Humanistische Union

Transparenz als Datenschutzprinzip – Ansätze und Umsetzungsprobleme

Datenschutz kann nur effektiv sein, wenn die Betroffenen wissen, wer Daten über sie verarbeitet und was genau mit diesen Daten geschieht. Dieser Beitrag diskutiert die Ansätze für transparentere Datenverarbeitung, die in der EU-Datenschutzgrundverordnung geregelt wurden. Dabei zeigt sich, dass die praktische Umsetzung unter vielen Aspekten noch verbesserungsbedürftig ist.

1. Einleitung: Synergien zwischen Transparenz und Datenschutz

Transparenz ist ein komplexes Konzept mit vielfältigen Aspekten (zur Übersicht: August & Osrecki 2019). Auf den ersten Blick können Datenschutz und Transparenz widersprüchlich erscheinen. Werden Informationen zur Privatsphäre für Außenstehende transparent gemacht, so kann dies die Privatsphäre beeinträchtigen. Zugleich ist Transparenz aber eine essentielle Voraussetzung für den Selbstbestimmungsaspekt des Datenschutzes: Betroffene können ihre Rechte nur dann effektiv wahrnehmen und durchsetzen, wenn sie wissen, wer welche Daten über sie verarbeitet. Nicht zufällig sind die meisten Datenschutzbeauftragten daher inzwischen auch für Informationsfreiheit und damit für (Verwaltungs-)Transparenz zuständig.

Dieser Beitrag geht der Frage nach, welche Ansätze die EU-Datenschutzgrundverordnung (DSGVO) enthält, um Datenverarbeitung für die Betroffenen transparent(er) zu machen und welche Probleme bei der Umsetzung auftreten. Dabei wird gezeigt, dass Transparenzanforderungen, die nur abstrakt formuliert sind, in ihren Auswirkungen begrenzt bleiben, solange datenverarbeitende Unternehmen und Behörden sie nicht in ihre Abläufe und Handlungsroutinen integrieren. Die weitere Konkretisierung von Transparenzanforderungen, etwa durch Standards für die Unterstützung von Transparenz durch Technikgestaltung, ist bisher nur in wenigen Bereichen vorangekommen und bedarf daher zusätzlicher rechtspolitischer und praxisorientierter Initiativen.

Ansätze für eine transparente(re) Datenverarbeitung stoßen allerdings auf strukturelle Hindernisse. Transparenz kann zwar das Vertrauen in Datenverarbeitung steigern und damit auch die Akzeptanz selbst hoheitlicher Datenerhebung verbessern (näher hierzu Kugelmann 2001, S. 14ff.; Aden, Fährmann & Bosch 2020, S. 5ff.). Allerdings sind Unternehmen und Behörden längst nicht immer an Transparenz interessiert, sondern verfolgen auch gegenläufige Interessen, insbesondere an der möglichst ungestörten Nutzung von Daten für vielfältige Zwecke. Intransparente Datenverarbeitung macht es Betroffenen schwer, kritisch zu hinterfragen, was genau mit einmal erhobenen Daten geschieht.

2. Transparenz als rechtlich konkretisiertes Datenschutzprinzip

Mit dem explizit formulierten Auskunftsanspruch und der prominenten Stellung als DSGVO-Grundsatz hat Transparenz heute einen hohen normativen Stellenwert. In den folgenden Abschnitten wird gezeigt, dass die praktische Ausgestaltung dieser Rechte diesem hohen Stellenwert vielfach bisher noch nicht gerecht wird und dass die Transparenzthematik größerer Aufmerksamkeit bedürfte. Insofern erscheint es symptomatisch, dass der im Juni 2020 veröffentlichte Bericht der Europäischen Kommission über zwei Jahre Anwendungspraxis der DSGVO das Thema Transparenz nur am Rande erwähnt (Europäische Kommission 2020, S. 1, 4 und 10).

Rechtliche Regelungen zur Transparenz von Datenverarbeitung wurden nicht erst mit der DSGVO neu entwickelt. Bereits seit den 1980er Jahren ist Transparenz ein Kernbestandteil des Datenschutzes. Nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) setzt individuelle Selbstbestimmung über die eigenen Daten und über die Privatsphäre voraus, dass die Einzelnen wissen, wer Informationen über sie hat. In diesem Sinne argumentierte das BVerfG bereits in seiner Volkszählungsentscheidung aus dem Jahr 1983, die das Recht auf informationelle Selbstbestimmung als Grundrecht etablierte, abgeleitet aus der Menschenwürde und der Allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG):

„*Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden*“ (BVerfGE 65, 1 (43)).

Aus dem Grundrecht auf informationelle Selbstbestimmung folgen daher auch Auskunfts- und Aufklärungsansprüche der von Datenverarbeitung Betroffenen. In der EU-Grundrechtecharta (GRCh) wurde diese Transparenzidee explizit ausformuliert. Nach Art. 8 Abs. 2 Satz 2 GRCh hat jede Person „*das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.* “ Art. 42 GRCh gewährt darüber hinaus Zugang zu Dokumenten der EU-Organe.

Auch aus dem in der Vergangenheit wenig beachteten Grundrecht auf Informationsfreiheit (Art. 5 Abs. 1 Satz 1, 2. Halbsatz GG) lässt sich unter den Rahmenbedingungen von Digitalisierung und *Open Government* eine Verpflichtung des Staates ableiten, sein Handeln durch Veröffentlichung von Informationsbeständen transparenter zu machen. Der Staat verfügt über vielfältiges Wissen, das auch für die Bürger*innen interessant ist, von statistischen Informationen bis zu Fachwissen zu Gesundheitsrisiken. Einmal digitalisiert, können solche Informationen mit wenig Aufwand auch online bereitgestellt werden (ausführlich zur Begründung Lederer 2015, S. 439ff.) und so zu mehr Transparenz beitragen.

Art. 5 Abs. 1 lit. a DSGVO erwähnt Transparenz als Datenschutzgrundsatz. Damit gehört sie zu den Leitprinzipien des Datenschutzes – gemeinsam mit Grundsätzen wie Rechtmäßigkeit und Zweckbindung der Datenverarbeitung und deren Fairness – letztere etwas unglücklich in der offiziellen deutschsprachigen

Fassung mit „*Treu und Glauben*“ übersetzt (zur Kritik hieran auch Roßnagel 2019, Art. 5 Rn. 47; Roßnagel/Geminn 2020, S. 46). In der parallel verabschiedeten Richtlinie (EU) 2016/680 für den Datenschutz im Polizei- und Strafjustizbereich wird das Transparenzgebot nicht explizit erwähnt, ist aber auch hier als Bestandteil des Fairnessgebots zu beachten (so auch Tzanou 2017, S. 26; Johannes & Weinhold 2018, S. 65). Fairness und Transparenz sind eng miteinander verknüpft. Transparente Abläufe sind eine zentrale Voraussetzung dafür, dass Betroffene Entscheidungen als fair und legitim empfinden und letztlich akzeptieren (vgl. hierzu Kugelmann 2001, S. 14ff.; de Fine Licht u.a. 2014, S. 115).

DSGVO-Begründungserwägung Nr. 13 macht deutlich, dass die Grundverordnung die Transparenz von Datenverarbeitung, wie sie bereits seit langem im Datenschutzrecht etabliert war, zu stärken beansprucht:

„*Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.*“

Hier werden bereits drei zentrale Ansätze sichtbar, die den Stellenwert von Transparenz erhöhen: (1) Das Transparenzgebot schließt ausdrücklich auch zukünftige Datenverarbeitung mit ein und damit insbesondere die Frage, für welche weiteren Zwecke bereits erhobene Daten genutzt werden dürfen und sollen. (2) Informationen über Datenverarbeitung müssen leicht zugänglich, also auffindbar sein. Und (3) die Informationen müssen so bereitgestellt werden, dass nicht nur Expert*innen verstehen, worum es geht und dass der Aufwand für das Finden und Verstehen der bereitgestellten Informationen sich für die Betroffenen in vernünftigen Grenzen hält.

2.1 Informations- und Auskunftsrechte als Kern der Datenverarbeitungstransparenz

Kernelemente transparenter Datenverarbeitung sind Informationspflichten und Auskunftsrechte, die in Art. 12 bis 15 DSGVO geregelt sind. Sie sind mit weiteren Informationsansprüchen verknüpft, insbesondere bei Datenschutzverstößen (Art. 33, 34), und bilden zugleich die Voraussetzung für Berichtigungs- und Löschungsansprüche (Art. 16).

In der deutschen Rechts- und Verwaltungstradition waren Auskunftsrechte auf die an Verwaltungsverfahren beteiligten Personen beschränkt, die zudem ein berechtigtes Interesse an den betreffenden Informationen geltend machen mussten. Die bis heute geltende Regelung hierzu in § 29 Abs. 1 Satz 1 Verwaltungsverfahrensgesetz (VwVfG) wirkt unter den Rahmenbedingungen der Digitalisierung schon beinahe altertümlich: „*Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.*“ Dieses Recht wird im folgenden Absatz für Fälle gleich wieder eingeschränkt, in denen „ *die ordnungsgemäße Erfüllung der Aufgaben der Behörde beeinträchtigt, das Bekanntwerden des Inhalts der Akten dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder*

dritter Personen, geheim gehalten werden müssen“ (ausführlich zu dieser Regelung Kugelmann 2001, S. 243ff.).

Im Vergleich dazu sind die Betroffenenrechte in Art. 12ff. DSGVO klar an Transparenz orientiert und gehen über ein abstraktes Postulat weit hinaus. Den Verantwortlichen für die Verarbeitung personenbezogener Daten werden Pflichten auferlegt, die der Praxis Maßstäbe für ihr Handeln an die Hand geben. So sind den Betroffenen Informationen „*in präziser transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln*“ (Art. 12 Abs. 1 Satz 1). Die Formulierungen denken somit Umgehungsstrategien für Transparenz gleich mit, indem sie Präzision und Verständlichkeit einfordern, was bei komplexen technischen Abläufen keinesfalls selbstverständlich ist. Für die praktische Umsetzung dieser Transparenzpostulate sind indes weitere Handreichungen und perspektivisch auch rechtsverbindliche Regelungen erforderlich, die Standards für eine gute Transparenzpraxis definieren (Ansätze hierzu: Article 29 Data Protection Working Party 2018b, S. 6ff.; vgl. auch Dix 2019, Art. 12 Rn. 12ff.; Roßnagel/Geminn 2020, S. 65f.).

Für die Datenerhebung bei den Betroffenen (Art. 13) und bei Dritten (Art. 14) ist in der DSGVO geregelt, welche Informationen den Betroffenen bereitgestellt werden müssen (zur umstrittenen Systematik: Dix 2019, Art. 13 Rn. 3). Im Rahmen des Auskunftsrechts haben Betroffene auch Anspruch auf eine „*Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind*“ (Art. 15 Abs. 3 Satz 1), wobei allerdings die Rechte Dritter, deren Daten mit betroffen sind (z.B. weil sie gemeinsam mit der Auskunft verlangenden Person auf einer Liste stehen) nicht beeinträchtigt werden dürfen. Die praktische Umsetzung kann mit erheblichem Aufwand verbunden sein, insbesondere bei Unternehmen und Behörden, die mit der Person, die Auskunft verlangt, auf komplexe Weise verbunden sind – etwa bei Studierenden einer Hochschule, deren Daten parallel von Immatrikulations- und Prüfungsämtern, Lehrplanung und Bibliotheken verarbeitet werden. Die Auskunftsfähigkeit erfordert daher technische Vorkehrungen, um die betreffenden Daten mit vertretbarem Aufwand finden zu können. Empfehlenswert sind auch Absprachen mit der Person, die Auskunft begehrt, um möglichst Einvernehmen über die gewünschten Informationen und die Form der Übermittlung einer „Kopie“ zu erzielen (so auch Dix 2019, Art. 15 Rn. 29).

2.2 Weitere Transparenzansätze: Zertifizierung, Datenschutz-Folgenabschätzung und Informationspflichten bei Datenschutzverstößen

Das Transparenzgebot wird in weiteren DSGVO-Regelungen konkretisiert. Hier seien insbesondere die Regelungen zur Zertifizierung von Datenschutzstandards (Art. 42) genannt, die sich zur Förderung von Datenschutzsiegeln und -prüfzeichen bekennen. Eine solche Zertifizierung kann für Betroffene nachvollziehbar und damit transparent machen, dass die DSGVO-Standards eingehalten werden. Allerdings basiert die Zertifizierung auf Freiwilligkeit, so dass insbesondere solche Unternehmen und Behörden davon Gebrauch machen dürften, die besonders auf das Vertrauen der Betroffenen angewiesen sind, um an deren Daten zu gelangen.

Die Transparenz von Datenverarbeitung kann auch durch eine Datenschutz-Folgenabschätzung gefördert werden (Art. 35). Sie ist allerdings nur bei Einführung neuer Verarbeitungsformen und Technologien vorgeschrieben, die mit hohen Risiken für Rechte und Freiheiten der Betroffenen verbunden sind. Die

Datenschutz-Folgenabschätzung ist eine spezielle Variante der Technikfolgenabschätzung, wie sie in Deutschland und anderen Ländern bei der Einführung und rechtlichen Rahmung neuer Technologien seit langem etabliert ist. Die Technikfolgenabschätzung und die Datenschutz-Folgenabschätzung fungieren auch als Instrumente zur Herstellung von Transparenz bei der Technologieentwicklung (näher hierzu Friedewald 2017; Aden & Fährmann 2020; Grunwald 2010).

Die Informationspflichten bei Datenschutzverstößen (*Data Breach Notification*, Art. 33, 34) sind ein weiteres Transparenzinstrument, das durch die DSGVO aufgewertet wurde. Kommt es zu Gefährdungen des Schutzes personenbezogener Daten, so dürfen solche Vorfälle nicht „unter den Teppich gekehrt" werden. Vielmehr ist die Datenschutzaufsicht innerhalb von 72 Stunden zu informieren (Art. 33), bei schwerwiegenden Vorfällen müssen auch die Betroffenen (Art. 34) benachrichtigt werden. Datenschutzvorfälle können vielfältige Ursachen haben – von der Nichtbeachtung datenschutzrechtlicher Pflichten über Nachlässigkeiten, die dazu führen, dass Daten Unbefugten zur Kenntnis gelangen, bis zu gezielten Cyberangriffen. Die Informations- und Benachrichtigungspflichten können zu mehr Transparenz beitragen. Darüber hinaus kann die *Breach Notification* eine präventive Funktion erfüllen, da Abhilfemaßnahmen geboten sind, die dazu beitragen, vergleichbare Vorkommnisse zukünftig zu vermeiden (Art. 33 Abs. 4). Bisher liegen keine empirisch gesicherten Erkenntnisse dazu vor, inwieweit die Meldepflichten in der Praxis eingehalten werden und zu welchen Konsequenzen sie führen. Abgrenzungsprobleme bereitet die Frage, in welchen Fällen auf eine Meldung verzichtet werden kann, weil keine Risiken für Rechte und Freiheiten der Betroffenen zu erwarten sind (Art. 33 Abs. 1) und wann die Benachrichtigung der Betroffenen entfallen kann (Art. 34 Abs. 3; ausführlich hierzu Dix 2019, Art. 33 Rn. 10-15 und Art. 34 Rn. 12-17). Die Datenschutzbeauftragten haben zu diesen Fragen Empfehlungen herausgegeben (Article 29 Data Protection Working Party 2018a; in Deutschland u.a. Engelbrecht 2019). Auch hier dürften mittelfristig verbindliche Konkretisierungen zu erwarten sein.

2.3 Transparente Technikgestaltung und Transparenz durch Technikgestaltung

Transparenz kann auch durch die Technikgestaltung und datenschutzfreundliche Voreinstellungen technischer Anwendungen unterstützt werden. Art. 25 DSGVO etabliert diese Grundsätze als Pflichten, bekannter unter den englischen Bezeichnungen *Privacy by Design and by Default*. *Privacy by Design* ist ein Schlüsselkonzept zur Verbesserung von Datenschutzstandards und zur Herstellung von Transparenz an der Schnittstelle zwischen Technik und Recht. Nach diesem Grundsatz darf die datenschutzkonforme Techniknutzung nicht dem Verhalten der Nutzer*innen überlassen bleiben, sondern sie muss durch geeignete technische und organisatorische Maßnahmen bereits während der Technikentwicklung sichergestellt werden. Welche genauen Anforderungen hieraus folgen, ergibt sich aus der DSGVO allerdings nicht. Aufgrund vielfältiger technischer Anwendungen ist der Erfolg dieses Transparenzansatzes entscheidend davon abhängig, ob es gelingt, das Postulat datenschutzfreundlicher Technikgestaltung durch geeignete Verfahrensvorkehrungen in die Technikentwicklung zu integrieren.

Zwei sich ergänzende Aspekte lassen sich unterscheiden: transparente Technikgestaltung und Transparenz durch Technikgestaltung. *Transparente Technikgestaltung* erscheint auf den ersten Blick schwierig, da Technik im Zeitalter der Digitalisierung komplex und für Nutzer*innen daher nur schwer nachvollziehbar ist (ausführlich hierzu Kornwachs 2010). Zudem haben viele Technikentwickler*innen kein gesteigertes Interesse daran, ihre Technik transparent zu gestalten, da dies Nachahmungen erleichtern und die Kommerzialisierung neuer Produkte erschweren könnte. Auch unter Wahrung dieser Interessen gibt es indes

vielfältige Möglichkeiten, den Nutzer*innen Informationen über technische Abläufe bereitzustellen, damit sie darüber entscheiden können, inwieweit sie eine Technik nutzen möchten. Zudem kann das technische Design dazu beitragen, durch die Vermeidung von Überkomplexität Transparenz zu sichern. Noch weiter geht die Transparenz, wenn technische Informationen gezielt offengelegt werden, damit Nutzer*innen und andere Entwickler*innen damit weiterarbeiten können, wie dies etwa bei *Open Source*-Software der Fall ist (vgl. Kornwachs 2010, S. 304ff.).

Transparenz durch Technikgestaltung bewegt sich auf der Ebene der Anwendung selbst. Technische Anwendungen können so ausgestaltet werden, dass Nutzer*innen nachvollziehen können, welche Daten über sie erhoben werden und für welche Zwecke diese verarbeitet werden. Dies kann insbesondere durch Hard- und Softwareeinstellungen erreicht werden, die sicherstellen, dass Nutzer*innen sich jederzeit über Verarbeitungszwecke, Löschfristen usw. informieren können (näher hierzu Aden & Fährmann 2020).

3. Transparenzdefizite und emanzipatorische Potenziale von Transparenz - Schlussfolgerungen und Ausblick

Dieser Beitrag hat gezeigt, dass die DSGVO den Stellenwert von Transparenz als Datenschutzprinzip gestärkt hat. Die Transparenzregeln in der DSGVO sind gegenüber der vorherigen Rechtslage unter manchen Aspekten ausgebaut und konkretisiert worden. Jedoch führen diese Regelungen allein noch nicht automatisch zu transparenteren Abläufen der Datenverarbeitung.

Unter den Rahmenbedingungen der Digitalisierung stößt die Herstellung von Transparenz auf strukturelle Grenzen. Selbst wer alle Datenverarbeitungsvorgänge nachvollziehen möchte, wäre damit angesichts immer größer werdender Datenmengen und komplexer technischer Abläufe strukturell überfordert (hierzu auch Roßnagel 2019, Art. 5 Rn. 61f.). Hinzu kommt, dass Unternehmen und auch manche Behörden weiterhin ein großes Interesse haben, Datenbestände möglichst ungestört auswerten zu können. Transparenz kann zu kritischen Nachfragen führen und ist für diejenigen, die sie gewährleisten müssen, mit Aufwand verbunden und daher potenziell lästig. Die Verfügungsgewalt über Wissen führt zu asymmetrischen Machtbeziehungen (näher hierzu Aden 2004, S. 62ff.; Tzanou 2017, S. 26) – Wissen ist eine Grundlage für Macht, Nichtwissen trägt zu Ohnmacht bei. Aufgrund gegenläufiger Interessen dürfte es somit kaum möglich sein, die emanzipatorischen Potenziale von Transparenz auf freiwilliger Basis zu entfalten. Vielmehr sind verbindliche staatliche Regeln erforderlich. Informationsfreiheit und Transparenz als Datenschutzgrundsatz sollten dabei in ihren Verknüpfungen gemeinsam weiterentwickelt werden (vgl. hierzu auch Brink 2017).

Für die Transparenzregeln der DSGVO sind folglich weitere Konkretisierungen erforderlich, die verbindliche Transparenzstandards etablieren. Hierzu können Vorgaben des Europäischen Datenschutzausschusses (zu dessen Rolle Dix in diesem Heft) ebenso beitragen wie konkretisierende Gesetzgebung und die zukünftige Rechtsprechung des Gerichtshofs der EU (EuGH).

Prof. Dr. Hartmut Aden ist Jurist und Politikwissenschaftler. Er ist Professor für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft an der Hochschule für Wirtschaft und Recht Berlin,

zugleich Vizepräsident für Forschung (seit April 2020) und Mitglied des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS Berlin). Webseite: www.hwr-berlin.de/prof/hartmut-aden.

Literaturverzeichnis

Aden, H. (2004): Herrschaft und Wissen. In: ders. (Hg.), *Herrschaftstheorien und Herrschaftsphänomene*, Wiesbaden: Verlag für Sozialwissenschaften, S. 55-70.

Aden, H. & Fährmann, J. (2020): Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie, *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 29 (3), S. 24-29.

Aden, H., Fährmann, J. & Bosch, A. (2020): Intransparente Polizeikontrollen – rechtliche Pflichten und technische Möglichkeiten für mehr Transparenz. In: Hunold, D./Ruch, A. (Hg.): *Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts.* Wiesbaden: Springer VS, S. 3-22.

Article 29 Data Protection Working Party (2018a): Guidelines on Personal data breach notification under Regulation 2016/679. WP250rev.01. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (aufgerufen am 15.12.2020).

Article 29 Data Protection Working Party (2018b): Guidelines on transparency under Regulation 2016/679. wp260rev.01, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (aufgerufen am 15.12.2020).

August, V. & Osrecki, F. (2019): Transparency Imperatives: Results and Frontiers of Social Science Research. In: dies. (Hg.), *Der Transparenz-Imperativ*. Wiesbaden: Springer VS, S. 1-34.

Brink, S. (2017): Anregungen für künftige Transparenzgesetze. In: Hill, H., Kugelmann, D. & Martini, M., *Perspektiven der digitalen Lebenswelt*. Baden-Baden: Nomos, S. 89-98.

De Fine Licht, J., Naurin, D., Esaiasson, P. & Gilljam, M. (2014): When Does Transparency Generate Legitimacy? Experimenting on a Context-Bound Relationship, *Governance*, 27(1), S. 111-134.

Dix, A. (2019): Kommentierung zu Art. 12 bis 20 und zu Art. 33 und 34 DSGVO. In: Simitis, S., Hornung, G. & Spiecker genannt Döhmann, I. (Hg.) *Datenschutzrecht.* Baden-Baden: Nomos, S. 617-694 und S. 835-848.

Engelbrecht, K. (2019) Meldepflicht und Benachrichtigungspflicht des Verantwortlichen. Erläuterungen zu Art. 33 und 34 Datenschutz-Grundverordnung. Orientierungshilfe. München: Der Bayerische Landesbeauftragte für den Datenschutz, https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf (aufgerufen am 15.12.2020).

Europäische Kommission (2020): Mitteilung […]: Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, Brüssel: COM(2020)264 final.

Fährmann, J., Aden, H. & Bosch, A. (2020): Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzesänderung, *Kriminologisches Journal*, 52 (2), S. 135–148.

Friedewald, M. (2017): Datenschutz-Folgenabschätzung. In: *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 26 (1–2), S. 66–71.

Grunwald, A. (2010) Transparenz in der Technikfolgenabschätzung. Konzeptionelle Erwartungen und ihre Einlösung. In: Jansen, S.A., Schröter, E., Stehr, N. & Wallner, C. (Hg.): *Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen.* Wiesbaden: VS Verlag für Sozialwissenschaften, S. 309-329.

Johannes, P.C. & Weinhold, R. (2018): Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze. Baden-Baden: Nomos.

Kornwachs, K. C. (2010): Transparenz in der Technik. In: Jansen, S.A., Schröter, E., Stehr, N. & Wallner, C. (Hg.): *Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen.* Wiesbaden: VS Verlag für Sozialwissenschaften, S. 292-308.

Kugelmann, D. (2001): Die informatorische Rechtsstellung des Bürgers. Tübingen: Mohr Siebeck.

Lederer, B. (2015): Open Data. Informationsöffentlichkeit unter dem Grundgesetz. Berlin: Duncker & Humblot.

Roßnagel, A. (2019): Kommentierung zu Art. 5 DSGVO, in: In: Simitis, S., Hornung, G. & Spiecker genannt Döhmann, I. (Hg.) *Datenschutzrecht.* Baden-Baden: Nomos, S. 363-399.

Roßnagel, A. & Geminn, C. (2020) Datenschutz-Grundverordnung verbessern. Änderungsvorschläge aus Verbrauchersicht. Baden-Baden: Nomos

Tzanou, M. (2017): The Fundamental Right to Data Protection. Oxford and Portland: Hart Publishing.

---

https://www.humanistische-union.de/publikationen/vorgaenge/231-232/publikation/transparenz-als-datenschutzprinzip-ansaetze-und-umsetzungsprobleme/
Abgerufen am: 24.06.2024