit der eigentlichen Kommentierung wird dieser Handkommentar dem vom Verlag genannten Anspruch gerecht, dass die Abweichungen zwischen dem röm.-kath. und dem staatlichen Datenschutzrecht schnell erkennbar sind.

Als Fazit lässt sich festhalten, dass dieser Handkommentar ein nützliches Hilfsmittel zum Verständnis des römisch-katholischen Datenschutzrechts darstellt. Wenn nun noch der Titel dem Inhalt angepasst würde, wäre das Werk uneingeschränkt zu empfehlen.

Cartoon

https://www.medical-tribune.de/praxis-und-wirtschaft/ehealth/artikel/e-rezept-kommt-2022-per-code-in-die-app/

Tim Cook
CEO, Apple, Inc.

19. August 2021

Sehr geehrter Herr Cook,

Bild: iStock.com/prim91

die unterzeichnenden Organisationen, die sich weltweit für Bürgerrechte, Menschenrechte und digitale Rechte einsetzen, fordern Apple auf, die am 5. August 2021 angekündigten Pläne zum Einbau von Überwachungsfunktionen in iPhones, iPads und andere Apple-Produkte aufzugeben. Obwohl diese Funktionen dazu gedacht sind, Kinder zu schützen und die Verbreitung von Material über sexuellen Kindesmissbrauch einzudämmen, sind wir besorgt, dass sie zur Zensur geschützter Äußerungen eingesetzt werden, die Privatsphäre und Sicherheit von Menschen auf der ganzen Welt bedrohen und katastrophale Folgen für viele Kinder haben werden.

Apple hat angekündigt, dass es einen Algorithmus für maschinelles Lernen einsetzt, um Bilder in seinem Textnachrichtendienst Messages zu scannen, um sexuell eindeutiges Material zu erkennen, das an oder von Personen gesendet wird, die in Familienkonten als Kinder identifiziert werden. Diese Überwachungsfunktion wird direkt in die Apple-Geräte eingebaut. Wenn der Algorithmus ein sexuell eindeutiges Bild erkennt, warnt er den Nutzer, dass das Bild möglicherweise sensibel ist. Er sendet auch eine Benachrichtigung an den Organisator eines Familienkontos, wenn ein Nutzer unter 13 Jahren das Bild senden oder empfangen möchte.

Algorithmen zur Erkennung von sexuell eindeutigem Material sind notorisch unzuverlässig. Sie neigen dazu, fälschlicherweise Kunst, Gesundheitsinformationen, Bildungsressourcen, Lobbyarbeit und andere Bilder zu kennzeichnen. Das Recht der Kinder, solche Informationen zu senden und zu empfangen, wird durch die UN-Konvention über die Rechte des Kindes geschützt. Darüber hinaus geht das von Apple entwickelte System davon aus, dass die betreffenden Konten „Eltern“ und „Kind“ tatsächlich einem Erwachsenen gehören, der Elternteil eines Kindes ist, und dass diese Personen eine gesunde Beziehung zueinander haben. Dies ist nicht immer der Fall; ein missbräuchlich handelnder Erwachsener kann der Organisator des Kontos sein, und die Folgen einer elterlichen Benachrichtigung könnten die Sicherheit und das Wohlergehen des Kindes gefährden. LGBTQ+-Jugendliche auf Familienkonten mit unsympathischen Eltern sind besonders gefährdet. Diese Änderung hat zur Folge, dass iMessages diesen Nutzern keine Vertraulichkeit und keinen Schutz der Privatsphäre mehr durch ein Ende-zu-Ende-verschlüsseltes Nachrichtensystem bietet, bei dem nur der Absender und der vorgesehene Empfänger Zugriff auf die gesendeten Informationen haben. Sobald diese Hintertür eingebaut ist, könnten Regierungen Apple dazu zwingen, die Benachrichtigung auf andere Konten auszuweiten und Bilder zu erkennen, die nicht nur aus sexuellen Gründen anstößig sind.

Apple kündigte außerdem an, in das Betriebssystem seiner Produkte eine Hash-Datenbank mit CSAM-Bildern einzubauen, die vom National Center for Missing and Exploited Children in den Vereinigten Staaten und anderen Kinderschutzorganisationen bereitgestellt wird. Es wird jedes Foto, das seine Nutzer in die iCloud hochladen, mit dieser Datenbank abgleichen. Wenn eine bestimmte Anzahl von Übereinstimmungen erreicht ist, wird der Account deaktiviert und der Nutzer und die Bilder werden den Behörden gemeldet. Viele Nutzer laden routinemäßig die von ihnen aufgenommenen Fotos in iCloud hoch. Für diese Nutzer ist die Bildüberwachung etwas, das sie nicht abwählen können; sie wird in ihr iPhone oder ein anderes Apple-Gerät und in ihren iCloud-Account integriert sein.

Sobald diese Funktion in die Apple-Produkte eingebaut ist, werden das Unternehmen und seine Konkurrenten unter enormen Druck geraten – und möglicherweise von Regierungen auf der ganzen Welt gesetzlich dazu verpflichtet, Fotos nicht nur auf CSAM zu scannen, sondern auch auf andere Bilder, die eine Regierung für bedenklich hält. Dabei kann es sich um Bilder von Menschenrechtsverletzungen, politischen Protesten, Bildern, die von Unternehmen als „terroristische“ oder gewalttätige extremistische Inhalte gekennzeichnet wurden, oder sogar um wenig schmeichelhafte Bilder eben jener Politiker handeln, die das Unternehmen unter Druck setzen werden, sie zu scannen. Und dieser Druck könnte sich auf alle auf dem Gerät gespeicherten Bilder erstrecken, nicht nur auf die in iCloud hochgeladenen. Damit hat Apple den Grundstein für Zensur, Überwachung und Verfolgung auf globaler Basis gelegt.

Wir unterstützen die Bemühungen zum Schutz von Kindern und sprechen uns entschieden gegen die Verbreitung von CSAM aus. Aber die von Apple angekündigten Änderungen gefährden Kinder und andere Nutzer, sowohl jetzt als auch in Zukunft. Wir fordern Apple dringend auf, diese Änderungen zurückzunehmen und das Engagement des Unternehmens für den Schutz seiner Nutzer durch eine Ende-zu-Ende-Verschlüsselung zu bekräftigen. Wir fordern Apple außerdem auf, sich regelmäßiger mit zivilgesellschaftlichen Gruppen und mit gefährdeten Bevölkerungsgruppen zu beraten, die von den Änderungen an seinen Produkten und Diensten unverhältnismäßig stark betroffen sein könnten.

Mit freundlichen Grüßen

Access Now (Global) ■ Advocacy for Principled Action in Government (United States) ■ African Academic ■ Network on Internet Policy (Africa) ■ AJIF (Nigeria) ■ American Civil Liberties Union (United States) ■ Aqualtune Lab (Brasil) ■ Asociación por los Derechos Civiles (ADC) (Argentina) ■ Association for Progressive Communications (APC) (Global) ■ Barracón Digital (Honduras) ■ Beyond Saving Lives Foundation (Africa) ■ Big Brother Watch (United Kingdom) ■ Body & Data (Nepal) ■ Canadian Civil Liberties Association ■ CAPÍTULO GUATEMALA DE INTERNET SOCIETY (Guatemala) ■ Center for Democracy & Technology (United States) ■ Centre for Free Expression (Canada) ■ CILIP/ Bürgerrechte & Polizei (Germany) ■ Código Sur (Centroamerica) ■ Community NetHUBs Africa ■ Dangerous Speech Project (United States) ■ Defending Rights & Dissent (United States) ■ Demand Progress Education Fund (United States) ■ Derechos Digitales (Latin America) ■ Digital Rights Foundation (Pakistan) ■ Digital Rights Watch (Australia) ■ DNS Africa Online (Africa) ■ Electronic Frontier Foundation (United States) ■ EngageMedia (Asia-Pacific) ■ Eticas Foundation (Spain) ■ European Center for Not-for-Profit Law (ECNL) (Europe) ■ Fight for the Future (United States) ■ Free Speech Coalition Inc. (FSC) (United States) ■ Fundación Karisma (Colombia) ■ Global Forum for Media Development (GFMD) (Belgium) ■ Global Partners Digital (United Kingdom) ■ Global Voices (Netherlands) ■ Hiperderecho (Peru) ■ Instituto Beta: Internet & Democracia – IBIDEM (Brazil) ■ Instituto de Referência em Internet e Sociedade - IRIS (Brazil) ■ Instituto Liberdade Digital - ILD (Brazil) ■ Instituto Nupef (Brazil) ■ Internet Governance Project, Georgia Institute of Technology (Global) ■ Internet Society Panama Chapter ■ Interpeer Project (Germany) ■ IP.rec - Law and Technology Research Institute of Recife (Brazil) ■ IPANDETEC Central America ■ ISOC Bolivia ■ ISOC Brazil - Brazilian Chapter of the Internet Society ■ ISOC Chapter Dominican Republic ■ ISOC Ghana ■ ISOC India Hyderabad Chapter ■ ISOC Paraguay Chapter ■ ISOC Senegal Chapter ■ JCA-NET (Japan) ■ Kijiji Yeetu (Kenya) ■ LGBT Technology Partnership & Institute (United States) ■ Liberty (United Kingdom) ■ mailbox.org (EU/DE) ■ May First Movement Technology (United States) ■ National Coalition Against Censorship (United States) ■ National Working Positive Coalition (United States) ■ New America's Open Technology Institute (United States) ■ OhmTel Ltda (Columbia) ■ OpenMedia (Canada/United States) ■ Paradigm Initiative (PIN) (Africa) ■ PDX Privacy (United States) ■ PEN America (Global) ■ Privacy International (Global) ■ PRIVACY LATAM (Argentina) ■ Progressive Technology Project (United States) ■ Prostasia Foundation (United States) ■ R3D: Red en Defensa de los Derechos Digitales (Mexico) ■ Ranking Digital Rights (United States) ■ S.T.O.P. - Surveillance Technology Oversight Project (United States) ■ Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)Access Now (Global) ■ Advocacy for Principled Action in Government (United States) ■ African Academic ■ Network on Internet Policy (Africa) ■ AJIF (Nigeria) ■ American Civil Liberties Union (United States) ■ Aqualtune Lab (Brasil) ■ Asociación por los Derechos Civiles (ADC) (Argentina) ■ Association for Progressive Communications (APC) (Global) ■ Barracón Digital (Honduras) ■ Beyond Saving Lives Foundation (Africa) ■ Big Brother Watch (United Kingdom) ■ Body & Data (Nepal) ■ Canadian Civil Liberties Association ■ CAPÍTULO GUATEMALA DE INTERNET SOCIETY (Guatemala) ■ Center for Democracy & Technology (United States) ■ Centre for Free Expression (Canada) ■ CILIP/ Bürgerrechte & Polizei (Germany) ■ Código Sur (Centroamerica) ■ Community NetHUBs Africa ■ Dangerous Speech Project (United States) ■ Defending Rights & Dissent (United States) ■ Demand Progress Education Fund (United States) ■ Derechos Digitales (Latin America) ■ Digital Rights Foundation (Pakistan) ■ Digital Rights Watch (Australia) ■ DNS Africa Online (Africa) ■ Electronic Frontier Foundation (United States) ■ EngageMedia (Asia-Pacific) ■ Eticas Foundation (Spain) ■ European Center for Not-for-Profit Law (ECNL) (Europe) ■ Fight for the Future (United States) ■ Free Speech Coalition Inc. (FSC) (United States) ■ Fundación Karisma (Colombia) ■ Global Forum for Media Development (GFMD) (Belgium) ■ Global Partners Digital (United Kingdom) ■ Global Voices (Netherlands) ■ Hiperderecho (Peru) ■ Instituto Beta: Internet & Democracia – IBIDEM (Brazil) ■ Instituto de Referência em Internet e Sociedade - IRIS (Brazil) ■ Instituto Liberdade Digital - ILD (Brazil) ■ Instituto Nupef (Brazil) ■ Internet Governance Project, Georgia Institute of Technology (Global) ■ Internet Society Panama Chapter ■ Interpeer Project (Germany) ■ IP.rec - Law and Technology Research Institute of Recife (Brazil) ■ IPANDETEC Central America ■ ISOC Bolivia ■ ISOC Brazil - Brazilian Chapter of the Internet Society ■ ISOC Chapter Dominican Republic ■ ISOC Ghana ■ ISOC India Hyderabad Chapter ■ ISOC Paraguay Chapter ■ ISOC Senegal Chapter ■ JCA-NET (Japan) ■ Kijiji Yeetu (Kenya) ■ LGBT Technology Partnership & Institute (United States) ■ Liberty (United Kingdom) ■ mailbox.org (EU/DE) ■ May First Movement Technology (United States) ■ National Coalition Against Censorship (United States) ■ National Working Positive Coalition (United States) ■ New America's Open Technology Institute (United States) ■ OhmTel Ltda (Columbia) ■ OpenMedia (Canada/United States) ■ Paradigm Initiative (PIN) (Africa) ■ PDX Privacy (United States) ■ PEN America (Global) ■ Privacy International (Global) ■ PRIVACY LATAM (Argentina) ■ Progressive Technology Project (United States) ■ Prostasia Foundation (United States) ■ R3D: Red en Defensa de los Derechos Digitales (Mexico) ■ Ranking Digital Rights (United States) ■ S.T.O.P. - Surveillance Technology Oversight Project (United States) ■ Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) ■ Sero Project (United States) ■ Simply Secure (United States) ■ Software Freedom Law Center, India ■ SWOP Behind Bars (United States) ■ Tech for Good Asia (Hong Kong) ■ TEDIC (Paraguay) ■ Telangana (India) ■ The DKT Liberty Project (United States) ■ The Sex Workers Project of the Urban Justice Center (United States) ■ The Tor Project (Global) ■ UBUNTEAM (Africa) ■ US Human Rights Network (United States) ■ WITNESS (Global) ■ Woodhull Freedom Foundation (United States) ■ X-Lab (United States) ■ Zaina Foundation (Tanzania) Sero Project (United States) ■ Simply Secure (United States) ■ Software Freedom Law Center, India ■ SWOP Behind Bars (United States) ■ Tech for Good Asia (Hong Kong) ■ TEDIC (Paraguay) ■ Telangana (India) ■ The DKT Liberty Project (United States) ■ The Sex Workers Project of the Urban Justice Center (United States) ■ The Tor Project (Global) ■ UBUNTEAM (Africa) ■ US Human Rights Network (United States) ■ WITNESS (Global) ■ Woodhull Freedom Foundation (United States) ■ X-Lab (United States) ■ Zaina Foundation (Tanzania)

https://cdt.org/insights/international-coalition-calls-on-apple-to-abandon-plan-to-build-surveillance-capabilities-into-iphones-ipads-and-other-products/