

Selbstbestimmung und Designdatenschutz

Der Trend im Datenschutzrecht bzw. im grundrechtlichen Informationsschutz zugunsten der Persönlichkeit bewegt sich in Richtung «X by design» – wobei X für verschiedene Ansätze zum Schutz der Persönlichkeit stehen kann. Der Schutz der Datensubjekte soll durch die Vorgabe von Designparametern vermehrt in Informationssysteme und -artefakte eingebaut, und deren Nutzer durch den gezielten Einsatz von Heuristiken zur Minderung ihres Risikos bewegt werden. In diesem Beitrag werden die Konzepte des selbstbestimmten und des designbasierten Datenschutzes kurz zusammengefasst, einander gegenübergestellt, und der Übergang von einem Regelungskonzept zum anderen untersucht. Anhand der Darstellung dieses Zusammenspiels soll aufgezeigt werden, was wir durch Design gewinnen können, wo Gefahren für die Rechte der Betroffenen lauern, und was dabei für die rechtsstaatlich geschützten Freiheiten auf dem Spiel steht.

Philip Glass, 24. Februar 2019, www.datalaw.ch/datenschutz-selbstbestimmung-u-design/

Der vorliegende Beitrag bildete die Grundlage für meinen Vortrag zum selben Thema am Internationalen Rechtsinformatik Symposium IRIS 2019 in Salzburg (<https://www.univie.ac.at/RI/IRIS2019/>) und ist im Tagungsband sowie im Jusletter IT vom 21. Februar 2019 (<https://jusletter-it.weblaw.ch/issues/2019/IRIS.html>) veröffentlicht.

1. Selbstbestimmung als Grundwert des Datenschutzrechts

1.1. Willenserklärung und gesetzliche Bearbeitungsbefugnis

[1] Der bisher dominierende Ansatz im schweizerischen Recht ist jener des Datenschutzes mittels privatautonomer Vereinbarung von Datenbearbeitungsprozessen zwischen Privaten auf der einen, sowie auf gesetzlicher Erlaubnis basierte Bearbeitung von Personendaten durch öffentliche Organe auf der anderen Seite.¹

[2] Das Konzept basiert zunächst auf dem Grundsatz der Privatautonomie, wie er im ZGB und OR verankert ist, schlussendlich aber auf dem Schutz gegen Verletzung der Persönlichkeit i.S.v. Art. 28 ZGB².³ Auf der Ebene des Schutzes verfassungsrechtlicher Individualrechte, deren Schutz der Staat im Schweizerischen Recht gemäss Art. 35 Abs. 3 BV⁴ sowohl im öffentlichen als auch im privaten Bereich soweit wie möglich zur Geltung bringen muss,⁵ bedeutet Datenschutz per Willenserklärung einen Datenschutz mittels Umsetzung des Grundrechts auf informationelle Selbstbestimmung durch die Betroffenen im Einzelfall. Die Einwilligung in bzw. Erlaubnis von Datenbearbeitungen – sei es individuell durch

¹ Vgl. dazu Art. 13 Abs. 1 DSG (Bundesgesetz über den Datenschutz vom 19. Januar 1992 [DSG; SR. 235.1]): «Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.»

² Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (ZGB; SR 210).

³ Vgl. die Botschaft des Bundesrates zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003 BBl 2003 2101, 2127.

⁴ Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

⁵ BIAGGINI, BV Kommentar: Bundesverfassung der Schweizerischen Eidgenossenschaft, Orell Füssli, Zürich 2017, Art. 35 N. 4, 7 u. 21.

Zustimmung oder kollektiv durch Gesetz – rechtfertigt damit verbundene Persönlichkeitsverletzung und lässt diese Bearbeitungen als rechtmässig erscheinen.⁶ Das Erfordernis einer Zustimmung löst aus Sicht des Datenschutzrechts indes ein statisches Moment aus, wenn solche Zustimmungen als formale Bearbeitungsvoraussetzungen oder auch rechtliche Bearbeitungsgrundlagen behandelt werden, ohne eine Anleitung zur Schonung⁷ der bedrohten Rechte zu geben. Mit Unterschrift gilt die betreffende Systemarchitektur und gelten die betreffenden Datenbearbeitungen als genehmigt ohne weiteren Anreiz zur kontinuierlichen Optimierung derselben

1.2. Die Idee eines quasi Eigentums an eigenen Personendaten

[3] Ein Konzept zur Stärkung der Rechtsposition von Datensubjekten ist die Idee, Daten als quasi Eigentum von Personen zu qualifizieren, derentwegen die Daten als Personendaten gelten.⁸ Im Vordergrund steht jene Person, von der die aus den Daten formbare Information stammt, und auf welche sie nach wie vor verweist – das Datensubjekt. Denkbar sind indes auch Datenrechte von Personen, auf welche aggregierte Daten angewendet werden, indem ihnen die daraus verfügbare Information aufgrund bestimmter Merkmale als Pseudopersonendatum⁹ zugewiesen wird – eher Datenobjekte. Es ist sehr fraglich, ob es sinnvoll wäre, bei Zurechnung von Information die betreffenden Daten als quasi Eigentum der individualisierten Person zu betrachten.

[4] Abgesehen von den praktischen Problemen, die mit der Natur von Daten, Information und deren Zusammenspiel zu tun haben, spricht m.E. insbesondere die rechtstypische Verfügungsmacht des Eigentumsrechts gegen dieses Konzept. THOUVENIN weist richtigerweise darauf hin, dass Eigentum an Personendaten durch Verkauf übertragen und auf den Erwerber übergehen und dieser dem Datensubjekt nun die Nutzung der vormals eigenen Personendaten verbieten könnte.¹⁰ Der Einzelne wäre in der Lage, seine Persönlichkeitsrechte komplett zu verkaufen, was dem persönlichkeitsrechtlichen Verbot der übermässigen Bindung zuwiderlaufen würde.

[5] Entscheidend – und allgemein anerkannt – erscheint mir, dass der Personenbezug von Daten bzw. deren Informationsgehalt bezüglich einer bestimmten Person eine rechtlich abgesicherte Gestaltungsmacht bezüglich der Bearbeitungsparameter für diese Daten auslösen kann. Diese Gestaltungsmacht ergibt sich aus der Persönlichkeit dieser Person und ist im Persönlichkeitsrecht verankert. Es geht also nicht darum, Datenträger einzufordern und wegzuschliessen, sondern es wird das Recht eingeräumt, soweit wie möglich in privatautonomer Weise über Art, Umfang, Zeitpunkt und Zweck der Bearbeitung eigener Personendaten mitzubestimmen, mithin darum, berechnete Erwartungen an die kontextgerechte Vertraulichkeit der übermittelten Information geltend zu machen.¹¹ Aufgrund ihrer Wurzeln im Persönlichkeitsrecht kann man sich dieser Gestaltungsmacht nicht vollends entäussern. Entsprechend

⁶ Deutlich Art. 13 Abs. 1 DSGVO.

⁷ Zum Konzept der Schonung siehe DRUEY, Der Kodex des Gesprächs – Was die Sprechaktlehre dem Juristen zu sagen hat, Nomos, Baden-Baden 2015, S. 402 f.

⁸ Ausführlich FRÜH, Roboter und Privacy: Informationsrechtliche Herausforderungen datenbasierter Systeme, Aktuelle Juristische Praxis (AJP), 2/2017, 147 ff.; THOUVENIN, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, Schweizerische Juristenzeitung (SJZ) 113/2017, S. 21.

⁹ Daten, die über Wahrscheinlichkeit einer Person zugerechnet werden; dazu GLASS, Bearbeitung, S. 198.

¹⁰ THOUVENIN, *ibid.* S. 31.

¹¹ NISSENBAUM, Privacy in Context – Technology, Policy, and the Integrity of Social Life, Stanford Law Books, Stanford California, 2010, S. 231: «a right to live in a world in which our expectations about the flow of personal information are, for the most part, met».

ist auf der anderen Seite der Gesetzgeber gefordert einzuschreiten, wenn diese Gestaltungsmacht aufgrund struktureller Umstände im Einzelfall vom einzelnen Individuum nicht wirksam umgesetzt werden kann.

1.3. Der Gefahr der Unterwanderung der Selbstbestimmung durch privatautonome Ansätze

[6] Der Nachteil der autonomen Sicherung von Privatheit durch selbstbestimmte Ermächtigung zur Datenbearbeitung ist, dass sie regelmässig gerade dort nicht funktioniert, wo die Risiken für die Betroffenen besonders gross sind.¹² Ironischerweise – denn das Datenschutzrecht entsprang gerade dem Bedürfnis, die zunehmend unübersichtliche und komplexe Natur von Informationssystemen und deren Nutzung rechtlich einzufangen und dem Individuum Instrumente zur Verteidigung seiner Selbstwahrnehmung und -darstellung in die Hand zu geben.

[7] Tatsächlich aber ist die Verwirklichung der Privatautonomie in vielen Bereichen des Datenschutzrechts darauf beschränkt, selber bestimmen zu können, welchen Anbieter man wählt (dies gilt oft auch für kleinere bis mittelgrosse Gemeinden sowie für spezialisierte Verwaltungsstellen). Insbesondere aber in Massengeschäften werden sowohl akzessorische als auch weiterführende Datenbearbeitungen (z.B. zu Marketingzwecken, für soziologische Experimente, Verkauf an Werbekunden) als nicht verhandelbare Bestandteile der allgemeinen Geschäftsbedingungen (AGB) in die betreffenden Verträge integriert und dies oftmals nur andeutungsweise. Die Wirkung eines solchen Datenschutzes erschöpft sich regelmässig darin, dem Kunden einen minimalen Standard zu garantieren, dessen Inhalt mehr durch Marktstrukturen als durch rechtliche Vorgaben oder gar seine eigenen Vorstellungen zum Schutz seiner digitalen Persönlichkeit bestimmt wird.¹³

[8] Damit einhergehend eröffnet sich für die (privaten wie öffentlich-rechtlichen) Datenbearbeiter ein rechtlich weit offenes Feld für die technologische Steuerung der Nutzer.¹⁴ Das Recht greift frühestens dann, wenn eine Datenschutzverletzung erfolgt ist; es handelt sich demnach um eine nachträgliche Steuerung, deren Effektivität insofern unsicher ist, als sie nur wirken kann, wenn geklagt wird. Zudem wirkt eine Steuerung über Einwilligung nicht gegenüber Dritten (z.B. Cyberstalking, gezielte Desinformation) und kann im Gegenteil die Haftung für schädliche Dritteinwirkung einschränken, wenn eine solche Einschränkung vertraglich gültig vereinbart wurde.

1.4. Zusammenfassung

[9] Im Wesentlichen basieren datenschutzrechtlich motivierte Einwilligungsarchitekturen auf der Idee des Rechtes auf informationelle Selbstbestimmung und sollen eine Umsetzung dieses Rechts durch

¹² HARTZOG, *Privacy's Blueprint – The Battle to Control the Design of New Technologies*, Harvard University Press 2018, S. 56 ff. spricht für das US-amerikanische Recht von einer *design gap* der datenschutzrelevanten Klagen.

¹³ BAERISWYL, *Neuer Datenschutz für die digitale Welt – Ein wirksames Datenschutzkonzept muss die tatsächlichen Risiken für die Privatheit minimieren können*, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2011.1, S. 7, spricht in diesem Zusammenhang bereits 2011 von einer «faktischen Aufhebung der Datenschutzrechte»; HARTZOG, *Privacy's Blueprint*, S. 62 ff.

¹⁴ HOFFMANN-RIEM, *Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht*, *Archiv des öffentlichen Rechts (AöR)* 142 1/2017, S. 23; HARTZOG, *Privacy's Blueprint*, S. 57.

Kontrolle über die Bearbeitung bzw. Nutzung «eigener» Personendaten bewirken. Die Kontrolle wirkt also über die rechtliche Verfügungsmacht bezüglich der Art und Weise sowie Zweck der Nutzung von persönlichen Informationen durch bestimmte Dritte. Es handelt sich um ein einfach verständliches Konzept, das aus dem zivilrechtlichen Persönlichkeitsrecht übernommen wurde. Die Grundannahmen des Konzepts zeigen sich indes zunehmend als nicht zutreffend. Es eröffnet einen grossen Spielraum für Datenbearbeiter, der nachträglich nur in Fällen der offensichtlichen Persönlichkeitsverletzung – wenn die Zustimmung beispielsweise als erzwungen (Monopolproblem) oder sittenwidrig im Sinne des ZGB erscheint – rechtlich eingeschränkt werden kann. Dadurch wird ein Risiko der Aushebelung von Rechtsschutz durch Einwilligung sowie auch der «Erosion von Nutzerautonomie»¹⁵ gefördert.

[10] Insgesamt deutet vieles darauf hin, dass die selbstbestimmte, gewillkürte Kontrolle durch Einwilligung in die Bearbeitung von Personendaten im privaten Recht, wie im öffentlichen Recht, ihre Funktion, Persönlichkeitsverletzungen zu verhindern, nicht oder nur ungenügend erfüllt.¹⁶ Vielmehr ist sie aufgrund der wirtschaftlichen, politischen, technischen und informationellen Kräfteverhältnisse zwischen den Akteuren oftmals nicht geeignet, eine tatsächliche Kontroll- und Entscheidungsfunktion hinsichtlich der Verwirklichung von informationeller Selbstbestimmung wahrzunehmen.

2. Designdatenschutz

2.1. Privacy by design und andere Designansätze

[11] Designdatenschutz geht davon aus, dass die Persönlichkeit von Datensubjekten und -objekten in vielen Bereichen besser geschützt werden kann, wenn die zugrundeliegenden Informationssysteme mit Blick auf die Ermöglichung und Verwirklichung von Privatheit ausgestaltet sind. Dabei nutzen design-basierte Datenschutzansätze die Eigenschaft von Code, als gewillkürte Gesetzmässigkeit zu funktionieren und so Werte zu transportieren. Von entscheidender Bedeutung ist dabei die Einsicht, dass codierte Architekturen und Algorithmen immer Werte transportieren.¹⁷ Neben der Datenbearbeitung an sich treten nun die technischen Bedingungen der Datenbearbeitung in den Fokus rechtlicher Beurteilung. Diese Bedingungen sollen, verkörpert durch das jeweilige Informationssystem, in Kombination mit dessen Anwendungsumgebung den Spielraum für die Nutzung von Personendaten möglichst auf die rechtlich zulässigen Kontextbezüge reduzieren.¹⁸ Durch Designdatenschutz lassen sich Risiken für die Rechte der Betroffenen stabilisieren, indem Entscheidungsspielräume von Datenbearbeitern, die in der Regel ausserhalb des Einflussbereichs der Datensubjekte liegen, rechtlich vordefiniert und technisch eingeschränkt werden.

[12] Die Schweizer Lehre stützt sich in Zusammenhang mit design-orientiertem Datenschutz auf das

¹⁵ HOFFMANN-RIEM, Verhaltenssteuerung, S. 21.

¹⁶ Dazu auch BAERISWYL, Neuer Datenschutz, S. 8.

¹⁷ LESSIG, Code Version 2.0, 2006, S. 6: «we can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground»; HILDEBRANDT, Algorithmic Regulation and the Rule of Law, Phil.Trans. R. Soc. A 376: 2017035, 2018, <http://dx.doi.org/10.1098/rsta.2017.0355>, S. 7.

¹⁸ Vgl. HARASGAMA/TAMÒ, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: Weber/Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Schulthess, Zürich/Basel/Genf 2014, S. 131.

Konzept *privacy by design*^{19, 20}, das mittlerweile Eingang in Art. 25 DSGVO gefunden hat²¹ und für die Schweiz ebenso als Doppelpinzip (by design und default) im revidierten DSG des Bundes aufgenommen werden soll.²² Das Konzept stammt von ANN CAVOUKIAN und besteht aus sieben Prinzipien. Demnach ist Datenschutz ein proaktives Konzept, das dem Leitmotiv *privacy by default* folgt, in Informationssysteme eingebaut ist (*embedded privacy*) und, auf win-win-Situationen zwischen vermeintlich divergierenden Interessen ausgerichtet, über den gesamten Lebenszyklus von Information wirksam, für alle Beteiligten transparent erfolgt und stets Nutzer-zentriert umgesetzt wird.

[13] Die Grundidee eines integrierten, durch das System selbst verkörperten Datenschutzes wurde in verschiedenerlei Hinsicht aufgenommen und für ähnliche Rechts- und Designprobleme fruchtbar gemacht. Eine allgemeinere Methode der wertorientierten Technikgestaltung etwa bezeichnet der Ansatz *value sensitive design*²³ oder auch *design for value*²⁴. Es handelt sich um eine Methode, welche konzeptuelle, empirische, und technische Untersuchungen zu einem umfassenden Werkzeug zur Folgeabschätzung im Hinblick auf die künftige Verwirklichung von (moralischen) Werten bündelt.²⁵ Zentral ist stets die bereits im Rahmen von *privacy by design* hervorgestrichene proaktive Vorgehensweise. Diese weiterentwickelten Konzepte gehen davon aus, dass die Werte, die zu beachten sind, nicht von vornherein feststehen, sondern im Verlauf der Ausarbeitung eines Projektes ermittelt und miteinander in Gleichklang gebracht werden müssen²⁶ – beispielsweise durch Diskurs bzw. *participative design*²⁷. Es handelt sich somit um prozedurale Theorien²⁸, die (auch) im Hinblick auf Datenschutz eingesetzt werden sollen, und die das Recht aufnehmen und umsetzen kann. Durch die Prozeduralisierung des

¹⁹ Zum Konzept siehe CAVOUKIAN, Privacy by design, The 7 Foundational Principles, revised version 2011; siehe zudem die aktualisierte tabellarische Übersicht bei TAMÖ-LARRIEUX, Designing for Privacy and its Legal Framework – Data Protection By Design and Default for the Internet of Things, Springer Nature, Cham 2018, S. 85; SCHAAR, Privacy by design, IDIS (2010) 3:267, <https://doi.org/10.1007/s12394-010-0055-x>; zur weiteren Entwicklung HARTZOG, Privacy's Blueprint, S. 179 ff.; HILDEBRANDT, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar Publishing Inc. 2015, S. 214 ff.: "legal protection by design"; GLASS, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz – Regelungs- und Begründungsstrategien des Datenschutzes mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Univ. Basel, Dike, Zürich/St. Gallen 2017, S. 197 ff.; neu nun auch *contestability by design* als Designparameter zur Sicherung von automatisierten Entscheidungssystemen bei ALMADA, Contesting Automated Decisions: Limits to the Right to Human Intervention in Automated Decision-Making, SSRN Electronic Journal (2018), 10.2139/ssrn.3264189, S. 11 f.

²⁰ BAERISWYL, Neuer Datenschutz, S. 7; GASSER, Perspectives on the Future of Digital Privacy, Zeitschrift für Schweizerisches Recht (ZSR) 2015 II 335, S. 378 ff.; HARASGAMA/TAMÖ, Smart Metering, S. 131 ff.

²¹ Dazu EDPS, Preliminary Opinion on privacy by design, Opinion 5/2018, 31 May 2018.

²² Botschaft des Bundesrates zum Entwurf eines revidierten Datenschutzgesetzes vom 15. September 2018, BBl 2017 6941, 7029; ebenso vorgesehen ist Datenschutz durch Risikofolgeabschätzungen.

²³ FRIEDMAN, Value-Sensitive Design: A Research Agenda for Information Technology – A Report on the May 20-21, 1999 Value-Sensitive Design Workshop, https://vsdesign.org/outreach/pdf/friedman99VSD_Research_Agenda.pdf; FRIEDMAN/KAHN JR./BORNING, Value Sensitive Design and Information Systems, in: Zang/ Galetta (Eds.), Human-Computer Interaction and Management Information Systems: Foundations, 2nd Ed. London New York 2015, S. 348 ff.

²⁴ VAN DEN HOVEN/VERMAAS/VAN DE POEL, Design for Values: An Introduction, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Dordrecht 2015, *passim*.

²⁵ FRIEDMAN/KAHN JR./BORNING, Value Sensitive Design and Information Systems, S. 351.

²⁶ Zur Debatte siehe DAVIS/NATHAN, Value Sensitive Design: Applications, Adaptations, and Critiques, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Dordrecht 2015, S. 20 ff.

²⁷ VAN DER VELDEN/MÖRTBERG, Participatory Design and Design for Values, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Dordrecht 2015, S. 41 ff.

²⁸ Zum Begriff TSCHENTSCHER, Prozedurale Theorien der Gerechtigkeit – Rationales Entscheiden, Diskursethik und prozedurales Recht, Nomos, Baden-Baden 2000, S. 132 ff.

Datenschutzrechts gewinnt dieses an Flexibilität. Der Einbezug der Datensubjekte (regelmässig vertreten durch die zuständigen Datenschutzbehörden) sowie weiterer Legitimationsquellen (Fachpersonen, NGOs, Kommissionen) kann auf diese Weise besser legitimierte informationstechnische Artefakte (Datenbanken, Zugriffsmatrixen, Userinterfaces) und Infrastrukturen hervorbringen.

[14] Gemeinsam ist den verschiedenen design-basierten Konzepten schliesslich, dass die Werte und ihre interdependente Gewichtung sowie das sich hieraus ergebende Wertungsmuster, das als Grundlage bzw. Zielwert für die funktionelle Ausrichtung eines Informationssystems dienen soll, innerhalb des Designprozesses offengelegt werden. Insgesamt eröffnet Designschutz die Möglichkeit einer rechtlich informierten Systemgestaltung, welche die Mitgestaltungs- und Begründungsrechte der Betroffenen integriert.

2.2. Datensicherheit als Designvorgabe

[15] Als bedeutender, wenn auch ambivalenter Designaspekt von Informationssystemen muss an dieser Stelle Datensicherheit aufgeführt werden.²⁹ Datensicherheit verfolgt das dreifache Ziel der Vertraulichkeit, Integrität und Verfügbarkeit von Daten – nicht aber das Ziel «Datenschutz».³⁰ Die genannten Ziele bilden die betriebliche Grundvoraussetzungen für die sinnvolle Nutzung – und damit intrinsische Schutzmotive – von Informationssystemen.

[16] Interessant ist in diesem Zusammenhang das Urteil vom 27. Februar 2008 des ersten Senats des deutschen Bundesverfassungsgerichts, in welchem das Gericht die beiden Aspekte der Datensicherheit und des Datenschutzes zu einem Recht auf Systemintegrität verknüpfte. Gemäss Urteil ist das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme subsidiär zur informationellen Selbstbestimmung «anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten».³¹ Die Verbindung der beiden Aspekte unter dem Blickwinkel des verfassungsrechtlichen allgemeinen Persönlichkeitsrechts zeigt deutlich auf, dass es sich um unterschiedliche Aspekte von Informationssystemen handelt, deren Ziele nicht automatisch deckungsgleich sind. Aus dieser Erkenntnis folgt, dass Datensicherheit als Systemkomponente ebenso für Datenschutzwerte ausgelegt werden muss wie das Informationssystem insgesamt – die Vorgabe privacy by design ist demnach auch für Datensicherheit zu beachten und durch deren Umsetzung nicht automatisch erfüllt.

[17] Die Ziele des Datenschutzes sind für Informationssysteme demnach stets extrinsische Integritätsmotive, d.h. sie verwirklichen sich ausserhalb des Informationssystems, namentlich im Schutz der Persönlichkeit von Personen, denen Daten bzw. Informationen zugeordnet werden, bestimmen indes die Gestaltung der Systemsicherheit bzw. den Bedeutungsgehalt der Systemintegrität mit.³² Datensicherheit ist damit eine wichtige Grundlage von Datenschutz, namentlich bildet sie die technische

²⁹ Siehe dazu die Hinweise auf die historische Entwicklung bei TAMÖ-LARRIEUX, Designing for Privacy, S. 84.

³⁰ Zur unterschiedlichen Zielrichtung GLASS, Bearbeitung, S. 138 f.

³¹ Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07; 1 BvR 595/07, Rz. 203.

³² Dazu GLASS, Singularisierung und Identifizierung, www.datalaw.ch, 27. Februar 2018, engl. Version: DOI: 10.5281/zenodo.1436396

Voraussetzung für die Durchsetzung von Datenschutzzielen.³³ Gleichwohl kann ein Informationssystem, das sämtlichen Anforderungen der Datensicherheit genügt, aus datenschutzrechtlicher Sicht Mängel aufweisen bzw. unnötige Risiken schaffen.³⁴

2.3. Die Ziele des Designdatenschutzes

[18] Für Datenschutz-orientiertes Design von Informationssystemen haben sich die Ziele in einem Rechtsstaat an den Grundprinzipien der Verfassung, insbesondere an den informationellen Aspekten der grundrechtlichen sowie der daraus fliessenden privatrechtlichen Persönlichkeitsrechte zu orientieren. Für die Schweiz zählen hierzu die Grundrechte insgesamt, insbesondere aber die informationelle Selbstbestimmung, die Meinungs- und Informationsfreiheit sowie die Kommunikationsgrundrechte.³⁵ Ebenso dazu gehören – vermittelt durch das Verwirklichungsgebot in Art. 35 BV – die privatrechtlichen Persönlichkeitsrechte, insbesondere auch die rechtsgeschäftliche Privatautonomie.³⁶ Das übergeordnete Ziel bildet die verfassungsrechtlich informierte Strukturierung von vernetzten Informationssystemen – mithin der technischen Umgebungsentelligenz (engl. *ambient intelligence*³⁷). Durch diese Strukturierung wird der von der Rechtsordnung gewährte Kontextrraum für die Bearbeitung von Personendaten abgesteckt.³⁸ Datenschutz wird insofern zu einem Umweltproblem in Bezug auf die Informationsumwelt bzw. die Infosphäre.³⁹ Das Problem verlagert sich von einer reinen Abwehr von ungewollter Datenbearbeitung hin zur gemeinsamen Gestaltung einer Autonomie-fördernden Informationsumwelt.

[19] Für das Datenschutzrecht ist somit von Bedeutung, dass Privacy stets nur ein Mittel zum Zweck der Verwirklichung von Autonomie, und diese wiederum die Grundlage für die Garantie der rechtlich geschützten Persönlichkeitsentfaltung und der Menschenwürde ist.⁴⁰ Entsprechend muss X by design verfassungsrechtlich interpretiert und beispielsweise in der Form von *legal protection by design*⁴¹ oder etwas abstrakter gefasst, *autonomy by design*⁴², als zentrales rechtsstaatliches Designprinzip für Informationssysteme verstanden werden.

³³ HARTZOG, Privacy's Blueprint, S. 104.

³⁴ So bereits WILDHABER, Informationssicherheit, S. 28: «Datensicherung ohne Datenschutz ist ohne weiteres möglich, Datenschutz ohne Datensicherung hingegen undenkbar».

³⁵ GLASS, Bearbeitung, S. 179 ff. m.w.H.

³⁶ Dazu GLASS, Die Schutzparameter des zivilrechtlichen und des verfassungsrechtlichen Persönlichkeitsrechts, www.datalaw.ch, 29. Mai 2018, engl. Version: DOI: 10.5281/zenodo.1436387.

³⁷ HOFFMANN-RIEM, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (Hrsg.), Big Data – regulative Herausforderungen, Baden-Baden 2018, S. 22 m.w.H.

³⁸ GLASS, Bearbeitung, S. 126 ff.

³⁹ Zum Begriff der Infosphäre FLORIDI, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford University Press 2014, S. 119.

⁴⁰ GLASS, Bearbeitung, S. 172.

⁴¹ HILDEBRANDT, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar, Cheltenham UK/Northampton MA 2015, S. 218.

⁴² GLASS, Bearbeitung, S. 197; FRIEDMAN, Introduction, in: Friedman (Ed.), Human Values and the Design of Computer Technology, CSLI Publications/Cambridge University Press 1997, S. 5: «At the same time, such systems can help users to realize their goals and intentions through their use of the technology – a human value which Nissenbaum and I [...] refer to as autonomy».

3. Der Mehrwert von Designdatenschutz

3.1. Legitimierung von Datenbearbeitungen von allgemeinem Interesse

[20] Der Mehrwert eines design-basierten Ansatzes liegt zunächst darin, dass auf diese Weise rechtliche Entscheidungsmacht von den beteiligten Parteien (Datensubjekte/-objekte und Datenbearbeiter) auf gesellschaftliche Entscheidungsstrukturen verlagert werden kann. Mit anderen Worten verwandelt der Übergang von einem privatautonomen zu einem design-orientierten Ansatz eine persönliche Frage in eine Frage der Gestaltung von Infrastruktur sowie der Gewichtung der damit verbundenen privaten und öffentlichen Interessen. Die wichtigsten Werturteile von gesamtgesellschaftlicher Bedeutung können so durch Verankerung im Recht und Übersetzung in Systemarchitekturen vorweggenommen werden. Zugleich bedingt die Aufgabe von konkreter Selbstbestimmung und Gestaltungsmacht den Aufbau von Vertrauen in die Legitimation und Funktion von Informationssystemen.⁴³

[21] Durch die Prozeduralisierung von Datenschutzstandards wird einerseits das einzelne Datensubjekt davon befreit, Formen der Datenbearbeitung zu rechtfertigen, die ein Ergebnis struktureller Phänomene darstellen und daher im Einzelfall selten individuell verhandelbar sind. Andererseits wird die Datenbearbeiterin von der rechts-ökologischen⁴⁴ Verantwortung entlastet, Bearbeitungsprozesse, die in ihrem Interesse liegen, gemeinwohlverträglich zu gestalten. Eine design-basierte Vorgehensweise ermöglicht mit anderen Worten die prozedurale, auf diskursive Abgleichung der gegenseitigen Interessen basierende stetige Weiterentwicklung der betreffenden Bearbeitungsprozesse über Zeit – und über die einzelnen Datenbearbeiter/-innen hinaus. Damit wandelt sich Datenschutzrecht von einer Frage des Erlaubens zu einer Frage des Gestaltens von Datenbearbeitungsprozessen unter ständigem Feedback sowohl der Gesellschaft als auch der Betroffenen, was eine transparente, fortlaufende Optimierung der Balance zwischen den beteiligten Werten bzw. Interessen ermöglicht.

3.2. Beförderung eines zyklischen Datenschutzverständnisses

[22] Als weiterer Vorteil führt der Design-Ansatz zudem weg von einem formalrechtlichen, statischen Datenschutz, der diskrete, in der Regel einmalig erfolgende Entscheidungen voraussetzt, hin zu einem materiell-rechtlichen, dynamischen Datenschutz. Dieser stützt sich auf fortlaufende, rechtlich angeleitete Risikobewertung und wird durch prozeduralisierende Rückbindung an rechtlich geschützte Interessen legitimiert. Ein solcher dynamischer Datenschutz erlaubt es insbesondere, die zeitliche Komponente zu berücksichtigen und damit die Bearbeitung und deren Auswirkungen im Rahmen von Risikobewertungen über den gesamten Lebenszyklus von Informationen und Daten hinweg zu begleiten und beurteilen. Dabei muss das Instrumentarium an die verschiedenen Phasen des Daten- und Informationszyklus angepasst werden.⁴⁵

[23] Für öffentlich-rechtliche Datenbearbeiter wird dadurch eine flexiblere Anwendung der

⁴³ CAVOUKIAN, Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D, IDIS (2010) 3: 247.

⁴⁴ DRUEY, Der Kodex des Gesprächs, S. 397 ff.

⁴⁵ TAMO-LARRIEUX, Designing for Privacy, S.149 ff.; EDPS, Preliminary Opinion, S. 15 f.

Datenschutz- und Sachgesetze unter Einbezug verschiedener Stakeholder ermöglicht, die darin münden kann, dass die Beurteilung von Projekten nicht so sehr von der Bestimmtheit der betreffenden Rechtsgrundlage abhängig ist, sondern vom Zusammenspiel der Legitimation dieser Rechtsgrundlage mit dem jeweiligen grundrechtlichen Risikoprofil eines Projekts über Zeit, verbunden mit den Massnahmen zur laufenden datenschutzrechtlichen Optimierung dieses Profils. Es bedeutet insbesondere auch, dass identifizierte Risiken für einen gewissen Zeitraum – beispielsweise im Rahmen eines Pilotprojektes – als Restrisiko akzeptiert werden können, wenn spezifische Massnahmen zur Risikominde- rung erst in absehbarer Zeit ausgereift bzw. verfügbar sind.

[24] Für privat handelnde Datenbearbeiterinnen eröffnet ein prozedurales Datenschutzverständnis zusätzlich die Möglichkeit eines öffentlich verhandelten, flexiblen rechtlichen Mindeststandards, der Raum lässt für eine strategische Differenzierung bzw. Abgrenzung gegenüber anderen Marktteilnehmern.

4. Die ambivalente Sicherung der Selbstbestimmung durch Design

[25] Bei der Einführung und Umsetzung von prozeduralen Datenschutzkonzepten darf jedoch nicht vergessen gehen, dass die Gestaltung von Informationssystemen und Interfaces mit Blick auf die Optimierung von Gemeinwohlinteressen (wie beispielsweise den Belangen des Datenschutzes) einen Eingriff in die Grund- bzw. Persönlichkeitsrechte aller Beteiligten darstellen und bis zu einer gesamtgesellschaftlichen Relativierung von zentralen Bestandteilen der bisherigen Verfassungsordnung führen kann.⁴⁶ Im Zuge der Umsetzung von Designschutz werden auf der einen Seite jene Parteien eingeschränkt, welche aufgrund der Macht- bzw. Marktverhältnisse die Systemarchitektur weitgehend ohne Konsultation von vertraglichen Gegenparteien festlegen könnten. Auf der anderen Seite hat die Optimierung des Nutzer- oder Kundenverhaltens durch die gezielte Ausnutzung von Heuristiken eine stark manipulative Komponente, auch wenn dies zum Wohl der Betroffenen geschieht. Es ist daher darauf zu achten, dass jene, deren Verhalten (hier: vermittelt durch Informationssysteme) geändert werden soll, soweit wie möglich «Autoren ihres eigenen Handelns» bleiben.⁴⁷ Für das Schweizer Recht bedeutet dies, dass solche Eingriffe rechtsstaatlich legitimiert erfolgen und die Persönlichkeit der Betroffenen respektieren müssen. Aufgrund ihrer Eingriffscharakteristik erscheint die Regelung von Designvorgaben für Informationssysteme durch den Staat daher nur dort legitim, wo dies in Ausübung von grundrechtlichen Schutzpflichten i.S.v. Art. 35 BV⁴⁸ in transparenter Weise erfolgt und verhältnismässig erscheint. Letzteres Kriterium verlangt zudem, dass staatliche Regelungen bei relativ geringer Grundrechtsbelastung erst subsidiär in Betracht gezogen werden sollten, während die Wahrung der Rechte der strukturell schwächeren Parteien zunächst in der Form einer Obliegenheit den strukturell stärkeren Vertragsparteien überbunden wird.⁴⁹

⁴⁶ HILDEBRANDT, Smart Technologies, S. 216, warnt, dass die unausweichliche Angleichung von Funktionsmechanismen des Rechts an die neue Informationsumgebung nicht die Substanz der bisherigen rechtlich geschützten Werteordnung erodieren dürfe.

⁴⁷ HILDEBRANDT, Algorithmic Regulation, S. 5; «treated as authors of their own actions».

⁴⁸ BIAGGINI, BV Kommentar, Art. 35 Rz. 7 m.w.H.

⁴⁹ GLASS, Schutzparameter, Rz. 18 m.w.H.

5. Abschliessende Bemerkungen

[26] Durch Designschutz verlagert sich die Entscheidungsbefugnis bezüglich Datenbearbeitungen zunehmend in die technische Sphäre. Als Folge treten Autonomie- und Vertrauensdefizite klarer zutage und müssen insbesondere durch die Rückkoppelung an kompatible rechtsstaatliche Legitimationsnetzwerke⁵⁰, die Verstärkung und Betonung der Informations- und Begründungspflichten bezüglich Daten, Zwecke, Modelle, Risikobewertungen, Output-Erwartungen sowie weitere Verwertung, aufzufangen sein. Besonders wertvoll wäre die Entwicklung einer rechtsstaatlich begleiteten Dialogkultur zwischen Datensubjekten und -objekten sowie Datenbearbeitern, die idealerweise in der Lage wäre, das ursprüngliche Versprechen des Datenschutzrechts als Instrument zur Verwirklichung von informationeller Selbstbestimmung und Autonomie plausibel einzulösen. Mit dieser Entwicklung einhergehend wandelt sich die Rolle der Datenschutzbehörden hin zu aufsichtsbefugten Dienstleistungsanbietern, die den Verwaltungsstellen bei der Gestaltung, Weiterentwicklung und fortlaufenden Integrierung ihrer Informationssysteme beratend zur Seite stehen und hierbei jeweils die Interessen jener vertreten, die sich nicht in geeigneter Weise in die Diskussion um die Funktionalität von Systemarchitekturen und Prozessabläufe einbringen können – der Allgemeinheit.

[27] Die legitimatorischen Grenzen des neuen technischen Datenschutzes sind noch nicht vollends erkennbar. Aus der grundrechtlichen Schutzrichtung von Designschutz kann man ableiten, dass sie entlang von Einzelfällen und typischen Fallgruppen verlaufen wird. Dies als grundrechtlich angeleitete Reaktion auf die Verwerfungen in der Informationslandschaft und Eintritt von entsprechenden Risikofolgen bei den Betroffenen. Erst aus der Praxis von Datenschutzbehörden und Gerichten wird sich mit der Zeit ein deutlicheres Bild davon ergeben, welche Designansätze unter welchen Umständen im Stande sind, die Persönlichkeitsrechte und Grundrechte der Betroffenen genügend zu schützen, ohne diese zu bevormunden. Umgekehrt wird sich auch zeigen, welche Formen der Datenbearbeitung typischerweise als übermässig bindend im Sinne des Zivilgesetzbuches bzw. als Verletzung von persönlichkeitsrechtlichen Kerngehalten der Verfassung gelten und zu vermeiden sind. Schliesslich wird die Erarbeitung und Verabschiedung von Designvorgaben als eine Form der Rechtsetzung bzw. -anwendung eng an die betreffende Gesetzgebungskompetenz gebunden sein und den Regeln über die Delegation dieser Kompetenzen unterstehen müssen.

6. Literatur

ALMADA MARCO, Contesting Automated Decisions: Limits to the Right to Human Intervention in Automated Decision-Making, SSRN Electronic Journal (2018), 10.2139/ssrn.3264189.

BAERISWYL BRUNO, Neuer Datenschutz für die digitale Welt – Ein wirksames Datenschutzkonzept muss die tatsächlichen Risiken für die Privatheit minimieren können, digma – Zeitschrift für Datenrecht und Informationssicherheit, 2011.1, S. 6–11.

BIAGGINI GIOVANNI, BV Kommentar: Bundesverfassung der Schweizerischen Eidgenossenschaft, Orell Füssli, Zürich 2017.

⁵⁰ HOFFMAN-RIEM, Innovation und Recht – Recht und Innovation, Recht im Ensemble seiner Kontexte, Mohr Siebeck, Tübingen 2016, S. 104 f.

CAVOUKIAN ANN, Privacy by Design, The 7 Foundational Principles, May 2010; <http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf> (aufgerufen am 6. Januar 2019).

CAVOUKIAN ANN, Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D, IDIS (2010) 3: 247.

DAVIS JANET/NATHAN LISA P., Value Sensitive Design: Applications, Adaptations, and Critiques, in: Van den Hoven/Vermaas/Van De Poel (Eds.), Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain, Springer, Dordrecht 2015.

DRUEY JEAN NICOLAS, Der Kodex des Gesprächs – Was die Sprechaktlehre dem Juristen zu sagen hat, Nomos, Baden-Baden 2015.

FLORIDI LUCIANO, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, Oxford University Press 2014.

FRIEDMAN BATYA, Introduction, in: Friedman (Ed.), Human Values and the Design of Computer Technology, CSLI Publications/Cambridge University Press 1997, S. 1–13.

FRIEDMAN BATYA, Value-Sensitive Design: A Research Agenda for Information Technology – A Report on the May 20–21, 1999 Value-Sensitive Design Workshop, August 23 1999; https://vsdesign.org/outreach/pdf/friedman99VSD_Research_Agenda.pdf (aufgerufen am 06. Januar 2019).

FRIEDMAN BATYA/KAHN JR. PETER H./BORNING ALAN, Value Sensitive Design and Information Systems, in: Zang/ Galetta (Eds.), Human-Computer Interaction and Management Information Systems: Foundations, 2nd Ed. M.E. Sharpe, London/New York 2015.

FRÜH ALFRED, Roboter und Privacy: Informationsrechtliche Herausforderungen datenbasierter Systeme, Aktuelle Juristische Praxis (AJP), 2/2017, S. 141–151.

GASSER URS, Perspectives on the Future of Digital Privacy, Zeitschrift für Schweizerisches Recht (ZSR) 2015 II 335–448.

GLASS PHILIP, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz – Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Univ. Basel, Dike, Zürich /St. Gallen 2017.

GLASS PHILIP, Die Schutzparameter des zivilrechtlichen und des verfassungsrechtlichen Persönlichkeitsrechts, www.datalaw.ch, 29. Mai 2018; engl. Version DOI: 10.5281/zenodo.1436387.

GLASS PHILIP, Singularisierung und Identifizierung, www.datalaw.ch, 27. Februar 2018; engl. Version DOI: 10.5281/zenodo.1436396.

HARASGAMA REHANA/TAMÒ AURELIA, Smart Metering und Privacy by Design im Big-Data-Zeitalter: Ein Blick in die Schweiz, in: Weber/Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Schulthess, Zürich/Basel/Genf 2014, S. 117–150.

HARTZOG WOODROW, Privacy's Blueprint – The Battle to Control the Design of New Technologies, Harvard University Press 2018.

- HILDEBRANDT MIREILLE, Algorithmic Regulation and the Rule of Law, *Phil. Trans. R. Soc. A* 376: 2017035.
- HILDEBRANDT MIREILLE, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar, Cheltenham UK/Northampton MA 2015.
- HOFFMAN-RIEM WOLFGANG, Innovation und Recht – Recht und Innovation, *Recht im Ensemble seiner Kontexte*, Mohr Siebeck, Tübingen 2016.
- HOFFMANN-RIEM WOLFGANG, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem (Hrsg.), *Big Data – regulative Herausforderungen*, Baden-Baden 2018, S. 11–80.
- HOFFMANN-RIEM WOLFGANG, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, *Archiv des öffentlichen Rechts (AöR)* 142 1/2017, S. 1–42.
- LESSIG LAWRENCE, *Code: And Other Laws of Cyberspace*, Version 2.0, Basic Books, New York 2006.
- NISSENBAUM HELEN, *Privacy in Context – Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford California 2010.
- SCHAAR PETER, Privacy by design, *IDIS* (2010) 3:267. DOI: 10.1007/s12394-010-0055-x.
- TAMÒ-LARRIEUX AURELIA, *Designing for Privacy and its Legal Framework – Data Protection By Design and Default for the Internet of Things*, Springer Nature, Cham 2018.
- THOUVENIN FLORENT, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, *Schweizerische Juristen-Zeitung (SJZ)* 113/2017, S. 21–32.
- TSCHENTSCHER AXEL, *Prozedurale Theorien der Gerechtigkeit – Rationales Entscheiden, Diskursethik und prozedurales Recht*, Nomos, Baden-Baden 2000.
- VAN DEN HOVEN JEROEN/VERMAAS PIETER E./VAN DE POEL IBO, Design for Values: An Introduction, in: Van den Hoven/Vermaas/Van De Poel (Eds.), *Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain*, Springer, Dordrecht 2015.
- VAN DER VELDEN MAJA/MÖRTBERG CHRISTINA, Participatory Design and Design for Values, in: Van den Hoven/Vermaas/Van De Poel (Eds.), *Handbook of Ethics, Values, and Technological Design – Sources, Theory, Values and Application Domain*, Springer, Dordrecht 2015.
- WILDHABER BRUNO, *Informationssicherheit – rechtliche Grundlagen und Anforderungen an die Praxis*, Diss. Univ. Zürich, Schulthess, Zürich 1994.