Gerät die Datenverarbeitung außer Kontrolle?[1]

Alexander Dix

Prolog

Die Furcht des Menschen vor dem Verlust der Kontrolle über eigene Geschöpfe hat immer wieder Niederschlag in Mythologie und Literatur gefunden. Die griechische Prometheus-Sage beschreibt den Titanen, der den ersten Menschen aus Lehm geschaffen hat, allerdings mit fehlerhaften Eigenschaften, unter deren Folgen die Menschheit noch heute leidet. Die Legende vom Golem berichtet vom Geschöpf des Rabbi Löw, das den Auftrag erhielt, Wasser ins Haus zu schaffen und damit nicht aufhörte, weil er keine entsprechende Anweisung erhalten hatte. In einer anderen Version wurde der Rabbi Löw in dem Moment, als er den Golem tötete, von diesem erschlagen. Johann Wolfgang v. Goethe hat in seiner Ballade vom „Zauberlehrling“ (1797) möglicherweise an die Golem-Legende angeknüpft. Wenig später verfasste Mary Shelley den Roman „Frankenstein oder der moderne Prometheus“ (1818), in dem sie einen Wissenschaftler ein intelligentes Monster erschaffen lässt, über das er die Kontrolle verliert.

Es wäre verfehlt, diese mythologischen und literarischen Vorbilder angesichts der rasanten technischen Entwicklung etwa im Bereich des *machine learning* und der künstlichen Intelligenz zum Anlass für Alarmismus oder Fatalismus zu nehmen, zumal die Entwicklung der künstlichen Intelligenz erst am Anfang steht. Yuval Harari stellt allerdings die Frage, was aus unserer Gesellschaft wird, wenn hochintelligente Algorithmen uns besser kennen als wir selbst.[2]

Im modernen Verfassungsstaat dürfen technische Produkte mit Auswirkungen auf die Rechte des Einzelnen nur dann eingesetzt werden, wenn dabei rechtliche Anforderungen erfüllt werden. Es ist das Verdienst von Alexander Roßnagel, die Bedeutung einer verfassungsverträglichen Technikgestaltung – im Unterschied zu einer lediglich reaktiven Rechtsdurchsetzung – in diesem Zusammenhang hervorgehoben zu haben.[3] Verfassungs- und rechtsverträglich ist eine Technikgestaltung nur dann, wenn sie kontrollierbar ist und kontrolliert wird. In einem zentralen Bereich der modernen Technik, der automatisierten Datenverarbeitung und insbesondere der Verarbeitung personenbezogener Daten, stellt sich aber immer drängender die Frage, ob noch jemand in der Lage ist, sie zu kontrollieren. Dabei geht

---

[1] Erstmals veröffentlicht in: Hentschel, A./Hornung, G./Jandt, I. (Hrsg.), Mensch-Technik-Umwelt: Verantwortung für eine sozialverträgliche Zukunft, Festschrift für Alexander Roßnagel zum 70. Geburtstag, Baden-Baden 2020, S. 245 ff.

[2] *Harari*, Homo Deus – Eine Geschichte von Morgen, München 2017, 608; vgl. auch *Tene/Polonetsky*, Taming the Golem: Challenges of Ethical Algorithmic Decision-Making, North Carolina Journal of Law and Technology 19(2017), 125 f.

[3] *Roßnagel/Hornung/Geminn/Johannes* (Hrsg.), Rechtsverträgliche Technikgestaltung und technikadäquate Rechtsentwicklung. 30 Jahre Projektgruppe verfassungsverträgliche Technikgestaltung, Kassel 2018, https://www.upress.uni-kassel.de/katalog/abstract.php?978-3-7376-0602-8.

es nicht um Kontrolle als Selbstzweck, sondern darum, dass jede Form von Kontrollverlust das Recht des Einzelnen in Frage stellt, grundsätzlich selbst über die Verwendung seiner Daten bestimmen zu können.

Einige praktische Beispiele aus der jüngsten Vergangenheit mögen das illustrieren:

Im August 2019 veranstaltete das niederländische Justizministerium zusammen mit dem Europäischen Datenschutzbeauftragten das erste Haager Forum (EU Software and Cloud Suppliers Customer Council), bei dem sich Vertreter von Behörden aus Europa trafen, um über die Ergebnisse einer Prüfung der Cloud-Angebote von Microsoft zu beraten. Ziel dieser Zusammenkunft war es nach einer Pressemitteilung des Europäischen Datenschutzbeauftragten, „die Kontrolle über IT-Dienste und Produkte zurückzugewinnen, die von großen Diensteanbietern bereitgestellt werden."[4] Auch die deutsche Datenschutzkonferenz hat festgestellt, dass die Datenübermittlung bei der Nutzung des Betriebssystems Windows 10 an Microsoft durch Einstellungen der Software nicht vollständig unterbunden werden kann. „Da die Übertragung verschlüsselt an Microsoft erfolgt, ist nicht abschließend festzustellen, ob und wenn ja welche personenbezogenen Daten an Microsoft übermittelt werden".[5] Die deutschen Datenschutzbeauftragten weisen in ihrem Beschluss darauf hin, dass der Aufwand, den die Verantwortlichen bei einer datenschutzkonformen Nutzung von Windows 10 treiben müssen, gegenwärtig erheblich ist und sich minimieren ließe, „wenn Microsoft den Verantwortlichen einfache Möglichkeiten insbesondere zur permanenten Deaktivierung aller Datenübermittlungen bereitstellen würde."[6]

Im September 2019 wurde durch Recherchen des Bayerischen Rundfunks und der US-Investigativplattform ProPublica bekannt, dass weltweit 16 Millionen medizinische Datensätze von Patienten aus 50 Ländern, darunter eine Million Datensätze eines US-Anbieters radiologischer Untersuchungen, auf unsicher konfigurierten Servern (Picture Archiving and Communication System Server – PACS) unverschlüsselt lagerten, so dass Unbefugte jederzeit auf sie hätten zugreifen können. Betroffen waren auch rund 13.000 Patienten in deutschen Krankenhäusern. Berichte über derart unsicher konfigurierte Server soll es bereits 2016 gegeben haben, ohne dass dies erkennbare Konsequenzen gehabt hätte.[7] Im November 2019 war das Klinikum Fürth Opfer eines Cyberangriffs mit dem Trojanervirus „EMOTET", was zur Folge hatte, dass tagelang

---

[4] https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en (zuletzt abgerufen am 14.5.2020). Der Apple-Chef Tim Cook hat 2018 die Befürchtung geäußert, die Datenschutzprobleme könnten bald so groß werden, dass sie nicht mehr lösbar seien (https://www.heise.de/mac-and-i/meldung/Apple-Chef-Datenschutzprobleme-bald-zu-gross-um-sie-zu-beheben-4202736.html, zuletzt abgerufen am 14.5.2020).

[5] Positionierung der DSK zum datenschutzkonformen Einsatz von Windows 10 vom 3.4.2019, https://www.datenschutzkonferenz-online.de/media/dskb/20190403_positionierung_windows_10.pdf (zuletzt abgerufen am 14.5.2020).

[6] S. Positionierung der DSK (Fn. 5).

[7] https://www.heise.de/newsticker/meldung/Unsicher-konfigurierte-Server-leaken-Daten-von-Millionen-Patienten-4531255.html (zuletzt abgerufen am 14.5.2020).

die Notaufnahme für Patienten geschlossen werden musste.[8] 2018 verursachte ein weltweiter Cyberangriff mit dem Virus „WannaCry“ allein beim britischen National Health Service einen Schaden von 92 Millionen Pfund.[9]

Im Zuge der durch Edward Snowden initiierten Enthüllungen über die Überwachungspraktiken der National Security Agency (NSA) erreichte die US-Bürgerrechtsorganisation Electronic Frontier Foundation 2013 beim Justizministerium die Offenlegung von Dokumenten, aus denen hervorging, dass die NSA zeitweise rechtswidrig US-Bürger ohne die vorgeschriebene richterliche Anordnung überwacht habe. Zur Begründung wurde darauf hingewiesen, dass niemand innerhalb des Nachrichtendienstes „volles Verständnis dafür gehabt habe, wie das System arbeite“.[10] 2018 wurde bekannt, dass die NSA abgehörte Kommunikationsinhalte, die als Beweismittel vor Gericht hätten dienen sollen, versehentlich gelöscht hat.[11] Auch der britische Inlandsgeheimdienst MI5 konnte nach einem Bericht der zuständigen Aufsichtsinstanz (Investigatory Powers Commissioner‘s Office) vom Mai 2019 nicht in ausreichendem Maße sicherstellen, dass die gesetzlichen Bestimmungen für seine Tätigkeit in einer bestimmten technischen Umgebung eingehalten werden.[12]

Seit 2016 erhält in Indien jeder Mensch eine zwölfstellige Identifikationsnummer („Aadhaar“), die in einer zentralen Datenbank mit den biometrischen Merkmalen dieser Person (Fingerabdrücke aller zehn Finger, Iris-Scans beider Augen und Foto des Gesichts) sowie mit direkt personenbezogenen Daten (Name, Geburtsdatum, Geschlecht, Adresse) verknüpft wird. Dadurch verfügt das bevölkerungsreichste Land der Erde mit der Aadhaar-Datenbank (Central Identities Data Repository-CIDR) mit 1,2 Milliarden Datensätzen über die größte biometrische Datensammlung der Welt. Im Januar 2018 war es Unbekannten möglich, auf die Daten von über einer Milliarde Menschen unbefugt zuzugreifen. Auch später kam es wiederholt zu Datenlecks bei Aadhaar.[13] Dennoch hat das indische Verfassungsgericht diese Datenbank mit seinem Urteil vom 26.9.2018 für verfassungskonform erklärt und lediglich ihre Nutzung durch private Unternehmen eingeschränkt.[14]

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt Bremen, Imke Sommer, erklärte Ende 2019 gegenüber dem

---

8 https://www.heise.de/newsticker/meldung/Klinikum-Fuerth-geht-nach-Hackerangriff-wieder-zu-Normalitaet-ueber-4617966.html (zuletzt abgerufen am 14.5.2020).

9 https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ (zuletzt abgerufen am 14.5.2020).

10 Süddeutsche Zeitung v. 12.9.2013, 8 („Eingriff in die Privatsphäre“).

11 https://www.heise.de/newsticker/meldung/Lauschprogramm-NSA-hat-verfahrensrelevante-Daten-versehentlich-geloescht-3948184.html (zuletzt abgerufen am 14.5.2020).

12 Vgl. die schriftliche Mitteilung des britischen Innenministers Javid, https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2019-05-09/HCWS1552/ (zuletzt abgerufen am 14.5.2020).

13 https://techcrunch.com/2019/01/31/aadhaar-data-leak/ (zuletzt abgerufen am 14.5.2020).

14 Justice Puttaswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012.

„Tagesspiegel“, sie könne wegen der eingeschränkten personellen Ressourcen ihrer Behörde die Einhaltung der Datenschutz-Grundverordnung nicht durch eine umfangreiche Prüftätigkeit kontrollieren, sondern sei darauf angewiesen, dass Betroffene selbst auf Missstände aufmerksam machen.[15]

Diese Beispiele für Szenarien des Kontrollverlusts[16] lassen sich bestimmten Kategorien zuordnen und zugleich soll untersucht werden, wie erfolgversprechend die weltweit verstärkten regulatorischen Gegenstrategien gegen solche Kontrollverluste sind.

I. Technische Risiken

Die Zahl der Hacker-Angriffe und Cyber-Attacken auf staatliche und private Datenbestände nimmt ständig zu. Allein in den USA wurden seit 2005 mehr als 9.300 Datenlecks mit mehr als 10 Milliarden betroffenen Datensätzen gemeldet.[17] Die Zahl der betroffenen Personen ist unbekannt. Während in Deutschland im Jahr 2016 allein im Bereich der Telekommunikationsanbieter 258 Meldungen über Sicherheitsverletzungen bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit eingingen, nahm diese Zahl bis 2017 auf knapp 830 Meldungen zu.[18] Es vergeht kaum ein Tag, in dem keine neuen Sicherheitslecks in der Datenverarbeitung bekannt werden. Neben möglichen oder realisierten Angriffen auf vernetzte Fahrzeuge oder intelligente Stromnetze seien nur die Fälle der Personen erwähnt, die in ihrem Smart Home gefangen waren,[19] oder des Nutzers einer gehackten Ring Camera, dessen Kinder von Angreifern beobachtet und belästigt wurden.[20]

Dabei sind Angriffe auf Krankenhäuser besonders bedrohlich, weil sie – wie im Fall des Klinikums Fürth - die Aufnahme von Patienten verhindern, die Verfügbarkeit von lebenswichtigen Patientendaten beeinträchtigen oder diese verfälschen. Insofern ist die bei manchen IT-Managern oder Gesundheitspolitikern anzutreffende Auffassung, Datenschutzbedenken hätten nur Gesunde, zumindest fahrlässig. Geradezu erschreckend sind aber Fälle wie die der ungesicherten PACS-Server, bei denen nicht etwa kriminelle Energie von Hackern, sondern die schlichte Nachlässigkeit bei der

---

[15] Der Tagesspiegel v. 21.12.2019, 17 („Teurer Datenschutz“).

[16] Ein weiteres wesentliches Beispiel, das hier nicht näher untersucht wird, ist die Online- und App-gestützte Werbung, zu der die norwegische Verbraucherschutzorganisation Forbruker Radet eine umfassende Untersuchung veröffentlicht hat: Out of control – How consumers are exploited by the onlinje advertising industry, 14.1.2020, https://www.forbrukerradet.no/out-of-control/ (zuletzt abgerufen am 14.5.2020).

[17] https://privacyrights.org/data-breaches (zuletzt abgerufen am 14.5.2020).

[18] *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, 27. Tätigkeitsbericht 2016-2017, 107.

[19] https://www.stern.de/digital/smarthome/das-smart-home--eine-horrorvision-3457156.html (zuletzt abgerufen am 14.5.2020).

[20] https://www.theguardian.com/technology/2019/dec/27/ring-camera-lawsuit-hackers-alabama (zuletzt abgerufen am 14.5.2020).

Konfiguration oder dem Betrieb von Servern dazu führt, dass sensitive Gesundheitsinformationen öffentlich abrufbar sind.

Das Internet wurde ursprünglich als eine dezentrale und damit hochsichere, weil hoch verfügbare Infrastruktur konzipiert. Das ist zwar heute nicht mehr uneingeschränkt der Fall, weil Regierungen (wie z.B. jüngst in Indien) den lokalen Zugang zum Netz unterbinden können. Von vornherein aber war die Kommunikation über das Internet per se unsicher, soweit die Kommunikationspartner keine besonderen Sicherheitsmaßnahmen (etwa Verschlüsselung) ergriffen. Das bedeutet, dass jeder Anschluss eines Computers oder eines intelligenten Geräts an das Internet diese einem erhöhten Überwachungsrisiko aussetzt. Von dem NSA-Kryptologen Robert Morris Sr. stammen die drei Regeln der Computer-Sicherheit (sic!): Regel 1: Besitze keinen Computer; Regel 2: Schalte ihn nicht ein; Regel 3: Benutze ihn nicht.[21] Dabei setzt Morris offenbar voraus, dass heutzutage alle Computer vernetzt sind. Auch wenn Entnetzung für den privaten Nutzer von sozialen Netzen eine empfehlenswerte Strategie zur Wiedergewinnung von Autonomie bis hin zum „Digital Detox“ sein mag,[22] realistisch ist die Forderung nach einem Verzicht auf das Internet heute weder für Organisationen noch für Einzelpersonen.

Der wachsenden Bedrohung der Cybersicherheit begegnen die Gesetzgeber seit einiger Zeit mit speziellen Normen zur Gewährleistung eines Mindestschutzes vor entsprechenden Angriffen. Die Europäische Union hat mit der RL (EU) 2016/1148[23] und der VO (EU) 2019/881[24] Regeln für einen Europäischen Zertifizierungsrahmen für die Cybersicherheit erlassen, die eine Überarbeitung des deutschen IT-Sicherheitsgesetzes nötig machen. Im Vordergrund dieser Bemühungen steht allerdings der Schutz von kritischen Infrastrukturen, nicht aber jede Form der Verarbeitung von personenbezogenen Daten, auch soweit sie sensitiver Natur sind.[25] Die Zertifizierung von Cybersicherheit spielt eine wichtige Rolle bei der Zulassung der Beteiligung ausländischer Hersteller wie z.B. Huawei beim Bau und Betrieb öffentlicher kritischer Infrastrukturen wie z.B. dem 5G-Netz, die gegenwärtig politisch kontrovers diskutiert wird. Ob dieser Versuch, Kontrollverlusten in zentralen Bereichen der

---

[21] Zit. nach *Ferguson*, The Square and the Tower – Networks, Hierarchies and the Struggle for Global Power, New York 2018, 410.

[22] *Staeheli*, Digitale Befreiung? Von wegen!, https://www.faz.net/aktuell/wirtschaft/digitec/von-wegen-digitale-befreiung-die-kunst-der-entnetzung-16174867.html?premium (zuletzt abgerufen am 14.5.2020).

[23] Richtlinie (EU) Nr. 2016/1148 des Europäischen Parlaments und des Rates v. 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Schutzniveaus von Netz- und Informationssystemen in der Union, ABl. EU L 194/1.

[24] Verordnung (EU) Nr. 2019/881 des Europäischen Parlaments und des Rates v. 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. EU L 151/15.

[25] Das Unionsrecht eröffnet zwar die Möglichkeit, Krankenhäuser als schutzbedürftige kritische Infrastrukturen einzustufen (vgl. Anhang II zum Rechtsakt zur Cybersicherheit), der deutsche Gesetzgeber hat dies aber bisher nicht getan.

Infrastruktur vorzubeugen, erfolgreich sein kann, soll hier nicht näher analysiert werden.[26]

Allerdings ist die Zertifizierung von Produkten und Verfahren generell ein Mittel zur verfassungsverträglichen Technikgestaltung, das auch in die Europäische Datenschutz-Grundverordnung aufgenommen wurde[27] und deshalb künftig eine wichtige Rolle bei der unionsweiten Umsetzung von Datenschutzstandards spielen dürfte. Ein weiteres Mittel zur Eindämmung von Sicherheitsverletzungen, die *security breach notification*, haben die Gesetzgeber in Europa aus den USA übernommen.[28] Die Pflicht zur Meldung und Veröffentlichung von Datenpannen hat sowohl in den USA als auch in Europa erhebliche praktische Bedeutung. Ob ihre erzieherische Wirkung auf die Verantwortlichen allerdings – wie erhofft – tatsächlich auch zu höheren Investitionen in die IT-Sicherheit führt, bedarf noch der Untersuchung. Denkbar wäre zumindest auf längere Sicht auch, dass sich durch die häufigen Meldungen über Datenpannen ein gewisser Gewöhnungseffekt (*data breach fatigue*) jedenfalls in der Öffentlichkeit einstellt.[29] Dem könnte in Europa die Sanktionsbewehrung dieser Pflicht in der Grundverordnung entgegenstehen. Sie hat dazu geführt, dass die Aufsichtsbehörden zumindest in Deutschland seit Mai 2018 eine Vielzahl von Meldungen über Datenpannen erhalten haben, die teilweise nur aus Unkenntnis oder vorsorglich abgegeben wurden. Die deutschen Aufsichtsbehörden haben deshalb eine Beschränkung der Meldepflicht auf solche Datenpannen vorgeschlagen, die voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der Betroffenen führen oder geführt haben.[30] Dies würde zu einer Angleichung der Voraussetzungen für die Meldepflicht gegenüber den Aufsichtsbehörden und den Betroffenen führen.

Eine Bedrohung der Sicherheit von informationstechnischen Systemen kann aber auch vom Gesetzgeber selbst ausgehen, der auf Drängen der Sicherheitsbehörden diesen die heimliche Infiltration solcher Systeme mithilfe des sog. Staatstrojaners zur Bekämpfung bestimmter Kriminalitätsformen gestattet. Damit legitimiert der Staat die gezielte Durchbrechung von Kontrollmechanismen auf den Endgeräten verdächtiger Personen. Das Bundesverfassungsgericht hat als Reaktion auf derartige sicherheitskritische Regelungen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. Computer-Grundrecht) entwickelt,[31] dessen Reichweite vom einfachen Gesetzgeber allerdings bisher nicht präzisiert wurde. Stattdessen hat der Gesetzgeber im neuen BKA-

---

[26] Dazu näher *Bendiek/Schallbruch*, Europas dritter Weg im Cyberraum, SWP-Aktuell Nr. 60, November 2019.

[27] Art. 42, 43 DSGVO.

[28] Art. 33, 34 DSGVO.

[29] *Zorabedian*, Data Breach Fatigue Makes Every Day Feel like Groundhog Day, https://securityintelligence.com/data-breach-fatigue-makes-every-day-feel-like-groundhog-day/ (zuletzt abgerufen am 14.5.2020).

[30] Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO, November 2019, 11 f.

[31] BVerfGE 120, 274.

Gesetz[32] Vorschriften zum Einsatz solcher Infiltrationstechniken aufgenommen, bei denen man den Eindruck gewinnen muss, er habe die Grenzen des verfassungsrechtlich gerade noch Hinnehmbaren austesten wollen. Das Bundesverfassungsgericht wurde bereits wieder angerufen und wird über die Verfassungskonformität auch dieses Gesetzes zu befinden haben.

Einen erheblich weiter reichenden Kontrollverlust würde es bewirken, wenn der Staat die Hersteller von Hard- und Software verpflichten würde, in ihre Produkte generell Hintertüren einzubauen, die eine jederzeitige heimliche Überwachung durch Sicherheitsbehörden ermöglichen würde. Denn eine derartige Regelung würde die technisch vermittelte Kommunikation prinzipiell unsicher machen. Ob derartige Hintertüren von Strafverfolgern oder Geheimdiensten im Interesse des Gemeinwohls oder von kriminellen Angreifern ausgenutzt werden, ließe sich nicht zuverlässig unterscheiden. Dasselbe gilt für die Pflicht zur Hinterlegung oder Herausgabe von Generalschlüsseln, wie sie immer wieder in der Debatte über verschlüsselte Kommunikation ins Spiel gebracht wird. Noch in ihrer Digitalen Agenda 2014-2017 hatte die Bundesregierung den Anspruch erhoben, Deutschland zum „Verschlüsselungs-Standort Nr. 1“ machen zu wollen.[33] Dieser Anspruch wird konterkariert durch die Forderung nach unbeschränkter Überwachbarkeit der privaten Kommunikation, wie sie Sicherheitsbehörden permanent erheben.

Die Kontrollierbarkeit der Datenverarbeitung ist allerdings kein rein technisches Problem und lässt sich dementsprechend auch nicht rein technisch – gewissermaßen auf Knopfdruck - lösen. Technikgestaltung kann einen wesentlichen Beitrag zur Kontrollierbarkeit der Datenverarbeitung leisten (s. dazu 4.). Datenschutz beschränkt sich aber nicht auf die Sicherung von einmal erhobenen Datenbeständen. Kontrollverluste drohen vielmehr auch durch wirtschaftliche und organisatorische Entscheidungen, vor allem aber durch eine überhandnehmende Datensammlung durch staatliche Stellen und Unternehmen.

II. Privatisierung und Monokultur der Technikanbieter

Edward Snowden hat die Bedeutung privater Unternehmen als Auftragnehmer der US-Geheimdienste beschrieben. Er nennt den *Homo contractus* die „wichtigste Spezies im US-Staatsdienst 2.0“.[34] Private Unternehmen können IT-Spezialisten höhere Gehälter zahlen als die staatliche Verwaltung. Die Knappheit der öffentlichen Kassen führt auch zu einem *brain drain,* einer ständigen Ausdünnung des Datenverarbeitungs-Sachverstandes im unmittelbaren Staatsdienst. Hinzu kam bei den US-Geheimdiensten zumindest in der Vergangenheit, dass nicht nur einzelne Privatfirmen in ihrem Auftrag handelten, sondern eine ganze Kette von Unterauftragnehmern. Selbst strikte Sicherheitsüberprüfungen aller bei diesen Privatfirmen Beschäftigten (soweit sie mit vertraulichen Informationen in Kontakt kamen) und auch von Edward Snowden selbst konnten nicht verhindern, dass dieser streng geheime Informationen

---

[32] § 49 BKAG.

[33] Vgl. auch die von der Bundesregierung 2016 veröffentlichte Charta zur Stärkung der vertrauenswürdigen Kommunikation, https://www.krypto-charta.de/charta.html (zuletzt abgerufen am 14.5.2020).

[34] *Snowden*, Permanent Record, Frankfurt a.M. 2019, 144.

an Journalisten weitergab. Das führt zwar zu einer begrüßenswerten und notwendigen öffentlichen Debatte über die Überwachungspraxis der Geheimdienste weltweit, allerdings lag darin zugleich ein Kontrollverlust, der von anderen Beschäftigten dieser Unternehmen z.B. aus Profitgier hätten genutzt werden können. Whistleblower, die wie Snowden aus ethischen Motiven heraus handeln und Sicherheitsmechanismen umgehen, kann es auch im unmittelbaren Staatsdienst geben. Die besonderen Umstände des Outsourcings von Datenverarbeitung an Ketten von privaten Auftragnehmern haben aber möglicherweise den Kontrollverlust im Fall von Snowden zusätzlich begünstigt.

Auch wenn es in Europa möglicherweise keine vergleichbar weitreichende Praxis der Beauftragung privater Firmen durch Behörden und insbesondere durch Geheimdienste gibt, ist doch das Grundproblem auch hier anzutreffen. Der Staat kann es sich vielfach nicht leisten, gut bezahlte IT-Experten zu beschäftigen oder eigene Soft- und Hardware zu entwickeln, sondern muss den entsprechenden Sachverstand und die nötigen Produkte von Privaten kaufen, um seine Aufgaben zu erfüllen. Dabei trifft er gegenwärtig auf marktbeherrschende Unternehmen meist aus dem Silicon Valley, deren Produkte und Dienstleistungen er in Anspruch nehmen muss, um handlungsfähig zu bleiben. Das Beispiel von Windows 10 zeigt, wie groß die Marktmacht eines Software-Herstellers wie Microsoft mittlerweile ist und welcher koordinierter Anstrengungen es bei den Kunden (den Mitgliedstaaten und der Europäischen Union) bedarf, um festgestellte Kontrolldefizite zu beheben. Die entstandene Monokultur etwa bei den Betriebssystemen macht es schwierig, die von den Herstellern „angebotenen“ Bedingungen abzulehnen oder auch nur zu modifizieren. Solange in Europa weder die Regierungen noch die Unternehmen Produkte anbieten können, die mit der außereuropäischen Technologie konkurrieren können, bleiben sie von dieser abhängig.

Ob die Zentralisierung der Datenverarbeitung den Kontrollverlust begünstigt oder eher die Kontrolle von Datenbanken erleichtert, lässt sich nicht eindeutig beantworten. Eine dezentrale Datenhaltung erfordert auch dezentrale Kontrollverfahren, wie sie in einer föderalen Struktur wie in Deutschland verfassungsrechtlich vorgegeben sein können. Das führt auch zu einem erhöhten Kontrollaufwand und entsprechenden Abstimmungsnotwendigkeiten. Die dezentrale Struktur des Internets ist andererseits gerade im Hinblick auf eine erhöhte Ausfallsicherheit entwickelt worden. Wenn Datenbestände an verschiedenen Orten gespiegelt und gesichert werden, können sie auch besser vor Verlust geschützt werden. Zentrale Datenbanken sind andererseits – wie das Beispiel der weltgrößten Biometrie-Datenbank Aadhaar zeigt – bevorzugtes Angriffsziel; erfolgreiche Angriffe oder Datenlecks haben bei ihnen regelmäßig größere Schadensfolgen, weil Sicherungsvorkehrungen nur einmal überwunden werden müssen.eng

III. Grenzüberschreitende Datenverarbeitung und entgrenzte Datensammlung

Die zunehmende weltweite Vernetzung hat verstärkte grenzüberschreitende Datenflüsse ausgelöst, die bereits im August 1989 die Internationale Konferenz der Datenschutzbeauftragten zur Forderung nach einer effektiven Datenexportkontrolle veranlasste. Danach sollte jeder Datenexporteur prüfen, ob der Datenschutz beim Empfänger im Ausland, insbesondere die Einhaltung der Betroffenenrechte,

gewährleistet ist.[35] Die Grundidee, dass nationale Datenschutzstandards nicht durch die Verlagerung der Datenverarbeitung ins Ausland umgangen werden dürfen, was letztlich nur durch internationale Standards erreichbar ist, hatte bereits in der Konvention No. 108 des Europarats von 1981 Niederschlag gefunden.[36] Diese Organisation war es auch, die 1992 erstmals einen Mustervertrag mit Regeln zum Datenexport veröffentlichte. Mit der Europäischen Datenschutzrichtlinie von 1995 wurde ein Regelwerk installiert, das neben Standardvertragsklauseln auch andere Instrumente zur Sicherstellung eines adäquaten Datenschutzniveaus auch in außereuropäischen Ländern enthielt.[37] Dieses Regelwerk ist in weiterentwickelter Form in die Datenschutz-Grundverordnung übernommen worden und hat dazu beigetragen, dass in einer Vielzahl von Ländern Datenschutz-Gesetze verabschiedet wurden, die sich am europäischen Modell orientieren.

Dazu zählt auch der Anfang 2020 in Kraft getretene kalifornische Consumer Privacy Act (CCPA), der zu mehreren gesetzgeberischen Initiativen in anderen US-Bundesstaaten und zu Diskussionen über ein bisher fehlendes Bundesgesetz für den privaten Sektor im Kongress geführt hat. Dabei plädieren mittlerweile selbst Chefs von Silicon-Valley-Unternehmen nicht zuletzt aufgrund der wachsenden Kritik an ihrem Umgang mit Kundendaten für eine Bundesgesetzgebung nach europäischem Muster. Die Entscheidung der Europäischen Kommission vom Januar 2019, den Datenschutz in Japan als angemessen anzuerkennen, und ein entsprechendes Freihandelsabkommen haben zur Bildung des „weltweit größten Raums für sicheren Datenverkehr“ geführt.[38] Die Kontrolle des Exports personenbezogener Daten ist nicht nur eine Notwendigkeit zur Sicherstellung von Grundrechtsstandards, sondern auch wesentliche Voraussetzung für eine florierende vernetzte Weltwirtschaft. Der verstorbene Europäischen Datenschutzbeauftragten Giovanni Buttarelli hat daher die Grundverordnung mit Recht als einen „Fanfarenstoß“ für einen neuen globalen Goldstandard für das digitale Zeitalter bezeichnet.[39] Trans- und internationale Datenschutzstandards bedürfen der koordinierten Durchsetzung durch nationale Datenschutzbehörden, deren unabhängiger Status in Art. 8 Abs. 3 der Europäischen Grundrechte-Charta festgeschrieben ist (dazu näher unter 5.).

Die Datenschutz-Grundverordnung ist zum einen eine Reaktion auf die unzureichende Harmonisierung des Datenschutzrechts in der Europäischen Union seit 1995, die die Kommission dazu bewogen hat, zum Mittel der unmittelbar geltenden Verordnung zu greifen. Zum anderen soll sie aber auch eine effektivere Kontrolle der immer umfassenderen Verarbeitung und kommerziellen Nutzung personenbezogener Daten durch große Unternehmen gerade im Internet ermöglichen. Diese Unternehmen sind

---

[35] *Berliner Beauftragter für Datenschutz und Informationsfreiheit*, Internationale Dokumente zum Datenschutz bei Telekommunikation und Medien 1983-2013, 28 ff.

[36] Art. 12 der Konvention zum Schutz des Menschen bei der automatischen Verarbeitung von Daten (No. 108).

[37] Art. 25 f. der RL 95/46/EG.

[38] Presserklärung von Kommissarin Jourova v. 23.1.2019, https://ec.europa.eu/commission/presscorner/detail/de/IP_19_421 (zuletzt abgerufen am 14.5.2020).

[39] ***Buttarelli*, The EU GDPR as a clarion call for a new global digital gold standard, International Data Privacy Law 2016, 77 f.**

fast durchgängig in den Vereinigten Staaten ansässig und vertraten vor 2018 lange Zeit die Auffassung, sie seien nicht an europäisches Datenschutzrecht gebunden. Dem hat der Unionsgesetzgeber mit der Einführung des Marktortprinzips ein Ende bereitet, so dass außereuropäische Unternehmen (z.B. auch aus China) zumindest dann europäisches Recht befolgen müssen, wenn sie Waren oder Dienstleistungen Personen (gleich welcher Staatsangehörigkeit) in Europa anbieten oder deren Verhalten beobachten.[40] Auch das Marktortprinzip ist deshalb eine Form der Kontrolle von grenzüberschreitender Datenverarbeitung, denn die gewonnenen Daten werden in aller Regel in die außereuropäischen Sitzländer exportiert.

Auch wenn die meisten personenbezogenen Daten im Zeitalter des Internets von privaten Unternehmen verarbeitet werden, deren datengetriebenes Geschäftsmodell auf der Beobachtung des Nutzerverhaltens beruht („Überwachungsdividende")[41], setzen auch staatliche Stellen insbesondere im Sicherheitsbereich verstärkt auf die Sammlung und Auswertung von Daten, um Bedrohungen durch besonders gemeinschaftsschädliche Formen der Kriminalität effektiver zu bekämpfen. Schon vor dem 11. September 2001 wurden die Befugnisse der Sicherheitsbehörden zur Datenerhebung in immer kürzeren Abständen zur Bekämpfung der organisierten Kriminalität ausgeweitet. Die Geschichte des immer länger werdenden Katalogs der Befugnisse zur heimlichen Telekommunikationsüberwachung nach § 100a StPO ist insoweit nur ein instruktives Beispiel unter mehreren. Keine dieser erweiterten Befugnisse wurden bezüglich ihrer Effektivität einer aussagekräftigen unabhängigen Evaluationskontrolle unterzogen,[42] wie dies angesichts der intensiver werdenden Eingriffe in das Recht auf informationelle Selbstbestimmung, die Unverletzlichkeit der Wohnung und das Telekommunikationsgeheimnis von Verfassungs wegen geboten wäre.[43] Die kontinuierliche Ausweitung von Befugnissen zur Datenerhebung und Beobachtung für staatliche Stellen waren nicht begleitet von einer verstärkten Kontrolle der damit verbundenen Grundrechtseingriffe.

Zudem liegt in der Erweiterung entsprechender Befugnisse selbst ein allmählicher Kontrollverzicht jedenfalls dann, wenn nicht nur wie bei § 100a StPO ein Katalog von Anlassstraftaten ständig verlängert wird, sondern die Voraussetzungen („Straftat von erheblicher Bedeutung") vom Gesetzgeber immer unschärfer formuliert werden. Auch ist zu beobachten, dass neue Befugnisse zur technikunterstützten Beobachtung von Personen, die zunächst z.B. nur zur Bekämpfung terroristischer Straftaten eingeführt wurden, alsbald auch in anderen Bereichen angewandt werden oder ihre Anwendung zumindest befürwortet wird. So wurde die vom Europäischen Gerichtshof[44] inzwischen für grundrechtswidrig erklärte Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten im unmittelbaren Zusammenhang mit

---

[40] Art. 3 Abs. 2 DSGVO.

[41] *Zuboff*, Das Zeitalter des Überwachungskapitalismus, Frankfurt a.M. 2018, 201 f. und passim.

[42] Vgl. dazu *Albers*, Die verfassungsrechtliche Bedeutung der Evaluierung neuer Gesetze zum Schutz der Inneren Sicherheit, in: Deutsches Institut für Menschenrechte (Hrsg.), Menschenrechte – Innere Sicherheit – Rechtsstaat, Dokumentation der Konferenz v. 27.6.2005, 21 ff.

[43] BVerfGE 109, 279, 339 f. (Akustische Wohnraumüberwachung).

[44] EuGH, Urt. v. 8.4.2014, Rs. C-293/12 u. C-594/12, ECLI:EU:C:2014:238 – Digital Rights Ireland.

Terroranschlägen zunächst nur zur Abwehr entsprechender Straftaten befürwortet, später aber ganz allgemein zur Bekämpfung einer Straftat von erheblicher Bedeutung i.S.d. § 100a StPO oder einer „mittels Telekommunikation“ begangenen Straftat (also z.B. einer Beleidigung am Telefon).[45] Entsprechendes gilt für die heimliche Infiltration oder Online-Durchsuchung von Computern, die gegenwärtig nur der Polizei gestattet ist,[46] nach dem Willen des Bundesinnenministers aber künftig auch den Geheimdiensten erlaubt werden soll. Generell ist datenschutzpolitisch eine Tendenz zur allmählichen Erosion der Zweckbindung *(function creep)* festzustellen. Zunächst für extreme Kriminalitätsformen und Ausnahmesituationen geschaffene Befugnisse werden zunehmend als Routineinstrument für die Arbeit der Sicherheitsbehörden ausgestaltet und genutzt.

Besonders deutlich wird die ausufernde und jedenfalls zeitweise außer Kontrolle geratene Datenerhebungspraxis im Geheimdienstbereich. Die von Edward Snowden bekannt gemachte Massenüberwachung durch die National Security Agency etwa mit den Programmen PRISM, UPSTREAM und dem Auswertungswerkzeug XKEYSCORE führt zu einer nahezu lückenlosen Überwachung der weltweiten Telekommunikation und Internet-Nutzung. Dabei werden zunächst alle Telekommunikationsdaten (zunächst bei der NSA selbst, später bei den US-Telekommunikationsanbietern) gespeichert und anschließend unter Einsatz von Schlüsselwörtern (Filtern) in Bezug auf bestimmte verdächtige Zielpersonen ausgewertet, um dann die Kommunikation auch inhaltlich zu überwachen. Die NSA sieht in der ungezielten Speicherung sämtlicher Telekommunikationsdaten keine rechtlich relevante Datenerhebung und hält sie deshalb für zulässig.[47] Generell bedarf nach US-amerikanischem Rechtsverständnis erst die gezielte Nutzung personenbezogener Daten und nicht schon die Speicherung des gesamten ungefilterten Datenstroms (Metadaten und Inhaltsdaten) einer Rechtfertigung. Hinsichtlich der rechtswidrigen Erhebung der Kommunikationsdaten von US-Amerikanern, die offenbar durch einen zeitweiligen Verlust der Kontrolle über das technische Überwachungssystem verursacht und durch das Versagen der richterlichen Kontrolle durch den Foreign Intelligence Surveillance Court begünstigt wurde, ist von einem „doppelten Zauberlehrlingseffekt“ gesprochen worden.[48] Die Einbeziehung ganzer Ketten von privaten Firmen als Auftragnehmer der Nachrichtendienste (s.o. 2.) multipliziert diesen Effekt noch. Gerade wenn man Geheimdienste auch in demokratischen Staaten für notwendig hält, muss dieser vielfache Kontrollverlust zutiefst beunruhigen.

Auch der Bundesnachrichtendienst überwacht die Telekommunikation ungezielt, wenngleich bei weitem nicht mit denselben Ressourcen wie die Geheimdienste der Five Eyes (USA, Großbritannien, Australien, Kanada und Neuseeland). Er tat dies

---

[45] § 100g StPO. Gegen die Vorschrift sind mehrere Verfassungsbeschwerden anhängig.

[46] § 49 BKAG. Auch gegen diese Bestimmung ist eine Verfassungsbeschwerde anhängig.

[47] Vgl. *Snowden* (Fn. 34), 228.

[48] *Dix*, Notwendigkeit und Chancen eines modernen europäischen Rechtsrahmens angesichts von „PRISM“ und „TEMPORA“, in Bub/Wolfenstetter (Hrsg.), Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing, Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT Sicherheit, Wiesbaden 2014, 9.

bereits in der Zeit der ausschließlich analogen Kommunikation durch die strategische Post- und Fernmeldekontrolle, die das Bundesverfassungsgericht als verfassungskonform angesehen hat.[49] Auch der BND hat allerdings die Software XKEYSCORE zur Kontrolle der digitalen Kommunikation eingesetzt. Ob dies datenschutzkonform geschah, konnten die Bundesbeauftragten für den Datenschutz nicht überprüfen, weil das Bundesinnenministerium hierzu Auskünfte verweigerte.[50] Auch ein entsprechender Prüfbericht im Zuge des NSA-Untersuchungsausschusses wurde als geheim eingestuft. Inwieweit diese Geheimhaltung gerechtfertigt war, konnte nicht verifiziert werden. Auch wenn etwa aus Gründen des Quellenschutzes bestimmte Informationen geheimhaltungsbedürftig sein können, führt die pauschale Ablehnung einer unabhängigen Prüfung zu einem inakzeptablen Kontrolldefizit. Das Bundesverfassungsgericht hat schon 1984 einen zentralen Zusammenhang zwischen geheimer Kommunikationsüberwachung und unabhängiger Kontrolle gesehen. Da heimliche Eingriffe in das Kommunikationsgeheimnis von den Betroffenen keiner gerichtlichen Kontrolle unterzogen werden können, ist ihre Verfassungskonformität von einer effektiven unabhängigen Kontrolle durch weisungsunabhängige staatliche Organe (G 10-Kommission und Datenschutzbeauftragte) abhängig.[51] In seinem wegweisenden Urteil vom 19.5.2020 hat das Bundesverfassungsgericht festgestellt, dass der Bundesnachrichtendienst bei der Überwachung der Auslandskommunikation bisher keiner unabhängigen Kontrolle unterliegt, die den Anforderungen des Grundgesetzes genügt.[52]

Die marktbeherrschenden Internet-Konzerne verfolgen ihrerseits überwachungsorientierte Geschäftsmodelle, indem sie systematisch die Daten von Nutzern als Gegenleistung für erbrachte Dienste sammeln und zur Profilbildung nutzen. Daneben agieren große Datenhändler, die direkt vom Verkauf personenbezogener Daten profitieren. Die so entstandenen Datenbestände sind ungleich größer und aussagekräftiger als alle Datensammlungen unter direkter staatlicher Kontrolle. Indem die Geheimdienste – wie die Snowden-Enthüllungen verdeutlicht haben – sowohl legal (front-door access) als auch illegal (backdoor access)[53] Zugang zu den Datenbeständen der Privatunternehmen haben, verliert die Unterscheidung zwischen staatlicher und privater Überwachung an Bedeutung und es entsteht ein nachrichtendienstlich-industrieller Komplex,[54] der an die Stelle des militärisch-industriellen Komplexes getreten ist, vor dem Präsident Eisenhower in

---

[49] BVerfGE 67, 157.

[50] Die Bundesbeauftragte Andrea Voßhoff hat dies 2014 beanstandet und die Kontrolle im Bereich der Nachrichtendienste insgesamt als unzureichend bezeichnet, BfDI, 25. Tätigkeitsbericht, 35 ff. Auch in ihrem 27. Tätigkeitsbericht (2017-2018, S. 68 f.) kritisierte sie weiterhin bestehende kontrollfreie Räume in diesem Bereich.

[51] Vgl. bereits BVerfGE 30, 1, 4. Leitsatz. Im Urt. v. 24.4.2013 (BVerfGE 133, 277 (Rn. 207, 214 ff.)) hat das Gericht diesen Gedanken auf Verbunddateien wie die Antiterrordatei erstreckt.

[52] BVerfG 1 BvR 2835/17, Rn. 324., ZD 2020, 409 m. Anm. *Petri*.

[53] Diese Unterscheidung stammt von *Rubinstein/Van Hoboken*, zit., nach *Hijmans,* The European Union as Guardian of Internet Privacy, Cham 2016, 106.

[54] So der frühere Präsident der Bundesakademie für Sicherheitspolitik, Hans-Dieter Heumann, zit. nach Der Tagesspiegel v. 19.1.2014.

seiner Abschiedsrede im Januar 1961 warnte. Es ist nicht die Frage, wann wir in einer Überwachungsgesellschaft leben, sondern ob und wie wir die mit der gegenwärtigen Informationsgesellschaft zwangsläufig verbundene Überwachung[55] kontrollieren können. Zudem schadet die nach den Snowden-Enthüllungen nur unwesentlich modifizierte Überwachungspraxis der Geheimdienste dem internationalen und insbesondere transatlantischen Datenverkehr, denn der Europäische Gerichtshof hat sowohl den im „Safe Harbor" als auch im „Privacy Shield" festgelegten Datenschutz in den USA als dem wichtigsten Handelspartner Europas die Angemessenheit abgesprochen.[56] Der Gerichtshof wird sich darüber hinaus in drei weiteren Vorabentscheidungsverfahren[57] mit der Frage zu befassen haben, ob eine Vorratsdatenspeicherung für Zwecke der Strafverfolgung oder der nationalen Sicherheit mit Unionsrecht vereinbar ist. Der Europäische Gerichtshof ist schon jetzt neben dem Europäischen Gerichtshof für Menschenrechte und den nationalen Verfassungsgerichten eine der Schlüsselinstanzen für die Kontrolle der grundrechtskonformen Datenverarbeitung in Europa.[58]

IV. Transparenz und Kontrolle durch Technikgestaltung

Transparenz ist eine notwendige, wenngleich keine hinreichende Bedingung für die effektive Kontrolle jeder Datenverarbeitung. Deshalb ist es zu begrüßen, dass der europäische Gesetzgeber in der Datenschutz-Grundverordnung die Pflichten zur proaktiven Information des Betroffenen erheblich ausgeweitet[59] und auch seine Rechte zur Steuerung der Datenverarbeitung (Rechte auf Korrektur[60], Löschung[61], Einschränkung der Verarbeitung[62] und Widerspruch[63]) präzisiert und um neue Elemente (Recht auf Datenübertragbarkeit[64], sog. Recht auf Vergessenwerden[65])

---

[55] So der für den britischen Information Commissioner 2006 erstellte Bericht des Surveillance Studies Network, A Report on the Surveillance Society, https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf (zuletzt abgerufen am 14.5.2020). Vgl. auch *Hijmans* (Fn. 53), 102.

[56] EuGH, Urt. v. 6.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems I; Urt. v. 16.7.2020, Rs. C-311/16, ECLI:EU:C:2020:559 – Schrems II.

[57] Rechtssachen C-623/17 – Privacy International; C-511/18 – La Quadrature du Net; C-520/18 – Ordre des barreaux francophone et germanophone et al.; vgl. dazu die Schlussanträge des Generalanwalts Sanchez-Bordona v. 15.1.2020, ECLI:EU:C:2020:6.

[58] *Docksey /Hijmans*, The Court of Justice as a Key Player in Privacy and Data Protection, EDPL 2019, 300, 311 ff.

[59] Art. 12-14 DSGVO.

[60] Art. 16 DSGVO.

[61] Art. 17 Abs. 1 DSGVO.

[62] Art. 18 DSGVO.

[63] Art. 21 DSGVO.

[64] Art. 20 DSGVO.

[65] Art. 17 Abs. 2 DSGVO; siehe dazu den Beitrag von *Hornung* in diesem Band, S. 371 ff.

ergänzt hat. Alle diese Rechte stärken die Möglichkeiten der von der Datenverarbeitung betroffenen Person, diese im Anwendungsbereich des Unionsrechts (also nicht gegenüber Nachrichtendiensten) zu kontrollieren. Allerdings bedürfen diese Rechte teilweise noch der Weiterentwicklung und Ergänzung, um tatsächlich die Kontrollmöglichkeiten des Einzelnen zu verbessern. So ist etwa das neue Recht auf Datenübertragbarkeit zu eng gefasst und ihm fehlt die Verpflichtung zur Bereitstellung der Daten in einem interoperablen Format. Diese und andere Änderungen sollten nach den detaillierten Vorschlägen von Roßnagel und Geminn[66] bei der anstehenden ersten Evaluation der Grundverordnung aufgegriffen werden. Auch die Transparenz von Algorithmen muss vor dem Hintergrund der eingangs erwähnten Frage Hararis rechtlich und ethisch präzisiert werden. Ob die Datenschutz-Grundverordnung den Einsatz von Verfahren der automatisierten Entscheidungsfindung verbietet, die nicht aussagekräftig erklärbar sind, wird kontrovers diskutiert.[67] Die Datenethikkommission der Bundesregierung empfiehlt jedenfalls in bestimmten Bereichen eine Pflicht zur Erklärung von algorithmischen Entscheidungen, die über die von der Grundverordnung verlangte Information über die involvierte Logik und Tragweite hinausgeht und sich auch nicht auf unmittelbar Betroffene beschränkt.[68]

Die Europäische Datenschutz-Grundverordnung hat mit der Pflicht zur Verwendung von datenschutzgerechten Produkten und Verfahren, die den Prinzipien des *privacy by design and by default* entsprechen,[69] einen wichtigen Schritt zur unionsweiten Kontrolle der Datenverarbeitung durch Technikgestaltung getan. Allerdings sind Adressaten dieser Pflicht ausschließlich die Verantwortlichen, nicht die Hersteller oder gar Entwickler der Technik. Die „Designer" sind bisher gerade nicht durch die *privacy by design*-Vorschrift der Grundverordnung in die Pflicht genommen. Darin liegt eine wesentliche Schwäche des europäischen Rechtsrahmens, auch wenn die Pflicht zur Verwendung von datenschutzfreundlicher Technik indirekt zur einer stärkeren Nachfrage nach entsprechender Technik führen dürfte. Denn keine Aufsichtsbehörde wird ein Bußgeld gegen einen Datenverarbeiter verhängen können, der die Pflicht zum Einsatz datenschutzgerechter Produkte unverschuldet verletzt, weil es solche Produkte auf dem Markt noch nicht gibt. Rechtlich möglich wäre es allenfalls, dass die Aufsichtsbehörden eine entsprechende Datenverarbeitung untersagt. Dass eine solche Maßnahme ergriffen wird oder vor Gericht Bestand hat, ist aber umso unwahrscheinlicher, je wichtiger die entsprechende Datenverarbeitung (z.B. im Sicherheits- oder Gesundheitsbereich) ist. Deshalb ist die Forderung nach einer Einbeziehung der Hersteller in den Adressatenkreis der Grundverordnung und die Schaffung einer entsprechende Produkthaftpflicht nachvollziehbar und konsequent.[70]

---

[66] *Roßnagel/Geminn*, Evaluation der DS-GVO aus Verbrauchersicht, Kassel 2019, 66 ff.

[67] Vgl. *Dix,* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Baden-Baden 2019, Art. 12 DSGVO, Rn. 12, Art. 13 DSGVO, Rn. 16, Art. 15 DSGVO, Rn. 25.

[68] *Datenethikkommission*, Gutachten (2019), S. 187.

[69] Art. 25 DSGVO.

[70] *Roßnagel/Geminn*, (Fn. 66), 77 f.; Erfahrungsbericht der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, 2019, 15 ff.

Schon jetzt werben die großen Plattformbetreiber wie Google und Facebook damit, dass sie durch neue Wahlmöglichkeiten den Nutzenden ihrer Dienste „die Kontrolle“ geben. Das mag man als Reaktion auf den neuen europäischen Rechtsrahmen verstehen, auch wenn derartige Slogans vermutlich eher auf Marketing-Überlegungen beruhen und die Angebote bezüglich ihrer Rechtskonformität erst noch beurteilt werden müssen. Das war lange nicht möglich, weil die großen Internet-Konzerne sowohl den betroffenen Nutzenden als auch den Aufsichtsbehörden die schon vor dem Inkrafttreten der Grundverordnung gebotene Transparenz verweigert haben. Einige Internet-Konzerne scheinen zu realisieren, dass sich mit informationeller Fremdbestimmung ihrer Nutzer auf Dauer nicht genug Geld verdienen lässt.

Ein weiterer hier zu berücksichtigender Aspekt ist die Frage, unter wessen Kontrolle die personenbezogenen Daten eines Nutzers überhaupt verarbeitet werden. Sowohl Hard- als auch Software sind bisher meist so gestaltet, dass sie der Nutzende in der Regel weder kognitiv noch physisch beherrscht. Die meisten Fitnesstracker erlauben keine ausschließlich lokale Speicherung der teilweise sensitiven (weil gesundheitsbezogenen) Fitnessdaten, sondern zwingen den Nutzenden entsprechender Geräte oder Apps, die Daten zur Auswertung oder zum Vergleich mit anderen Personen an den Hersteller der Hardware oder den Anbieter der dazugehörenden Apps zu übermitteln. Der Nutzende muss auf Kontrolle verzichten oder ihm wird eine Kontrollmöglichkeit suggeriert, die in Wirklichkeit nur sehr eingeschränkt besteht. Datenverarbeitung ist aber nur dann datenschutzkonform, wenn der Nutzende sie selbst kontrollieren kann und nicht darauf vertrauen muss, dass ein Hersteller oder Diensteanbieter seine Daten sicher und nicht zweckfremd verarbeiten wird. Wenn das nicht auf dem Endgerät des Nutzenden möglich ist, dann sollte dieser z.B. die Möglichkeit haben, die Daten in verschlüsselter Form in eine Cloud hochzuladen, wo sie nur mit seiner Zustimmung entschlüsselt werden können. Die Möglichkeit einer Verarbeitung unter der primären Kontrolle des Betroffenen sollte ein Zertifizierungskriterium für datenschutzgerechte Technikgestaltung nach der Grundverordnung[71] werden.

V. Kontrollstrukturen und -ressourcen

Der beste Rechtsrahmen und die im europäischen Primärrecht und den nationalen Verfassungen festgeschriebenen Grundrechtsgarantien verlieren an Wirkmacht, wenn ihre Beachtung nicht effektiv kontrolliert wird. Deshalb garantiert die Europäische Grundrechte-Charta in Art. 8 neben dem Menschenrecht auf Datenschutz auch die unabhängige Datenschutzkontrolle.

Die Effektivität dieser Kontrolle muss sowohl innerstaatlich im föderalen Gefüge wie auch auf Unionsebene gewährleistet werden. In beiden Fällen ist mit guten Gründen auf eine zentrale Kontrollinstanz verzichtet worden. Umso mehr müssen kontrollfreie Räume und negative Kompetenzkonflikte durch Kooperation soweit wie möglich ausgeschlossen werden. Das Bundesverfassungsgericht hat die Notwendigkeit einer effektiven Datenschutzkontrolle im Bundesstaat bei polizeilichen Verbunddateien betont und den Datenschutzaufsichtsbehörden sogar eine bestimmte Prüffrequenz aufgegeben.[72]

---

[71] Art. 42 DSGVO.

[72] BVerfGE 133, 277 (Rn. 207, 214 ff.).

Auf europäischer Ebene hat der Gesetzgeber präzisere Vorgaben für die Kooperation der nationalen Datenschutzbehörden gemacht[73] und mit dem Europäischen Datenschutzausschuss ein Gremium mit eigener Rechtspersönlichkeit geschaffen, das die zentrale Aufgabe hat, die Grundverordnung durch Leitlinien und bewährte Verfahren zu konkretisieren und für eine einheitliche Rechtsanwendung in der Praxis zu sorgen.[74] Ob sich dieser organisatorische Rahmen bewährt, muss sich noch zeigen. Der Europäische Datenschutzausschuss hat zwar bereits zahlreiche Leitlinien veröffentlicht, jedoch noch keinen Gebrauch von seiner Befugnis gemacht, im Kohärenzverfahren[75] verbindliche Entscheidungen in Streitfällen etwa bei negativen Kompetenzkonflikten zu fällen. Immerhin können auf diese Weise kontrollfreie Räume vermieden werden. Der Bundesgesetzgeber hat entsprechende Regelungen im Bundesdatenschutzgesetz für den innerstaatlichen Bereich getroffen.[76] Auch die Einführung einer Untätigkeitsklage, die Betroffene nach der Grundverordnung gegen Aufsichtsbehörden erheben können, erhöht die Kontrolldichte in Fällen, in denen Aufsichtsbehörden Beschwerden – aus welchen Gründen auch immer – nicht nachgehen oder die Betroffenen nicht informieren.[77] Ebenso bedeutet die neu geschaffene Möglichkeit der Verbandsbeschwerde oder -klage[78] eine Verbesserung der Kontrolloptionen für Verbraucher, aber auch Beschäftigte, die Gewerkschaften mit der Wahrnehmung ihrer Rechte beauftragen können. Von der Einführung einer Popularklage hat der europäische Gesetzgeber allerdings abgesehen.

Schließlich sind die rechtlichen Anordnungs- und Kontrollressourcen der Aufsichtsbehörden durch den erweiterten Sanktionskatalog[79] der Grundverordnung erheblich gestärkt worden, was bereits vor deren Inkrafttreten im Mai 2018 dem Datenschutz einen deutlich höheren Stellenwert in der Prioritätenliste vieler Unternehmen verschaffte, auch wenn viele datenschutzrechtliche Pflichten nicht erst durch die Grundverordnung begründet wurden. Eine Anweisungsbefugnis der Aufsichtsbehörde, wie sie die Grundverordnung jetzt mit unmittelbarer Wirkung vorsieht,[80] gab es dagegen vor dem Inkrafttreten der Grundverordnung in Deutschland für den öffentlichen Bereich nicht.

Die rechtlichen Kontrollressourcen sind allerdings ungleich verteilt, je nachdem ob Behörden oder Unternehmen die Datenverarbeitung verantworten. Das ist deshalb nicht gerechtfertigt, weil es für die Betroffenen keinen Unterschied macht, ob öffentliche oder private Stellen in ihre Grundrechte eingreifen. Ein Unterschied besteht nur darin, dass private Datenverarbeiter sich ihrerseits auf Grundrechte berufen

---

[73] Art. 60 ff. DSGVO.

[74] Art. 68 ff. DSGVO.

[75] Art. 63 ff. DSGVO.

[76] §§ 18, 19 BDSG.

[77] Art. 78 Abs. 2 DSGVO.

[78] Art. 80 DSGVO.

[79] Art. 83, 84 DSGVO.

[80] Art. 58 Abs. 2 lit. d DSGVO.

können. Der Unionsgesetzgeber hat es den Mitgliedstaaten – vor allem auf Druck der Bundesregierung – jedoch ermöglicht, die Verhängung von Bußgeldern gegenüber Behörden auszuschließen.[81] Das tut das Bundesdatenschutzgesetz ausdrücklich[82] und geht noch einen Schritt weiter: es schließt sogar die Anweisungsbefugnis der Aufsichtsbehörden gegenüber den Polizei- und Strafverfolgungsbehörden aus und belässt es bei den bisherigen Befugnissen zur bloßen Beanstandung datenschutzwidrigen Verhaltens.[83] Das gilt entsprechend auf Landesebene und hat bereits dazu geführt, dass die Landesdatenschutzbeauftragten in Berlin und Brandenburg keine wirksame Handhabe gegen die rechtswidrige Speicherpraxis der Polizeibehörden in diesen Ländern hatten.[84] Das ist mit den Vorgaben des Unionsrechts[85] nicht zu vereinbaren, das „wirksame Abhilfebefugnisse“ für die Aufsichtsbehörden fordert.[86]

Auch die notwendigen materiellen Kontroll-Ressourcen, mit denen die Aufsichtsbehörden zur Sicherung ihrer Unabhängigkeit nach der Grundverordnung in angemessenem Umfang ausgestattet werden müssen,[87] sind ungleich verteilt. Das gilt sowohl auf europäischer Ebene als auch in Deutschland, wo trotz eines deutlichen Stellenaufwuchses auf Bundesebene und in einzelnen Ländern gerade die Aufsichtsbehörden in kleineren oder finanzschwächeren Bundesländern nach wie vor unzureichend ausgestattet sind. Das beeinflusst naturgemäß auch die Kontrollpraxis mit der Folge, dass vielfach nur noch anlassbezogen geprüft werden kann, wie es z.B. in Bremen der Fall ist. Es bleibt abzuwarten, wann die Kommission erstmals Vertragsverletzungsverfahren gegen einen Mitgliedstaat einleitet, der seiner Verpflichtung zur Bereitstellung der notwendigen materiellen Ressourcen nicht nachkommt.

VI. Fazit

Ob die Datenverarbeitung außer Kontrolle gerät, lässt sich noch nicht absehen. Festzustellen ist aber, dass die Zahl der Datenlecks ebenso zunimmt wie die der Kontrolldefizite und kontrollfreien Räume. Zugleich führt das staatliche und privat-kommerzielle Überwachungsinteresse zu einer immer stärker ausufernden Verarbeitung von Personendaten. Wenn teilweise von einem durch die Digitalisierung und das Internet ausgelösten „Daten-Tsunami“ gesprochen wird, könnte dies den Eindruck erwecken, die digitalisierte Datenverarbeitung sei ein Naturereignis, dem der

---

[81] Art. 83 Abs. 7 DSGVO.

[82] § 43 Abs. 3 BDSG.

[83] § 16 Abs. 2 BDSG.

[84] Der Tagesspiegel v. 29.12.2019, 15 („Unkontrollierte Sammelwut“); Der Tagesspiegel v. 8.1.2020, 10 („Märkische Datenautobahn“).

[85] Art. 47 Abs. 2 RL (EU) 2016/680.

[86] Krit. auch *Wieczorek*, in: Kühling/Buchner, DSGVO – BDSG, 2. Aufl., München 2018, § 16 BDSG, Rn. 29.

[87] Art. 52 Abs. 4 DSGVO.

Mensch und die Gesellschaft ohnmächtig gegenüberstehen. Die Datenverarbeitung ist aber vom Menschen gemacht und von ihm verfassungsverträglich zu gestalten. Das ist nicht nur die Beschreibung einer Möglichkeit, sondern ein rechtliches und ethisches Gebot.

Kontrollfreie Räume lassen sich ebensowenig völlig ausschließen wie Sicherheitslücken in technischen Produkten. Staat und Gesellschaft sind aber aufgefordert, diese effektiv zu begrenzen. Dazu ist eine intelligente Regulierung mit einer Verpflichtung der Hersteller zur verfassungsverträglichen Technikgestaltung nach dem Prinzip des *privacy by design and by default* ebenso notwendig wie wirksame Kontrollstrukturen und gut ausgestattete Aufsichtsbehörden. Selbst diese werden die Kontrolle ohne die Unterstützung von Whistleblowern, investigativen Journalisten und kritischen Betroffenen nicht gewährleisten können. Letztlich muss auch die „Datenreligion“[88] hinterfragt werden, die allein in der Anhäufung von immer größeren Mengen personenbezogener Daten die Lösung aller Probleme sieht. Dabei steht der Nutzen der Auswertung von anonymisierten Daten etwa für Forschungszwecke nicht in Frage. Aber auch die Feststellung, ob und wie lange Daten als anonymisiert anzusehen sind, bedarf in regelmäßigen Abständen der erneuten Kontrolle.[89]

[88] Zu diesem Begriff *Harari* (Fn. 2), 563 ff.

[89] Im Zweifel müssen daher auch anonymisierte Datenbestände nach Zweckerreichung oder -wegfall gelöscht werden, so die Forderung der EU-Kommission im Zusammenhang mit der Bereitstellung von anonymisierten Standortdaten aus der Telekommunikation zur Bekämpfung der Corona-Pandemie 2020 (Empfehlung EU 2020/518 v. 8.4.2020 für ein gemeinsames Instrumentarium der Union für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten, ABlEU L 114/7 v. 14.42020, Ziff. 20).