Stefan Strauß

Wachsende Identitätsschatten – wo endet Privatsphäre?

Zum Grundproblem sozio-technischer Identifizierbarkeit beim Datenschutz

Mit der Datenschutzgrundverordnung entsteht ein neues Europäisches Datenschutzregime, das einige Verbesserungen beim Schutz der Privatsphäre verspricht. Doch wie aussichtsreich ist wirksamerer Schutz der Privatsphäre im Zeitalter von Big Data und hochgradig vernetzten Technologien tatsächlich? Dieser Beitrag diskutiert kritisch die Grenzen des Datenschutzes aufgrund einer stetig wachsenden sozio-technischen Identifizierbarkeit und schlägt eine Typologie von Identitätsinformation als Beitrag zur systematischeren Erfassung datenschutzrelevanter Informationsprozesse vor, um dieses Grundproblem einzudämmen.

Wie weit trägt die Datenschutzgrundverordnung?

Die Datenschutzgrundverordnung (DSGVO) ist ein zentraler Meilenstein zur mittel- und langfristigen Stärkung des Datenschutzniveaus und eröffnet neue Handlungsspielräume. Neben deutlich erhöhtem Sanktionsrahmen sind vor allem zwei eng verzahnte Instrumente wesentlich: Datenschutz-Folgenabschätzungen (Privacy Impact Assessment – PIA) und Maßnahmen für Privacy-by-Design (PbD). Inwieweit sich Datenschutzstandards wirklich nachhaltig stärken lassen, ist jedoch noch weitgehend offen. Fortschreitende Digitalisierung und *Big-Data*-Paradigmen verleiten vielfach zu erweiterter Datennutzung und strapazieren das Ideal informationeller Selbstbestimmung (BVerfG 1983). Datenhandel und Profiling erfordern zwar im Sinne der DSGVO die Durchführung von PIA, sofern die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben kann (Art. 35 DSGVO). Ob Datensammelpraktiken damit deutlich eingrenzbar sind, wird sich zeigen, denn viele verschiedene Akteure agieren hier im rechtlichen Graubereich und erfassen große Datenmengen scheinbar beiläufig. Die jüngsten Vorfälle rund um *Facebook* und *Cambridge Analytica* verdeutlichen, wie umfang- und folgenreich diese Praktiken sein können (Davies 2018). Ohne breiten öffentlichen Diskurs wissen Betroffene davon meist gar nichts oder bleiben eher ratlos zurück. Konsequentes Nichtnutzen von Anwendungen oder Verweigern der Zustimmung zur Datenverarbeitung sind schwierig und digitale Informationsflüsse gerade bei vernetzten Verarbeitungskontexten de facto kaum kontrollierbar. Die DSGVO ist wichtig, aber alleine nicht ausreichend für Verbesserungen. Auch rechtskonforme Datenverarbeitung kann ethisch problematisch sein und tief in die Privatsphäre eindringen. Technische Trends von *smarten* Technologien, autonomen Fahrzeugen, dem *Internet der Dinge* usw. machen klar: Vernetzte Systeme bzw. Anwendungskontexte nehmen weiter zu und digitale Informationsflüsse lassen sich noch schwerer kontrollieren. Steigende Vernetzung bedeutet mehr Daten und damit mehr Möglichkeiten zur Verkettung und Aggregation unterschiedlicher Datenbestände. Es bleibt daher trotz DSGVO fraglich, inwieweit der wachsenden Komplexität digitaler Technologien bzw. sozio-technischer Systeme wirksam begegnet werden kann. Datenschutz-Analysen oder PIA sind meist kontextspezifisch und je nach Technologie unterschiedlich. Selbst Auffassungen über personenbezogene Daten können dabei variieren. Beispiel ist die in vielen Ländern unterschiedlich diskutierte Frage, inwieweit IP-Adressen als personenbezogen gelten. Ähnliches gilt für den Begriff *Metadaten* oder die unscharfe Abgrenzbarkeit zwischen direkt und indirekt personenbezogenen Daten. Zunehmend automatisierte Datenverarbeitung und technisch generierte Informationen verwischen die Grenzen. Noch fehlen gemeinsame Standards, das ist eine grundsätzliche Hürde für ein höheres Datenschutzniveau.

Öffentliche wie private Institutionen haben zwar wichtigen Handlungsspielraum bei der Umsetzung der DSGVO, doch mit offenen Fragen, was auf Kosten der Wirksamkeit von PIA und

PbD abseits rechtlicher Vorgaben gehen kann. PIA und PbD setzen detailliertes Wissen über Art und Struktur personenbezogener Daten sowie die verarbeitenden Informationssysteme voraus. Der je nach Anwendungsbereich mitunter hohe Komplexitätsgrad kann die Wirksamkeit von Datenschutz-Maßnahmen auch bei Rechtskonformität enorm beeinträchtigen. Mittelfristig ist mit unterschiedlichen Vorgehensmodellen und Handlungsabläufen zur DSGVO-Umsetzung zu rechnen, beispielsweise beim gebotenen Datenverarbeitungs-Verzeichnis, der PbD-Implementierung oder der konkreten Durchführung von PIA. Hier besteht Wildwuchsgefahr, die in der Praxis zu variierenden Datenschutzstandards auch in Europa führen könnte.

Sozio-technische Identifizierbarkeit als Kernproblem des Datenschutzes

Abseits rechtlicher Normen hängt die Wirksamkeit von Datenschutz-Maßnahmen wesentlich vom technischen und konzeptionellen Verständnis über jene Mechanismen ab, die auf die Privatsphäre einwirken. In der digital vernetzten Gesellschaft ist aber zusehends schwieriger fassbar, *was* unter personenbezogenen Daten eigentlich zu verstehen ist. *Big Data* ist symptomatisch für die verschwimmende Grenze zwischen personenbezogenen und nicht-personenbezogenen Daten (Strauß 2018). Wege aus dieser Misere erfordern neue Perspektiven auf bestehende Datenschutz-Konzepte, um den Anforderungen der digitalen Welt besser gerecht werden zu können. Wesentlich ist dabei, dass Identifikation der zentrale Mechanismus bei der personenbezogenen Datenverarbeitung ist: Die Möglichkeiten, eine Person zu identifizieren, sind ausschlaggebend für das Ausmaß der Auswirkungen auf die Privatsphäre dieser Person. Identifizierbarkeit ist das primäre Risiko für die Privatsphäre, das weitere Risiken nach sich ziehen kann (Strauß 2017). Das klingt zunächst trivial, meint Datenschutz doch seit jeher Informationen über identifizierte oder identifizierbare Personen[1]. Technische Standards verwenden zudem meist den (u. a. in den USA gängigen) Begriff der „personally identifiable information" (PII)[2]. In der Praxis werden diese Begriffe aber oft sehr unterschiedlich breit oder eng ausgelegt, was zu Problemen führen kann.[3] Das gleiche gilt für personenbezogene Daten, die je nach nationaler Gesetzgebung variabel interpretierbar sind. Erschwerend kommt hinzu, dass persönliche Identität selbst nicht nur statische, sondern auch dynamische Züge aufweist. Paul Ricoeur unterscheidet zwei Wesenszüge von Identität: Zum einen ist Identität etwas fortwährend Beständiges *(idem* bzw. *Gleichheit)* (Ricoeur 1992). Dementsprechend kann Identität durch gleichbleibende Attribute repräsentiert werden und wird dadurch unterscheidbar von anderen Entitäten. Zum anderen ist Identität aber auch dynamisch und in permanenter Entwicklung *(ipse* bzw. *Selbstheit).* In Summe lässt sich Identität daher als dialektisches Konzept aus Gleichheit und Selbstheit bzw. statischen und dynamischen Komponenten begreifen (Strauß 2017). Das ist insofern relevant, als digitale Technologien veränderte und noch dynamischere Formen der Identifikation hervorbringen können. Digitale Information ist an sich bereits dynamisch. Mit Verarbeitung von digitalen Informationen, die auf die Identität einer Person verweisen, wird auch die Identifizierbarkeit einer Person selbst zur variablen Größe. Als Konsequenz hängt die Wirksamkeit von Maßnahmen wie PbD erheblich vom jeweiligen Begriffsverständnis über personenbezogene Daten oder Identitätsinformation ab. Versteht man Identität nur als unveränderbares, statisches Konzept, das aus klar definierten Attributen besteht wie typischerweise Name, Geburtsdatum und -Ort usw., eindeutigen Personenkennzeichen oder biometrischen Merkmalen, bleiben dynamischere Attribute, die ebenso zur Identifikation nutzbar sind (Datenspuren, Quasi-Identifikatoren, technische IDs, Fingerprinting-Techniken usw.) außen vor. Gerade Profiling und ähnliche Praktiken machen aber starken Gebrauch von relativ dynamischen Identitätsattributen als vermeintlichen Nebenprodukten der Nutzung digitaler Technologien. Hier wird die Problematik wachsender digitaler „Identitätsschatten" (Strauß 2017) sichtbar. Die vorherrschende Standard-Einstellung in sozio-technischen Systemen im Sinne einer *Identifiability-by-Default* begünstigt diese Problematik. Technologien begünstigen durch mangelnde oder eingeschränkte Datenschutz- und Sicherheitskonzepte Identifizierbarkeit häufig eher als sie zu verhindern. Bei der Nutzung technischer Anwendungen werden oft zusätzliche Identifikatoren erzeugt, die Rückschlüsse auf einzelne Personen erlauben. So besteht ein inhärenter Konflikt zwischen Privacy-by-Design und Identifiability-by-Default (ebd.). Zu enge oder unpräzise Auffassungen von personenbezogenen Daten erschweren wirksamen Schutz.

Rechtlich gelten neben Namen primär Personenkennzeichen, Identifikationsnummern etc. sowie spezifische Personen-Merkmale als personenbezogene Daten. Das betrifft zwar grundsätzlich auch technische Identifikatoren. In der Praxis ist aber oft unklar, inwieweit technische Information als personenbezogen gilt oder nicht: Sind es etwa *nur* IP-Adressen oder auch andere Kennungen, Metadaten etc.? Unabhängig von der rechtlichen Beurteilung ist eine Präzisierung sinnvoll – gerade aufgrund wachsender Identitätsschatten. Bei jeder Nutzung digitaler Technologien entstehen viele Möglichkeiten zur indirekten bzw. impliziten Identifikation. Mittels Aggregation verschiedener Daten können Quasi-Identifikatoren erzeugt werden, wodurch eine Person auch ohne Zutun oder Wissen identifizierbar wird (ebd.). Gängiges Beispiel ist das Erstellen digitaler Fingerabdrücke *(Fingerprinting)* durch bloße Nutzung einer Technologie zur Verfolgung von Internet-NutzerInnen und das Erzeugen entsprechender Benutzer-Profile (Gierow 2017). Die dazu genutzten Informationen sind oft keine personenbezogenen Daten im engeren Sinn, die Auswirkungen für die Privatsphäre aber dennoch erheblich. Es bedarf daher eines tieferen Verständnisses von Identifizierbarkeit und Identitätsinformation in sozio-technischen Systemen, um datenschutzrelevante Verarbeitungsvorgänge genauer zu erfassen, Datenschutz-Folgeabschätzungen systematischer durchzuführen sowie PbD-Konzepte wirksamer zu gestalten. Denn im Kern geht es um das Erkennen und Schützen von Identitätsinformation, direkter wie indirekter.

Vier Dimensionen von Identifizierbarkeit

Ein wirksames Konzept von Identitätsinformation statt personenbezogener Daten ist relevant, weil es Personenbezug einbezieht und zugleich hilft, technisch generierte Daten mit möglichem Personenbezug nicht zu vernachlässigen. Identifizierbarkeit ist Grundvoraussetzung für Identifikation und ermöglicht Information zu verarbeiten, die direkt oder indirekt auf die Identität einer Person verweist. Identifizierbarkeit setzt grundsätzlich die Verfügbarkeit von Identitätsinformation vor-

aus (Strauß 2017). Die Crux ist hierbei, genauer zu spezifizieren, was unter Identitätsinformation zu verstehen ist, die im zeitlichen Verlauf eher zu- als abnimmt[4]. Streng genommen sind vollständige Aufzählungen aufgrund des dynamischen Charakters von Identität und digitaler Information zum Scheitern verurteilt. Um das Ausmaß von Identifizierbarkeit dennoch besser fassen zu können, schlage ich eine Typologie von Identitätsinformation vor, die von vier grundlegenden, aufeinander aufbauenden Dimensionen ausgeht (Abbildung 1): Substanzielle, räumlich-zeitliche, relationale und interaktionale Identitätsinformation.

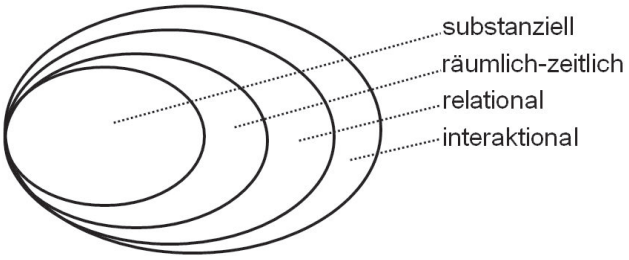

Abbildung 1: Vier Dimensionen von Identitätsinformation

Diese vier Dimensionen erlauben es Identitätsinformation genauer zu spezifizieren. Sie leiten sich aus einer systemtheoretischen Perspektive ab: Ein sozio-technisches System besteht nicht nur aus der Summe seiner Elemente, sondern auch aus den Beziehungen (Relationen) zwischen diesen Elementen innerhalb und außerhalb des Systems (seiner Umwelt) in unterschiedlichen räumlich-zeitlichen Kontexten. Auf ähnliche Weise lässt sich eine Person als systemische Entität begreifen, die über substanzielle Merkmale verfügt, Relationen bzw. Beziehungen zu anderen hat, und mit ihrer Umwelt und anderen Entitäten in unterschiedlichen räumlich-zeitlichen Kontexten interagiert. Diese Informationstypen sind maßgebliche Bestandteile der informationellen Identitäts-Repräsentation. Ausmaß und Zusammenspiel von Informationen entlang dieser Dimensionen haben daher Auswirkungen auf die Identifizierbarkeit der Person. Das gilt auch für die zur Informationsverarbeitung verwendeten Technologien, denn auch eine Technologie hat eine Art substanziellen Kern, wird in räumlich-zeitlichen Kontexten eingesetzt, hat meist interne und externe Relationen zu anderen technischen Komponenten und interagiert mit diesen. Die Beschaffenheit eines sozio-technischen Systems, das Identitätsinformation verarbeitet, kann daher Auswirkungen auf die Qualität dieser Information haben. Gerade digitale Technologien bestehen meist aus vielen miteinander vernetzten Komponenten (bzw. Teilsystemen). Die Identifizierbarkeit und damit der Schutz der Privatsphäre der Person hängen daher wesentlich von der Beschaffenheit und Konfiguration jener sozio-technischen Systeme ab, die ihre Identitätsinformation verarbeiten. Eine weitere Differenzierung zwischen personen-spezifischen (PII) und technologie-spezifischen Identitätsinformationen (TII) ist daher sinnvoll. Beide Typen können anhand der genannten vier Grunddimensionen beschrieben werden.

PII – Personen-spezifische Identitätsinformation

PII meint all jene Informationen, die direkt oder indirekt auf die Identität einer Person verweisen. Das deckt sich zunächst mit dem gängigen Verständnis von personenbezogenen Daten (im Sinne von DSGVO u. ISO), die in unterschiedlichen Formen häufig erhoben werden. Doch entlang der oben genannten Dimensionen entsteht ein differenzierteres Bild – PII lassen sich damit wie folgt zuordnen (Strauß 2017):

- Substanzielle PII (P1) meint wesentliche Identitätsmerkmale, also all jene Informationen, die sozusagen die *Substanz* der Identität einer Person beschreiben. Neben dem Namen als primären Identifikator sind das typischerweise wesentliche Merkmale über Aussehen und Beschaffenheit der Person wie Augen- und Haarfarbe, Größe, Gewicht, Geschlecht oder biometrische Merkmale wie Fingerprints, Gesichts-, Iris- oder auch Sprachmuster bis zur DNS.

- Räumlich-zeitliche PII (P2) meint all jene Information, die räumliche und/oder zeitliche Merkmale über die Person beschreibt. Geläufig sind v. a. Alter, Geburtsdatum und -Ort, Nationalität, Anschrift(en) privat/beruflich, Wohnort, Arbeitsplatz, Aufenthaltsort usw.

- Relationale PII (P3) umfasst alle Information über Beziehungen im engeren und weiteren Sinn. Typischerweise sind das etwa persönlicher Beziehungsstatus (verheiratet/ledig), Beschäftigungsstatus, Informationen über Arbeitgeber, Familie, Verwandte und Freunde usw.

- Interaktionale PII (P4) meint all jene Information, die bei Interaktionen der betroffenen Person mit anderen (Entitäten) entsteht wie persönliche Interessen, Aktivitäten, Verhalten, Meinungen usw. Darunter fallen auch sensible Informationen wie politische und religiöse Einstellungen, sexuelle Vorlieben etc.

Die genannten Beispiele können keine vollständige Auflistung bieten sondern sollen diese vier Grundtypen von Identitätsinformation näher erläutern. PII enthalten also vor allem Aspekte

Stefan Strauß

Foto: ITA/Peissl

Dr. **Stefan Strauß** ist promovierter Wirtschaftsinformatiker am Institut für Technikfolgen-Abschätzung (ITA) an der Österreichischen Akademie der Wissenschaften in Wien. Er forscht an der Schnittstelle zwischen Informatik und Gesellschaft, insbesondere zu Governance sozio-technischer Systeme, Privatsphäre, Sicherheit und Überwachung, digitaler Identität und Privacy Impact Assessment. Weitere Forschungsinteressen im Feld der Informations- und Computerethik.

wie: Was ist der substanzielle Kern der Identitätsinformation bzw. welche Informationen beschreiben primär die Identität einer Person? Welche Informationen beschreiben darüber hinaus räumlich-zeitliche Kontexte, Relationen und Interaktionen diese Person betreffend? Die informationelle Identität der Person lässt sich so als Satz von Informationen verstehen, der zum einen weitgehend invariante, substanzielle Identitätskriterien aufweist wie eben Name, Geburtsdatum, Geschlecht, biometrische Merkmale usw. Zum anderen gibt es aber eine Reihe weiterer Informationen, die auf die Identität der Person verweisen können. Diese Informationen sind vergleichsweise eher dynamischer Natur. Anhand der weiteren Typen (räumlich-zeitlich, relational, interaktional) lässt sich diese Dynamik systematischer fassen.

Alle PII-Typen sind auch mit technischen Mitteln abbildbar und werden meist dementsprechend verarbeitet. Allerdings kann sich dadurch die Beschaffenheit der Identitätsinformation selbst verändern. Bei Einsatz und Nutzung von Technologien werden meist weitere Informationen erzeugt, die das Ausmaß an Identifizierbarkeit der betroffenen Person erhöhen. Neben PII führe ich daher zusätzlich die Kategorie *Technologie-spezifische Identitätsinformation (TII)* ein.

TII – Technologie-spezifische Identitätsinformation

TII umfasst jede Information, die bei der Anwendung oder Nutzung einer Technologie entsteht und direkt oder indirekt auf die Identität einer Person verweist. Entlang der oben genannten Dimensionen lassen sich TII wie folgt zuordnen (Strauß 2017):

- Substanzielle TII (T1) meint Informationen technischen Ursprungs, die primär an der Verarbeitung von PII beteiligt sind. Typische Beispiele sind Identifikatoren wie Benutzernamen bzw. IDs (z. B. Benutzername eines Online-Dienstes wie Google, Facebook und Co., E-Mailadresse, Session IDs etc.) oder Kennungen von Geräten (z. B. IP-Adressen, MAC-Adresse, SIM Card IDs, IMEI usw.). Hier kann eine weitere Unterscheidung zwischen Anwendungs- und Geräte-spezifischen TII sinnvoll sein.

- Räumlich-zeitliche TII (T2) meint Information über den Nutzungskontext einer Technologie oder Anwendung. Typische Beispiele sind Zeitstempel, Zeitzone, Standortdaten (Geo-Lokalisierung), Login-Zeiten, -Dauer und ähnliche Informationen über technische Nutzer-Aktivitäten.

- Relationale TII (T3) sind all jene Informationen, die zusätzlich bei der Technologie-Nutzung anfallen, durch Relationen der primären Technologie oder Anwendung mit weiteren Komponenten. Gemeint sind hier vor allem Teil-Systeme der primären Technologie bzw. Anwendung. Das können Software-Komponenten wie Datenbanken, Software des Betriebssystems, Browser, Apps, Social Plugins und Logins usw. sein, aber auch einzelne verbaute Hardware-Komponenten, sogar Kameras, Mikrofone usw. Diese Teil-Systeme müssen nicht direkt von einer Person genutzt werden, um Identitätsinformationen zu verarbeiten oder zusätzliche zu erzeugen. Das können etwa verschiedene Metadaten sein. So verfügt eine Webcam über eine eigene ID, die mitunter Rückschlüsse auf die Nutzer ermöglicht. Ähnliches gilt für spezifische Kennungen von Software, etwa Webbrowsern. In diese Kategorie fallen auch Informationen über Hard- und Softwarekonfigurationen, die sich für die Erzeugung von Quasi-Identifikatoren und damit Fingerprinting-Technik eignen, wie spezifische Einstellungen, Webbrowser-History, bis hin zu Schriftgrößen und Bildschirmauflösung.

- Interaktionale TII (T4) meint Informationen, die bei der Nutzung bzw. Interaktion entstehen. Typischerweise sind das technisch erzeugte Benutzer-Inhalte, beispielsweise gesendete Nachrichten, Postings, Kommentare, *Likes,* sonstiges Text-, Bild- oder Ton-Material wie Fotos, Audio- und Videodateien, aber auch technische Information über Kontakte usw. Wie soziale Medien verdeutlichen, ist die Liste von Online-Inhalten hier nahezu beliebig erweiterbar. Auch Metadaten über die Interaktion sind hier gemeint, wie Orts- und Zeitstempel, Anzahl an Nachrichten und beteiligten Kommunikationspartnern, Interaktions- oder Gesprächsdauer etc. Sogar Hardware-Interaktion erzeugt Datenspuren wie Nutzungsmuster von Keyboard, Maus, Touchscreens usw., aus denen potenziell digitale Fingerprints generiert werden können.

Zusammenfassung und Fazit

Die fortschreitende digitale Transformation der Gesellschaft bringt immer gravierendere Herausforderungen für den Datenschutz. Die DSGVO eröffnet Potenzial für eine nachhaltige Stärkung des Schutzniveaus. Das erfordert aber auch ein tieferes Verständnis für jene sozio-technischen Mechanismen, die die Privatsphäre maßgeblich beeinträchtigen können. Das ist wesentlich für die Entwicklung längerfristig wirksamer Schutzkonzepte. Die vorgestellte Typologie kann einen wertvollen Beitrag zur systematischeren Analyse digitaler Informationsflüsse mit Datenschutz-Relevanz leisten. Solche Analysen sind wesentlich für PIA, die nicht nur ein rechtliches Erfordernis in bestimmten Fällen, sondern ein zentrales Instrument für Datenschutz-konforme Technikgestaltung und damit PbD darstellt. Die Typologie ist weitgehend Technologie-neutral und unterstützt bei der Erfassung von Informationen, die direkt oder indirekt auf die Identität einer Person verweisen und damit potenziell datenschutz- und sicherheitsrelevant sind. Die genannten Dimensionen bzw. Grundtypen sind in unterschiedlichem Ausmaß in jedem sozio-technischen System zu finden. Gerade TII verdeutlichen die Fülle technischer Identitätsinformationen und deren weitreichende Folgen für die Privatsphäre bei unkontrollierter Verarbeitung. Vor allem relationale und interaktionale TII können sich je nach analytischer Perspektive überlappen, was eine eindeutige Zuordnung teils erschwert. Trotzdem ist eine Differenzierung nützlich, um das Ausmaß der Identifizierbarkeit genauer zu erfassen. Auch sind nicht alle Arten von TII à priori datenschutzrelevant. Das hängt wesentlich vom konkreten Anwendungskontext ab und inwieweit die Informationen gezielt verarbeitet und gespeichert werden. Werden IP-Adressen oder technische Identifikatoren gar nicht erfasst, sind sie zumindest keine TII mit Datenschutzrelevanz in Bezug auf die konkrete Anwendung. Das gleiche gilt für Informationen für potenzielles Fingerprinting, über die Anwendungsbetreiber oft gar keine Kontrolle haben. Allerdings können diese Informationen sicherheitsrelevant sein, und Kenntnis darüber wichtig zur Verbesserung von Schutzmaßnahmen. Gerade sicherheitsbewusste Un-

ternehmen sollten ihre Informationsprozesse im Detail kennen, um diese wirksamer schützen zu können. TII als eigene Kategorie ermöglichen die Berücksichtigung jener Informationsarten, die implizit auf die Identität einer Person verweisen und daher besonders schwer kontrollierbar sind. Das trägt zur Datensparsamkeit, aber auch zum Erkennen von etwaigen Sicherheitslücken bei, was nicht nur den betroffenen Personen, sondern auch Technologie-Betreibern und Entwicklern zugutekommt.

Literatur

DSGVO – Datenschutzgrundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

Davies H (2018): Facebook told me it would act swiftly on data misuse – in 2015. The Guardian, March 26, https://www.theguardian.com/commentisfree/2018/mar/26/facebook-data-misuse-cambridge-analytica

BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil)

Strauß S (2017): Chasing shadows: the interplay of privacy and (digital) identification – toward an identifiability-based framework for privacy impact assessment. Dissertation, Fakultät für Informatik, Technische Universität Wien

McCallister E; Grance, T.; Scarfone, K. (2010): Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Recommendations of the National Institute of Standards and Technology (NIST), Special publication 800-122. U.S. Department of Commerce.

ISO – International Standards Organisation (2011): Information technology – Security techniques – Privacy framework. ISO/IEC 29100:2011(E). 1st edition 2011-12-15.

Schwartz PM.; Solove DJ (2011): The PII problem: privacy and a new concept of personally identifiable information. New York University Law Review (86): 1814-1894.

Ricoeur P (1992); Oneself as Another. (Translated by Kathleen Blamey). University of Chicago Press.

Gierow H (2017): Nutzer lassen sich über Browser hinweg tracken, Golem, 17. Januar, https://www.golem.de/news/fingerprinting-nutzer-lassen-sich-ueber-browser-hinweg-tracken-1701-125627.html

Hansen M, Pfitzmann A, Steinbrecher S (2008): Identity management throughout one's whole life. Information Security Technical Report 13(2008): 83-94.

Strauß S (2018) Big Data – within the tides of securitisation? In: A.R. Saetnan et al. (eds.): The Politics of Big Data – Big Data, Big Brother?, Routledge, 46-67

Anmerkungen

1 *vgl. Art. 4 DSGVO*
2 *McCallister et al. 2010; ISO 2011*
3 *vgl. z. B. Schwartz/Solove 2011*
4 *vgl. Hansen et al. 2008*

Alexander Roßnagel

Datenschutz-Grundverordnung – was bewirkt sie für den Datenschutz?

Die Datenschutz-Grundverordnung der Europäischen Union hat hohe Erwartungen geweckt und wird mit großen Hoffnungen erwartet. Der Beitrag untersucht, ob diese berechtigt sind und ob die Verordnung dazu beitragen kann, den Datenschutz tatsächlich zu verbessern. Das Ergebnis ist gemischt: Nüchtern betrachtet führt sie weder zu einem einheitlichen Datenschutzrecht in Europa noch zu Datenschutzregelungen, die den modernen Herausforderungen gerecht werden. Gewisse Hoffnungen sind jedoch berechtigt, dass sie den Vollzug des Datenschutzrechts verbessert.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

1. Datenschutz-Grundverordnung – Ziele und Erwartungen

Nach mehreren Jahren vorbereitender Arbeiten, des Vorschlags der Kommission vom anschließenden Gesetzgebungsprozess [illegible] mit ihrer Verabschiedung vor [illegible] in Kraft getreten. Sie gilt vom die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO)[1] am 25. Mai 2016 in Kraft getreten. Sie gilt vom 25. Mai 2018 an mit all ihren Regelungen[2] in allen Mitgliedstaaten unmittelbar und wird Teil ihrer Rechtsordnung.

Die DSGVO sollte durch eine Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation, abkürzend E-Privacy-VO genannt, bereichsspezifisch ergänzt werden. Diese Verordnung soll die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) von 2002 ablösen.

Die DSGVO wurde mit großen Versprechen angekündigt[6], mit hohen Erwartungen versehen[7], mit tiefen Enttäuschungen aufgenommen[8] und durch viel Lobby-Arbeit beeinflusst.[9] Sie wird im Ergebnis sehr unterschiedlich bewertet. Sie wird – vor allem von den an ihrem Entstehen Beteiligten – als „Meilenstein" bezeichnet[10], als „Goldstandard" gepriesen[11] sowie als „Beginn einer neuen Zeitrechnung im Datenschutzrecht"[12] und als „festes Fundament für die anstehenden Herausforderungen der Digitalisierung" gefeiert.[13] Umgekehrt wird sie von anderen zu „einem der schlechtesten Gesetze des 21. Jahrhunderts" gekürt und für das Datenschutzrecht als „größte Katastrophe des 21. Jahrhunderts" bezeichnet.[14]