ZUM VERHÄLTNIS VON RECHT UND TECHNIK: RECHTSDURCHSETZUNG DURCH TECHNIKGESTALTUNG

Walter Hötzendorfer

Abstract: Eine der vielen verschiedenen Beziehungen zwischen Recht und Technik besteht darin, dass Rechtsdurchsetzung auch durch Technikgestaltung erfolgen kann. Nach Erörterung der Grundlagen dieses Prinzips werden dessen spezifische Ausgestaltung als Privacy by Design und konkrete Normierung in Art. 25 DSGVO näher beleuchtet. Ein Fortschritt in der praktischen Umsetzung von Privacy by Design soll mit der hier postulierten Unterscheidung der sich aus Art. 25 DSGVO ergebenden Anforderungen in konkrete Standardanforderungen und abstrakte Anforderungen erreicht werden. Schließlich wird auch ein besonderer Fokus auf die Bedeutung von Privacy by Architecture gelegt.

Inhaltsverzeichnis

A. EINLEITUNG

Recht und Technik, das sind die beiden großen Themenfelder, die Erich Schweighofer miteinander verbindet. Es gibt viele ganz unterschiedliche Verbindungen von Recht und Technik. Die beiden Verbindungen von Recht und Technik, die das Schaffen von Erich Schweighofer bestimmen, sind einerseits die Rechtsinformatik (im engeren Sinne) als Anwendung von Methoden der Informatik auf juristische Gegenstände mit dem Ziel, Rechtswissenschaft und Rechtspraxis mit eben diesen Methoden zu unterstützen,[1] die von der Rechtsinformation bis hin zu AI and Law reicht und auch das umfasst, was in jüngerer Zeit als Legal Tech bezeichnet wird, und andererseits das IT-Recht. Das IT-Recht, verstanden als die Regulierung der Gestaltung und Anwendung informationstechnischer Entwicklungen in unserer Gesellschaft, soll in diesem und im nachfolgenden Beitrag von Christof TSCHOHL im Vordergrund stehen. Die beiden Beiträge bauen aufeinander auf und fügen den beiden genannten Varianten der Verbindung von Recht und Technik noch eine dritte hinzu: Technik kann auch zur Umsetzung und Durchsetzung des Rechts, insbesondere auch der Menschenrechte, eingesetzt werden. Der hier postulierte Regulierungsansatz kann somit als Rechtsdurchsetzung durch Technikgestaltung bezeichnet werden.

Die Beschäftigung mit diesem Thema im vorliegenden Beitrag ist in drei Teile gegliedert. Im ersten Teil werden die Grundlagen der Rechtsdurchsetzung durch Technikgestaltung erläutert. Der zweite Teil enthält aktuelle Erkenntnisse des Autors zu Privacy by Design, der in der Praxis wohl bedeutendsten Ausprägung des Prinzips der Rechtsdurchsetzung durch Technikgestaltung. Im dritten Teil des Beitrags wird der Fokus auf die Architekturgestaltung von Systemen gelegt. Der nachfolgende Beitrag von TSCHOHL betrachtet das Prinzip der Rechtsdurchsetzung durch Technikgestaltung auf einer grundrechtlichen und rechtsstaatlichen Ebene und befasst sich mit der Rechtsstaatlichkeit durch Technikgestaltung.

[1] Frei nach HERBERGER, Ein akademisch-traumatischer Streit um die Rechtsinformatik, in diesem Band.

B. GRUNDLAGEN

Ausgangspunkt des Prinzips der Rechtsdurchsetzung durch Technikgestaltung ist die Erkenntnis, dass das Recht nur einer von mehreren Faktoren ist, die das menschliche Handeln von außen determinieren. Andere solche Faktoren sind gesellschaftliche Einflüsse und moralische Werte sowie insbesondere die vorhandenen faktischen Handlungsmöglichkeiten, die ihrerseits häufig durch die technischen Gegebenheiten determiniert werden.[2]

In diesem Sinne beschreibt LESSIG in seiner New Chicago School Theory vier Faktoren der Regulierung (modalities of regulation): das Recht, soziale Normen, den Markt und die physische Architektur.[3] Software wird von LESSIG dabei als eine Form der Architektur betrachtet, da sie dieselbe Wirkung wie Architektur habe.[4] Software, allgemeiner: Technikgestaltung, physische Architektur und auch der Markt entfalten eine unmittelbare regulatorische Wirkung. Sie geben faktische Handlungsmöglichkeiten vor. Die Einhaltung dieser Vorgaben ist nicht vom Willen des Betroffenen beeinflussbar; andere Handlungsmöglichkeiten als die faktisch vorgegebenen kann er nicht ergreifen. Dies kann als präventive Regulierung bezeichnet werden. Rechtsnormen und soziale Normen entfalten eine mittelbare regulatorische Wirkung. Sie belegen Handlungen mit Konsequenzen. Der Betroffene kann sich aber auch entscheiden, andere als die von diesen Normen als zulässig vorgegebenen Handlungsmöglichkeiten zu ergreifen. Dies kann als repressive Regulierung bezeichnet werden.[5]

Bei LESSIG findet sich auch die Erkenntnis, dass das Recht die Besonderheit aufweist, auf die anderen drei Faktoren, die sozialen Normen, den Markt und die physische Architektur, einwirken zu können.[6] In Anlehnung an REIDENBERG[7] ist daher festzuhalten,

---

2 Siehe dazu bereits ausführlich HÖTZENDORFER, Datenschutz und Privacy by Design im Identitätsmanagement, Österreichische Computer Gesellschaft (OCG), Wien 2016, S. 74 ff. m.w.N.

3 LESSIG, CODE version 2.0, Basic Books, Cambridge, MA 2006, S. 121 ff. Die New Chicago School Theory wurde von LESSIG erstmals publiziert in LESSIG, The New Chicago School, The Journal of Legal Studies 1998, 661–691.

4. LESSIG, CODE version 2.0, Basic Books, Cambridge, MA 2006, S. 124 f.

5 Vgl. HÖTZENDORFER in Knyrim, DatKomm Art. 25 Rz. 3.

6 LESSIG, CODE version 2.0, S. 130.

7 REIDENBERG, Lex informatica: the formulation of information policy rules through technology, Texas Law Review 1998, 553–593.

dass politische Vorgaben im Kontext der Technikregulierung auf drei verschiedene Arten umgesetzt werden können: Erstens können politische Vorgaben direkt durch Technikgestaltung umgesetzt werden. DE HERT und THUMFART sprechen in Bezug auf die faktische Dominanz der großen Digitalkonzerne von «de facto regulation by technical design».[8] Dies soll hier als Regulierung durch Technikgestaltung bezeichnet werden. Anzumerken ist, dass Technik auch eine derartige faktische regulatorische Wirkung entfalten kann, ohne dass dies intendiert ist.[9]

Zweitens können politische Vorgaben durch Rechtsnormen umgesetzt werden, die sich an die Gestalter der Technik richten und diese verpflichten, die politischen Vorgaben in der Technikgestaltung umzusetzen. Dies ist es, was im Zentrum des vorliegenden Beitrags steht und als Rechtsdurchsetzung durch Technikgestaltung bezeichnet wird. Es handelt sich dabei aus der Perspektive der Endanwender der Technik um präventive Regulierung.

Drittens können politische Vorgaben durch Rechtsnormen umgesetzt werden, die sich an die Nutzer der Technik richten, und diesen vorgeben, die Technik auf bestimmte Weise zu nutzen oder nicht zu nutzen. Hierbei handelt es sich um «klassische» repressive Regulierung.

Repressive Regulierung eignet sich durchaus gut für die Regulierung zahlreicher Lebensbereiche, vor allem weil diese eine gewisse Flexibilität zulässt und unserer liberalen Gesellschafts- und Rechtsordnung entspricht. Was wie ein Rechtsverstoß aussieht, muss nicht in jedem Fall ein Rechtsverstoß sein, man denke nur an den einfachen Fall der Notwehr oder an Schrankenregelungen im Urheberecht.[10] Ein rechtstaatliches Verfahren zur Durchsetzung repressiver Regulierung ist sehr gut dazu geeignet, solche Ausnahmeregelungen und Nuancierungen zu berücksichtigen.

---

8 DE HERT/THUMFART, The Microsoft Ireland case, the CLOUD Act and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question regulatory state monopolies, in diesem Band.

9 Vgl. das erste Kranzberg'sche Gesetz (KRANZBERG, Technology and History: «Kranzberg's Laws», Technology and Culture 1986, 544–560).

10 Vgl. BERNZEN/KEHRBERGER, Rechtsdurchsetzung durch Informationstechnik, RW 2019, 374–407, S. 389.

Die Notwendigkeit eines solchen Verfahrens der Durchsetzung post factum, an dessen Ende Konsequenzen gesetzt werden, ist aber zugleich die wesentliche Schwäche der repressiven Regulierung. Es kann besonders schwierig sein, dass es zu so einem Verfahren faktisch überhaupt kommt. Dies beginnt bereits mit der Notwendigkeit, dass die Nichteinhaltung zunächst von jemandem festgestellt werden muss, der ein Verfahren anstrengt, und das Verfahren bedeutet einen zeitlichen und häufig auch einen finanziellen Aufwand. Dies ist ein Grund dafür, dass präventive Regulierung in bestimmten Fällen besser geeignet sein kann, ein regulatorisches Ziel zu erreichen, als repressive Regulierung. Im Datenschutz ist dies besonders ausgeprägt der Fall, weil es hier besonders schwierig ist, auf Verstöße überhaupt aufmerksam zu werden, diese nachzuweisen und Ansprüche gegen den Verantwortlichen durchzusetzen, der überdies in vielen Fällen nicht der österreichischen Jurisdiktion unterliegt. Hinzu kommt, dass in vielen Fällen der durch die Nichteinhaltung eingetretene Schaden nicht mehr rückgängig gemacht werden kann. Einem unbefugten Datenverwender oder gar der Öffentlichkeit kann die Kenntnis einer Information naturgemäß nicht mehr entzogen werden, was eine Wiedergutmachung häufig unmöglich macht.[11]

Zur Durchsetzung des Datenschutzrechts und allgemein auch zur Verhinderung der Überschreitung staatlicher Befugnisse[12] erscheint daher präventive Regulierung als ein geeignetes und angemesses Mittel, um diesen und ähnlichen Defiziten zu begegnen. Damit soll jedoch nicht schlechthin der Verbreitung des Prinzips einer Rechtsdurchsetzung durch Informationstechnik das Wort geredet werden. Beispiele dafür reichen von Uploadfiltern im Urheberrecht bis hin zu Fahrzeugen, die das Überschreiten der zulässigen Höchstgeschwindigkeit überhaupt nicht mehr zulassen; solche Maßnahmen bringen in der Regel erhebliche Risiken, Fehleranfälligkeit und andere Schwächen mit sich, die es abzuwägen gilt, wenn in einem bestimmten Anwendungsgebiet über Rechtsdurchsetzung durch Informationstechnik nachgedacht wird.[13] Schließlich ist

---

11 Vgl. HÖTZENDORFER, Datenschutz und Privacy by Design im Identitätsmanagement, Österreichische Computer Gesellschaft (OCG), Wien 2016, S. 77.

12 Siehe dazu TSCHOHL, Zum Verhältnis von Recht und Technik: Rechtsstaatlichkeit durch Technikgestaltung, in diesem Band.

13 Siehe dazu ausführlich BERNZEN/KEHRBERGER, Rechtsdurchsetzung durch Informationstechnik, RW 2019, 374–407.

noch anzumerken, dass Regulierung durch technische Maßnahmen i.d.R. Software beinhaltet und damit auch die der Software inhärenten Eigenschaften der potenziellen Instabilität, Fehlerhaftigkeit und Manipulierbarkeit.[14]

C. PRIVACY BY DESIGN

Eine bedeutende, weil tatsächlich normativ verankerte Ausprägung des Prinzips der Rechtsdurchsetzung durch Technikgestaltung ist Privacy by Design. Privacy by Design bedeutet, Datenschutz bei der Gestaltung eines Systems von Beginn an zu berücksichtigen, sodass die Verwirklichung der Datenschutzgrundsätze bereits im System angelegt ist, und eine nicht intendierte/nicht zweckkonforme Verwendung des Systems durch technische und organisatorische Maßnahmen möglichst von vornherein zu verhindern. Die Umsetzung von Privacy by Design bedeutet somit, bereits von Beginn des Systementwicklungsprozesses an, einige wenige Grundprinzipien des Datenschutzes durch Einsatz geeigneter Design-Strategien, Design Patterns und Privacy-enhancing Technologies (PETs) unter Einbeziehung von Wissen über häufige Fehler, die Rechtslage, aktuelle Bedrohungen und Angriffsmethoden etc. umzusetzen. Dies wirkt sich sowohl auf die Architektur als auch auf viele Detailaspekte der Gestaltung von Systemen aus. Eine zentrale Maßnahme zur Umsetzung von Privacy by Design ist konsequente Datenminimierung. Dies betrifft mehrere Dimensionen: Art der Daten, Umfang der Daten, Speicherdauer, Kreis der Zugriffsberechtigten etc. Ein weiterer wesentlicher Aspekt der Umsetzung ist es, Privacy by Design als Denkweise («Mindset»), d.h. als grundlegende Einstellung zum Umgang mit personenbezogenen Daten zu betrachten und möglichst weit unter jenen zu verbreiten, die mit personenbezogenen Daten arbeiten oder Systeme entwickeln, deren Zweck die Verarbeitung personenbezogener Daten ist.[15]

---

[14] Vgl. GRIMMELMANN, Regulation by Software, Yale Law School Student Prize Papers, Paper 46, 2005, abrufbar unter http://digitalcommons.law.yale.edu/ylsspps_papers/46 (alle URLs in diesem Beitrag wurden zuletzt abgerufen am 21.11.2019), S. 1742 ff.

[15] Vgl. HÖTZENDORFER, Datenschutz und Privacy by Design im Identitätsmanagement, Österreichische Computer Gesellschaft (OCG), Wien 2016, S. 84 ff. m.w.N.

An dieser Stelle sei angemerkt, dass natürlich unterschieden werden kann zwischen Privacy by Design als programmatischem datenschutzpolitischem Konzept, wie es von CAVOUKIAN[16] und später auch von der Internationalen Konferenz der Datenschutzbeauftragten in einer Resolution[17] postuliert wurde, und Data Protection by Design/Datenschutz durch Technikgestaltung, wie es Art. 25 DSGVO als rechtliche Verpflichtung vorsieht.[18] Diese Unterscheidung wird im Folgenden jedoch nicht getroffen, denn der Begriff Privacy by Design bezieht sich hier sowohl auf Art. 25 DSGVO sowie dessen Umsetzung als auch auf das zugrundeliegende datenschutzpolitische Konzept, soweit sich dieses in Art. 25 DSGVO manifestiert.

II. Art. 25 DSGVO im Kontext der DSGVO

Die Einbettung von Art. 25 DSGVO in der Systematik der DSGVO kann wie folgt beschrieben werden: Aufbauend auf den Datenschutzgrundsätzen des Art. 5 DSGVO verpflichten drei Bestimmungen, Art. 24, 25 und 32 DSGVO, den Verantwortlichen – unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen –, geeignete technische und organisatorische Maßnahmen zu treffen, um eine DSGVO-konforme Datenverarbeitung sicherzustellen.

16 CAVOUKIAN, Privacy by Design: The 7 Foundational Principles, 2009, abrufbar unter https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

17 Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel, 27-29 October, 2010, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf.

18 Vgl. JASMONTAITE/KAMARA/ZANFIR-FORTUNA/LEUCCI, Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR, EDPL, 2018, 168–189, S. 172.

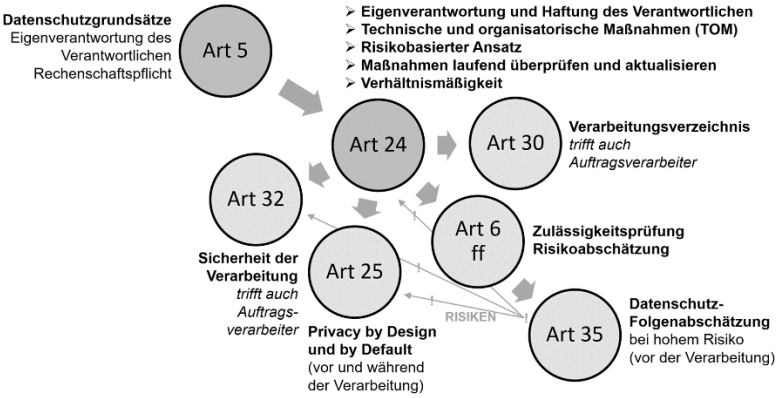

Abbildung 1. Einbettung von Art. 25 DSGVO in der Systematik der DSGVO

Um diese Bestimmungen erfüllen zu können, insbesondere um abwägen zu können, welche Maßnahmen angemessen sind, müssen die Risiken jeder einzelnen Verarbeitungstätigkeit abgeschätzt werden. Aus praktischer Sicht erfolgt diese Risikoabschätzung im Zuge der Prüfung der Zulässigkeit einer Verarbeitungstätigkeit, die wiederum mit der Eintragung der Verarbeitungstätigkeit in das Verarbeitungsverzeichnis nach Art. 30 DSGVO einhergehen sollte. Wenn diese Risikoabschätzung ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen ergibt, sieht Art. 35 DSGVO die besondere Pflicht zu einer systematischen Risikoabschätzung nach den Vorgaben des Art. 35 Abs. 7 DSGVO vor (Datenschutz-Folgenabschätzung). Die festgestellten Risiken fließen wiederum ein in die Abwägung betreffend die Angemessenheit von Maßnahmen zur Erfüllung der Art. 24, 25 und 32 DSGVO.

Diese drei Bestimmungen überschneiden einander in ihrem materiellen Gehalt, sodass i.d.R. nicht festgelegt werden kann, ob eine bestimmte Maßnahme aufgrund von Art. 24, 25 oder 32 DSGVO zu treffen ist, oder aufgrund von zwei oder allen drei dieser Bestimmungen. Allerdings sieht nur Art. 25 DSGVO in Abs. 1 die Verpflichtung vor, entsprechende Maßnahmen nicht nur «zum Zeitpunkt der eigentlichen Verarbeitung» zu treffen, sondern auch bereits «zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung».

Auch ein Blick auf die in ErwGr. 78 Satz 3 der DSGVO beispielhaft aufgezählten Maßnahmen zur Umsetzung von Art. 25 DSGVO lässt erkennen, dass der Regelungsgehalt des Art. 25 DSGVO sich mit jenem anderer Bestimmungen der DSGVO deutlich überschneidet, denn alle dort genannten Maßnahmen sind – sofern jeweils angemessen – auch aufgrund anderer Bestimmungen der DSGVO verpflichtend.[19]

Beides spricht dafür, dass entsprechend den oben erläuterten Grundlagen des Prinzips Privacy by Design das Treffen von Maßnahmen «zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung», also in der Technikgestaltung, den Kern des exklusiven Regelungsgehalts von Art. 25 Abs. 1 DSGVO ausmacht. Für BAUMGARTNER und GAUSLING besteht in Bezug auf den Zeitpunkt der eigentlichen Verarbeitung überhaupt kein eigenständiger Regelungsgehalt von Art. 25 Abs. 1 DSGVO, weil ab diesem Zeitpunkt insbesondere Art. 24 Abs. 1 und Art. 32 Abs. 1 im Ergebnis dieselben Verpflichtungen normieren.[20] Dazu ist anzumerken, dass nur Verstöße gegen Art. 25 und Art. 32 DSGVO gem. Art. 83 Abs. 4 lit. a DSGVO unmittelbar mit Geldbußen bedroht sind, nicht jedoch Verstöße gegen Art. 24 DSGVO.

Aus der Perspektive der Rechtsdurchsetzung ist anzumerken, dass naturgemäß auch eine auf präventive Regulierung abzielende Bestimmung wie Art. 25 DSGVO ihrerseits der Durchsetzung auf repressivem Wege bedarf. Allerdings wird dies deswegen wesentlich erleichtert, weil Art. 25 DSGVO – wie letztlich die geamte Regelungssystematik der DSGVO – so ausgestaltet ist, dass der Verantwortliche dazu in der Lage sein muss, den Nachweis zu erbringen, dass zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung eine Beurteilung stattgefunden hat, welche technischen und organisatorischen Maßnahmen aufgrund dieser Bestimmung zu treffen sind.[21]

Eine bemerkenswerte Entscheidung zu Art. 25 DSGVO ist der – noch nicht rechtskräftige – Bußgeldbescheid der Berliner Datenschutzbehörde in Höhe von rund 14,5 Millionen Euro gegen die Deutsche Wohnen SE wegen Verstoßes gegen Art. 25 Abs. 1

---

19 Vgl. FEILER/FORGO, DSGVO, Art. 25 Anm. 3.

20 BAUMGARTNER/GAUSLING, ZD 2017, 308, S. 310; ebenso BAUMGARTNER in Ehmann/Selmayr, DSGVO, Art. 25 Rz. 12.

21 So ausdrücklich auch der Europäische Datenschutzausschuss, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, vom 13. November 2019, S. 10.

DSGVO sowie Art. 5 DSGVO, u.a. weil diese für die Speicherung personenbezogener Daten von Mieterinnen und Mietern ein Archivsystem verwendete, das keine Möglichkeit vorsah, nicht mehr erforderliche Daten zu entfernen.[22]

III. Umsetzung von Privacy by Design in der Praxis

Im Hinblick auf die praktische Umsetzung sollte Privacy by Design als Prozess betrachtet werden.[23] Das gilt sowohl für das Datenschutzmanagement innerhalb einer Organisation als auch für die Entwicklung datenverarbeitender Systeme. Jedoch ist dies nicht im Sinne eines standardisierten Prozesses oder Vorgehensmodells zu verstehen. Es ist wohl nicht möglich, ein allgemeingültiges Vorgehensmodell zu entwickeln, dessen Umsetzung, insbesondere auch durch Personen, die keine Datenschutzexperten sind, gewissermaßen automatisch zu einem mit Art. 25 DSGVO konformen System führen würde. Vielmehr ist es stets erforderlich, auf die Gegebenheiten des jeweiligen Systems individuell einzugehen.

Das bedeutet jedoch nicht, dass Privacy by Design für jedes zu entwicklende System etwas gänzlich anderes bedeuten würde. Vielmehr kann unterschieden werden in einerseits weitgehend allgemeingültige und andererseits individuelle, systemspezifische Anforderungen, die sich aus Art. 25 Abs. 1 DSGVO ergeben. Eine Standardisierung konkreter, unmittelbar umsetzbarer Privacy-by-Design-Anforderungen erscheint daher zumindest in gewissen Teilbereichen möglich.

---

22 Pressemitteilung der Berliner Beaftragten für Datenschutz und Informationsfreiheit vom 5. November 2019, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf. Anzumerken ist, dass bisher seit Ingeltungtreten der DSGVO in Europa viel mehr Verstöße gegen Art. 32 DSGVO als gegen Art. 25 DSGVO gehandet wurden (siehe z.B. GDPR Enforcement Tracker, https://www.enforcementtracker.com).

23 Vgl. ENISA, Privacy and Data Protection by Design – from policy to engineering, abrufbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, S. 3 sowie MORTON/SASSE, Privacy is a process, not a PET, Proceedings of the 2012 workshop on New security paradigms - NSPW 12, ACM Press, New York 2012, S. 87.

Somit ergibt sich folgender dualer Ansatz zur Umsetzung von Privacy by Design bei der Entwicklung von datenverarbeitenden Systemen, wie in Abb. 2 dargestellt:[24] Die Privacy-by-Design-Anforderungen, die sich aus Art. 25 DSGVO ergeben, können unterschieden werden in konkrete Standardanforderungen, die in einer standardisierten Form umgesetzt werden können, und abstrakte Anforderungen, die einer individuellen, systemspezifischen Umsetzung bedürfen.

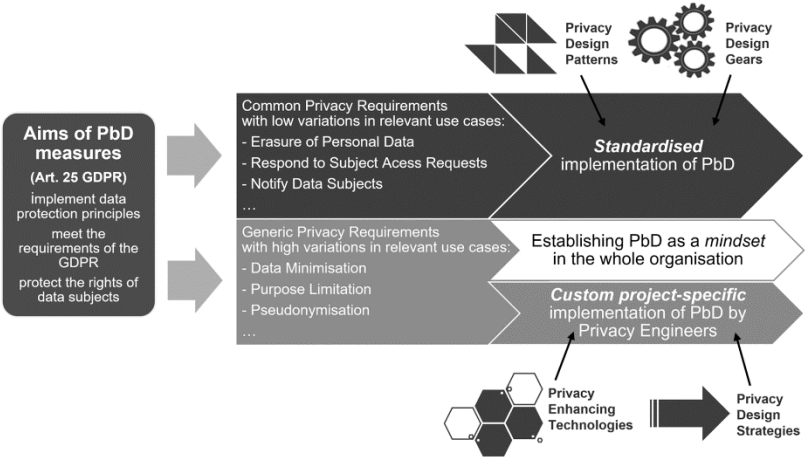

Abbildung 2. Die aus Art. 25 DSGVO abzuleitenden Anforderungen an die Technikgestaltung können unterschieden werden in konkrete Standardardanforderungen (oben), die standardisiert umgesetzt werden können, und abstrakte Anforderungen (unten).[25]

[24] Dank gebührt an dieser Stelle Ernst O. WILHELM, mit dem ich diesen dualen Ansatz gemeinsam entwickelt habe.

[25] Diese Grafik wurde erstmals präsentiert in einem gemeinsamen Vortrag von Walter HÖTZENDORFER und Ernst O. WILHELM mit dem Titel «Privacy by Design: Eine Konkretisierung» beim Internationalen Rechtsinformatik-Symposion IRIS2018.

1. Konkrete Standardanforderungen

Die konkreten Standardanforderungen sind jene, die nahezu jedes datenverarbeitende System in ähnlicher Form erfüllen muss. Es handelt sich dabei um detaillierte Anforderungen, die nicht oder nur geringfügig vom Kontext abhängen und daher keiner weiteren systemspezfischen Konkretisierung mehr bedürfen. Es ist somit auch keine besondere Datenschutz-Expertise erforderlich, um diese Anforderungen umzusetzen. Sie eignen sich daher zur Umsetzung mittels Checklisten oder in ähnlicher standardisierter Form. Solche konkreten Standardanforderungen ergeben sich insbesondere aus den Betroffenenrechten nach Art. 12 ff. DSGVO. Beispielsweise ist es eine konkrete Standardanforderung an jedes System, das zur Verarbeitung von personenbezogenen Daten entwickelt wird, dass es möglich sein muss, personenbezogene Daten zu löschen.[26] Dabei handelt es sich um eine unmittelbar umsetzbare Anforderung, die für alle solchen Systeme in gleicher Weise besteht und direkt aus Art. 5 Abs. 1 lit. b und Art. 17 DSGVO abgeleitet weren kann.

Diese und einige weitere konkrete Standardardanforderungen sind in der folgenden Tabelle beschrieben:

Bestimmung	**Bezeichnung**	**Abgeleitete Anforderunge**
Art. 5 Abs. 1 lit. b und Art. 17 DSGVO	Recht auf Löschung	Es muss möglich sein, personenbezogene Daten zu löschen.
Art. 18 DSGVO	Recht auf Einschränkung der Verarbeitung	Es muss möglich sein, den Zugriff auf personenbezogene Daten einzuschränken, sodass diese gespeichert bleiben, wie sie sind, jedoch nicht mehr für die vorgesehenen Verarbeitungszwecke, sondern nur noch im Rahmen von Art. 18 DSGVO

[26] Vgl. die oben bereits erwähnte diesbezüglich von der Berliner Datenschutzberhörde verhängte Geldbuße (Pressemitteilung der Berliner Beaftragten für Datenschutz und Informationsfreiheit vom 5. November 2019, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf).

		verarbeitet oder eingesehen werden können.
Art. 20 DSGVO	Recht auf Datenübertragbarkeit	Wenn die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht, müssen die personenbezogenen Daten, die dem Verantwortlichen vom Betroffenen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format exportiert werden können.
Art. 15 Abs. 1 lit. h i.V.m. Art. 22 DSGVO	Recht auf Auskunft (über Algorithmen)	Die «Logik» eines Algorithmus, der eine Entscheidung trifft, die für eine natürliche Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, muss erklärt werden können.

Tabelle 1. Nicht erschöpfende Liste konkreter, unmittelbar umsetzbarer Standardanforderungen der DSGVO

Darüber hinaus könnte man neben diesen zwingenden konkreten Standardanforderungen weitere herausarbeiten, die zwar nicht zwingend sind, aber die Umsetzung der DSGVO erheblich erleichtern. Ein Beispiel für eine solche Anforderung ist die Möglichkeit, die Herkunft von Daten direkt in Verbindung mit diesen Daten speichern zu können, um darüber gem. Art. 15 Abs. 1 lit. g DSGVO Auskunft geben zu können. Eine solche Anforderung ist sehr nahe am Konzept der Privacy Design Patterns, wie sie in Abb. 2 in Bezug auf die konkreten Standardanforderungen dargestellt sind. Design Patterns sind bewährte Entwurfsmuster zur Lösung wiederkehrender Probleme, die i.d.R. in einer bestimmten strukturierten Form beschrieben sind.[27]

[27] Eine Sammlung von Privacy Design Patterns findet sich unter https://www.privacypatterns.org.

Einen Schritt weiter kann man noch mit der Definition konkreter Funktionalitäten zur ganz oder teilweise automatisierten Erfüllung bestimmter Anforderungen der DSGVO gehen. Diese werden in Abb. 2 als «Privacy Design Gears» bezeichnet.[28] Beispiele dafür sind ein Portal, bei dem Betroffene direkt durch Abruf personenbezogener Daten ihre Rechte auf Auskunft und/oder Datenübertragbarkeit ausüben können, oder automatisierte Trigger, die melden, wenn bestimmte Daten gelöscht werden müssen oder wenn bestimmte Vorgänge eine Informationspflicht nach Art. 13 oder 14 DSGVO auslösen.

2. Abstrakte Anforderungen

Demgegenüber sind die abstrakten Anforderungen solche, die nicht unmittelbar umsetzbar sind, weil ihre Umsetzung stark vom jeweiligen zu entwickelnden System abhängt. Was eine solche Anforderung, wie z.B. Datenminimierung oder Pseudonymisierung, für ein bestimmtes System bedeutet, hängt sehr stark von den Umständen des Einzelfalles ab. Es bedarf daher einer systemspezifischen Konkretisierung dieser Anforderungen, bevor diese umgesetzt werden können. Dabei kann auf Privacy Enhancing Technologies[29] zurückgegriffen und als Zwischenschritte in dieser Konkretisierung können die von HOEPMAN entwickelten Privacy Design Strategies[30] herangezogen werden. Eine standardisierte Checkliste zur unmittelbaren Umsetzung der abstrakten Anforderungen erscheint jedoch nicht denkbar.

Es ist daher unerlässlich, dass jene Personen, die an der Entwicklung eines Systems beteiligt sind, den Datenschutz mitbedenken und in der systemspezifischen Konkretisierung der abstrakten Anforderungen geschult sind. Privacy by Design sollte daher als Denkweise («Mindset») in der Organisation etabliert werden. Zusätzlich können in der

---

28 Idee und Begriff stammen von Ernst O. WILHELM, präsentiert im gemeinsamen Vortrag mit dem Titel «Privacy by Design: Eine Konkretisierung» beim Internationalen Rechtsinformatik-Symposion IRIS2018.

29 Siehe dazu sogleich.

30 HOEPMAN, Privacy Design Strategies (The Little Blue Book), abrufbar unter https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf; siehe auch ENISA, Privacy and Data Protection by Design – from policy to engineering, abrufbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

Entwicklung Experten hinzugezogen werden, um die systemspezifische Konkretisierung der abstrakten Anforderungen zu erarbeiten. In einem agilen Softwareentwicklungsprozess kann dies z.B. durch einen Pool von Privacy Enigneers erfolgen, aus dem je nach Bedarf die einzelnen (Scrum-)Teams beschickt werden.[31] In kleineren Strukturen kann dies im einfachsten Fall auch ein einzelner Experte sein. Es ist aber m.E. unerlässlich, dass sich die Gestalter von Technologie selbst mit den einschlägigen Datenschutzanforderungen und letztlich mit den gesellschaftlichen Auswirkungen ihrer Entwicklungen befassen.

D. PRIVACY BY ARCHITECTURE

Nach diesen Detailerwägungen gilt es, nochmals einen Schritt zurückzutreten, um einen gesamtheitlichen Blick auf die Ebene der Praxis der Technikgestaltung im Kontext des Datenschutzes zu werfen. Es soll betont werden, dass Privacy by Design nicht nur in vielen Detailfragen der Technikgestaltung beachtet und umgesetzt werden muss, sondern dass dies bereits bei grundlegenden Fragen der Systemgestaltung beginnt.

Die Gestaltung technischer Systeme sollte sich daher bereits am Anfang mit der Frage befassen, wie man bereits durch die Gestaltung der Systemarchitektur Datenschutzanforderungen und -grundsätze erfüllen kann und dadurch bei der näheren Ausgestaltung des Systems auftretende Datenschutzfragen und -probleme vermeiden kann. Dies kann als Privacy by Architecture bezeichnet werden.[32]

Ein Beispiel dafür ist die Architektur des Systems, das derzeit unter Beteiligung des Autors im H2020-Projekt FeatureCloud entwickelt wird.[33] Es handelt sich dabei um ein System zur medizinischen Forschung in großen Mengen von Patientendaten mittels Machine

---

31 Siehe dazu TERBU/HÖTZENDORFER/LEITNER/BONITZ/VOGL/ZEHETBAUER, Privacy and Security by Design im agilen Softwareentwicklungsprozess. In: Schweighofer, E., Kummer, F., Hötzendorfer, W., Borges, G. (Hrsg.): Netzwerke. Tagungsband des 19. Internationalen Rechtsinformatik Symposions IRIS 2016, Österreichische Computer Gesellschaft (OCG), Wien, 2016, 457–464.

32 Der Begriff stammt aus SPIEKERMANN/CRANOR, Engineering Privacy, IEEE Transactions on Software Engineering 2009, 67–82, wird allerdings dort etwas anders verwendet.

33 Siehe unter https://featurecloud.eu.

Learning. Wie in Abb. 3 ersichtlich, ist das System nach dem Grundsatz Privacy by Architecture so aufgebaut, dass die Patientendaten für Forschungszwecke nicht in eine große zentrale Datenbank kopiert werden müssen, sondern in den Krankenhäusern und Forschungseinrichtungen, in denen sie anfallen, verbleiben können. Die Machine-Learning-Algorithmen werden so gestaltet, dass sie dort dezentral auf die Daten angewendet werden können und nur aggregierte Ergebnisse («Features») an eine zentrale Stelle geschickt werden, die in der Folge ein Gesamtergebnis errechnet. Dieser Ansatz fügt zwar in Bezug auf das Machine Learning eine neue Komplexitätsebene hinzu, löst aber zugleich eine Vielzahl rechtlicher und faktischer Probleme hinsichtlich der Verarbeitung der Daten zu Forschungszwecken und soll somit letztlich zur faktischen Verfügbarkeit einer vielfach größeren Datenmenge für die medizinische Forschung führen.

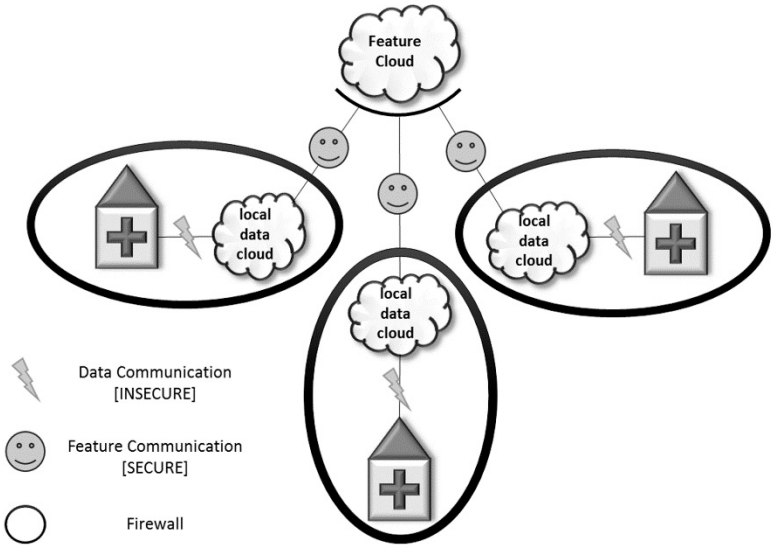

Abbildung 3. Privacy by Architecture am Beispiel des Forschungsprojekts FeatureCloud

Privacy by Architecture ist somit als fundamentaler Bestandteil von Privacy by Design zu betrachten, der hier jedoch separat betont werden soll. Wie das Beispiel der FeatureCloud-Architektur zeigt, lassen sich mit einzelnen Designentscheidungen

betreffend die Architektur eines Systems weitreichende Auswirkungen auf den Datenschutz erzielen. Damit ergibt sich die nachfolgend dargestellte «Qualitätspyramide» von Paradigmen zur Umsetzung von Datenschutzanforderungen in der Technikgestaltung.

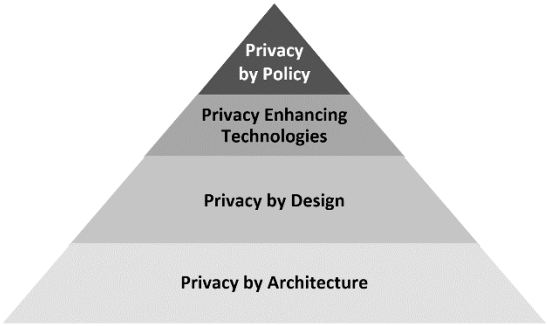

Abbildung 4. «Qualitätspyramide» von Paradigmen zur Umsetzung von Datenschutzanforderungen in der Technikgestaltung

Das Fundament bildet Privacy by Architecture. Bei der Gestaltung der Systemarchitektur fallen die Grundsatzentscheidungen hinsichtlich der Datenschutzkonformität und Datenschutzfreundlichkeit eines Systems. Entscheidungen auf dieser Ebene haben – wie allgemein in der Technikgestaltung – naturgemäß die weitreichendsten Auswirkungen. Danach folgen auf der nächsten Ebene im Systementwicklungsprozess alle weiteren Privacy-by-Design-Entscheidungen bis hin zur einzelnen Zeile Code, über die ein Entwickler i.d.R. alleine und ad hoc entscheidet. Zur Umsetzung der Datenschutzanforderungen können Privacy Enhancing Technologies (PETs) herangezogen werden. Diese sollten jedoch – wie hier gezeigt – auf dem Fundament von Privacy by Architecture und by Design bereits im Technikgestaltungsprozess systematisch in die Systeme integriert werden, denn es ist nicht wirksam, Systeme nachträglich um PETs zu ergänzen.[34] Sind die Systeme schließlich diesem Prozess folgend nach den Vorgaben von Art. 25 DSGVO gestaltet, können im Betrieb jene Anforderungen umgesetzt werden, die

[34] Vgl. ENISA, Privacy and Data Protection by Design – from policy to engineering, abrufbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design, S. 5.

nicht unmittelbar in der Technikgestaltung umgesetzt werden konnten. Dies ist die Domäne von Privacy by Policy, einem Konzept, dass sich weitgehend auf Information und informationelle Selbstbestimmung des Betroffenen beschränkt.[35] Wie gezeigt wurde, ergibt sich ein effektiver Datenschutz jedoch nur dann, wenn die darunterliegenden Systeme bereits datenschutzkonform gestaltet wurden und insbesondere auch das Prinzip Privacy by Default berücksichtigt wurde, damit auch jene Betroffenen adäquat geschützt sind, die nicht aktiv von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen, wofür es mannigfache Gründe geben kann.

E. SCHLUSSFOLGERUNGEN

Recht und Technik, die beiden großen Themenfelder, die Erich Schweighofer miteinander verbindet, stehen in vielfacher Weise miteinander in Beziehung. Im vorliegenden Beitrag wurde der Fokus auf die Umsetzung und Durchsetzung des Rechts mittels Technik gelegt. Zunächst wurde zwischen repressiver und präventiver Regulierung unterschieden, und Rechtsdurchsetzung durch Technikgestaltung als Mittel der präventiven Regulierung beschrieben. Dabei wurde betont, dass Rechtsdurchsetzung durch Technikgestaltung nur in bestimmten Fällen herangezogen werden sollte, und keineswegs alle Probleme durch präventive Regulierung gelöst werden können, geschweige denn sollten.

Wie gezeigt wurde, weist das Datenschutzrecht Besonderheiten auf, die den Einsatz des Prinzips der Rechtsdurchsetzung durch Technikgestaltung in diesem Rechtsgebiet rechtfertigen. Normativ ist dies nunmehr mit Art. 25 DSGVO umgesetzt. Ein Ziel des vorliegenden Beitrags ist es, mit der in Kapitel C postulierten Unterscheidung der sich aus Art. 25 DSGVO ergebenden Anforderungen in konkrete Standardanforderungen und abstrakten Anforderungen einen Fortschritt in der praktischen Umsetzung von Privacy by Design zu erzielen. Einige konkrete Standardanforderungen, die sich aus der DSGVO für alle Systeme, die personenbezogene Daten verarbeiten, in gleicher Weise ergeben und unmittelbar umsetzbar sind, wurden herausgearbeitet. Hier ergibt sich ein

[35] Vgl. SPIEKERMANN/CRANOR, Engineering Privacy, IEEE Transactions on Software Engineering 2009, 67–82, S. 73.

Ansatz, die Forschung fortzusetzen, um weitere konkrete Standardanforderungen der DSGVO herauszuarbeiten.

Aus der Perspektive der Rechtsdurchsetzung wurde betont, dass naturgemäß auch eine auf präventive Regulierung abzielende Bestimmung wie Art. 25 DSGVO ihrerseits der Durchsetzung auf repressivem Wege bedarf. Soweit ersichtlich gibt es seit Wirksamwerden der DSGVO erst wenige Entscheidungen zu Art. 25 DSGVO, eine bedeutsame Entscheidung ist allerdings nunmehr ergangen und konnte somit in diesem Beitrag aufgegriffen werden.

Die Beziehung zwischen Recht und Technik, die in diesem Beitrag beleuchtet wurde, wird im nachfolgenden Beitrag von TSCHOHL weiter vertieft. Dieser betrachtet das Prinzip der Rechtsdurchsetzung durch Technikgestaltung auf einer grundrechtlichen und rechtsstaatlichen Ebene und befasst sich mit der Rechtsstaatlichkeit durch Technikgestaltung.