Unsere Daten: Status quo

Die großen Konzerne sammeln unsere Daten

> »Unternehmen und nicht mehr die Staaten sind in den freien Demokratien der Welt die eigentliche Gefahr für den Datenschutz. Sie stellen die größte unmittelbare Herausforderung für den Datenschutz dar. (Michael Sandel)«[1]

Es sind vor allem unsere Daten, die in unvorstellbarem Umfang gesammelt und verwertet werden, die unsere Privatsphäre erodieren lassen. Gesammelt werden sie sowohl von den großen Konzernen als auch vom Staat.

Die Global Player unter den Datensammlern

Will man mehr über diese Gefährdung wissen, muss man sich diese Unternehmen und deren Praktiken genauer ansehen. Exemplarisch seien hier Google, Apple, Facebook, Amazon und Microsoft herausgegriffen, fünf große Konzerne, die für ihre Datensammlungen berüchtigt sind.[2]

1 Bohsem 2016.

2 Für die Konzerne Google, Apple, Facebook, Amazon und Microsoft wird häufig das Akronym GAFAM verwendet.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Google

> »Google ist zuallererst ein global agierender Werbekonzern. Kommerzielle Anzeigen sind das Business, mit dem Google seine Milliarden macht.«[3]

Die Datensammelwut von Google zeigt sehr schön das folgende Beispiel:

> »Französische Sicherheitsforscher des Unternehmens Eurecom haben 2000 Gratis-Apps für Android-Smartphones aus 25 verschiedenen Kategorien im Google Play Store geladen und auf einem Samsung-Smartphone ausgeführt. Der Netzwerkverkehr der Apps nach außen wurde abgefangen und analysiert. Demnach steuerten die Programme heimlich insgesamt 250 000 verschiedene Webadressen an und gaben Daten weiter.«[4]

Neuere Untersuchungen bestätigen diesen Trend. Die Datensammelwut nimmt stetig zu, wie nachstehendes Beispiel zeigt.

> »Forscher der Universität Oxford betrachteten fast eine Million Apps, die im ›Google Play Store‹ bereitgestellt sind. So gut wie alle haben Tracker eingebaut, die von amerikanischen Unternehmen sind. Siebenhunderttausend der Apps verbinden sich ausschließlich mit verschiedenen Profilbildungsfirmen in den Vereinigten Staaten. Mehr als hunderttausend Apps senden ihre Tracking-Daten zusätzlich in andere Länder, in denen Profilfirmen sitzen.«[5]

3 BigBrotherAward, 2013.

4 Spehr 2015.

5 Kurz 2018.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Larry Page, Sergey Brin und Eric Schmidt, Gründer und Verwaltungsrat der Google Inc., Mountain View, Kalifornien, USA, erhielten 2013 den BigBrotherAward in der Kategorie Globales Datensammeln.

> »Bei diesem Preisträger kritisieren wir nicht einen einzelnen Datenschutzverstoß. Wir prangern auch nicht einzelne Sätze in seinen Geschäftsbedingungen an. – Nein, der Konzern selbst, sein globales, allumfassendes Datensammeln, die Ausforschung der Nutzerinnen und Nutzer als Wesenskern seines Geschäftsmodells und sein de facto Monopol – das ist das Problem.«[6]

> »Google weiß, wer wir sind, wo wir gerade sind und was uns wichtig ist. Google weiß nicht nur, nach welchen Begriffen wir vorher gesucht haben, sondern auch, welche davon wir tatsächlich angeklickt haben. Google weiß minutiös, an welchem Tag wir zu welcher Zeit wach waren, für welche Personen, Nachrichten, Bücher wir uns interessiert haben, nach welchen Krankheiten wir recherchiert haben, welche Orte wir besucht haben, welche Videos wir uns angeschaut haben, welche Werbung uns angesprochen hat.«[7]

Apple

Der Gewinn von Apple basiert nicht primär auf Werbung, sondern zunächst einmal auf dem Verkauf von Produkten. Doch sollte das nicht darüber hinwegtäuschen, dass Apple sich durchaus für die Daten seiner Kunden interessiert und diese auch in großem Stil sammelt.

Wenn man in irgendeiner Form Kontakt mit Apple aufnimmt, sei es, dass man eine Apple ID erstellt, einen Konsumentenkredit beantragt, ein Produkt kauft, oder ein Softwareupdate herunterlädt: Es werden stets alle anfallenden Daten gespeichert. Das sind beispiels-

6 BigBrotherAward, 2013.

7 Ebd.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

weise Name, Adresse, Telefonnummer, E-Mail-Adresse, Informationen zur bevorzugten Kontaktaufnahme, Gerätekennungen, IP-Adressen, Standortinformationen, Kreditkarteninformationen und Profilinformationen, wenn der Kontakt über ein soziales Netzwerk erfolgt.[8]

Im Handy wird der Aufenthaltsort gespeichert mit Tages- und Uhrzeit, sofern man diese Option nicht abgeschaltet hat. Man kann also genau verfolgen, wo man sich wann aufgehalten hat.[9]

> »Siri [Sprachassistent von Apple] weiß noch nach zwei Jahren, was Nutzer den Sprachassistenten von Apple fragen. Denn so lange werden die Daten auf dem Server festgehalten.«[10]

Diese Daten werden nicht nur gespeichert.

> »Apple und seine verbundenen Unternehmen können diese personenbezogenen Daten untereinander austauschen. Sie können solche Daten auch mit anderen Informationen verbinden, um Produkte, Dienstleistungen, Inhalte und Werbung anzubieten oder zu verbessern.«[11]

Dass von diesen Möglichkeiten der Datenweitergabe reichlich Gebrauch gemacht wird, zeigt ein Experiment der *Washington Post*. Es deckt auf, dass 5.400 versteckte App Tracker unsere Daten verschlungen haben – in einer einzigen Woche. Apple verspricht Datenschutz, aber iPhone-Apps geben die Daten ihrer Nutzer an Tracker, Werbefirmen und Forschungsunternehmen weiter.[12]

---

8 Vgl. Apple Datenschutzrichtlinie, 2019.

9 Vgl. Giordano 2018.

10 Apple speichert Siri-Daten bis zu zwei Jahre, 2013.

11 Apple Datenschutzrichtlinie, 2019.

12 Vgl. Fowler 2019.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

2011 erhielt die Apple GmbH in München den BigBrotherAward in der Sparte Kommunikation »für die Geiselnahme ihrer Kunden mittels teurer Hardware und darauffolgende Erpressung, den firmeneigenen zweifelhaften Datenschutzbedingungen zuzustimmen.«[13]

> »Apples Firmenstrategie scheint darauf ausgelegt zu sein, möglichst viele Nutzerdaten zu erfassen, ähnlich wie es soziale Netzwerke auch tun. Werbepartner freuen sich darauf, mit Hilfe von Apple möglichst zielgruppengerechte und standortbezogene Werbung auf dem Telefon anzeigen zu können.«[14]

> »Damit die Werbung optimal auf deine Bedürfnisse abgestimmt ist, bietet dir Apple Anzeigen im App Store und in Apple News auf der Basis von Informationen wie deinem Suchverlauf im App Store oder den gelesenen Artikeln in Apple News.«[15]

> »Seit Mittwoch [17.10.2019] bietet Apple an, sämtliche Daten einsehen, herunterladen und löschen zu können, die die i-Geräte bisher über den jeweiligen User gesammelt haben.«[16]

Wer dies einmal ausprobiert und sich die gesammelten Daten angeschaut hat, für den ist klar, dass die Aussage von Apple, dass Privatheit ein fundamentales Menschenrecht ist,[17] hier ad absurdum geführt wird. Bemerkenswert ist auch, dass ein Löschen nur über ein Löschen

13 Der BigBrotherAward 2011 in der Kategorie »Kommunikation« geht an die Apple GmbH, 2011.

14 Ebd.

15 Apple Interessenbezogene Werbung im App Store und in Apple News deaktivieren, 2020.

16 Giordano 2018.

17 Vgl. Apple Privacy, 2020.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

des Accounts möglich ist. Erkennbar ist dies an den Möglichkeiten, die Apple anbietet, wenn man sich in seinen Account eingeloggt hat.[18]

Facebook

Die Nutzung von Facebook ist für Anwender kostenlos. Sie bezahlen die Nutzung dieser Plattform mit ihren Daten.

Jemand hat einmal gesagt: »Facebook ist eine Content-Fabrik.«[19] Der Rohstoff, der hier verarbeitet wird, ist Content, d h. Inhalte, also letztlich Daten. Zu diesen datenbezogenen Inhalten zählt alles, was auf Facebook erfasst wird, dazu gehört jede Information, jeder Like, jeder Share, jedes Selfie, jede aufgerufene Seite, jeder einzelne Klick, einfach alles. Diese Daten werden akribisch erfasst und analysiert. Sie dienen letztlich dazu, die Nutzer dahingehend zu beeinflussen, dass kommerzielle oder politische Werbung erfolgreich platziert werden kann.[20]

Facebook gibt die Daten seiner Nutzer an Werbekunden weiter. Das Tool ›Audience Insights‹ ist nichts anderes als eine riesige Datenbank mit den Daten der Nutzer von Facebook mit entsprechenden Abfragemöglichkeiten.

Dieses Tool steht allen Nutzern von Facebook zur Verfügung die einen Account für Werbeanzeigen haben. Diese Nutzer können damit Zielgruppen definieren, z.B. alle schwangeren Frauen im Bundesstaat New York mit Hochschulabschluss. Diese Zielgruppe können sie dann genauer analysieren, etwa wie viele dieser Frauen Single sind, wie viele in einer Partnerschaft leben, wie viele einer höheren Einkommensschicht angehören usw. An diese Zielgruppe können sie dann über den Werbeanzeigen-Manager die entsprechende Werbung schicken.[21]

2011 erhielt die Facebook Deutschland GmbH den BigBrother-Award in der Kategorie Kommunikation »für die gezielte Ausfor-

18 Vgl. Apple Daten und Datenschutz, 2020.

19 Kaeser 2018.

20 Vgl. ebd.

21 Vgl. Küchemann 2014; Roth 2020.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

schung von Menschen und ihrer persönlichen Beziehungen hinter der netten Fassade eines vorgeblichen Gratisangebots.«[22]

> »Die Fakten: Facebook sammelt alles an Daten, was sie bekommen können. Nicht nur Name, Adresse, Profilbild, Telefon, Handynummer, Fotos, Texte, Statusupdates, Aufenthaltsort, Nachrichten an Freunde, besuchte Webseiten und und und …«[23]

Amazon

Auch Amazon speichert die Daten seiner Kunden. Bei jedem Kontakt mit Amazon, sei es, dass man nach einem Produkt sucht, auf der Webseite von Amazon eine Bestellung aufgibt, mit dem Sprachdienst von Amazon spricht oder mit Amazon per Mail oder Telefon oder anderweitig kommuniziert: Alle dabei anfallenden Daten werden gespeichert. Das können z.B. Name, Adresse, Telefonnummer, E-Mail-Adresse, Passwörter, Zahlungsinformationen, Alter, Standort, Personen, an die Einkäufe versendet wurden, E-Mail-Adressen von Freunden und anderen Personen, IP-Adresse, Logins, und vieles mehr sein. Will man bei Amazon ein Produkt kaufen, muss man ein Amazon-Konto eröffnen. E-Mail-Adresse, Name, Adresse und Telefonnummer werden erfasst. Wählt man *Zahlung auf Rechnung*, muss man das Geburtsdatum angeben. Will man per Kreditkarte bezahlen, wird diese dauerhaft abgespeichert.

Amazon kennt damit unsere emotionalen Vorlieben und unsere finanziellen Möglichkeiten. Amazon verfügt u.a. über exakte und umfangreiche Bonitätsdaten. All diese Daten werden unter anderem zur Einblendung zielgruppengenauer Werbung genutzt.[24]

---

22 Der BigBrotherAward 2011 in der Kategorie »Kommunikation« geht an die Facebook Deutschland GmbH, 2011.

23 Ebd.

24 Vgl. Amazon Datenschutzerklärung, 2019; Wer weiß was über die Nutzer: Die wirkliche Datenkrake heißt Amazon, 2011; Daten-Speicherung.de – minimum data, maximum privacy, o.J.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Amazon bietet seinen Kunden in den USA 10 Dollar dafür, dass sie eine Browser-Erweiterung installieren (Amazon Assistant for Chrome). Diese soll den Nutzern dabei helfen, Preise im Internet zu vergleichen. Erst im Kleingedruckten erfährt man, dass das Programm das komplette Surfverhalten des Nutzers auswertet.[25]

Microsoft

Auch Microsoft sammelt die Daten seiner Kunden. Groß war die Aufregung nach der Einführung von Windows 10. Denn man stellte fest, dass dieses Betriebssystem umfangreiche System- und Nutzungsinformationen an Microsoft sendet. Verschiedene Datenschutzbehörden wurden aktiv.

So mahnte die französische Datenschutzbehörde CNIL Microsoft wegen Windows 10 ab. »Sie kritisiert vor allem eine ›übermäßige‹ Datensammlung ohne Einwilligung der Nutzer. Außerdem seien Anwenderdaten nicht ausreichend geschützt.«[26]

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) führte eine groß angelegte Studie zu Systemaufbau, Protokollierung, Härtung und der Sicherheitsfunktionen in Windows 10, kurz »SiSyPHuS Win10«, durch. Ein Teilergebnis dieser Untersuchung ist, dass zwar die Möglichkeit besteht, die Datenerfassung und -übermittlung vollständig zu deaktivieren. Das ist aber nur unter hohem Aufwand möglich und zwingt Nutzer dazu, bestimmte Dienste abzuschalten.[27]

Das niederländische Ministerium für Sicherheit und Justiz befasste sich damit, dass Microsoft Office noch mehr Telemetriedaten (das sind z.B. Daten über die individuelle Nutzung von Word, Excel, PowerPoint und Outlook) als Windows 10 sammelt. Es beauftragte die u.a. auf Datenschutz spezialisierte Firma Privacy Company mit einer

25 Vgl. Langer 2019.

26 Greif 2016.

27 Vgl. Matthes/Dachwitz 2018; Vgl. BSI untersucht Sicherheitseigenschaften von Windows 10, 2018.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Datenschutz-Folgenabschätzung für Microsoft Office. Die Ergebnisse zeigen u.a., dass personenbezogene Daten wie Metadaten und Inhalte illegal gespeichert werden, die im Falle von Behörden sogar geheimhaltungsbedürftiges Material betreffen können. Riskant ist darüber hinaus die Speicherung der Daten außerhalb der EU wegen des umstrittenen Privacy-Shield-Abkommens sowie die fehlende Kontrolle über die Art der übertragenen Daten und deren spätere Löschung.[28]

Mittlerweile befasst sich auch der Europäische Datenschutzbeauftragte mit Microsoft. Grund dafür ist, dass die EU-Institutionen sich bei ihren täglichen Aktivitäten auf Microsoft Dienste und Produkte verlassen. Dies schließt die Verarbeitung großer Mengen personenbezogener Daten ein. Es soll deshalb geprüft werden, ob die zwischen Microsoft und den EU-Institutionen geschlossenen vertraglichen Vereinbarungen in vollem Umfang mit den Datenschutzbestimmungen vereinbar sind.[29]

Inzwischen wurde bekannt, dass Microsoft die Office-Suite 365 um Funktionen erweitert (Stand 24.11.2020), mit denen Unternehmen die Arbeitsgepflogenheiten ihrer Belegschaft detailliert beobachten können. Bertold Brücher, Rechtsexperte beim DGB, hält einen rechtskonformen Einsatz für ausgeschlossen. Das Beispiel zeigt sehr deutlich, dass es bisher nicht gelungen ist, Microsoft hier Einhalt zu gebieten.[30]

2020 kommt eine Arbeitsgruppe der deutschen Datenschutzkonferenz zu dem Schluss, dass kein datenschutzgerechter Einsatz von Microsoft 365 möglich sei. Außerdem fordert sie dazu auf, das Problem der Abhängigkeit von Microsoft anzugehen. Immerhin verwenden 96 Prozent aller Behörden Produkte aus dem Microsoft-Office-Paket.[31]

Diese fünf hier aufgezählten Unternehmen Google, Apple, Facebook, Amazon und Microsoft stehen exemplarisch für die vielen an-

28 Vgl. Beiersmann 2018; Bordel 2018; Boehring 2018.

29 Vgl. Der Europäische Datenschutzbeauftragte, 2019.

30 Vgl. Schüler 2020.

31 Vgl. Ballweber 2020.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

deren, die die Daten ihrer Kunden in ganz großem Stil sammeln. Die Liste dieser Unternehmen ließe sich beliebig fortsetzen.

Der Staat sammelt unsere Daten

> »Wenn es zu einer Katastrophe kommt, besteht die Tendenz möglichst schnell zu reagieren, um die Dinge sofort zu beheben. (Susan Landau)«[32]

Diese oft sehr wenig durchdachten Reaktionen auf Katastrophen beinhalten in den meisten Fällen den Ruf nach noch mehr Daten. Zwar benötigt der Staat Daten seiner Bürger, um diese verwalten zu können, wie z.B. die Daten der Melderegister, Daten zur Rentenversicherung, Steuerdaten usw. Doch gerade im Zuge der Bedrohung durch Terror und Kriminalität verlangt der Staat den Zugriff auf immer weitere Daten.

Hierzu einige Beispiele:[33]

> »Die Attacken in Paris im November 2015 und in San Bernardino im Dezember 2015 haben die Forderung der Regierung nach weiterem Zugriff auf elektronische Kommunikation – Telefone, EMails und Browser Chronik – neu entfacht, um Terrorismus zu verhindern.«[34]

32 »Whenever there's a disaster, there's a tendency to do a knee-jerk reaction to fix things right away. (Susan Landau)« Sadeghi/Dessouki 2016.

33 Es sei hier angemerkt, dass bei einigen dieser Beispiele die sogenannte Vorratsdatenspeicherung erwähnt wird, auf die später noch genauer eingegangen wird.

34 »These recent attacks (attacks in Paris in November 2015 and in San Bernardino in December 2015) reignited calls for more government access to people's electronic communications-phones, emails and Internet browsing history – to prevent terrorism.« Jasen 2016.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

»Nach den Terroranschlägen auf ›Charlie Hebdo‹ [07.01.2015] fordern Politiker und Behörden schon wieder die Vorratsdatenspeicherung.«[35]

»Innenpolitiker verschiedener Parteien, Vertreter des Bundesinnenministeriums und der Chef des Bundesamts für Verfassungsschutz fordern dieser Tage einen verbesserten Zugriff auf Daten aus sozialen Netzwerken. Sie berufen sich dabei auf den Amoklauf in München und auf terroristisch motivierte Straftaten in den letzten Wochen.«[36]

»[Am 30. Juli 2016] wird das Telekommunikationsgesetz abgeändert, so dass die Daten der Käufer der mehr als sechzehn Millionen SIM-Karten für Mobiltelefone, die in Deutschland pro Jahr ohne Vertrag verkauft werden, demnächst mit Identitätsdokumenten abgeglichen werden müssen. Die Informationen sind jeweils zu speichern und sicher zu verwahren, falls ein behördlicher ›Bedarfsträger‹ einen Blick darauf werfen möchte.«[37] Dies soll einer verbesserten Terrorismusbekämpfung dienen.

»Die Niederlande planen eine Verschärfung der Massenüberwachung von Internet und Kommunikation durch ihre Geheimdienste. […] Zukünftig soll es den Geheimdiensten erlaubt sein, jeglichen Internetverkehr abzuhören, Computer und Handys zu hacken und Rohdaten ungefiltert an befreundete Dienste weiterzugeben. […] Wie auch in Deutschland wird die nun angestrengte Reform mit der gestiegenen Gefahr von Cyberkriminalität und Terroranschlägen begründet.«[38]

35 Lobo 2015.

36 Schaar 2016.

37 Kurz 2016.

38 Rebiger 2016.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

> »Nach den Ausschreitungen vor dem Reichstagsgebäude [im August 2020] will die CDU die Kompetenzen der Polizei erweitern – vor allem um die Vorratsdatenspeicherung.«[39]

Diese Vorratsdatenspeicherung – von Politikern immer wieder gefordert, von Bürgerrechtlern und Datenschutzexperten vehement bekämpft – beinhaltet, dass alle bei Telekommunikationsvorgängen anfallenden Verbindungsdaten vorsorglich aufbewahrt werden. Damit ist nachvollziehbar, wer mit wem per Telefon oder Handy in Verbindung gestanden oder das Internet genutzt hat. Man spricht hier auch von einer anlasslosen, d.h. ohne konkreten Verdacht erfolgenden Überwachung der gesamten Bevölkerung. Denn diese Verbindungsdaten sind weit aussagekräftiger als mancher sich das vorstellen mag. Sie sagen oft mehr über Menschen aus als die eigentlichen Inhalte der Kommunikation.[40]

Die Vorratsdatenspeicherung hat eine wechselvolle Geschichte. Immer wieder wurde sie eingeführt, um danach wieder aufgehoben zu werden.

Ihren Beginn hat sie mit der EU-Richtlinie zur Vorratsdatenspeicherung (2006/24/EG), die am 15. März 2006 in Kraft trat.

> »Mit ihr wurden die EU-Mitgliedstaaten verpflichtet, die Speicherung von Verkehrs- und Standortdaten sowie Daten zur Feststellung der Identität der jeweiligen Teilnehmer nach nationalem Recht sicherzustellen. Den Providern wurde auferlegt, die Verbindungsdaten nahezu aller Kommunikationsvorgänge für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten aufzubewahren.«[41]

39 CDU-Spitze fordert nach Corona-Demo mehr Befugnisse für Polizei, 2020.

40 Vgl. Vorratsdatenspeicherung: Alle Menschen unter Generalverdacht, o.J.

41 Ebd.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Die Vorratsdatenspeicherung wurde dann mit Urteil vom 2. März 2010 vom Bundesverfassungsgericht verboten. Mit Wirkung vom 18.12.2015 ist sie jedoch wieder in Kraft gesetzt worden.

> »[Danach] soll spätestens ab 1. Juli 2017 zehn Wochen lang nachvollziehbar sein, wer mit wem per Telefon oder Handy in Verbindung gestanden oder das Internet genutzt hat. Bei Handy-Telefonaten und SMS wird auch der jeweilige Standort des Benutzers festgehalten und vier Wochen lang gespeichert. In Verbindung mit anderen Daten wird auch die Internetnutzung nachvollziehbar.«[42]

Derzeitiger Stand: Das Bundesverwaltungsgericht in Leipzig hatte am 25. September 2019

> »entschieden, dem Gerichtshof der Europäischen Union (EuGH) eine Frage zur Auslegung der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) vorzulegen. Von der Klärung dieser Frage hängt die Anwendbarkeit der im Telekommunikationsgesetz enthaltenen Regelungen zur Vorratsdatenspeicherung ab.«[43]

Bis zur endgültigen Entscheidung ist damit die Pflicht zur Datenspeicherung ausgesetzt.

Anlass für dieses Urteil waren die Klagen der Telekom und des Münchener Internet-Service-Provider SpaceNet gegen die Pflicht zur Datenspeicherung.[44]

Auch wenn die Speicherpflicht derzeit ausgesetzt ist, hat die Vorratsdatenspeicherung noch immer viele Befürworter. Jüngstes Beispiel ist Manuela Schwesig, Ministerpräsidentin von Mecklen-

42 Stoppt die Vorratsdatenspeicherung, o.J.

43 VBVerwG. Pressemitteilung 2019

44 Vgl. Schäfer 2019.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

burg-Vorpommern, die sich mit Datum vom 08.09.2020 für die Wiedereinführung der Vorratsdatenspeicherung aussprach.[45] Dies soll der verstärkten Bekämpfung von Kinderpornografie und extremistischen Straftaten dienen. Dazu hat sie einen Antrag an den Bundesrat gestellt, man möge die Einführung der Mindestspeicherpflicht soweit möglich bereits jetzt vorbereiten, um bei einem entsprechenden Urteil des Europäischen Gerichtshofes sofort handlungsfähig zu sein.[46]

Am 6. Oktober 2020 hat der Europäische Gerichtshof seine Urteile zu drei Klagen gegen die Vorratsdatenspeicherung aus dem Vereinigten Königreich, Frankreich und Belgien verkündet. Danach ist eine flächendeckende und pauschale Speicherung von Internet- und Telefon-Verbindungsdaten *nicht* zulässig. Ausnahmen sind aber möglich, wenn es um die Bekämpfung schwerer Kriminalität oder den konkreten Fall einer Bedrohung der nationalen Sicherheit geht.[47] Das Urteil für Deutschland liegt zwar noch nicht vor. Es dürfte aber kaum anders ausfallen. Die Aktion von Manuela Schwesig erweist sich damit im Nachhinein als sinnloser und wenig durchdachter Aktionismus.

Eine weitere sehr umstrittene Regelung ist die Regelung über die Weitergabe von Flugpassagierdaten.

> »Das [EU] Parlament hat [am 14.04.2016] die neue Richtlinie zur Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität verabschiedet. Die Regeln verpflichten Luftfahrtgesellschaften dazu, ihre Fluggastdaten für Flüge von der EU in Drittländer und andersherum den nationalen Behörden zur Verfügung zu stellen.«[48]

45 Vgl. Schwesig 2020.

46 Vgl. ebd.

47 Vgl. EuGH verbietet Vorratsdatenspeicherung erneut, 2020; Vorratsdatenspeicherung ist nur in Ausnahmen zulässig, 2020.

48 Parlament stimmt EU-Richtlinie über Verwendung von Fluggastdaten zu, 2016.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

> »Diese Informationen müssen für einen Zeitraum von fünf Jahren vorgehalten werden. Sechs Monate nach der Übermittlung allerdings müssen die Daten unkenntlich gemacht werden, d.h. Datenelemente wie zum Beispiel der Name, die Anschrift oder Kontaktdaten dürfen nicht mehr sichtbar sein.«[49]

> »Ich will nicht so weit gehen zu sagen, die Unschuldsvermutung würde außer Kraft gesetzt. Aber sie wird abgeschwächt in ihrer Bedeutung für den Rechtsstaat. Und das halte ich wirklich für fatal.«[50]

Dies ist eine Warnung der Philosophin Beate Rössler vor all diesen Datensammlungen. Denn in den meisten Fällen werden die Daten aller Bürger erfasst, unabhängig davon, ob ein Verdachtsmoment vorliegt oder nicht. Zudem bedeuten diese Datensammlungen immer auch eine Überwachung der Bevölkerung.

Völlig verändert hat sich die Situation seit Beginn der Corona-Pandemie. Auf einmal wird alles dem Schutz der Gesundheit untergeordnet. Was umgekehrt bedeutet, dass alle Urteile diesen Jahres bezüglich Datensicherheit, Personenrechte und das Recht auf ›Privaten Raum‹ (nicht nur das Recht auf Privatheit, sondern auf Freiheit im Privaten) unter dem Eindruck von Covid-19 stehen. Die demokratische Zumutung rechtfertigt sich im Angesicht der tödlichen Bedrohung, die ein für das Auge unsichtbares Virus wie Sars-Cov-2 darstellt. Es gilt, zwischen so vielen Daten und ›demokratischen Zumutungen‹ wie nötig, um Covid-19 einzudämmen und so vielen Freiheiten und Rechten wie möglich, die Balance zu wahren.

> »Diese Pandemie ist eine demokratische Zumutung; denn sie schränkt genau das ein, was unsere existenziellen Rechte

49 Ebd.

50 Rössler 2016.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

> und Bedürfnisse sind – die der Erwachsenen genauso wie die der Kinder. Eine solche Situation ist nur akzeptabel und erträglich, wenn die Gründe für die Einschränkungen transparent und nachvollziehbar sind, wenn Kritik und Widerspruch nicht nur erlaubt, sondern eingefordert und angehört werden – wechselseitig.«[51]

In diesem Zusammenhang lohnt es sich, einen Blick auf die Corona-App zu werfen. Diese App soll helfen, Infektionsketten zu erkennen und zu durchbrechen. Zu diesem Zweck werden sehr sensible Informationen über Corona-Infektionen weitergegeben. Daher wurde bei der Entwicklung der App großen Wert auf ausreichenden Datenschutz und Sicherheit gelegt.

Bei der installierten App erhält man eine anonymisierte Nachricht, wenn sich eine infizierte Person für mindestens 15 Minuten und in einem Umkreis von 2 m oder weniger in der Nähe des jeweiligen Appnutzers aufgehalten hat. Dazu muss die infizierte Person allerdings ebenfalls die App installiert haben. Nur wenn die Menschen verstanden haben, warum diese App so wichtig ist und wenn sie überzeugt sind, dass sie dieser App vertrauen können, werden sie sie auch einsetzen.[52]

Um dieses Vertrauen zu rechtfertigen, haben in Österreich drei Organisationen den Quellcode der österreichischen App analysiert. Das Ergebnis ist ein langer Bericht, der Mängel aufzeigt und Verbesserungsvorschläge macht. Diese wurden von den Entwicklern der App bereitwillig aufgegriffen. Teilweise wurden sie sofort umgesetzt, zum Teil wurde ihre Umsetzung für einen späteren Zeitpunkt anvisiert.

---

51 Regierungserklärung von Bundeskanzlerin Dr. Angela Merkel, 2020.

52 Die App wurde 22,8 Millionen Mal heruntergeladen. Stand 19.11 2020. Vgl. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_20112020.pdf?__blob=publicationFile. [Letzter Zugriff 19.11.2020].

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Eine solche Zusammenarbeit ist nicht unbedingt selbstverständlich. Das zeigt das Beispiel Deutschlands. Dort haben mehrere Organisationen einen offenen Brief an die Regierung geschickt, indem sie u.a. darum baten, den Argumenten und ›Vorbehalten‹ von ›Experten‹ mehr Gehör zu schenken. Hauptkritikpunkt war dabei der zentrale Ansatz, den die deutsche Bundesregierung ursprünglich verfolgte. Dieser Brief wurde von rund 300 internationalen Wissenschaftlerinnen und Wissenschaftlern unterzeichnet.[53] Erfreulicherweise hat auch Deutschland sich inzwischen für eine dezentrale Speicherung der Daten entschieden.

> »Die Corona-App ist zwar Open Source – der Programmcode ist für alle einsehbar und die Software gratis – nicht aber die Schnittstelle zum Betriebssystem.«[54]

Dahinter beginnt das Firmengeheimnis von Google und Apple. Grassegger, ein Schweizer Journalist, hat dies einmal so beschrieben: »Es ist, als ob man die Bauanleitung einer Tür veröffentlicht, aber nichts über das Zimmer dahinter.«[55]

Das ist wohl einer der Gründe, warum die Corona-App keine Daten über individuelle Erkrankungen liefert und die Identität der Infizierten verschleiert.[56] Zu groß ist die Angst davor, dass persönliche Daten missbraucht werden könnten.[57]

---

53 Denn eine zentrale Speicherung wäre deshalb so problematisch, weil die Sicherheit dieser hochsensiblen Daten nicht wirklich gewährleistet werden kann. Auch ist das Risiko einer De-Anonymisierung deutlich höher als bei einer dezentralen Lösung. Zudem besteht die Gefahr, dass diese Daten auch für andere Zwecke verwendet werden. Die Privatheit der Nutzer ist so nicht ausreichend sichergestellt.

54 Grassegger 2020

55 Grassegger 2020.

56 Berichtet wird dies explizit über die SwissCovid App, aber das gilt sicherlich auch für die deutsche und die österreichische Corona-App.

57 Vgl. Grassegger 2020.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

Neueste Entwicklungen zeigen, wie groß die Datensammelwut des Staates ist. So hat die EU-Kommission einen Gesetzesentwurf vorlegt, der das Teilen wertvoller Datensätze innerhalb der Europäischen Union erleichtern soll und mit dem der Zugang sowohl zu persönlichen Daten von Nutzern als auch zu nicht-persönlichen Daten erleichtert werden soll. Dass hier Datenschützer vor allem wegen der Daten von Nutzenden erhebliche Bedenken haben, liegt auf der Hand, denn diese sind durch Gesetze wie die Datenschutzgrundverordnung geschützt.[58]

Vor diesem Hintergrund ist es nicht verwunderlich, dass es auch kritische Stimmen zum Verhalten des Staates gibt:

> »Der Staat, so das Bild, ist nicht nur Partner in der Abwehr von Risiken und Verletzungen, er ist nicht nur Baumeister und Helfer bei der Konstruktion von Schutzwällen, welche die Sicherheit der Informationsverarbeitung gewährleisten; er ist bei dieser Verarbeitung auch Spion und Lauscher an der Wand, gegen die Interessen derer, für deren Kommunikation er sich interessiert.«[59]

Dieses Zitat ist insofern bemerkenswert, als es von einem Repräsentanten des Staates, einem Verfassungsrichter, kommt, der die Rolle des Staates durchaus zwiespältig sieht. Es entstammt einem Vortrag auf dem 7. Deutschen Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am 14. Mai 2001. Winfrid Hassemer war durchaus bewusst, dass dem Veranstalter des Kongresses, dem BSI, diese Aussage wohl kaum genehm sein würde.

In diesen Zusammenhang passt auch eine Aussage von Obama auf der South By Southwest Interactive, einer wichtigen Technikkonfe-

58 Vgl. Fanta, A./Kamps, L. 2020.

59 Hassemer 2001. Winfried Hassemer, verstorbener deutscher Strafrechtler, einst Vizepräsident des deutschen Bundesverfassungsgerichts.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

renz in Austin, Texas. Er plädiert dort für eine gesunde Skepsis gegenüber dem Staat.

> »Wir alle schätzen unsere Privatsphäre, unsere Gesellschaft beruht auf der Verfassung und den Bürgerrechten (Bill of Rights), sowie auf einer gesunden Skepsis gegenüber übergroßer Regierungsmacht.«[60]

60 »All of us value our privacy, and this is a society that is built on a Constitution and a Bill of Rights and a healthy skepticism about overreaching government power.« Remarks by the President at South By Southwest Interactive, 2016.

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.14361/9783839456057-003 https://www.inlibra.com/de/agb - Open Access -