und Gefahrenabwehr droht bei zeitgleicher Anordnung verschiedener heimlicher Überwachungsmaßnahmen die Gefahr einer Rundumüberwachung.[184]

c) Kompensatorische Maßnahmen durch vorausschauendes Datenschutzrecht. Das einfachrechtlich geprägte Datenschutzrecht ermöglicht einen vorausschauenden Umgang der Datenverarbeitung. Gerade durch die Grundsätze des **Datenschutzes durch Technikgestaltung** und durch **datenschutzfreundliche Voreinstellungen** (vgl. Art. 25 DS-GVO) sind wirksame technische Mechanismen zur Rechtsdurchsetzung zu implementieren. Die Berücksichtigung dieser Vorgaben kann auch die Schwere eines Eingriffs im Eingriffsbündel der Überwachungsgesamtrechnung von vornherein durch geeignete technisch-organisatorische und verfahrensrechtliche Maßnahmen minimieren.[185] Weitere Sicherungsmaßnahmen stellen die bestehenden einfachrechtlichen Auskunftsrechte für Betroffene dar, die im Zusammenspiel mit den der Datenverarbeitung vorgelagerten Informations- und nachgelagerten Benachrichtigungspflichten[186] für **Transparenz** sorgen. Gleichsam gewährleisten die Befugnisse der Datenschutzaufsichtsbehörden eine Missbrauchskontrolle.[187] **47**

2. Die eingriffsausschließende Grundrechtsausübung. Ein Verzicht auf das Grundrecht der informationellen Selbstbestimmung ist Bürgern nicht möglich.[188] Ein **Grundrechtsausübungsverzicht** durch den Grundrechtsträger hätte in der Praxis zudem keine den Staat ermächtigende Auswirkung. Der Bürger kann jedoch, anders als dies bei der Menschenwürde der Fall ist[189], über das Vorliegen eines Eingriffs weitreichend disponieren und Verarbeitungen seiner personenbezogenen Daten durch den Staat, aber auch Dritte selbstbestimmt initiieren und unterstützen.[190] Diese Dispositionsmöglichkeit kann der Grundrechtsträger durch eine eingriffsausschließende **Grundrechtsausübung** sowie mithilfe von **Einwilligungen** vornehmen. **48**

Eine staatliche Datenverarbeitung kann nur in eng umgrenzten Ausnahmefällen keinen Eingriff in die informationelle Selbstbestimmung darstellen. Eine solche Ausnahme bildet etwa der Fall, dass die betroffene Person ihre personenbezogenen Daten selbst **allgemein zugänglich macht,** die in diesem Zusammenhang durch den Staat zur Kenntnis genommen werden.[191] Eine solche Grundrechtsausübung des Grundrechtsträgers kann nicht gleichzeitig ein Grundrechtseingriff des Staates sein. Werden diese personenbezogenen Daten jedoch nachfolgend mit weiteren Daten verknüpft und erhalten sie hierdurch einen erweiterten Aussagewert, kommt wiederum ein Eingriff in die informationelle Selbstbestimmung in Betracht.[192] **49**

3. Die Einwilligung als eingriffsausschließendes Gestaltungselement. Die Einwilligung als gestaltendes Element wirkt ebenfalls auf der **Eingriffsebene** und ist keine Einschränkung oder Begrenzung des Schutzbereichs.[193] Nur so kann sichergestellt werden, dass dem Grundrechtsträger jederzeit die Grundrechtsausübung möglich bleibt und einmal erteilte Einwilligungen jederzeit modifiziert werden können. Daher besitzt die Einwil- **50**

[184] *Braun* in Gola/Heckmann, 13. Aufl. 2019, BDSG § 47 Rn. 24; *Schantz* in Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Kap. A Rn. 165.
[185] *Schantz* in Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Kap. A Rn. 165.
[186] BVerfGE 125, 260 (336) = NJW 2010, 833; *Schantz* in Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Kap. A Rn. 168.
[187] BVerfGE 125, 260 (320) = NJW 2010, 833; *Schantz* in Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Kap. A Rn. 169 und 170.
[188] Zum Grundrechtsverzicht vgl. allgemein *Dreier* in Dreier Vor Rn. 129 ff.; Sachs in Sachs Vor Abschn. I Rn. 52; zur Einwilligung *Klement* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 7 Rn. 18.
[189] *Dreier* in Dreier Vor Rn. 133 mwN.
[190] Die Gerichte haben dieser Dispositionsbefugnis im Zusammenhang mit der Menschenwürde Grenzen gesetzt, hierzu BVerwGE 64, 274 (279), VG Neustadt NVwZ 1993, 98 (99).
[191] BVerfGE 120, 351 (361, 362); 142, 234 (251 f.).
[192] BVerfGE 120, 351 (362) = NJW 2008, 2099.
[193] *Scheurer,* Spielerisch Selbstbestimmt, 2019, 34, 93; *Jarass* ZEuP 2017, 310 (329).

ligung lediglich eine **eingriffsausschließende Wirkung.** Ein Eingriff ist nämlich nur dann anzunehmen, wenn hiermit gegen oder auch ohne den Willen des Grundrechtsträgers gehandelt wird.[194] Besteht ein expliziter oder auch nur konkludenter entsprechender Wille, stellt die Datenverarbeitung keinen Eingriff mehr dar.[195]

51 **4. Die Anforderungen an die Einwilligung im Verfassungskontext.** Zum Grundrechtsgebrauch gehört auch die Möglichkeit, über den Umgang mit den eigenen Daten zu disponieren, so dass in diesem Fall kein Eingriff in die informationelle Selbstbestimmung anzunehmen ist. In diesem Zusammenhang müssen zwei Ebenen zum Schutz des Betroffenen auseinandergehalten werden. Erstens hat der Staat die Willensbildung des Einzelnen zu achten **(passive Schutzpflicht).** Zweitens muss der Staat den Bürger befähigen, eine entsprechende Grundrechtsausübung selbstbestimmt vornehmen zu können **(aktives Schutzpflicht).**

52 **a) Autonomieschutz und formelle Wirksamkeitsvoraussetzungen der Einwilligung.** Die **Selbstbestimmung** des Einzelnen ist, unabhängig davon, wo man sie grundrechtlich verorten mag, auch auf der informationellen Ebene zu achten. Autonomieschutz ist Persönlichkeitsschutz und hat auch einen Bezug zur Menschenwürde, weil der freie Wille des Einzelnen ihn gerade als geschütztes Subjekt der Rechtsordnung (und damit nicht als bloßes Objekt staatlichen Handelns) kennzeichnet. In einer zunehmend digitalisierten, automatisierten und vernetzten Welt (→ Rn. 1 ff.), in der individuelles Entscheiden und Handeln vom jeweiligen Kontext der hierdurch erzeugten oder hierfür genutzten Daten nicht mehr getrennt werden kann, ist sicherzustellen, dass eine staatliche Datenverarbeitung am Willen des Grundrechtsträgers auszurichten ist. Hieraus ergeben sich im Umkehrschluss auch **formelle Wirksamkeitsvoraussetzungen** für die Einwilligung.

53 So muss der Einzelne für die wirksame Erklärung der Einwilligung zunächst einen Willen bilden und diesen auch äußern. Somit bedarf es zunächst der **Einwilligungsfähigkeit** des Grundrechtsträgers.[196] Kinder und Personen, die die Konsequenzen ihrer Handlung nicht abschätzen können, können danach nicht eingriffsverhindernd in eine Datenverarbeitung einwilligen. Ist die Person fähig, selbstbestimmte Entscheidungen zu treffen, bedarf es für eine eingriffsausschließende Grundrechtsausübung eines **ausdrücklich oder konkludent geäußerten Willensentschlusses.**[197] Schweigen genügt mithin nicht. Bei der Willensbekundung muss der Betroffene auch über das notwendige Bewusstsein verfügen, dass er gerade eine (grundrechtsrelevante) Einwilligung tätigt. Diese wie auch die folgenden Anforderungen sind in Vorschriften wie den Art. 7, 8 und 12 DS-GVO niedergelegt[198], entsprechen aber bereits einer am Menschenbild des Grundgesetzes und des europäischen Verfassungsrechts orientierten Grundrechtsauslegung.[199]

54 Aufgrund der Grundrechtsrelevanz der Einwilligung kann diese nicht durch Dritte für den Grundrechtsträger erklärt werden, sondern muss durch ihn **persönlich** vorgenommen werden.[200] Im Rahmen der Einwilligungserklärung in Bezug auf die eigenen Daten kann sich der Grundrechtsträger auch menschlicher oder technischer Unterstützung bedienen. Eine Einwilligung in eine Datenverarbeitung, die die informationelle Selbstbestimmung eines Dritten tangieren würde, ist hingegen nicht möglich. Auch in Bezug auf dem Grundrechtsträger zuzuordnende personenbezogene Daten, die gleichsam Informationen zu anderen Grundrechtsträgern beinhalten, besteht mithin keine eingriffsausschließende **Dispositionsbefugnis.**

---

194 BVerfGE 120, 351 (362) = NJW 2008, 2099; *Dreier* in Dreier Vor Rn. 129.
195 *Dreier* in Dreier Vor Rn. 129 mwN; so auch *Bethge* VVDStRL 57, 45.
196 So auch *Sachs* in Sachs Vor Abschn. I Rn. 56, der insoweit von „Einsichtsfähigkeit" spricht; vgl. *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 32 ff.
197 BVerfGE 106, 28 (44 ff.) = NJW 2003, 2375; *Sachs* in Sachs Vor Abschn. I Rn. 55.
198 Hierzu exemplarisch *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 31 ff.
199 Hierzu *Scheurer,* Spielerisch selbstbestimmt, 2019, 93 ff., 114 f.
200 Gegen eine wirksame Einwilligung des Betreuers in Zwangsbehandlungen zB BVerfGE 128, 282 (301 ff.).

Die Einwilligung muss sich zudem auf **bestimmte Datenverarbeitungsvorgänge** und **55**
auf bestimmte, den Grundrechtsträger betreffende Daten konkretisiert haben.[201] Allerdings ist die persönliche Autonomie des Einzelnen hinreichend gewahrt, wenn er die Möglichkeit besitzt, Datenverarbeitungen insoweit zu gestatten, dass er **typenbasierte Erklärungen** in Bezug auf Verarbeitungsprozesse und die zu verarbeitenden Daten abgibt und hierdurch Handlungslinien für die datenverarbeitende Stelle vorgibt. Blankoeinwilligungen genügen diesem Erfordernis nicht. Die informationelle Selbstbestimmung erfordert jedoch auch nicht, dass der Grundrechtsträger in jeden einzelnen Datenverarbeitungsprozess jedes gesonderten personenbezogenen Datums einzeln einwilligen muss. Eine Disposition nach Datenkategorien (zB Blutwerte, Röntgenbilder) ist mithin als ausreichend zu werten.

Die informationelle Selbstbestimmung schützt zwar nach ihrer Zielrichtung den Einzel- **56**
nen vor ungewollten Datenverarbeitungen. Dennoch besitzt dieses Grundrecht noch eine weitere Komponente – es sichert die **Autonomie des Einzelnen.** Hierdurch wird jeder geschützt, selbstbestimmt mit Daten, die einen Bezug zu seiner Person haben, zu verfahren. Daher darf der Staat den Einwilligenden bei seiner Willensbildung auch nicht täuschen oder ihn mittels Drohung zur Äußerung eines aufgedrängten Willens veranlassen. Die Einwilligung muss somit **freiwillig** durch den Berechtigten erklärt werden.

Aus Gründen des Autonomieschutzes wird teilweise vertreten, dass im Rahmen eines **57**
Über-Unterordnungs-Verhältnisses, wie dies zwischen einem Staat und seinen Bürgern besteht, keine freie Willensbildung möglich ist.[202] Vielmehr sei eine **latente unzulässige Willensbeeinflussung** anzunehmen. Damit wäre eine Einwilligung in eine Verarbeitung personenbezogener Daten gegenüber dem Staat niemals eingriffsausschließend möglich. Dem ist entgegenzuhalten, dass auch bei anderen Grundrechten Dispositionsbefugnisse hinsichtlich der Ausübung und Reichweite des Schutzbereichs mit eingriffsausschließender Wirkung durch den Grundrechtsträger bestehen. Da Grundrechtsschutz immer gegen den Staat gerichtet ist, wäre ein kategorischer Ausschluss dieser Möglichkeit vielmehr selbstbestimmungsverkürzend. Somit ist dieser Auffassung in ihrer Absolutheit nicht zu folgen; vielmehr besteht auch in dieser Konstellation die Möglichkeit der Einwilligung, die Dispositionsbefugnis kann jedoch im Einzelfall verkürzt werden. Im Staat-Bürger-Verhältnis gibt es Bereiche, in denen die freie Willensbildung des Betroffenen keine Bedeutung für die Rechtfertigung eines Eingriffs haben kann. Hierzu gehören insbesondere diejenigen staatlichen Aufgaben, die mit der Ausübung des staatlichen Gewaltmonopols zusammenhängen. Dies gilt insbesondere für die Strafverfolgung sowie repressives Exekutivhandeln, wie dies durch die **Eingriffsverwaltung,** etwa die Finanzämter oder Aufsichtsbehörden erfolgt.

Im Rahmen der **Leistungsverwaltung** kann die Einwilligung von Bürgern die staatliche **58**
Datenverarbeitung ermöglichen. Neben einer wirksamen Einwilligung des Betroffenen muss die Datenverarbeitung allerdings auch im **objektiven Interesse des Bürgers** liegen. Dies ist bei **staatlichen Angeboten** anzunehmen, von denen Bürger **freiwillig,** also ohne Rechtspflicht Gebrauch machen können. Hierzu gehört bspw. die freiwillige Krisenvorsorgeliste (ELEFAND) des Auswärtigen Amts, in die sich deutsche Staatsangehörige für die Dauer ihres Auslandsaufenthalts eintragen können, um in Not- oder Krisensituationen Unterstützung durch das Ministerium zu erhalten.[203] Gleiches gilt für die freiwillige Nutzung der elektronischen Patientenakte für Versicherte von gesetzlichen Krankenkassen.[204]

---

[201] Vgl. zur Bestimmtheit der Einwilligung *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 63 f.

[202] Vgl. zum öffentlichen Subordinationsverhältnis *Klement* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 7 Rn. 51 ff.; zum Machtungleichgewicht *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 52.

[203] https://krisenvorsorgeliste.diplo.de/ (abgerufen am 3.2.2022).

[204] BVerfG NJW 2021, 1300 mit Anm. *Rachut,* JurisPR ITR 5/2021 Anm. 5; hierzu auch *Heckmann/Rachut* in Rehmann/Tillmanns, E-Health / Digital Health, 2022, Kap. 3 E. Rn. 571 ff.

59 Darüberhinausgehend ist eine **Einschränkung der Einwilligungsmöglichkeit** und damit der Ausübung der informationellen Selbstbestimmung nur möglich, wenn und soweit dies zum Schutz weiterer verfassungsrechtlich geschützter, höherwertiger Interessen erfolgt. Diese Einschränkung der Ausübungsfreiheit einer Einwilligung muss gesetzlich normiert werden. Neben dem Schutz von Interessen Dritter kommen auch Staatsschutzinteressen in Betracht.

60 **b) Befähigung zur Grundrechtsausübung.** Aufgrund der zunehmenden **Komplexität digitaler Datenverarbeitungen** und daraus erwachsender Folgewirkungen ergibt sich ferner eine aktive **staatliche Bildungs- und Informationspflicht** in diesem Bereich. Dieser Vorgabe ist der Staat durch die Schaffung umfangreicher einfachgesetzlicher Informationspflichten nachgekommen. Diese aktive Handlungspflicht des Staates muss auch in der Praxis umgesetzt werden. Danach ist der Einzelne vor der Einwilligungserklärung über die Datenverarbeitung und damit verbundene Konsequenzen zu informieren. Wird dies im Einzelfall unterlassen und die weitergehende Befähigung, entsprechende Erklärungen zu verstehen, nicht durch Bildungsmaßnahmen hinreichend gefördert, ist trotz geäußerten Willens des Einzelnen ein Eingriff in die informationelle Selbstbestimmung anzunehmen. Je komplexer die Verarbeitung von Daten und die damit zusammenhängenden Folgewirkungen im Einzelfall für den Grundrechtsträger sind, desto umfassender müssen die jeweiligen Maßnahmen zur Sicherung der Handlungsbefähigung des Einzelnen sein. Nur so kann gewährleistet werden, dass der Einzelne in seiner **Handlungsautonomie** geschützt ist.

61 Ein **Eingriff** in die informationelle Selbstbestimmung ist damit nach dem modernen Eingriffsbegriff in jeder **Verarbeitung von Bürgerdaten** durch den Staat zu sehen, sofern die Person, deren personenbezogene Daten betroffen sind, nicht zuvor in Ausübung ihres freien Willens in diese Verarbeitung informiert eingewilligt hat.[205]

II. Schranken der informationellen Selbstbestimmung

62 Der **Grundrechtsinhaber** besitzt zwar umfassende Möglichkeiten der Grundrechtsausübung. Umgekehrt hat er jedoch kein „Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit".[206] Somit können auch Daten, die sich auf eine konkrete Person beziehen, „nicht ausschließlich dem Betroffenen allein zugeordnet werden [...]. Das Grundgesetz hat, wie in der Rechtsprechung des BVerfG mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der **Gemeinschaftsbezogenheit** und **Gemeinschaftsgebundenheit** der Person entschieden".[207]

63 Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) sowie dessen verschiedene Ausprägungen wie die informationelle Selbstbestimmung stehen formell unter dem **Vorbehalt der Schrankentrias,** dh der Verletzung von Rechten anderer, der verfassungsmäßigen Ordnung und des Sittengesetzes. Diese gehen in der verfassungsmäßigen Ordnung als Schranke auf.[208] Somit steht dieses Grundrecht unter einem einfachen **Gesetzesvorbehalt.**[209] Die Herleitung der informationellen Selbstbestimmung aus der Menschenwürde führt zu keinem anderen Ergebnis. Eine Einschränkung dieses Grundrechts bedarf daher einer gesetzlichen Grundlage. Aufgrund der pluralen Notwendigkeiten von Datenverarbeitungen zur staatlichen Aufgabenerfüllung insbesondere im Bereich der Ein-

[205] *Scheurer,* Spielerisch selbstbestimmt, 2019, 33; *Klement,* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO Art. 7 Rn. 18.
[206] BVerfGE 65, 1 (43 f.) = NJW 1984, 419.
[207] BVerfGE 65, 1 (44) = NJW 1984, 419 mit Verweis auf BVerfGE 4, 7 (15); 8, 274 (329); 27, 1 (7); 27, 344 (351 f.); 33, 303 (334); 50, 290 (353); 56, 37 (49).
[208] BVerfGE 6, 32; 65, 1 (43 f.).
[209] *Schantz* in Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Kap. A Rn. 158.

griffs- sowie Leistungsverwaltung gibt es im staatlichen Mehrebenensystem im Bund und den Ländern insgesamt über 1.200 Gesetzeswerke, die datenschutzrechtliche Regelungen beinhalten. Diese werden durch weitere 550 Rechtsverordnungen mit Vorgaben zum Datenschutz in Deutschland ergänzt. Gemeinsam enthalten diese Regelwerke **unzählige Ermächtigungen** zur Datenverarbeitung.[210]

III. Verfahrensvorkehrungen zur angemessenen Ausgestaltung der Datenverarbeitung

Damit die geschaffenen gesetzlichen Regelungen, die eine Datenverarbeitung auch ohne oder entgegen der Willensäußerung des Grundrechtsträgers gestatten, müssen diese Normen wiederum verfassungsgemäß sein und insbesondere dem **Grundsatz der Verhältnismäßigkeit** entsprechen. Der legitime Zweck einer Datenverarbeitung kann sich sowohl auf verfassungsrechtlich geschützte Interessen Dritter als auch auf überwiegende Allgemeininteressen[211] stützen. Des Weiteren muss die normative Begrenzung der informationellen Selbstbestimmung geeignet, erforderlich und im Einzelfall angemessen sein. **64**

Entsprechende Erlaubnistatbestände für die Datenverarbeitung bestehen in der Praxis sowohl für staatliche als auch für **privatwirtschaftliche Akteure.** Die informationelle Selbstbestimmung schützt nämlich nicht nur Bürger vor staatlichen Eingriffen, sondern verpflichtet auch den Staat, dem diesbezüglichen Grundrechtsschutz seiner Bürger durch die Schaffung einer entsprechenden Rechtsordnung Geltung zu verleihen.[212] Obwohl die Grundrechte vorrangig Abwehrrechte gegen den Staat darstellen, wurde mit der Volkszählungsentscheidung[213] durch das BVerfG der Staat in die Pflicht genommen, den Schutz der informationellen Selbstbestimmung einfachgesetzlich derart zu normieren, dass auch eine unbegrenzte Datenverarbeitung durch Private unterbunden wird. Somit hat diese Entscheidung einen wichtigen Meilenstein in der Geschichte des Datenschutzrechts gelegt. Eine den Grundrechtsträger auch vor Privaten nicht hinreichend schützende einfachgesetzliche Rechtsordnung kann dazu führen, dass das unregulierte Handeln Privater als mittelbarer Eingriff in die informationelle Selbstbestimmung dem Staat zuzurechnen ist. Für eine **Zurechnung** des schädlichen **Verhaltens Privater** genügt es regelmäßig, wenn dieses voraussehbar war und der Staat dem Handeln keinen Einhalt geboten hat.[214] Über die Regulierung hinaus muss der Staat auch **wirksame Durchsetzungsmechanismen** etablieren. Dieses Bedürfnis wird durch die Verbreitung moderner Datenverarbeitungstechnologien verstärkt. Für den Bürger müssen unabhängig von der datenverarbeitenden Stelle zum Beispiel Ansprüche geschaffen werden, wonach dieser jederzeit wissen kann, welche Informationen über ihn gespeichert werden und wer diese Daten zu welchem Zweck verarbeitet.[215] Ebenso hat die staatliche Datenschutzaufsicht nicht nur behördliche, sondern auch betriebliche Datenverarbeitungen zu kontrollieren. Sanktionen drohen prinzipiell allen Personen und Institutionen, die gegen geltendes Datenschutzrecht verstoßen.[216] **65**

Durch die globale, alle Lebensbereiche umfassende Datenverarbeitung im privatwirtschaftlichen Bereich entstehen auch außerhalb der staatlichen Sphäre weitreichende **Grundrechtsgefährdungslagen** für die von der Datenverarbeitung betroffenen Personen. **66**

Große datenverarbeitende Unternehmen verarbeiten nicht mehr nur Daten von Grundrechtsträgern und erstellen Profile, sondern nutzen die Möglichkeiten der **Informationstechnologie,** um Bürger zu veranlassen, ihre Dienste intensiver zu nutzen, was zu einer Generierung weiterer Daten und immer besserer Anwendungen für **Verhaltens-** **67**

---

[210] *Di Fabio* in Dürig/Herzog/Scholz GG Art. 2 Abs. 1 Rn. 179 spricht insoweit von staatlicher „Informationsvorsorge".
[211] BVerfGE 65, 1 (44) = NJW 1984, 419.
[212] BVerfGE 65, 1 (43) = NJW 1984, 419.
[213] BVerfGE 65, 1 (43) = NJW 1984, 419.
[214] *Voßkuhle/Kaiser* JuS 2009, 313.
[215] Vgl. BVerfGE 65, 1 (43) = NJW 1984, 419.
[216] Beachte aber auch die Ausnahmen in Art. 83 Abs. 7 DS-GVO, § 43 Abs. 3 BDSG.

prognosen führt. Diese Technologien ermöglichen in der Folge auch **Verhaltensbeeinflussungen** von Nutzern, wie das Datenanalyse-Unternehmen Cambridge Analytica mit der Einflussnahme auf die US-Wahlkampf-Kandidaturen sowie die Präsidentschaftswahl in den USA im Jahr 2016 aufgezeigt hat. Hierdurch wird die Autonomie der Bürger im Sinne einer freien, unbeeinflussten politischen Willensbildung und -betätigung, nachhaltig gefährdet.

68 Der Gesetzgeber hat daher die informationelle Selbstbestimmung durch ein umfassendes **einfachgesetzliches Regelwerk** für private Akteure konkretisiert. Der Schutz der informationellen Selbstbestimmung erfolgt nämlich nicht nur durch Achtung der Entscheidungsautonomie des Einzelnen, sondern wird auch durch weitere **Verfahrensvorschriften** sichergestellt, die die Befähigung der Bürger unterstützen sollen.[217] Wenn der Staat nicht alles beherrschen und beaufsichtigen kann, dann muss er die Grundrechtsträger zumindest zum Selbstschutz befähigen. Dies gilt gerade für den globalen digitalen Raum. Dem wird im Rahmen der Datenschutzregulierung unter anderem durch die Pflicht zur Bereitstellung von **Datenschutzerklärungen** und die Information über die Betroffenenrechte begegnet. Darüber hinaus hat der Gesetzgeber Vorgaben zum **Datenschutzmanagement** aufgestellt, die eine Implementierung von organisatorischen Sicherungsmechanismen bei datenverarbeitenden Stellen fordern. Diese werden durch das Verbotsprinzip ergänzt, wonach eine Verarbeitung personenbezogener Daten ohne das Vorliegen eines gesetzlichen Erlaubnistatbestandes oder einer informierten Einwilligung der betroffenen Person untersagt ist. Hinzu kommen weitergehende Kontrollmechanismen sowie Sanktionsregelungen.

69 Unabhängig von der verfassungsrechtlichen Wertung eines nationalen Datenschutzgesetzes muss dieses auch **europarechtskonform** gestaltet sein und daher im Anwendungsbereich der Datenschutzgrundverordnung[218] bzw. der JI-Richtlinie[219] oder der ePrivacy-Richtlinie[220] bzw. künftig der ePrivacy-Verordnung, den jeweiligen Spezifizierungsvorgaben genügen.

IV. Typische Gefährdungslagen und Auflösung von Grundrechtskollisionen

70 Durch die **Verarbeitung personenbezogener Daten** können verschiedene typische Gefährdungslagen entstehen, die es bei der Schaffung einfachrechtlicher Datenschutzregelungen zu berücksichtigen gilt. Das so entstehende Datenschutzrecht erweist sich gleichsam als „**konkretisiertes Verfassungsrecht**".[221] Gerade der umfassende politische Aushandlungsprozess der europäischen Datenschutzgrundverordnung[222] zeigt, wie bestehende **Grundrechtskollisionen** in schonenden Ausgleich gebracht und notwendige Erlaubnistatbestände und Sicherungsmechanismen geschaffen werden können.

71 **1. Verarbeitung personenbezogener Daten als abstraktes Gefährdungsszenario.** Die mit der Verarbeitung von personenbezogenen Daten geschaffene **abstrakte Gefahr** war Anlass für das BVerfG, das Grundrecht der informationellen Selbstbestimmung umfassend auszuprägen.[223] Das Gericht hat im Rahmen des **Volkszählungsurteils** daher die Selbstbestimmung des Einzelnen näher definiert. Danach darf grundsätzlich jeder eigenständig „entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden"[224].

---

217 *Di Fabio* in Dürig/Herzog/Scholz GG Art. 2 Abs. 1 Rn. 182.
218 VO (EU) 2016/679.
219 RL (EU) 2016/680.
220 RL (EU) 2002/58/EG.
221 Vgl. hierzu *Werner* in Mensch und Verwaltung, 1963, 83 ff.
222 Zur Entstehungsgeschichte der DS-GVO *Selmayr/Ehmann* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Einf. Rn. 9 ff.; *Paal/Pauly* in Paal/Pauly, DS-GVO – BDSG, 3. Aufl. 2021, Einl. Rn. 5 ff.; *Wolff/Brink* in BeckOK Datenschutzrecht, 38. Ed. 2021, Einl. Rn. 16 ff.; *Hornung/Spiecker gen. Döhmann* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Einl. Rn. 155 ff.
223 BVerfGE 65, 1 = NJW 1984, 419.
224 BVerfGE 65, 1 (42); 78, 77 (84); 103, 21 (33).

Die mit der Datenverarbeitung einhergehende Gefährdungslage ist durch die **elektronische Datenverarbeitung** gewachsen und durch die mit der Digitalisierung verbundene Vernetzung und Automatisierung sogar exponentiell gestiegen. Deshalb kann heute realistisch nicht davon ausgegangen werden, dass Bürger überhaupt noch einen Überblick darüber haben, wo, von wem und zu welchen Zwecken die eigenen Daten verarbeitet werden. Eine Rückverfolgbarkeit von Datenverarbeitungen ist aufgrund der mannigfaltigen Möglichkeiten in diesem Bereich technisch aktuell nicht sicherzustellen. Lediglich durch entsprechende Datenbankarchitekturen, digitale „Wasserzeichen" und ähnliche Vorkehrungen könnte perspektivisch Transparenz im Umgang mit personenbezogenen Daten hergestellt werden. 72

Durch die gestiegenen Möglichkeiten, Datenbanken und Profile anzulegen und diese zu verknüpfen, besteht das Risiko, das **Verhalten** von Individuen **vorhersehbar** zu machen und gegebenenfalls dieses Verhalten aufgrund der bestehenden Wissensbasis zu beeinflussen.[225] Je weitreichender die Nutzung von personenbezogenen Daten die Selbstbestimmung des Einzelnen tangiert, desto größer ist seine Gefährdungslage. Die informationelle Selbstbestimmung schützt den freien Willen und verbietet dessen Manipulation. Die Nutzung von datenbasierten Analysen zur manipulativen **Verhaltensbeeinflussung** eines einzelnen Bürgers in Form eines gezielten (staatlichen) Nudgings ist unzulässig.[226] 73

2. Konkrete Gefährdungslagen durch staatliche Datenverarbeitung. Die informationelle Selbstbestimmung schützt Bürger insbesondere vor ungerechtfertigten Eingriffen in Form von Datenverarbeitungen durch den Staat. Hierzu gehört die Datenerfassung im Einzelfall, allerdings auch die **systematische Erfassung von Daten** sowie die entsprechende Regulierung. Gerade im Bereich der Strafverfolgung gibt es verschiedene Datenverarbeitungen in offener (zB Durchsuchung und Sicherstellung) oder verdeckter Form (zB Online-Durchsuchung).[227] Im Rahmen zunehmender elektronischer Verwaltungsverfahren (zB elektronischer Fachverfahren[228]) und elektronischer Registerführung werden personenbezogenen Daten von Bürgern verarbeitet. Diese Datenverarbeitungen können im Einzelnen oder in der Gesamtbetrachtung dazu führen, dass die datenverarbeitende Behörde ein datenbasiertes Persönlichkeitsprofil einer Person erhält. Je größer der Personenkreis ist, der auf diese Daten zugreifen kann, desto höher wird die Gefahr für den Bürger bewertet. Mithin bedarf es bei der Einführung von entsprechenden **elektronischen Datenverarbeitungssystemen** eines angemessenen Rechte- und Rollenmanagements. Das mit einer entsprechenden Datenverarbeitung verbundene Risiko besteht vor allem in möglichen **Diskriminierungen** von Bürgern aufgrund bestimmter Merkmale. Dies geht bis zu Persönlichkeitsausprägungen und optischen Merkmalen eines Menschen, die in der deutschen Geschichte schon einmal für gravierende Repressalien genutzt wurden. Auch in der datenschutzrechtlichen Regulierung in Art. 9 DS-GVO wurden besonders schützenswerte sensible Daten benannt, deren Verarbeitung noch weiter eingeschränkt ist als jene bei sonstiger Datenverarbeitung. 74

Heimliche staatliche Datenverarbeitungen stellen ein gesteigertes Risiko für die informationelle Selbstbestimmung des Einzelnen dar, da hierbei der Betroffene um die Möglichkeit des Rechtsschutzes gebracht wird.[229] Deshalb sind heimliche Maßnahmen, die auch noch weitere Sicherheitsrisiken für die informationstechnischen Systeme des Einzelnen schaffen, wie dies beim sog. Bundestrojaner der Fall ist, auch als Eingriff in die informationelle Selbstbestimmung des Einzelnen zu werten, zumal hierbei der gesamte 75

[225] *Goanta/Mulders* EuCML 2019, 136 (142).
[226] Zum Begriff des Nudgings *Hufen* JuS 2020, 193 (193 f.); zu den verfassungsrechtlichen Maßstäben des Nudgings s. *Gerg,* Nudging: verfassungsrechtliche Maßstäbe für das hoheitliche Einwirken auf die innere Autonomie des Bürgers, 2019, 88 ff.
[227] *Blechschmitt* MMR 2018, 361.
[228] Technische Informationssysteme zur Datenverarbeitung im Rahmen von Verwaltungsaufgaben, zB bei der Steuerberechnung oder Registerführung.
[229] *Becker* NVwZ 2015, 1335 (1336); BVerfGE 120, 274 (325) = NJW 2008, 822.

Rechner ausspioniert werden kann und gleichsam keine Kenntnis über den Datenabfluss beim Betroffenen besteht. Ferner verstößt die heimliche Installation einer entsprechenden Software gegen das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme.[230]

76 Allerdings kann auch eine **heimliche staatliche Datenauswertung** gerechtfertigt werden, wenn hierdurch die Aufklärung schwerer Straftaten sowie deren Vollendung verhindert werden kann. In diesem Fall überwiegt bei einer generellen Abwägung das Grundrecht auf Leben und körperliche Unversehrtheit von Opfern einer Straftat sowie das Strafverfolgungsinteresse gegenüber der informationellen Selbstbestimmung des dringend Tatverdächtigen.[231]

77 In der **Veröffentlichung von Informationen** über Bürger oder Privatrechtssubjekte im Zuge des „staatlichen Informationshandelns" (staatliche Warnungen, Verbraucherinformationen) kann ebenfalls die informationelle Selbstbestimmung der Betroffenen tangiert sein. Sie tritt jedoch häufig hinter anderen (spezielleren) Grundrechten zurück.[232]

78 Auch die Erfassung von Bürgerdaten in (elektronischen) **Registern** kann als Eingriff gewertet werden, der wiederum – je nach konkreter Zwecksetzung und Ausgestaltung – verfassungsrechtlich auf der Grundlage der jeweiligen Registergesetze gerechtfertigt werden kann. Es gibt in Deutschland inzwischen über 375 einzelne Register, die dezentral oder zentralisiert betrieben werden.[233] Im Rahmen der Bundeskompetenzen wurden verschiedene **bereichsspezifische, zentralisierte Register** errichtet. Während das Bundeszentralregister die Strafrechtspflege bei der Verhängung von schuldangemessenen Strafen unterstützt und die Berücksichtigung von (einschlägigen) Vorstrafen in der Täterbiografie nachweisbar sichert, wird mit dem Fahreignungsregister sichergestellt, dass nur Personen ein Kraftfahrzeug führen, die sich bisher im Verkehr nicht als ungeeignet erwiesen haben.

79 Zudem gibt es ein **zentrales Vorsorgeregister** sowie ein **zentrales Testamentsregister.** Diese haben die Aufgabe, freiwillig eingereichte Dokumente einer Person für den Fall der Geschäftsunfähigkeit oder im Todesfall deutschlandweit abrufbar bereitzuhalten und hierdurch erst der Selbstbestimmung des Einzelnen Geltung zu verschaffen. Die thematisch getrennte (teilweise zentrale) Erfassung von Daten in Registern ist zulässig, wenn hierfür ein Gesetz entsprechend dem Gesetzesvorbehalt der informationellen Selbstbestimmung geschaffen wird und dieses einem legitimen Zweck dient. Der Registerzweck liegt in der Regel darin, bestimmte für die Erledigung von Verwaltungsaufgaben erforderliche Informationen effizient bereitzustellen. Ferner muss die Datenerfassung in einem staatlichen Register geeignet und erforderlich sowie die rechtliche (und technische) Gestaltung im Einzelnen angemessen sein. Über Tilgungsbestimmungen der hinterlegten Daten wird sichergestellt, dass die Daten nur so lange gespeichert werden, wie dies für den jeweiligen Zweck erforderlich ist.[234]

80 Ein Großteil der Register wird in den Ländern oder auf kommunaler Ebene geführt, so dass die **Registerlandschaft** einem **IT-Flickenteppich** gleicht und Daten vielfach redundant verarbeitet werden sowie teilweise veraltet und fehlerhaft sind. Beispielsweise werden die Melderegister durch die Meldeämter in den Kommunen dezentral geführt. Weitere lokal begrenzte Register sind die Personenstandsregister (Eheregister, Lebenspartnerschaftsregister, Geburtenregister, Sterberegister) bei den einzelnen Standesämtern. Durch die aktuelle Registerarchitektur müssen Bürger viele ihrer Daten immer wieder der Verwal-

[230] BVerfGE 120, 274 = NJW 2008, 822.
[231] BVerfGE 120, 274 (328) = NJW 2008, 822.
[232] BVerfGE 105, 252 = NJW 2002, 2621 (Glykol); BVerfGE 113, 63 (Junge Freiheit); BVerwG NVwZ-RR 2015, 425 (Warnung vor E-Zigaretten); BVerfGE 148, 40 („Lebensmittelpranger"); *Voßkuhle/Kaiser* JuS 2018, 343 (345) mwN.
[233] IT-Planungsrat, Registermodernisierung: Zielbild und Umsetzungsplanung, S. 12, abrufbar: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-05_Registermodernisierung.pdf (abgerufen am 31.1.2022).
[234] Vgl. BVerfGE 36, 174; zur Tilgung im BZRG bei Erledigung vgl. § 49 Abs. 1 S. 1 BZRG; zur Tilgung im Verkehrszentralregister vgl. § 29 StVG, zur Löschung von Daten bei Meldebehörden vgl. § 14 BMG.