ZUM VERHÄLTNIS VON RECHT UND TECHNIK: RECHTSSTAATLICHKEIT DURCH TECHNIKGESTALTUNG

Christof Tschohl

Abstract: Rechtsdurchsetzung durch Technikgestaltung ist, wie im Einleitungsbeitrag von HÖTZENDORFER dargestellt, eine effektive Methode zur Umsetzung politischer Vorgaben durch Rechtsnormen, welche dazu verpflichten, die Vorgaben in der Technikgestaltung umzusetzen. Staatliche Organe haben bei der Gestaltung technischer Hilfsmittel zur Vollziehung stets das rechtsstaatliche Prinzip zu beachten. Rechtsstaatlichkeit durch Technikgestaltung als modernes Verfassungsprinzip wird aus den Grundrechten abgeleitet und inkludiert vor allem auch die technische Absicherung verfahrensrechtlicher Bestimmungen, die der Rechtsstaatlichkeit und dem Rechtsschutz dienen.

Inhaltsverzeichnis

A. EINLEITUNG

Der Einleitungsbeitrag von WALTER HÖTZENDORFER zeigt, dass Rechtsdurchsetzung durch Technikgestaltung ein effektives Instrument sein kann und bereits zahlreiche etablierte Erkenntnisse für eine breite praktische Umsetzung vorliegen. Auf dem Weg zu solchen Erkenntnissen hat ERICH SCHWEIGHOFER uns nicht nur inspiriert und geleitet, sondern in der Arbeitsgruppe Rechtsinformatik (ARI) an der Universität Wien auch eine Plattform zur Forschungsarbeit zu diesem Thema geboten. Dementsprechend war die intensive Beschäftigung mit dem Thema Datenverarbeitung und -Austausch im Rahmen des Arbeitspakets zur internationalen Polizeikooperation im FP7 Projekt SMART[1] unter seiner Führung ein Meilenstein für meine weitere wissenschaftliche Arbeit. Die technische und rechtliehe Analyse der Systeme zum internationalen Datenaustausch beispielsweise von Interpol oder Europol förderte zutage, dass dort die oft hohen Vertraulichkeitsanforderungen mit einem engmaschigen, technisch umgesetzten Regelwerk durch sog. handling-codes abgesichert werden.[2]

[1] Projektlaufzeit von 2011 bis 2014, vgl. die Übersicht zum Projekt unter https://cordis.europa.eu/project/rcn/99234/factsheet/fr (25.11.2019).

[2] Siehe die publizierte Zusammenfassung der Ergebnisse der Universität Wien aus dem EU FP7 Projekt SMART bei: SCHWEIGHOFER/SCHREMS/HÖTZENDORFER/TSCHOHL: SMART surveillance and

Damit bestehen zu dem hier behandelten Themenfeld «Rechtsdurchsetzung durch Technikgestaltung» wesentliche internationale Beispiele. Wenn schon die Ermittlungsarbeit an sich Vertraulichkeit erfordert, sind auch nicht personenbezogene Objektdaten gleichermaßen (durch die technische Systemgestaltung) geschützt. Die Vorgaben sind also nicht allein dem Datenschutzrecht geschuldet. Der folgende Beitrag beschäftigt sich nun damit, ob und (wenn ja) wie weit sich aus dem Prinzip der Rechtsstaatlichkeit sowie aus den Grundrechten ein allgemeiner Grundsatz für «Rechtsstaatlichkeit durch Technikgestaltung» ableiten lässt. Zum Abschluss wird das Konzept bzw. dessen Notwendigkeit anhand zweier Beispiele kurz dargestellt.

B. RECHTSSTAATLICHKEIT UND DIGITALISIERUNG

I. Begriff und Funktion der Rechtsstaatlichkeit

Das rechtsstaatliche Prinzip kommt nach herrschender Auffassung insbesondere in der Gesetzesbindung der Vollziehung nach Artikel 18 B-VG zum Ausdruck. Für den Gesetzgeber ergibt sich daraus vor allem die Verantwortung, Normen hinreichend bestimmt und klar zu formulieren. Rechte und Pflichten der von der Vollziehung betroffenen Menschen müssen gesetzlich möglichst präzise geregelt sein und deren Durchsetzung durch entsprechende Institutionen garantiert sein.

Der Begriff «rechtsstaatliches Prinzip» fand 1949 erstmals Eingang in die Begründung eines Erkenntnisses des Verfassungsgerichtshofs (VfGH).[3] Drei Jahre später qualifizierte der VfGH (in VfSlg 2455/1952.) das rechtsstaatliche Prinzip bereits als leitenden Grundsatz der Bundesverfassung, dessen Abänderung als Gesamtänderung der Bundesverfassung zu qualifizieren ist: «Dem rechtsstaatlichen Prinzip entspricht es, dass alle Akte staatlicher Organe im Gesetz und mittelbar letzten Endes in der Verfassung be-

international data exchange between police authorities. In: SCHWEIGHOFER/KUMMER/HÖTZENDORFER (Hrsg.): Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2012, Jusletter IT, 2012, 541–548.

[3] Der VfGH vertrat in VfSlg 1804/1949 die Ansicht, dass das AVG in der Wahrung des Parteiengehörs «in verfahrensrechtlicher Beziehung einer der wichtigsten Sicherungen des rechtsstaatlichen Prinzips» erblicke.

gründet sein müssen, und dass für die Sicherung dieses Postulates wirksame Rechtsschutzeinrichtungen bestehen». Das der österreichischen Rechtsordnung immanente Konzept des «Fehlerkalküls» von Adolf Julius Merkl[4] antizipiert in dieser Hinsicht, dass in der Praxis des Rechts Fehler unvermeidbar sind und daher entsprechende Rechtsschutzsysteme geschaffen werden müssen, um einen Rechtsstaat zu etablieren. In diesem Sinne ist auch das – in Artikel 13 EMRK ausdrücklich in Österreich verfassungsgesetzlich verankerte – Gebot eines effektiven Rechtsschutzes eine wesentliche Säule der Rechtsstaatlichkeit. Das Gebot des effektiven Rechtsschutzes blieb auch weiterhin die zentrale Konstante in der Rechtsstaatsjudikatur des VfGH[5].

In seinem Erkenntnis VfSlg 11.196/1986 führte der VfGH Grundsätzliches zur Funktion der Rechtsstaatlichkeit in einer demokratisscchen Gesellschaft aus, weshalb ein ausführliches Zitat sinnvoll erscheint:

«Der VfGH kann von seiner im Prüfungsbeschluss bezogenen ständigen Judikatur zum rechtsstaatlichen Prinzip ausgehen (...). Ihr zufolge gipfelt der Sinn des rechtsstaatlichen Prinzips darin, dass alle Akte staatlicher Organe im Gesetz und mittelbar letzten Endes in der Verfassung begründet sein müssen und ein System von Rechtsschutzeinrichtungen die Gewähr dafür bietet, dass nur solche Akte in ihrer rechtlichen Existenz als dauernd gesichert erscheinen, die in Überstimmung mit den sie bedingenden Akten höherer Stufe erlassen wurden. Der Gerichtshof bleibt auch bei der im Einleitungsbeschluss an diese Annahme geknüpften Annahme, dass die hier unabdingbar geforderten Rechtsschutzeinrichtungen ihrer Zweckbestimmung nach ein bestimmtes Mindestmaß an faktischer Effizienz für den Rechtsschutzwerber aufweisen müssen. Zunächst ist hierzu die Klarstellung geboten, dass von faktischer Effizienz deshalb die Rede ist, weil unter Effizienz allein unter Umständen bloss das letzten Endes bewirkte Erreichen einer Entscheidung rechtsrichtigen Inhalts durch das Ergreifen von Rechtsbehelfen verstanden werden könnte, nicht aber auch die mitgemeinte Übersetzung einer solchen

[4] Wiederin, Die Stufenbaulehre ADOLF JULIUS MERKLS, in: GRILLER/RILL (Hrsg.), Rechtstheorie. Rechtsbegriff – Dynamik – Auslegung, Wien/New York 2011, S. 81–134, ausführlich zum «Fehlerkalkül» das gesamte Kapitel IV.

[5] Vgl. HIESL, Die Rechtsstaatsjudikatur des Verfassungsgerichtshofes, ÖJZ 1999,522 (Heft 14–15).

Entscheidung in den Tatsachenbereich. «Schutz» als Teilaspekt des Ausdrucks «Rechtsschutz» ist auf den Rechtsunterworfenen bezogen und meint nicht zuletzt die – rechtzeitige – Wahrung und Gewährleistung einer faktischen Position, weshalb Rechtsschutzeinrichtungen diesen Zweck notwendig in sich schließen.»[6]

Es geht dabei immer um das Verhältnis des einzelnen Menschen zum Staat. Im Rechtsstaat soll an die Stelle von Herrschaft durch Machtdemonstration, Willkür und Gewalt die verbindliche Kraft des Rechts treten, daher können der Staat und seine Amtsträger nur auf der Grundlage rechtlicher Regeln tätig werden. Sie können niemals mehr tun, als gesetzliche Vorschriften gestatten. Damit begrenzt der Rechtsstaat die Macht des Staates sehr deutlich und sieht strenge Verfahren für alle Handlungen des Staates und seiner AmtsträgerInnen vor.[7]

II. Die Funktion der Grundrechte im modernen Rechtsstaat

Die Grundrechte sind das Rückgrat der Verfassung und erfüllen die ansonsten praktisch werteneutrale[8] «Spielregelverfassung» der Republik Österreich mit Substanz. Rechtsstaatlichkeit ist für sich allein keinesfalls ein Garant für Gerechtigkeit im Recht, das hat

---

6 VfGH Erkenntnis vom 11.12.1986, G119/86 (VfSlg 11.196/1986) und seither ständige Rspr.

7 Vgl. die Ausführungen zum rechtsstaatlichen Prinzip auf der Website des österreichischen Parlaments unter https://www.parlament.gv.at/PERK/VERF/GRUND/ (25.11.2019).

8 Die einzige Stelle, an der die österr. Bundesverfassung einen klaren Wertekanon enthält, wurde durch BGBl. I Nr. 31/2005, mit Wirkung vom 10. Juni 2005 in Art. 14 B-VG, den Kompetenztatbestand des Schulwesens, in einem neuen Abs. 5a folgendermaßen eingefügt:

«(5a) Demokratie, Humanität, Solidarität, Friede und Gerechtigkeit sowie Offenheit und Toleranz gegenüber den Menschen sind Grundwerte der Schule, auf deren Grundlage sie der gesamten Bevölkerung, unabhängig von Herkunft, sozialer Lage und finanziellem Hintergrund, unter steter Sicherung und Weiterentwicklung bestmöglicher Qualität ein höchstmögliches Bildungsniveau sichert. Im partnerschaftlichen Zusammenwirken von Schülern, Eltern und Lehrern ist Kindern und Jugendlichen die bestmögliche geistige, seelische und körperliche Entwicklung zu ermöglichen, damit sie zu gesunden, selbstbewussten, glücklichen, leistungsorientierten, pflichttreuen, musischen und kreativen Menschen werden, die befähigt sind, an den sozialen, religiösen und moralischen Werten orientiert Verantwortung für sich selbst, Mitmenschen, Umwelt und nachfolgende Generationen zu übernehmen. Jeder Jugendliche soll seiner Entwicklung und seinem Bildungsweg entsprechend zu selbständigem Urteil und sozialem Verständnis geführt werden, dem politischen, religiösen und weltanschaulichen Denken anderer aufgeschlossen sein sowie befähigt werden, am Kultur- und Wirtschaftsleben Österreichs, Europas und der

das Nationalsozialistische Regime tragisch bewiesen. Es bedarf vielmehr zusätzlich einer inhaltlichen Absicherung der für eine Gesellschaft grundlegendsten Werte – nicht verstanden als eine bestimmte Ideologie sondern grundlegende materielle Determinanten einer freien und demokratischen Gesellschaft. Grundrechte sind in diesem Sinne nicht nur verfassungsgesetzlich gewährleistete subjektive Rechte sondern beinhalten zugleich Wertvorstellungen und Orientierungsnormen[9]. Der Kristalisationspunt aller Grundrechte ist dabei die unantastbare Würde des Menschen. Art. 1 EU Grundrechte-Charta). Den Grundrechten kommt eine zentrale Legitimations- und Sicherungsfunktion für die gesamte Rechtsordnung zu. Eine effektive umfassende Gewährleisung der Grundrechte ist letztlich das Ziel der Rechtsstaatlichkeit, die erst dadurch ihre Bedeutung in einer demokratischen Gesellschaft entfaltet.

Bereits die ideengeschichtlichen Wurzeln der Grundrechte bzw. der Menschenrechte[10] und deren praktische Umsetzung in den Verfassungen und Grundrechtskatalogen der amerikanischen Unabhängigkeitsbewegung beschäftigten sich intensiv mit der Interdependenz zwischen Demokratie, Gewaltenteilung, Rechtsstaat und Menschenrechten. Insbesondere das System der «checks and balances» wird dabei als Garant dafür gesehen, dass der Staat, von dem in der Regel die größten Bedrohungen für die Menschenrechte ausgehen, zugleich deren Einhaltung zu gewährleisten hat. Ohne rechtsstaatliches Verfahren lässt sich ein effizienter Grundrechtsschutz nicht bewirken. Die wesentlichen Elemente der Rechtsstaatlichkeit finden sich daher zugleich in den Verfahrensgrundrechten wieder, insbesondere in Art 6 EMRK und Art 47 EU Grundrechte-Charta. Aber auch die materiellen Grundrechte selbst entfalten nach der Rechtsprechung

Welt teilzunehmen und in Freiheits- und Friedensliebe an den gemeinsamen Aufgaben der Menschheit mitzuwirken.»

9 Vgl. BUCHINGER/HODASZ/PLANITZER/STEINKELLNER/TRETTER/TSCHOHL/APOSTOLOVSKI/KRONAWETTER/ KUMAR/STARL/CZECH/SCHÖPFER/KIEBER: Skriptum zum RiAA-Grundrechtsmodul, im Auftrag der Fachgruppe Grundrechte der Österreichischen Richtervereinigung, herausgegeben vom BMJ, 3. aktualisierte Auflage, Wien, (2014), 13f.

10 Die Unterscheidung der beiden Begriffe wird heute eher in Bezug auf ihren räumlichen Geltungsbereich getroffen: «Menschenrechte» sind solche, die weltweite (UN Pakte) oder zumindest (über)kontinentale Geltung (zB die EMRK) beanspruchen, «Grundrechte» diejenigen, die innerstaatlich garantiert sind (zB in Österreich das StGG 1867).

verfahrensrechtliche Wirkungen.[11] Demnach verpflichten die materiellen Grundrechte den Gesetzgeber auch, die für die umfassende Durchsetzbarkeit eines materiellrechtlichen Grundrechtsanspruchs notwendigen prozessualen Rechtspositionen einzuräumen.[12] In der Rechtssprechung des EGMR[13] mündet dies regelmäßig in der Formulierung staatlicher Schutzpflichten, die unter gewissen Umständen bis hinein in die Ebene zwischenmenschlicher Beziehungen reichen kann.[14] In einer Informationsgesellschaft müssen diese Prinzipien auch «online» gelten.

1. Die EU Grundrechte-Charta (GRC)

Seit dem Inkrafttreten des Vertrages von Lissabon[15] ist die europäische Grundrechte-Charta (GRC) im Primärrecht der Europäischen Union verbindlich verankert[16]. Für den Bedeutungsgehalt der Grundrechte ist die Auslegung der EMRK durch den Europäischen Gerichtshof für Menschenrechte (EGMR) beachtlich, weil Art 52 Abs. 3 GRC zur Tragweite der in der GRC garantierten Rechte ausdrücklich bestimmt: «So weit diese Charta Rechte enthält, die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, haben sie die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird. Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt.»

---

11 Gemäß der von Häberle erweiterten Status-Lehre Georg Jellineks verfügen materielle Grundrechte auch über einen «status activus processualis», vgl. MARTENS/HÄBERLE/BACHOF/BROHM, Grundrechte im Leistungsstaat (1972), 86ff.

12 Siehe vor allem die «Britischen Fürsorgefälle» zur Verpflichtung des Gesetzgebers, einfachgesetzlich Parteistellung einzuräumen, um dem Recht auf Achtung des Familienlebens zur Geltendmachung zu verhelfen (EGMR 8.7.1987, W. vs Vereinigtes Königreich; EGMR 8.7.1987, O. vs Vereinigtes Königreich, EGMR 8.7.1987, R. vs Vereinigtes Königreich).

13 Vgl. zB EGMR 16.7.2013, Mudric vs. Moldawien, 74839/10 (Schutzpflichten Art 3 EMRK).

14 Vgl. etwas ausführlicher BUCHINGER, et al: Skriptum zum RiAA-Grundrechtsmodul, im Auftrag der Fachgruppe Grundrechte der Österreichischen Richtervereinigung, herausgegeben vom BMJ, 3. aktualisierte Auflage, Wien, (2014), 12. Online verfügbar auf der Website des Ludwig Boltzmann Institut für Menschenrechte unter https://bim.lbg.ac.at/de/artikel/skriptum-grundrechtlichen-inhalten-fallbeispielen (25.11.2019).

15 BGBl. III Nr. 132/2009. Der Vertrag trat gem. Art. 6 Abs. 2 am 1. Dezember 2009 in kraft.

16 Gem. Art. 6 EUV ist die GRC mit den Verträgen gleichrangig.

Flankiert wird dies durch eine sog. Günstigkeitsklausel in Art 53 GRC: «Keine Bestimmung dieser Charta ist als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten auszulegen, die in dem jeweiligen Anwendungsbereich durch das Recht der Union und das Völkerrecht sowie durch die internationalen Übereinkommen, bei denen die Union, die Gemeinschaft oder alle Mitgliedstaaten Vertragsparteien sind, darunter insbesondere die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, sowie durch die Verfassungen der Mitgliedstaaten anerkannt werden.»

Bemerkenswert für den Grundrechtsschutz in der EU ist der neue Art 6 EUV, der in Abs. 2 kurz und bündig bestimmt: «Die Union tritt der (EMRK) bei.» Weiters normiert Abs. 3 die Grundrechte aus der EMRK und aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedsstaaten als allgemeine Grundsätze, die Teil des Unionsrechts sind. Im Gegensatz zur EMRK ist die Geltung der Grundrechtecharta in den Mitgliedstaaten sachlich eingeschränkt. Sie ist nur anwendbar, insoweit diese in Durchführung des Unionsrechts handeln.[17] Nach der Rechtsprechung des EuGH ist dies jedoch sehr weit auszulegen und gleichzusetzen mit dem «Anwendungsbereich des Unionsrechts», sodass die Grundrechtecharta nicht etwa nur dann zur Anwendung kommt, wenn die in Frage stehenden Bestimmungen in Umsetzung von Unionsrecht erlassen wurden.[18]

Grundsätzlich können nach der Rechtsprechung des Verfassungsgerichtshofes[19] und dem von ihm entwickelten «Äquivalenzgrundsatz» auch die von der GRC garantierten Rechte vor dem Verfassungsgerichtshof als verfassungsgesetzlich gewährleistete Rechte

17 Art 51 Grundrechtecharta; VfGH 14.3.2012, U 466/11-18 und U1836/11-13, Rz. 47.

18 EuGH 26.2.2013, C-617/10, Åkerberg Fransson, Rz. 17 ff. m.w.N. Siehe zum Anwendungsbereich auch Art 51 GRC. Nach der Rechtsprechung des EuGH gestaltet sich die Auslegung durchaus kompliziert, zB EuGH Siragusa, C-206/13, wonach eine Durchführung des Rechts der Union durch nationale Regelung vorliegt, wenn diese die Durchführung einer Bestimmung des Unionsrechts bezweckt, der Charakter der Bestimmung nicht so ist, dass durch sie andere als die unter Unionsrecht fallenden Ziele verfolgt werden (selbst wenn diese das Unionsrecht unmittelbar beeinflussen) und wenn es eine Regelung des Unionsrechts gibt, die für den Bereich spezifisch ist oder ihn beeinflussen kann.

19 Siehe dazu die nicht unumstrittene Leitentscheidung des VfGH vom 14.3.2012, U 466/11 u.a.

gemäß Art. 144 geltend gemacht werden. In Österreich steht schließlich die EMRK im Verfassungsrang und ist wie ein innerstaatlicher Grundrechtskatalog anzuwenden.[20]

In diesem Beitrag wird im Hinblick auf internationale Judikatur ein stärkerer Fokus auf die Rechtssprechung des EGMR zur EMRK gelegt,[21] vor allem weil es zur Einhaltung nationaler Verfahrensvorschriften und der Bedeutung der Rechtsstaatlichkeit deutlich mehr Judikatur aus Straßburg gibt.[22]

2. Das Grundrecht auf Datenschutz[23] als Modell

Datenschutz ist in der EU Grundrechte-Charta für den Anwendungsbereich des Unionsrechts als eigenes Grundrecht in Art 8 GRC normiert. Dieses noch sehr junge Grundrecht ist durch Art 8 EMRK – der das Recht auf Privat und Familienleben sowie den Schutz der Korrespondenz garantiert und als die Wiege des europäischen Datentschutzes gilt – in dessen Auslegung durch den EGMR determiniert.

Die konkrete Ausgestaltung des Grundrechts durch Sekundärrechtsakte sowie durch nationales Recht sind dabei stets durch das Grundrecht determiniert. Die bedeutendsten Rechtsquellen des Datenschutzrechts auf der Ebene des Sekundärrechts sind:

---

20 Art II Z 7 Bundesverfassungsgesetz vom 4. März 1964, mit dem Bestimmungen des Bundes-Verfassungsgesetzes in der Fassung von 1929 über Staatsverträge abgeändert und ergänzt werden BGBl 1964/59; vgl. auch ENNÖCKL, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, S. 21.

21 Siehe zum Verhältnis zwischen EMRK und EU ausführlich Heißl, Happy End einer unendlichen Geschichte? Der Beitritt der EU zur EMRK und seine Auswirkungen auf Österreich, in: HOLOUBEK/MARTIN/SCHWARZER (Hrsg.), Die Zukunft der Verfassung – Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag, S. 131.

22 Dies hängt auch damit zusammen, dass nach dem im Unionsrecht bis heute gültigen Grundsatz der Verfahrensautonomie der Mitgliedstaaten der EuGH eher selten auf entsprechende Fragestellungen im Rahmen von Vorabentscheidungsverfahren eingehen kann.

23 Die folgenden Ausführungen zum Datenschutzgrundrecht sind teilweise im Rahmen der Forschungsarbeit des KIRAS Forschungsprojekts «FLORIDA» entstanden, ein besonderer Dank gilt daher an dieser Stelle Markus Kastelitz. Eine gedrängte Darstellung der Projektergebnisse auf 24 Seiten ist seit kurzem publiziert: Kastelitz/Tschohl/Hötzendorfer, (Datenschutz)rechtliche Aspekte der polizeilichen Verarbeitung von Videomassendaten, in: JAHNEL (Hrsg.), Jahrbuch Datenschutzrecht 2019.

– Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO)[24]
– Übereinkommen 108 des Europarats («Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten», auch Europäische Datenschutzkonvention, kurz Datenschutzkonvention)

Als Grundregel gilt, dass jede Verwendung personenbezogener Daten ein Eingriff in das Grundrecht auf Datenschutz in seiner Ausprägung als Recht auf Geheimhaltung ist. Dieses Grundrecht ist in verschiedenen Rechtsquellen normiert, die nachfolgend kurz dargestellt werden. Das Grundrecht des Art. 8 Abs. 1 EMRK beinhaltet auch ein Recht auf Datenschutz, wie der Europäische Gerichtshof für Menschenrechte (EGMR) in zahlreichen Entscheidungen festgestellt hat.[25] Der Begriff des Privatlebens und somit der Schutzbereich dieser Bestimmung ist nach h.M. einer erschöpfenden Definition nicht zugänglich, sondern kann nur wirkungsbezogen definiert werden: Ob ein Eingriff in das Privatleben vorliegt, hängt davon ab, ob eine staatliche Maßnahme die Möglichkeit des Bürgers zur freien Persönlichkeitsentwicklung beeinträchtigt.[26]

Bei Art. 8 Abs. 1 EMRK handelt sich nicht um ein absolut geschütztes Grundrecht, sondern dieses kann im Interesse der Allgemeinheit, oder wenn es mit anderen Grundrechten kollidiert, eingeschränkt werden.[27] Ebenfalls ein (fast gleichlautendes) Grundrecht

---

[24] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

[25] Siehe insb. EGMR 26.3.1987, 9248/81, Leander, EGMR 25.3.1998, 9248/81, Kopp, EGMR 16.02.2000, 27798/95, Amann, EGMR 4.5.2000, 28341/95, ROTARU etc. Vgl. auch JAHNEL, Handbuch Datenschutzrecht, 2010, Rz. 2/16.

[26] Vgl ENNÖCKL, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 23 ff. mwN, der die verschiedenen «Erscheinungsformen» ausführlich darstellt.

[27] Daher lautet Art. 8 Abs. 2 EMRK: «Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechtes ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.»

auf Achtung des Privat- und Familienlebens sieht die Charta der Grundrechte der Europäischen Union in Artikel 7 vor. Hinzu kommt ein Grundrecht auf Schutz personenbezogener Daten in Artikel 8.

Seit Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 ist die Grundrechtecharta gleichrangig mit dem Primärrecht der EU (Art. 6 Abs. 1 EUV). Damit wurden Rechte, die bereits zuvor in der DSRL normiert waren, auf die Ebene des Primärrechts erhoben,[28] darunter mit dem Recht auf Auskunft und dem Recht auf Richtigstellung des Art. 8 Abs. 2 GRC auch die datenschutzrechtlichen Betroffenenrechte.

In Österreich besteht seit Inkrafttreten des Datenschutzgesetzes 1978 (DSG 1978) das Datenschutzgrundrecht des § 1 DSG im Verfassungsrang. Zur Vorbereitung auf die Durchsetzbarkeit der DSGVO ab 25.5.2018 wurde das DSG 2000 durch das «Datenschutz-Anpassungsgesetz»[29] grundlegend novelliert, ab § 4 DSG handelt es sich um eine völlig Neufassung. Nur die ersten drei Paragraphen blieben bestehen, da es verabsäumt wurde, die für deren Änderung erforderliche Zweidrittelmehrheit zu koordinieren.

Zu betonen ist, dass alle genannten Grundrechte für alle Menschen gleichermaßen gelten, d.h. ihre Anwendbarkeit ist insbesondere nicht auf Menschen mit einer bestimmten Staatsbürgerschaft oder einer Unionsbürgerschaft beschränkt. Das Grundrecht auf Datenschutz ist nicht Selbstzweck. Nicht die Daten sind schutzwürdig, sondern die Personen, auf welche sie sich beziehen. Schutzwürdige Positionen erwachsen dabei vor allem aus den verschiedenen Grundrechtsgarantien in allen Bereichen. Häufig lässt sich eine direkte Beziehung zwischen einem festgestellten Risiko und einer durch ein bestimmtes Grundrecht geschützten Sphäre des betroffenen Menschen herstellen. Insofern ist Datenschutz eine Art «Katalysator-Grundrecht», das seinen eigentlichen Gehalt aus der gesamten Grundrechtsordnung und letztlich dem Schutz der Würde des Menschen bezieht.

---

[28] Vgl. WESTPHAL, Grundlagen und Bausteine des europäischen Datenschutzrechts, in BAUER/REIMER (Hrsg.), Handbuch Datenschutzrecht, 2009, 53–94, S. 66.

[29] Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (Datenschutz-Anpassungsgesetz 2018), BGBl I 2017/120 vom 31. Juli 2017 sowie eine weitere Novellierung durch das «Datenschutz-Deregulierungsgesetz», BGBl I 2018/24 vom 15. Mai 2018.

Das Datenschutzgrundrecht und dessen Ausgestaltung durch Sekundärrecht und nationales Recht eignet sich damit als Modell für einen «design-thinking[30]»-Ansatz in der Gestaltung von im Dienste der Hoheitsverwaltung stehenden IT Systemen. Es bietet ein dynamisches, risikobasiertes Konzept, welches jede Systemgestaltung in seinem Anwendungsbereich ab der ersten Planung normativ erfasst und leitet. Datenschutz ist dabei nicht nur auf den Schutz der Privatsphäre sondern generisch auf den Schutz aller Grundrechte («Katalysator-Grundrecht») gerichtet.

Bezogen auf IT Systeme zum Einsatz in der Hoheitsverwaltung besteht außerdem eine sehr große Schnittmenge von Datenverarbeitungen innerhalb und außerhalb des Schutzbereichs des Datenschutzrechts. In der Regel werden personenbezogene Daten verarbeitet und die Regeln des Datenschutzrechts sind unmittelbar auf die Sachverhalte anwendbar. Allerdings ist dabei relativ offen, ob daraus eine (strenge) Umsetzung verfahrensrechtlicher Vorschriften durch die Technologiegestaltung als normatives Gebot abzuleiten ist. Die hier vertretene These: sofern die Verfahrensvorschrift ein wesentliches Element des Grundrechtsschutzes darstellt (Risikobezug), ist sie in der Technikgestaltung – nach dem Modell des Art 25 DSGVO – auch umzusetzen.

2.1. Das Konzept «human dignity by design»

Die Entwicklung des Datenschutzrechtes – vor dem Hintergrund rasant wachsender technologischer Möglichkeiten – steckte lange Zeit in einem formalistischen eingriffsabwehr-rechtlichen Denkschema fest, das den realen Verhältnissen nicht gerecht zu werden vermochte. Erst die DSGVO hat hier einen modernen und pro-aktiven Gestaltungsansatz normiert. Dies zeigt sich insbesondere in der Verpflichtung nach Art. 35 DSGVO zur Durchführung einer Datenschutz-Folgenabschätzung bei Datenverarbeitungen mit besonders hohem Risiko[31].

---

30 Unter Design Thinking wird eine spezielle Herangehensweise zur Bearbeitung komplexer Problemstellungen verstanden. Design Thinking ist dabei eine Methode, ein Set an Prinzipien, eine spezielle Denkhaltung und ein Prozess mit einer Vielzahl von unterstützenden Tools; siehe dazu https://wirtschaftslexikon.gabler.de/definition/design-thinking-54120 (25.11.2019).

31 Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 «wahrscheinlich ein hohes Risiko mit sich bringt» (WP 248 Rev. 01) 10 ff.

Die Schutzbedürftigkeit ist von den dahinterstehenden Verwendungszusammenhängen und den damit verbundenen Risiken her zu beurteilen. Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person führen zwar dazu, dass der Einzelne Einschränkungen seiner Grundrechte hinzunehmen hat, wenn überwiegende Allgemeininteressen dies rechtfertigen. Der Gesetzgeber muss aber zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herstellen. Es scheint daher sachgerecht, den «Datenschutz» nach einem Muster des «Risikorechts» und als «teilhaberechtliche» Konstruktion zu erfassen.[32]

Diesem Ansatz wird der neue in Art 25 DSGVO verankerte Grundsatz «Datenschutz durch Technikgestaltung» in vorbildlicher Weise gerecht. Eine vorgelagerte Datenschutz-Folgenaschätzung macht die Risiken transparent und verlangt die Formulierung technischer und organisatorischer Maßnahmen zur Reduktion oder bestenfalls Elimination dieser Risiken. Der von Walter Hötzendorfer im Eingangsbeitrag ausführlich behandelte Grundsatz «Datenschutz durch Technikgestaltung» sorgt nun dafür, dass diese Maßnahmen (bei sonstigen Sanktionen gegen den Verantwortlichen) auch unmittelbar in die Systeme «eingebaut» wird. Damit ist logisch zwingend verbunden, die Grundsätze bereits in der Normierung des Systems zu konkretisieren.

Wie bereits ausgeführt ist die Wurzel aller Grundrechtsgarantien die unantastbare Würde des Menschen. Weil der Datenschutz nicht Selbstzweck ist und immer im Hinblick auf den Schutzzweck und die Risiken der Betroffenen auszulegen ist, liegt in der Gewährleistung der Menschenwürde bei der Verarbeitung personenbezogener Daten der ultimative Schutzzweck des Datenschutzrechts begründet. Gut sichtbar wird dies im großen Feld Datenverarbeitung im Beschäftigungskontext. Art 88 DSGVO enthält diesbezüglich eine Öffnungsklausel und überlässt dem nationalen Recht die konkrete Ausgestaltung. Absatz 2 konkretisiert hierfür die Schutzzwecke, die das nationale Recht dabei verfolgen darf bzw. soll. Umfasst davon sind insbesondere «angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person (…)» am Arbeitsplatz. Hier zeigt sich,

[32] Ladeur, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, Jg 62, 45ff.

dass der Begriff der Privatsphäre am Arbeitsplatz keinen hilfreichen Bezugsrahmen bietet.

Die Menschenwürde als Ansatzpunkt und als justiziabler Begriff stellt sicher, das nur eine umfassende und sorgfältige Beschäftigung mit den konkreten Auswirkungen auf die betroffenen Menschen zu einem Ergebnis führt. Hier liegt nach Ansicht des Autors dieses Beitrags der Mehrwert des Konzepts «human dignity by design» («eingebaute Menschenwürde») und «data protection by design».

Im Österreichischen Arbeitsrecht gibt es seit Jahrzehnten konkrete Erfahrung und höchstgerichtliche Judikatur zum Begriff der Würde des Menschen. Gemäß § 96a Abs 1 Z 3 ArbVG bedarf nämlich die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der ArbeitnehmerInnen, sofern diese Maßnahmen bzw. Systeme die Menschenwürde berühren, zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates in Form einer notwendigen und erzwingbaren Betriebsvereinbarung.

Der OGH[33] stellt fest, dass sich der Konflikt zwischen widerstreitenden Persönlichkeitsrechten aus der Warte der Grundrechte betrachtet regelmäßig auch als Grundrechtskonflikt mit Drittwirkungseffekten darstellt. Die Persönlichkeitsrechte wirken, wenngleich durch den Arbeitsvertrag abgeschwächt und modifiziert, auch im dienstlichen Bereich fort und schützen dort den/die ArbeitnehmerIn insbesondere vor Erniedrigung, Ungleichbehandlung und Willkür. Durch zu große, über das für die Erreichung des Kontrollzwecks erforderliche Ausmaß hinausgehende Kontrolldichte bei der Arbeit kann jedenfalls die Menschenwürde im Sinne des § 96 Abs 1 Z 3 ArbVG berührt werden. Daher bedarf etwa die Einrichtung einer automationsunterstützten Telefonregistrieranlage im Betrieb, soweit sie personenbezogene Daten erfasst, immer der Zustimmung des Betriebsrates.[34]

Das arbeitsrechtliche Beispiel zeigt, dass die durchaus schwierige Aufgabe, den aus der Philosophie der Aufklärung stammenden Begriff der Würde des Menschen in der Rechtspraxis zu konkretisieren, bewältigbar ist und zu angemessenen Ergebnissen

33 8 ObA 288/01p; 9 ObA 109/06d = SZ 2002/83.

34 Ausführlich dazu: KNYRIM/TIEN, Die Datenschutz-Grundverordnung im Beschäftigtenkontext. Auswirkungen der DSGVO auf den Arbeitnehmerdatenschutz, ASoK 2017, 10/2017, 363.

führt. Das hier ansatzweise entwickelte Konzept «human dignity by design» bezieht seine Berechtigung nicht so sehr aus einer substanziell veränderten normativen Vorgabe sondern sondern aus einer Änderung der Geisteshaltung bei der Problemlösung.

C. GRUNDRECHTLICHE GEWÄHRLEISTUNGS- UND TECHNISCHE GESTALTUNGSPFLICHTEN[35]

Der hier fokussierte Bereich der öffentlichen Sicherheit steht praktisch in einem permanenten Spannungsverhältnis von Grundrechts-Kollisionen, die der Staat bestmöglich nach dem Verhältnismäßigkeitsgrundsatz ausbalancieren muss. Eingriffe in die Grundrechte der Subjekte der Ermittlungshandlungen sind in der Regel erforderlich, weil sie dem Schutz der Rechte und Freiheiten anderer Menschen (deren Rechtsgüter bedroht sind) dienen. Die Grundrechte entfalten hier eine horizontale Wirkung[36] in Bezug auf die Menschen untereinander, obwohl sie in erster Linie den Staat verpflichten.[37] Den Staat treffen nun nach der modernen Grundrechtsjudikatur grundrechtliche Gewährleistungspflichten, die so zu verstehen sind, dass er eine normative Gestaltung vorzunehmen hat, die einen wirksamen Schutz der verschiedenen Grundrechtspositionen bietet. Die Grundrechte enthalten dabei immer nur normative Anordnungen und beziehen sich insofern auf eine bestimmte Gestaltung von Rechtsnormen.[38]

Die Grundrechte haben damit in ihren unterschiedlichen Wirkungsdimensionen Einfluss auf die Entwicklung neuer Technologien und deren Innovationspfade, ungewollte

---

35 Vgl. TSCHOHL, Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, Dissertation, Universität Wien, Rechtswissenschaftliche Fakultät 2011, 26 ff, online unter http://othes.univie.ac.at/17556/ (25.11.2019).

36 Zum Begriff Horizontalwirkung sowie zum Problem der Drittwirkung der Grundrechte siehe mit weiteren Nachweisen Heißl, Grundrechtskollisionen am Beispiel von Persönlichkeitseingriffen sowie Überwachungen und Ermittlungen im Internet, Forschung aus Staat und Recht 181, 3; vgl. dazu auch MAYER/KUCSKO-STADLMAYER/STÖGER, Bundesverfassungsrecht, Rz 1334 («Horizontalgeltung»); sowie ÖHLINGER/EBERHARD, Verfassungsrecht, Rz 741.

37 Vgl. Heißl, Grundrechtskollisionen am Beispiel von Persönlichkeitseingriffen sowie Überwachungen und Ermittlungen im Internet, Forschung aus Staat und Recht 181, 32.

38 Dazu ausführlich Holoubek, Grundrechtliche Gewährleistungspflichten, 259 ff.

Schäden sollen durch grundrechtliche Schutz- und Gewährleistungspflichten verhindert werden.[39] Die staatliche Schutzpflicht gegenüber der Möglichkeit von Grundrechtsverletzungen erfordert, dass ein Rechtsrahmen geschaffen wird, der gewährleistet, dass die Abläufe des Verwaltungshandelns – insbesondere auch bei der Einbeziehung privater Akteure – konform mit den Grundrechten erfolgt.[40]

Im Kontext moderner Informationstechnologie sind damit Fragen technologischer Sicherungsmechanismen untrennbar verknüpft. So ist etwa die tatsächliche Umsetzung von (Zugriffs-)Dokumentations- und Informationspflichten eine unabdingbare Voraussetzungen für einen effektiven Rechtsschutz im Hinblick auf die Gewährleistung der «informationellen Selbstbestimmung»[41]. Wenn diese nicht im System automatisiert umgesetzt werden, sondern allein auf Basis organisatorischer Vorgaben durch menschliches Zutun erfolgen sollen, ist die Wirksamkeit in Zweifel zu ziehen, insbesondere bei hoch skalierenden und komplexen Systemen (bis hin zum «Data Warehouse»). Die Einhaltung komplexer Vorgaben kann in den Informationsprozessen nicht primär davon abhängig gemacht werden, dass die Rechts- und Systemanwender jederzeit explizite Kenntnis der normativen Vorgaben haben. Damit wäre menschliches Versagen geradezu vorprogrammiert.

Angesichts einer unüberschaubaren Zahl von Informationsverarbeitungsprozessen in ebenso unzähligen Verwaltungsbereichen lassen sich diese Aufgaben nur mit Hilfe entsprechender elektronischer Hilfsmittel bewältigen. Je komplexer die Aufgabenstellung und je höher die Risiken für die Beteiligten, desto mehr Aufwand ist geboten, um die

---

39 So das Resümee einer bemerkenswerten Analyse zum Beitrag der Grundrechte im Hinblick auf eine gesellschaftliche und staatliche Innovationsfolgenverantwortung, Eisenberger, Technik der Grundrechte – Grundrechte der Technik, in: HOLOUBEK/MARTIN/SCHWARZER (Hrsg.), Die Zukunft der Verfassung – Die Verfassung der Zukunft? Festschrift für Karl Korinek zum 70. Geburtstag, 128.

40 Siehe dieselbe Argumentation im Hinblick auf das Datenschutzgrundrecht schon bei Kotschy, Datenschutzrechtliche Fragen im Zusammenhang mit dem neuen Verbraucherkreditrecht, ÖBA 2011, 312.

41 Der VfGH hat die Formulierung «Recht auf informationelle Selbstbestimmung» im Erkenntnis zur Aufhebung der Vorratsdatenspeicherung (G47/2012 ua) synonym für das österreichische Datenschutzgrundrecht verwendet, angelehnt an das deutsche Bundesverfassungsgericht im «Volkszählungsurteil» aus 1983 (BVerfG E 65, 1–71).

Einhaltung der verfahrensrechtlichen Sicherungsvorschriften so in ein System einzubauen, dass die Anwender gar nicht anders können, als rechtlich korrekt zu handeln. Dort wo notwendigerweise Handlungs- und Entscheidungsspielräume bestehen bleiben müssen, ist mit flankierenden organisatorischen (und technisch abgesicherten) Maßnahmen in die Bahnen für rechtlich und sachlich richtige Entscheidungen zu lenken. Ein in diesem Zusammenhang zentrales Gebiet ist das Informationssicherheitsmanagement (ISMS). Dieses behandelt, dass innerhalb einer Organisation durch die Definition organisatorischer Abläufe, die eindeutige Benennung der verantwortlichen Personen sowie die Verwendung technischer Mittel sicherzustellen ist, dass Informationen nur für jene Zwecke verwendet werden, für die sie erhoben wurden («need to know»-Prinzip) und dabei die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen gewahrt wird.

Die aus den Grundrechten erwachsende Gewährleistungspflicht verlangt bereits vom Gesetzgeber, solche Gestaltungspflichten auf Basis einer Folgenabschätzung normativ zu verankern, wenn die Rechtsgrundlagen für Systeme geschaffen werden.

I. Fokus: Sektor der öffentlichen Sicherheit und Kriminalitätsbekämpfung

Der Bereich der öffentlichen Sicherheit, insbesondere die Feststellung, Verhütung und Verfolgung von Straftaten liegt besonders im Fokus, weil hier die Wahrscheinlichkeit für schwerwiegende Grundrechtseingriffe besonders hoch ist. Daher besteht hier auch ein dichteres Regelungswerk mit zahlreichen materiellen und verfahrensrechtlichen Vorschriften. Teilweise sanktioniert das Verfahrensrecht die Verletzung einzelner Bestimmungen mit Nichtigkeit des gesamten Rechtsakts.[42]

Beispielsweise lässt Art 5 Abs 1 EMRK einen Freiheitsentzug nur in den dort abschließend aufgezählten Fällen und «nur auf die gesetzlich vorgeschriebene Weise» zu. Die Einhaltung der innerstaatlichen Verfahrensvorschriften bei Freiheitsentziehungen wird

[42] Siehe zB die Nichtigkeitsdrohungen nach § 140 StPO in Bezug auf die modernen Ermittlungsmaßnahmen: Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten und von Personen, iVm § 281 StPO.

damit gewissermaßen zum Bestandteil des Grundrechts. Der EGMR nimmt hier die Kompetenz für sich in Anspruch, auch die Einhaltung des nationalen Rechts zu prüfen, weil Art 5 EMRK selbst auf das innerstaatliche Recht verweist.[43] Das Grundrecht ist hier mit den (einfachgesetzlichen) Verfahrensvorschriften eng verzahnt.

Schließlich verlangt die Eingriffsintensität des Strafrechts und auch des (zum Strafrecht weitgehend akzessorischen) Sicherheitspolizeirechts eine höhere Determinierung der gesetzlichen Grundlagen, auf welchen die Eingriffe basieren. Dieses erhöhte Bestimmtheitsgebot erfordert einen besonders sorgfältigen Umgang mit Sprache, der auch im Zuge der Formalisierung der Rechtssprache mit Methoden der Rechtsinformatik[44] fortgesetzt werden muss. Daher ist der Bereich öffentliches Recht und Strafrecht[45] ein ganz wichtiges Anwendungsfeld für das hier vorgestellte Konzept «Rechtsstaatlichkeit durch Technikgestaltung».

II. Rechtsgrundlagen zu polizeilicher Datenverarbeitung

Das wichtigste neue Instrument ist die gemeinsam mit der DSGVO verabschiedete Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Richtlinie für den Datenschutz bei Polizei und Strafjustiz, DSRL-PJ)[46]. Diese trat

---

43 Ständige Rsp, zB EGMR 6.7.2005, Beet u.a., Nr.47.676/99, Z 26 ff.

44 Diese Problemstellung zieht sich wie ein roter Faden durch die Arbeit des hier geehrten Professor Schweighofer, siehe zB SCHWEIGHOFER, KUMMER, HÖTZENDORFER, Transformation juristischer Sprachen, Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012, 23.–25. Februar 2012, books@ocg.at, Wien 2012.

45 Zu den Anwendungsmöglichkeiten der «Rechtsdurchsetzung durch Technik» insbesondere im Strafrecht siehe BERNZEN/KEHRBERGER, Rechtsdurchsetzung durch Informationstechnik, RW 2019, 374–407, S. 380 ff.

46 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, Abl. L 2016/119, 89.

am 5. Mai 2016 in Kraft und war von den Mitgliedstaaten gemäß Art. 63 Abs. 1 der Verordnung bis 6. Mai 2018 umzusetzen. Gemäß Art. 59 DSRL-PJ wurde der Rahmenbeschluss 2008/977/JI mit Wirkung vom 6. Mai 2018 aufgehoben.

Die Umsetzung erfolge durch die umfassende Novellierung des DSG[47] zur Anpassung der Rechtslage an die DSGVO sowie zur Umsetzung der DSRL-PJ und trat mit 25. Mai 2018 in Kraft.[48]

Zur Datenverarbeitung durch Polizeibehörden existieren darüber hinaus noch die folgenden spezifischen Regeln:

- INTERPOL: Rules on the Processing of Data (RPD), neu seit 1. Juli 2012, bieten klare Datenschutzregeln in Bezug auf jede einzelne Datenkategorie und beinhalten eine technische Abbildung der Datenschutzregeln im Design.[49]
- Europol – SIENA (Secure Information Exchange Network Application) basierend auf dem Beschluss des Rates 2009/371/JHA, normiert das Europol Information System (Artikel 11), Datensicherheitsmaßnahmen (Artikel 35), sowie automatisierte Durchsetzung von «handling codes».
- Schengen Information System (SIS) / das Schengener Durchführungsübereinkommen (SDÜ) normiert Datenschutz in Artikel 103 und 126 SDÜ unt enthält einen Verweis auf die Empfehlung Nr R (87) 15 sowie einen strengen Zweckbindungsgrundsatz (Artikel 102 SDÜ).
- Empfehlung Nr R (87) 15 des Ministerkomitees des Europarats vom 17. 9. 1987 zur Regelung der Benutzung personenbezogener Daten im Polizeibereich[50]. Sie ist nicht unmittelbar rechtsverbindlich aber materiell gültig durch zahlreiche Verweise im EU Recht, z.B. Europol, «Swedish Initiative» (Rahmenbeschluss 2006/960/JHA).

---

47 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) BGBl. I Nr. 165/1999 idF BGBl. I Nr. 14/2019.

48 Ab § 4 DSG handelt es sich um eine völlig Neufassung. Nur die ersten drei Paragraphen blieben bestehen, da es verabsäumt wurde, die für deren Änderung erforderliche Zweidrittelmehrheit zu koordinieren.

49 Online bei Interpol https://www.interpol.int/News-and-Events/News/2019/INTERPOL-reviews-its-rules-for-the-international-exchange-of-criminal-data (25.11.2019).

50 http://ec.europa.eu/justice/dataprotection/law/files/coe-fra-rpt-2670-en-471.pdf (Abgerufen am 25 11.2019).

Die vorgestellten Regelwerke sind keine Grundrechtsnormen. Sie enthalten aber vielfach konkrete Vorgaben, die in der Praxis durch eine rechtskonforme Technologiegestaltung, zu der das Recht selbst an vielen Stellen konkrete Anleitungen enthält, faktisch die größte mögliche Wirksamkeit erreichen[51]. Eine Technologiegestaltung, die auf solche Maßnahmen verzichtet, ist nicht auf dem «Stand der Technik»[52].

Auf dem «Stand der Technik» sind Maßnahmen, die aktuell technisch realisierbar sind auf gesicherten Erkenntnissen der Wissenschaft und Technik beruhen und in ausreichendem Maße zur Verfügung stehen. Es kommt somit auf die praktische Umsetzbarkeit an, nicht aber auf einen bereits weit verbreiteten Einsatz in der Praxis. Dies betrifft nicht nur Ausgestaltung einzelner Maßnahmen (zB Auswahl von Verschlüsselungsalgorithmen), sondern auch die vorgelagerte Auswahl der Arten von Maßnahmen. Daraus entsteht ein normativer Druck, solche Maßnahmen zu berücksichtigen und angemessen umzusetzen. Im Anwendungsbereich der DSGVO ist dies nunmehr mit strengen Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs gemäß Art 83 Abs. 4 lit a iVm Art 25 DSGVO bewehrt.

III. Bestimmtheit und Verhältnismäßigkeit von Eingriffen

Eine wesentliche Voraussetzung für eine präzise informationstechnische Umsetzung von Rechtsvorschriften ist die Bestimmtheit der wesentlichen Rechtsbegriffe. Dies ist für die Rechtsinformatik ein faktisches Erfordernis und zugleich grundrechtlich geboten. Nachfolgend wird anhand der ständigen Rechtsprechung des EGMR zu Art 8 EMRK ohne Anspruch auf Vollständigkeit ein normativer Rahmen skizziert.

---

51 Vgl. dazu oben HÖTZENDORFER, zum Verhältnis von Recht und Technik: Rechtsdurchsetzung durch Technikgestaltung, in diesem Band, ausführlich in Kapitel B Grundlagen.

52 Vgl MARTINI in PAAL/PAULY (Hrsg), Datenschutz-Grundverordnung, Beck [2017] Art. 25 Rz 39 mwN. Es kommt somit auf die praktische Umsetzbarkeit an, nicht aber auf einen bereits weit verbreiteten Einsatz in der Praxis Dies betrifft nicht nur die Ausgestaltung einzelner Maßnahmen (zB Auswahl von Verschlüsselungsalgorithmen), sondern auch die vorgelagerte Auswahl der Arten von Maßnahmen.

1. Bestimmtheit der gesetzlichen Grundlage

Eingriffe in den Schutzbereich des Art 8 EMRK sind nicht automatisch unzulässig, sondern bedürfen einer Rechtfertigung. Gemäß Art 8 Abs 2 EMRK ist zunächst eine gesetzliche Grundlage für Eingriffe erforderlich. Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK verankerten Rechtsstaatsprinzip leitet der EGMR zudem ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für die Bürger zugänglich sein muss.[53] Das Gesetz muss adäquate Hinweise über die Bedingungen und Umstände enthalten, unter denen die Behörden befugt sind, in das Recht auf Achtung des Privatlebens und des Briefverkehrs einzugreifen.[54]

Räumt das nationale Recht der Exekutive oder dem zuständigen Richter bei der Anordnung von Maßnahmen Ermessen ein, dann verlangt das Bestimmtheitserfordernis – auch und gerade bei geheimen Maßnahmen –, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen des Ermessens sowie die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind, insbesondere, dass vorhersehbar ist, unter welchen Umständen Eingriffe zulässig sind.[55] Die Anforderungen an die Vorhersehbarkeit im Einzelnen hängen von der Eingriffsintensität der jeweiligen Maßnahme ab. Im Hinblick auf das Missbrauchsrisiko, das insbesondere jedem geheimen Überwachungssystem innewohnt, müssen solche Maßnahmen auf einem besonders präzisen Gesetz beruhen.[56] Klare und detaillierte Bestimmungen müssen insofern einer immer komplexer werdenden Technologie Rechnung tragen.[57]

---

53 EGMR 24.08.1998 Lambert gg. Frankreich = ÖJZ 1999, S. 570ff.

54 EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 74–75 unter Verweis auf die Urteile EGMR 02.08.1984 Malone gg. das Vereinigte Königreich, RN 67; EGMR 30.07.1998 Valenzuela Contreras gg. Spanien, RN 46; und EGMR 12.05.2000 Khan gg. das Vereinigt Königreich, RN 26.

55 EGMR 02.08.1984 Malone gg. das Vereinigte Königreich = EuGRZ 1985, S. 17 ff.

56 EGMR 25.03.1998 Kopp gg. die Schweiz = ÖJZ 1999, S. 115 ff.

57 EGMR 28.06.2007 Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 74-75 unter Verweis auf die Urteile EGMR 24.04.1990 Kruslin gg. Frankreich, RN 33; EGMR 24.04.1990 Huvig gg. Frankreich, RN 32; EGMR 16.02.2000 Amann gg. die Schweiz, RN 56; und EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 93.

Auch wenn beispielsweise Strafverfolgungsorgane um die Herausgabe von Daten «bitten», ohne den Adressaten dazu zu verpflichten, ist es erforderlich, dass die freiwillige Übermittlung der angeforderten Daten nach innerstaatlichem Recht rechtmäßig und die Befugnis der Strafverfolgungsorgane zur Anforderung solcher Daten detailliert geregelt ist.[58] In jedem Fall muss der Staat angemessene Maßnahmen ergreifen, um zu verhindern, dass Dritte unbefugt Kenntnis von schutzwürdigen Inhalten im Zuge der Maßnahme erlangen.[59]

2. Erforderlichkeit und Verhältnismäßigkeit

Der Grundsatz der Verhältnismäßigkeit ist eine zentrale Konstante im gesamten europäischen Rechtskreis. Der Liberale Charakter der EMRK, der EU Grundrechte-Charta sowie auch der nationalen Grundrechte bürdet die Begründungslast zur Verhältnismäßigkeit dem Staat auf, der den Eingriff normieren und durchsetzen will. Dabei hat der Europäische Gerichtshof für Menschenrechte (EGMR) bald klargestellt, dass die EMRK ein «lebendiges Rechtsinstrument» («living instrument») ist, das «im Lichte der gegenwärtigen Verhältnisse» zu interpretieren ist und einen zeitgemäßen und effektiven Schutz vor Menschenrechtsverletzungen und Bedrohungen der Menschenrechte bezweckt.[60]

Für konkrete Aufgaben in der rechtskonformen Technologiegestaltung ist daher wesentlich, den Begriff der Verhältnismäßigkeit von einem Grundprinzip in ein Modell zu zerlegen, welches als Prüfraster in der Technologiegestaltung nutzbar gemacht werden kann. Hierzu bedarf es einer Konkretisierung des Rechtsbegriffs.

Die Prüfung der Verhältnismäßigkeit von Grundrechtseingriffen wird in der Grundrechtswissenschaft durch folgendes Frageschema gekennzeichnet, welches aus der ständigen Praxis der europäischen und nationalen Höchstgerichte ableitbar ist[61]:

---

58 EGMR 02.08.1984 Malone gg. das Vereinigte Königreich = EuGRZ 1985, S. 17 ff.

59 EGMR 17.07.2003 Craxi gg. Italien.

60 Sog. «living instrument»-Formel des EGMR 25.04.1978, Tyrer vs Vereinigtes Königreich.

61 Dazu ausführlich mwN BUCHINGER, et al: Skriptum zum RiAA-Grundrechtsmodul, im Auftrag der Fachgruppe Grundrechte der Österreichischen Richtervereinigung, herausgegeben vom BMJ, 3. aktualisierte Auflage, Wien, (2014), 28 ff.

1. Liegt ein Eingriff in bestimmte Grundrechte vor?
2. Ist der Eingriff gesetzlich vorgesehen (und hinreichend bestimmt)?
3. Dient der Eingriff einem legitimen Ziel?
4. Ist die Maßnahme abstrakt geeignet, das Ziel zu erreichen?
5. Gibt es gelindere Mittel, das Ziel zu erreichen?
6. Besteht ein angemessenes Verhältnis zwischen Risiken und Nutzen?

Dieses Prüfschema mag auf den ersten Blick trivial erscheinen. Zur strukturierten Beurteilung der Zulässigkeit einzelner Maßnahmen oder bestimmter Aspekte entfaltet dieses aber einen großen praktischen Mehrwert, gerade weil es relativ einfach ist. Hier sind sowohl der Gesetzgeber als auch die Vollziehung gleichermaßen adressiert. Die Abarbeitung dieses Schemas sorgt für eine strukturierte und damit stärker versachlichte Entscheidung. Der Grundsatz der Verhältnismäßigkeit wird häufig sehr unbestimmt verwendet. Das Schema zeigt jedoch, dass die Fragen 1. bis 5. sehr gut einer Objektivierbarkeit[62] zugänglich sind. Erst die 6. Frage lässt richtigen Spielraum für eine echte Werte- oder Güterabwägung. Praktisch nützlich ist dies vor allem im Planungs- und Designprozess von IT Systemen zum Einsatz in der Hoheitsverwaltung.

[62] Zumindest im Sinne einer intersubjektiven Nachvollziehbarkeit.

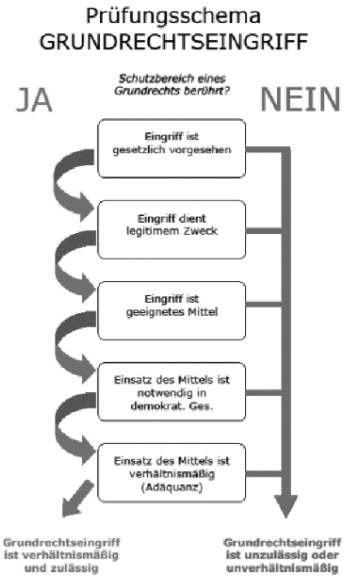

Abbildung 1. Prüfungsschema Grundrechtseingriff aus dem Grundrechte-Skriptum im Rahmen der österreichischen RichterInnenausbildung[63]

Liegt eine gesetzliche Grundlage der fraglichen Maßnahme nach den vorgenannten Kriterien vor, so muss die Maßnahme nach Art 8 Abs 2 EMRK zusätzlich in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig sein. Die einzelnen Staaten haben nach der Rechtsprechung des Gerichtshofs einen Beurteilungsspielraum bezüglich der Frage, ob eine Maßnahme zu einem der in Art 8 Abs 2 EMRK genannten Zwecke notwendig ist.

63 Siehe ausführlich zum Grundsatz der Verhältnismäßigkeit BUCHINGER, et al: Skriptum zum RiAA-Grundrechtsmodul, im Auftrag der Fachgruppe Grundrechte der Österreichischen Richtervereinigung, herausgegeben vom BMJ, 3. aktualisierte Auflage, Wien, (2014), 28 ff. Der Autor dieses Beitrages unterrichtet mit diesen Materialien (und regelmäßig aktualisierten Ergänzungen) seit 2008 in der österreichischen RichterInnenaus- und Fortbildung.

In einer demokratischen Gesellschaft notwendig ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend «dringendes soziales Bedürfnis» nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Eingriffsintensität nicht außer Verhältnis zu dem Gewicht des Zwecks steht. Der EGMR hat dazu eindeutig erklärt, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Rechte abgewogen werden müsse.[64] Eingriffe sind auf das erforderliche Maß beschränkt, aber ein bloßes Nützlichsein oder Wünschenswertsein genügt nicht.[65] Zur Beurteilung der Verhältnismäßigkeit von Grundrechtseingriffen maßgebend sind insbesondere die Gestaltung der Einschreitschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigungen. Es hängt unter anderem davon ab, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen und wie wahrscheinlich der Eintritt einer Rechtsgutverletzung ist.[66]

Die hier dargestellten Kriterien sind bei der Schaffung der normativen Grundlagen der Systeme sowie bei der Gestaltung der Organisation rund um das System als erstes zu Berücksichtigen. Sie richten sich aber auch an die Vollziehung, vor allem wenn in den Abläufen konkrete Interessenabwägungen erforderlich sind.

IV. Gestaltungspflichten für Systeme der Rechtsinformatik zum Einsatz im Bereich der Strafverfolgung

Im strafrechtlichen Ermittlungsverfahren oder in der sicherheitspolizeilichen Aufgabenerfüllung ist die Intensität der Grundrechtseingriffe wie bereits dargestellt besonders hoch. Dem entsprechend existiert auch zu diesen Problemstellungen die reichhaltigste Grundrechtsjudikatur, aus der sich konkrete Vorgaben zur Absicherung der Rechtsstaatlichkeit bei der Gestaltung von IT Systemen als Hilfsmittel ableiten lassen. Wesentlich ist hier, welche Anforderungen direkt aus den Grundrechten abgeleitet wurden. Damit werden zugleich klare Handlungspflichten auch für den Gesetzgeber normiert.

---

64 EGMR 26.03.1987 Leander gg. Schweden zur Achtung der Privatsphäre.

65 EGMR 25.03.1983 Silver gg. das Vereinigte Königreich = EuGRZ 1984, S. 147 ff.

66 So auch das deutsche Bundesverfassungsgericht in BVerfGE 100, 313 (375 f).

1. Anforderungen an einen effektiven Rechtsschutz[67]

Um die effektive Anwendung der oben genannten Prinzipien sicherzustellen, verlangt der Gerichtshof die folgenden Mindestsicherungen, die ausdrücklich im kodifizierten Recht angeordnet werden müssen, um Missbrauch zu vermeiden: Das Wesen der Straftaten, die Anlass zu einem Abhörbeschluss geben können; eine Definition jener Personengruppen, deren Kommunikation überwacht werden kann; eine Begrenzung der Dauer einer solchen Überwachung; das Verfahren, nach dem bei der Untersuchung, Verwendung und Speicherung der erlangten Daten vorgegangen wird; die Schutzmaßnahmen, die zur Anwendung kommen, wenn die Daten an Dritte übertragen werden; und die Umstände, unter denen die erlangten Daten gelöscht oder die Aufnahmen vernichtet werden können oder müssen.[68] Für den Fall, dass unbeteiligte Dritte von einer Überwachungsmaßnahme betroffen sind (zB als Gesprächspartner eines Verdächtigen), müssen Sicherungsvorkehrungen in Bezug auf deren Daten vorgesehen werden.[69]

2. Kontrolle der Behörden

Nach der Judikatur des EGMR stellt es eine Verletzung des Art 8 EMRK dar, wenn es an einer nachträglichen Überprüfung des Einsatzes geheimer Überwachungsmaßnahmen durch Einrichtungen oder Beamte fehlt, die entweder außerhalb der die Überwachungsmittel einsetzenden Dienstbehörde angesiedelt sind oder zumindest bestimmte Qualifikationen aufweisen müssen, die ihre Unabhängigkeit und die Einhaltung des Rechtsstaatsprinzips sicherstellen.[70]

---

67 Nachfolgend wird beispielhaft vor allem das prototypische Urteil des EGMR Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien vom 18.3.2013[67] zur Illustration der Schwerpunkte herangezogen. Beschw.Nr. 22373/04.

68 EGMR Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 76, unter Verweis auf das Urteil EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 95; vgl. auch EGMR 04.05.2000 Rotaru gg. Rumänien.

69 EGMR 16.02.2000 Amann gg. die Schweiz = ÖJZ 2001, S. 71 ff.

70 EGMR Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 85, im Unterschied zu den Urteilen EGMR 06.07.1978 Klass u.a. gg. Deutschland, RN 70, sowie Weber und Saravia, RN 57.

Zur Unverhältnismäßigkeit führt etwa ein Mangel an Kontrolle, ob diese Maßnahmen tatsächlich den Auflagen der Ermächtigungen für die Überwachungsmaßnahmen entsprechen oder ob die Originaldaten den Tatsachen entsprechend in die schriftlichen Berichte übernommen werden. Ebenso ein Mangel an unabhängiger nachprüfender Kontrolle, ob die Originaldaten innerhalb der erlaubten Frist tatsächlich gelöscht wurden, wenn sich die Überwachung als ergebnislos herausstellte. Insbesondere kritisierte der EGMR das Fehlen einer richterlichen Überprüfung der Überwachungsergebnisse zur Wahrung des Rechtsstaatsprinzips.[71]

Die Übermittlung von Informationen an andere Dienststellen hat sehr strengen Anforderungen gerecht zu werden. Die diesbezüglich notwendige Kontrolle könne etwa einem Beamten, der für die Ausübung eines Richteramts qualifiziert ist, oder einer unabhängigen Kommission anvertraut werden.[72]

Viele der hier angeführten Anforderungen betreffen zunächst verfahrensrechtliche Bestimmungen, organisatorische Vorkehrungen und gesetzlich geregelte Formalvoraussetzungen. Wenn solche normiert sind, dienen sie der Grundrechtsabsicherung und sind daher zwingend durch die Technikgestaltung angemessen abzusichern.

D. RECHTSSTAATLICHKEIT DURCH TECHNIKGESTALTUNG («RULE OF LAW BY DESIGN»)

Die bisherigen Ausführungen sollen zeigen, dass die österreichische Rechtsordnung, insbesondere in Symbiose mit dem Recht der EU alle staatlichen Organen einschließlich den Gesetzgeber dazu verpflichtet, bei jeder Technologiegestaltung zum Einsatz in der öffentlichen Verwaltung die Grundrechte sprichwörtlich «einzubauen». Abgeleitet aus dem modernen Prinzip «privacy by design» bzw. dem in Art 25 DSGVO normierten

71 EGMR Association for European Integration and Human Rights und Ekimdzhiev gg. Bulgarien, RN 85 unter Verweis auf die gegenteiligen Beispiele in den Fällen Klass u.a. gg. Deutschland, RN 20; EGMR 29.06.2006 Weber und Saravia gg. Deutschland, RN 100.

72 RN 89 des Urteils unter Verweis auf das Urteil im Fall EGMR 29.06.2006 Weber und Saravia, RN 125-28.

«data protection by design» wurde oben das Konzpet «human dignity by design» eingeführt und auf die Bedeutung der Interdependenz von Rechtsstaatlichkeit, Grundrechten und Demokratie hingewiesen. Das hier nun vorgestellte Konzept «rule of law by design» ist nichts weiter als eine logische Erweiterung dieser modernen Prinzipien der Informationsgesellschaft. Effektiver (Grund-)Rechtschutz ist in einer zunehmend digitalisierten staatlichen Verwaltung nur denkbar, wenn die Rechtslage möglichst präzise und ohne «Schlupflöcher» in Code umgesetzt wird. Im Idealzustand ist dann nur noch rechtmäßiges Verwaltungshandeln ist dann faktisch nur noch möglich, jedenfalls in den vollständig automatisierten Handlungssträngen.

Solche Technologien erfordern immer eine gesetzliche Grundlage. Am Beginn der legistischen Arbeit hierzu muss eine Wirkungsfolgenabschätzung durchgeführt und nachvollziehbar dokumentiert werden. Den Prüfraster bieten die Grundrechte, wobei eine Orientierung am Konzept der Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO[73] praktisch nützlich ist, weil es dazu einen immer höhere Detailierungsgrad gibt. Diese Folgenaschätzung muss in ein Pflichtenheft münden, welches entlang des Stufenbaus der Rechtsordnung für jeden Abschnitt möglichst klare Handlungsanweisungen nach einem strengen Bestimmtheitsgebot definiert. Dogmatisch wird «Rechtsstaatlichkeit durch Technikgestaltung» hier als Grundsatz vorgeschlagen, der aus den Grundrechten abgeleitet ist und deshalb auch verpflichtend für den einfachen Gesetzgeber wirkt. Er muss die Gestaltungspflichten konkretisieren und dabei – entlang des Stufenbaus der Rechtsordnung – die Regelungsverdichtung delegieren.

[73] Dazu ausführlich KASTELITZ/HÖTZENDORFER/RIEDL, Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, in JAHNEL (Hrsg), Jahrbuch Datenschutzrecht 2017 (2017) 113.

I. Machbarkeit und aktueller Bedarf

1. Praxisbeispiel: Durchlaufstelle (DLS) – strafrechtliche Ermittlung von Telekommunikationsdaten

Das für diesen Beitrag und mich persönlich prägendste Beispiel stammt aus meiner Erfahrung im Rahmen meines Dissertationsprojekts[74] am Ludwig Boltzmann Institut für Menschenrechte mit der Arbeit an der «Studie zur Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung»[75]. Die Notwendigkeit einer Umsetzung der Vorratsdatenspeicherung erforderte auch, die Schnittstelle zur Übergabe der Daten zwischen Behörden und Telekommunikationsanbietern rechtlich zu regeln. Das Konzept der Durchlaufstelle (DLS) wurde dazu als Referenzmodell im Rahmen der BIM-Datensicherheitsstudie entwickelt. Die DLS stellt eine Art elektronisches Postfach dar, über welches anfragende und abfragende Stellen miteinander kommunizieren und Informationen sicher austauschen. Die DLS ist ein Modell für technische und prozedurale Abläufe, nicht jedoch eine Art neue Behörde oder Dienststelle. Normiert wurde die DLS durch die «Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO)»[76]. Die Norm blieb auch nach der Aufhebung der Vorratsdatenspeicherung durch den VfGH[77] bestehen.

Vereinfacht gesagt geht es in dem Konzept darum, dass nur rechtlich gedeckte Auskunftsanfragen überhaupt möglich sind und vom System die begleitenden Rechtsschutzvorkehrungen zwingend eingefordert werden und nicht umgangen werden können. Eine durchgehende Protokollierung sichert den Rechtsschutz ab.

---

74 TSCHOHL, Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, Dissertation, Universität Wien, Rechtswissenschaftliche Fakultät 2011, 26 ff, online unter http://othes.univie.ac.at/17556/ (25.11.2019).

75 Siehe die Dokumentation und die Studie zum Download auf der Website des BIM unter https://bim.lbg.ac.at/de/digital-rights/studie-zur-datensicherheit-umsetzung-vorratsdaten-speicherung (25.11.2019).

76 BGBl. II Nr. 402/2011, zur DLS siehe insbesondere §§ 8 bis 24 der Verordnung sowie der Verweis in § 25 auf die Schnittstellendefinition EP020 in der Anlage zur Verordnung.

77 G47/2012 ua; darauf war die Konstruktion auch ausgelegt, weshalb die begleitende TKG Novellierung die Verordnungsermächtigung ausdrücklich auch auf § 94 TKG gestützt hatte.

2. Schema der Durchlaufstelle (DLS)

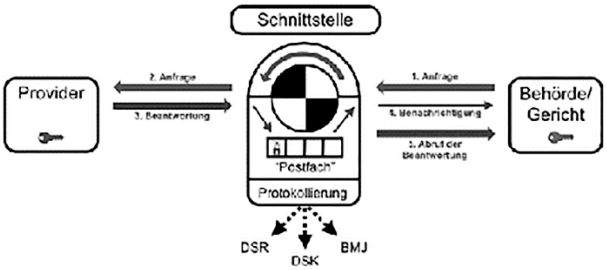

Abbildung 2. Schematische Darstellung der Durchlaufstelle (DLS) zur Ermittlung personenbezogener Daten durch Strafverfolgungsbehörden und Sicherheitspolizei bei Internet- und Telekommunikations-Dienstleistern

Die DLS hat vier Grundfunktionen: 1. Identifizierung, Authentifizierung, 2. Verschlüsselung (Datensicherheit im engeren Sinn), 3. Weiterleitung von Anfragen und deren Beantwortung (Postfachfunktion) und 4. Protokollierung der Auskunftsfälle einschließlich Erstellung einer Statistik. Hierfür muss sich in einer sicheren öffentlichen Infrastruktur ein Server befinden, über den – technisch gesehen – die Anfragen abgewickelt werden. Eine Kommunikation über diesen Server ist dabei nur möglich, wenn die entsprechenden Stellen über eine Berechtigung (Authentifizierung) verfügen. Die verschiedenen Aufgaben im Zusammenhang mit der DLS (zB Schlüsselverwaltung, Benutzerverwaltung, etc.) werden von verschiedenen Stellen übernommen, unabhängig davon, wo die DLS als Server rein physisch betrieben wird (konkret seit 2012 im BRZ). Die DLS ist zwingend die Drehscheibe zur Kommunikation für alle Auskunftsfälle. Kern ist dabei, dass die jeweilige Seite ihre Anforderung/Antwort sicher über die DLS samt des notwendigen Anhangs (Anbieter-Anordnung nach § 139 Abs. 3 StPO, CSV-Datei mit den begehrten Daten) übermittelt.

3. Bedarf aktuell: E-Evidence Regulation/Directive

Die EU unternimmt Schritte zur Verbesserung des grenzüberschreitenden Zugangs zu elektronischen Beweismitteln, indem sie die rechtlichen Rahmenbedingungen dafür

schafft, dass gerichtliche Anordnungen direkt an Diensteanbieter in anderen Mitgliedstaaten gerichtet werden können. Der Rat hat seinen Standpunkt zu einer Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen festgelegt[78]. Seither laufen die Verhandlungen mit dem Europäischen Parlament, wobei es bislang keine finale Einigung gibt.

Ermittler sollen digitale Beweise künftig direkt bei Internetdiensten aus anderen EU-Ländern abfragen können. Es sollen Europäische Herausgabeanordnungen und Sicherungsanordnungen eingeführt werden, mit denen elektronische Beweismittel eingeholt und gesichert werden können, unabhängig davon, wo sich die Daten befinden. Die Pläne sind äußerst riskant. Es fehlen Kontrollinstanzen und Rechtschutzvorkehrungen, die internationalen Rechtshilfemechanismen sollen nicht anwendbar sein.[79]

Im Vergleich zu dem mit der DLS gelösten Problem bringen die mit der E-Evidence Verordnung anvisierten Pläne eine Potenzierung der Herausforderungen. Es gilt nicht nur, das klassische n x m Problem für eine sichere Kommunikation zu lösen. Hier kommt hinzu, dass jeder Mitgliedstaat hier sein eigene nationales Recht hat und kaum Harmonisierung im Unionsrecht besteht.

Der gesamte Rechtspolitische Entstehungsprozess sollte nach dem Konzept «Rule of Law by Design» oder «Rechtsstaatlichkeit durch Technikgestaltung» bereits in der jetzigen Entstehungsphase dringend eine Evaluierung der bisherigen Entwürfe vornehmen. Der Unionsgesetzgeber wird sonst seine Gewährleistungspflichten verletzen.

E. SCHLUSSFOLGERUNGEN

Die Rechtsdurchsetzung durch Technikgestaltung ist ein vielversprechendes Feld für die Gegenwart und Zukunft der Rechtsinformatik. Hier bietet die Technologie große

---

78 Rat der EU, Pressemitteilung 7. Dezember 2018, Verordnung für den grenzüberschreitenden Zugang zu elektronischen Beweismitteln: Rat legt seinen Standpunkt fest: https://www.consilium.europa.eu/de/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/ (25.11.2019).

79 Siehe zur Kritik den zwar nicht wissenschaftlichen aber dennoch gut recherchierten Beitrag im Spiegel Online vom 11.6.2019, https://www.spiegel.de/netzwelt/netzpolitik/e-evidence-warum-die-eu-plaene-zu-digitalen-beweisen-gefaehrlich-sind-a-1270939.html (25.11.2019).

Chancen, Informationstechnologische Systeme in der staatlichen Verwaltung zu zuverlässigen Wächtern des Grundrechtsschutzes auszuprägen. Allerdings erfordert dies den erforderlichen Rechtspolitischen Willen, zumal der Ansatz zu einem Zeitpunkt beginnt, an dem noch gar kein Rechtsakt besteht, der an diesem Maßstab zu messen wäre. Bislang ist der VfGH eher zurückhaltend, Gesetze aufgrund von unterlassener Technologie-Normierung aufzuheben.

Das hier vorgestellte Konzept «Rechtsstaatlichkeit durch Technikgestaltung» versucht zu begründen, dass eine möglichst präzise Umsetzung rechtlicher Vorgaben durch Technologie ein verfassungsrechtlicher Imperativ ist, wenn die Vorgaben dem Schutz bestimmter Grundrechte dienen. Ein solches Prinzip – unabhängig vom Datenschutzgrundrecht oder den neuen Regeln nach der DSGVO – für den allgemeinen Bereich des Verwaltungshandelns, speziell im Hinblick auf die Absicherung von Verfahrensvorschriften aus der Verfassung zwingend abzuleiten, ist rechtswissenschaftlich nicht trivial. Der vorliegende Beitrag erhebt jedenfalls nicht den Anspruch, diese Begründung bereits dogmatisch einwandfrei geliefert zu haben. Hier schlummern noch viele rechtsdogmatische Fragen, die noch nicht einmal angesprochen wurden.

Gleichwohl erhebt der Beitrag den Anspruch, den Bedarf für ein solches Konzept dargestellt und zumindest ansatzweise begründet zu haben. Ich sehe jedenfalls einem wissenschaftlichen Diskurs zu den hier umrissenen Fragestellungen ebenso freudig wie gespannt entgegen. Möge uns Professor Erich Schweighofer dabei fachlich weiterhin herausfordern und mit seinem Wirken auch künftig wissenschaftlich bereichern.