

„Die Persönlichkeit ist eines unserer heiligsten Güter, einer der Tragpfeiler der menschlichen Kultur. Eine Rechtsordnung, die sich außerstande erklärt, ihr angemessenen Schutz zu verleihen, gesteht offen ihre Ohnmacht ein.“¹

„Der freiheitliche Staat lebt von Voraussetzungen, die er selbst nicht garantieren kann.“²

¹ Smoschewer, Ufita (1930), S. 349 (370).

² Böckenförde, Die Entstehung des Staates als Vorgang der Säkularisation, in: *ders*: Recht, Staat, Freiheit, 1991, S. 92 (112).

Einleitung und Gang der Untersuchung

A. Einleitung

Gegenstand dieser Untersuchung sollen die staatlichen Schutzpflichten der Bundesrepublik Deutschland für ihr Staatsvolk³ i.S.v. Art. 116 Abs. 1 GG sein. Anknüpfend an Entwicklungen zur Haftung für technische Großanlagen im Umweltrecht soll untersucht werden, ob und gegebenenfalls welche Art von Schutzpflichten der Staat für sein Staatsvolk im Informationszeitalter hat und wie weit diese Schutzmaßnahmen inhaltlich reichen. Im 1. Teil wird es darum gehen, die umfangreichen staatsrechtlichen Grundlagen, insbesondere auch unter Berücksichtigung des historischen Kontextes zu analysieren. Im 2. Teil wird sodann der Bezug der Kernaussagen der Rechtsprechung zu den Schutzbereichen relevanter Grundrechte - Recht auf informationelle Selbstbestimmung, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10 Abs. 1 GG, Art. 13 Abs. 1 GG abstrahiert und auf mögliche subjektiv-öffentlich rechtliche Ansprüche untersucht. Hierbei wird die Gefährdung des Persönlichkeitsrecht anhand von drei aktuellen Beispielen dargestellt werden. Es werden insbesondere die Begriffe Risiko und Gefährdung dogmatisch eingeordnet und es wird erörtert, welche konkreten Schutzmaßnahmen der Staat zum Schutz des allgemeinen Persönlichkeitsrecht treffen kann oder sogar zu treffen hat.

Mit den tiefgreifenden und grundlegenden technischen Veränderungen im Bereich der Informationstechnologie und der Vernetzung von Personalcomputern hat sich auch ein entsprechender weitgehender gesellschaftlicher Wandel vollzogen.⁴ Das tägliche Leben eines jeden Einzelnen ist ohne informationstechnische Verarbeitungssysteme kaum mehr vorstellbar. Sei es, dass bei der Erstellung dieser Arbeit ein Computer genutzt wird oder bei der Literaturrecherche neben klassischen Zeitschriften auch Datenbanken und Onlineartikel. Aber auch im privaten Umfeld vieler Bürger haben soziale Netzwerke und Informationsaustausch mittels technischer Geräte (Computer, Telefon, Handy, Smartphone, Tabletcomputer) Einzug gehalten. Weiter bieten selbst Fernseh- und andere Haushaltsgeräte die

³ Hinsichtlich des persönlichen Schutzbereichs ist bei den Grundrechten zwischen solchen, die für alle Menschen unabhängig von ihrer Staatsangehörigkeit gelten und jenen, die direkt an die Staatsangehörigkeit i.S.v. Art. 116 GG anknüpfen, zu unterscheiden. Art. 2 Abs. 1 GG gilt als Auffanggrundrecht für deutsche Staatsbürger und Ausländer gleichermaßen: *Murswiek/Rixen*, in: *Sachs*, Kommentar zum GG, 8. Aufl., 2018, Art. 2, Rn. 139.

⁴ *Härtel*, LKV 2019, 49 ff.

Möglichkeit, mit anderen Geräten zu kommunizieren, sprich zum Datenaustausch. Sämtliche der genannten Anwendungsbeispiele haben eine Gemeinsamkeit: technisch bedingt werden Daten erzeugt und gespeichert, sie sind quasi Schuhabdrücke, die jeder Mensch im Schnee hinterlässt. Diese Daten können gebündelt und ausgewertet werden, um sie anschließend konkreten Personen zuordnen zu können. Die Daten lassen sich auch verknüpfen, verändern, unterdrücken. Hierdurch können Dritte den betroffenen Bürgern enorme materielle und immaterielle Schäden zufügen. Es ist technisch beispielsweise möglich, die bei einer Bestellung eines Buches in einem Online-Buchgeschäft oder die von Geräten im Rahmen von deren zweckbestimmten Nutzung selbst erzeugten Daten so auszuwerten, dass z.B. anhand der so gewonnenen weiteren Aussagen quasi künftige Bestellungen vorgeschlagen werden. Soweit diese Möglichkeit noch als „Normalfall“ empfunden wird, so treten spätestens bei medizinischen Daten die Probleme offen zu Tage. Wer sammelt die Daten? Wer wertet sie aus? Wie werden diese Daten geschützt? Welche technischen Vorkehrungen werden getroffen? Entsprechen etwaig getroffene Schutzmaßnahmen dem Stand der Technik und sind diese in der Fachwissenschaft anerkannt? Wer fügt die Daten aufgrund welcher Rechtsgrundlage zusammen, um weitergehende Informationen zu generieren, die aus den Einzelinformationen selbst nicht erschlossen werden?

Die vorgenannten Beispiele von technischen Anwendungen, die mit Sicherheit keinen Anspruch auf Vollständigkeit hinsichtlich des grundrechtlichen Schutzbedarfs erheben, zeigen jedoch deutlich, in welchem Maß sie das Leben und die Lebensweise eines jeden Bürgers immer weiter durchdringen und auch beeinflussen. Niemand mag sich vorstellen, dass seine Daten, die der Hausarzt für die Behandlung benötigt, Dritten zur Kenntnis gelangen. Welches Risiko verbirgt sich für den Betroffenen, wenn höchstpersönliche Daten von Versicherungen oder Arbeitgebern ausgewertet werden können?

Auf Grund der Vielfältigkeit der möglichen grundrechtlich relevanten Gefährdungen wird sich diese Untersuchung auf zwei spezielle Problembereiche konzentrieren und diese näher erörtern:

- automatisierte und verdachtsunabhängige (Verkehrs-)Überwachung,
- Videoüberwachung des öffentlichen Raumes unter Einbeziehung der biometrischen Gesichtserfassung.

Ausgehend von den historischen Erklärungsmodellen zur Definition des Staates werden im Teil 2, Kapitel A diese Entwicklungen primär anhand des deutschen Verfassungsrechts

erörtert werden. Es werden hierbei sowohl das bürgerlich-liberale als auch das sozial-liberale Staatsmodell erörtert. Dabei wird auf die Abgrenzung der inneren und äußeren Sicherheit des Staates eingegangen. Anhand der philosophischen Erklärungstheorien dessen, was einen Staat ausmacht, wird untersucht, welche Schutzpflichten der Staat bei Gefährdungen des allgemeinen Persönlichkeitsrechts seiner Bürger ergreifen muss. Anhand von Leitentscheidungen des Bundesverfassungsgerichts wird hierbei die Entwicklung der Schutzpflichten erörtert. Hierbei wird aufzuzeigen sein, in welcher Beziehung die Gefährdung des allgemeinen Persönlichkeitsrechts im Allgemeinen und des Rechts auf informationelle Selbstbestimmung im Besonderen zu den staatlichen Schutzpflichten stehen.

Der bedeutendste Wegweiser für die Begründung von Schutzpflichten bei Gefährdungen des allgemeinen Persönlichkeitsrechts war die Entscheidung des Bundesverfassungsgerichts zur Volkszählung aus dem Jahr 1983.⁵ Die teils radikalen Umbrüche in der Informationsverarbeitung und Technologieverbreitung seit den letzten zwei Jahrzehnten des vorherigen Jahrtausends stellen die grundlegende Bedeutung dieser Entscheidung selbst im Zeitalter der Informationstechnologie nicht in Abrede. Man kann vielmehr feststellen, dass alle wesentlichen Entscheidungen zu aktuellen Entwicklungen (Vorratsdatenspeicherung, automatisierter Kfz-Kennzeichenabgleich oder Onlinedurchsuchung) ihre dogmatischen Wurzeln in der Entscheidung des Bundesverfassungsgerichts zur Volkszählung haben. Sie haben zunächst einmal dogmatisch ähnliche Gene, konkretisieren aber z.B. in der Entscheidung zur Onlinedurchsuchung die Beobachtungspflichten des Staates bei Gefährdungen durch den Einsatz neuer Technologien. So schuf das Bundesverfassungsgericht mit seiner Entscheidung zur Onlinedurchsuchung⁶ ein neues Grundrecht, welches die Gewährleistung und Vertraulichkeit und Integrität informationstechnischer Systeme in einem neuen eigenständigen Schutzbereich definierte.

Es ist zunächst festzustellen, dass nach dem 11.09.2001 die Sicherheitsbehörden in Aktionismus verfallen sind - gleichsam dem Motto huldigen: „Der Zweck heiligt die Mittel“. So wurden infolge der Terroranschläge in New York zahlreiche Gesetze im Rahmen des sog. Terrorismusbekämpfungsgesetzes⁷ verschärft. In das Pass- und Personalausweisgesetz wurden verpflichtend biometrische Merkmale aufgenommen (§ 5 V, IX PAuswG⁸ und § 4 III, 4 PassG für Fingerabdrücke). Das Gesetz über den Militärischen Abschirmdienst

⁵ BVerfG, Urteil v. 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83 = BVerfGE 65, 1 ff.

⁶ BVerfG, Urteil v. 27.2.2008 - 1 BvR 370/07 = BVerfGE 120, 274 = NJW 2008, 822 = DVBl. 2008, 582.

⁷ BGBl. 2002 I, Nr. 3 vom 11.1.2002, S. 361.

⁸ BGBl. 2009 I, Nr. 33 vom 24.6.2009, S. 1346.

und das Gesetz über den Bundesnachrichtendienst wurden im besonderen Maße an dem Präventionsgedanken neu justiert. Der Bundesgrenzschutz und das Bundeskriminalamt erhielten erweiterte Kompetenzen. Banken, Luftfahrtunternehmen, Postdienstleistern und Internet Providern wurden weitgehende Speicherpflichten über personenbezogene Daten ihrer Kunden und Auskunftspflichten gegenüber Verfassungsschutzämtern und Bundesnachrichtendienst auferlegt. Insbesondere wurde das G 10 Gesetz insoweit geändert, dass für alle deutschen Geheimdienste Kommunikations- und Reisewege von Privatpersonen wesentlich einfacher nachvollziehbar sind. Darüber hinaus wurde im Jahr 2004 in Berlin ein gemeinsames Terrorabwehrzentrum eingerichtet. Angesichts all dieser gesetzgeberischen Aktivitäten ist kritisch zu hinterfragen, ob diese vielfältigen Maßnahmen in der Gesamtbetrachtung rechtsstaatlichen Grundsätzen genügen oder schon ohne hinreichende Rechtfertigung den Schutzbereich der Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10, Art. 13 GG verfassungswidrig einschränken. Als konträre Position zu den gesetzgeberischen Maßnahmen ließe sich die Aussage formulieren: „Die Angst ist wie eine Autobahn für Sicherheitsgesetze.“⁹ Ist nicht vielmehr danach zu fragen, welche Mittel der Eingriffsverwaltung am besten geeignet sind, die Gefährdungen der öffentlichen Sicherheit und Ordnung zu beseitigen und dabei gleichzeitig das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG am wenigsten gefährden? Versteht es sich nicht von selbst, dass in einem Rechtsstaat jedes Mittel der Repression wie der Prävention mit der Verfassung vereinbar sein muss, um dem wesentlichen Pfeiler der Verfassung, dem Staatsstrukturprinzip des Art. 20 Abs. 3 GG zu entsprechen?

Bei all den vorgenannten gesetzgeberischen Aktivitäten ist zuzugeben, dass die Legislative bezogen auf die erforderliche Reaktion auf die Anschläge am 11.09.2001 unter enormem Zeitdruck stand. Hierbei haben die Sicherheitsbehörden, allen voran der Bundesinnenminister¹⁰ jedoch voreilig die Sicherheitsrelevanz ihres Handelns in den Focus gerückt und der Öffentlichkeit gegenüber erklärt, dass der deutsche Verfassungsstaat einen Vorrang der Sicherheit gegenüber der Freiheit einräume. Es scheint nicht einfach, in der konkreten Situation die jeweils geeigneten, aber zugleich auch nicht übermäßigen Mittel an

⁹ Prantl, Süddeutsche Zeitung vom 17.5.2010, abrufbar unter: <http://www.sueddeutsche.de/politik/innenministerium-das-schizophrene-orakel-1.106777> (Stand: 20.5.2018); Prantl/Freiberg, Terrorangst und offene Gesellschaft - Wie viel Überwachung muss sein?, Deutschlandradio Podcast vom 26.8.2006, abrufbar unter: <http://www.dradio.de/dkultur/sendungen/imgespraech/534793/> (Stand: 20.5.2018).

¹⁰ Greis, Golem vom 24.3.2016, abrufbar unter: <https://www.golem.de/news/innenminister-de-maiziere-datenschutz-ist-schoen-aber-sicherheit-hat-vorrang-1603-119975.html> (Stand: 21.5.2018); Krempl, heise online vom 24.3.2016, abrufbar unter: <https://www.heise.de/newsticker/meldung/Bundesinnenminister-Datenschutz-ist-schoen-Sicherheit-ist-besser-3150745.html> (Stand: 21.5.2018).

Repression oder auch Prävention heraus zu filtern; dies erfordert eine verfassungsrechtliche Interessen- bzw. Güterabwägung. Diese kann bei ganz besonderen Gefährdungen weder mit Standardfloskeln bewirkt noch mit der bloßen Lektüre von Gesetzeskommentaren bewältigt werden. Es ist vielmehr eine intensive Auseinandersetzung mit den tangierten Grundrechten aller betroffenen Grundrechtsträger erforderlich. Insbesondere ist zu berücksichtigen, dass Grundrechte den persönlichen Anwendungsbereich des Schutzbereichs differenziert danach ausgestalten, ob eine Person die deutsche Staatsbürgerschaft inne hat oder nicht.

Eine einseitige Entscheidung der Legislative zugunsten eines „Supergrundrechts der Sicherheit“ ohne konkrete Abwägung der Folgen und der betroffenen Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, 10, 13 GG und des sich auch aus der Rechtsprechung des Bundesverfassungsgerichts ergebenden Schutzauftrages des Staates erscheint vor dem Verbot, Grundrechte in ihrem Wesensgehalt einzuschränken (Art. 19 Abs. 2, 79 Abs. 3 GG), sowie der verfassungsrechtlichen Garantie des Art. 20 Abs. 3 GG nicht vertretbar. Mit der fortschreitenden Technisierung unserer Gesellschaft sind neue, offensichtlich höchst bedeutsame Gefährdungslagen für Grundrechte der Einzelnen entstanden. Dies zeigt sich ganz deutlich, wenn man einerseits die hierdurch beabsichtigte und bewirkte Steigerung der Effizienz von Vorgängen betrachtet. Ein Beispiel hierfür ist die Abrechnung der Gebühren für die Nutzung der Bundesautobahnen (Lkw-Maut)¹¹. Auf der anderen Seite sind mit der Technisierung der Gesellschaft auch ganz neue Wege der Verbrechensvorbeugung und -bekämpfung möglich (wie Online-Durchsuchung / „Bundestrojaner“)¹². Die Begründung von Sicherheitsgesetzen mit Gefährdungen der Gesellschaft und damit auch der Gefährdung von grundrechtlich verbürgten Freiheitsrechten ist in der Geschichte der Bundesrepublik nicht neu.¹³ Betrachtet man die Entwicklung der Sicherheitsgesetze in der Bundesrepublik seit den 1968er/1970er Jahren, fällt auf, dass in den 1970er

¹¹ *Borchers*, heise online vom 31.1.2008, abrufbar unter: <http://www.heise.de/newsticker/meldung/102761> (Stand: am 24.11.2019); *ders.*: heise online vom 5.8.2006, abrufbar unter: <http://www.heise.de/newsticker/meldung/76443> (Stand: 24.11.2019); *ders.*: heise online vom 22.5.2006, abrufbar unter: <http://www.heise.de/newsticker/meldung/73380> (Stand: 23.11.2019); *Ziegler*, heise online vom 28.11.2005, abrufbar unter: <http://www.heise.de/newsticker/meldung/66722> (Stand: 23.11.2019).

¹² *Kuri*, heise online vom 8.2.2008, abrufbar unter: <http://www.heise.de/newsticker/meldung/103217> (Stand: 23.11.2019); *Krempf*, heise online vom 2.1.2008, abrufbar unter: <http://www.heise.de/newsticker/meldung/101194> (Stand: 23.11.2019); *Kuri*, heise online vom 25.8.2007, abrufbar unter: <http://www.heise.de/newsticker/meldung/94898> (Stand: 23.11.2019); *Borchers*, heise online vom 31.1.2008, abrufbar unter: <http://www.heise.de/newsticker/meldung/102797> (Stand: 23.11.2019).

¹³ *Bielefeldt*, Freiheit und Sicherheit im demokratischen Rechtsstaat, S. 4, abrufbar unter: http://www.institut-fuer-menschenrechte.de/uploads/tx_commerce/essay_no_1_freiheit_u_sicherheit_i_demokratischen_rechtsstaat_1.pdf (Stand: 7.11.2018).

Jahren Sicherheitsgesetze mit dem RAF-Terror begründet worden. Dies wandelte sich in den 1990er Jahren. Dann wurden Sicherheitsgesetze wie der Große Lauschangriff¹⁴ mit der Bekämpfung der organisierten Kriminalität gerechtfertigt und insbesondere Art. 13 GG eingeschränkt. Abgesehen von den Gefährdungen des jeweiligen Jahrzehnts ist festzustellen, dass zunehmend eine Tendenz der Legislative besteht, im Vorfeld konkreter Gefahrenabwehrmaßnahmen aktiv zu werden.¹⁵ Durch die immer weitere Verschiebung von Eingriffsbefugnissen in das Vorfeld von konkreten Gefährdungen für Rechtsgüter besteht aber die Gefahr, dass die Grundrechtsberechtigten von der Ausübung ihrer freiheitlich garantierten Grundrechte keinen Gebrauch mehr machen (wollen oder können). *Hassemer*¹⁶ erkennt hierin eine Polverschiebung zu Lasten der Freiheit in Richtung der Sicherheit. Vor dem 11.09.2001 für undenkbar gehaltene Grundrechtseingriffe sind nun, bemerkenswerter Weise auch ohne breiten öffentlichen Protest von der Legislative umgesetzt worden. Es erscheint gerade so, als habe der Gesetzgeber die Werte des Grundgesetzes weiterhin zur Disposition gestellt.¹⁷ Und die Prämisse, ein Staat sei schwach, d.h. dessen Ordnung sei zugunsten der Freiheit ausgerichtet, stellt jedoch gerade keine Legitimation für einen starken Staat, dessen Ordnung zugunsten der Sicherheit ausgelegt ist, dar.¹⁸ Diese Arbeit hat daher das Ziel, zunächst die vielfältige Rechtsprechung zum Persönlichkeitsrecht systematisch zu beschreiben und zu analysieren. Darauf aufbauend wird im Hinblick auf die fortschreitenden Möglichkeiten des Einsatzes technischer Mittel näher untersucht, wie weit der Schutzbereich des Persönlichkeitsrechts (Art. 2 Abs. 1 GG) im Zeitalter der Informationstechnologie reicht. Anhand der Videoüberwachung des öffentlichen Raumes unter Nutzung der biometrischen Gesichtserfassung soll untersucht werden, ob der Schutzbereich der in Betracht kommenden Grundrechte angesichts aktueller Entwicklungen anders definiert werden muss. Zudem werden anhand der beiden Beispiele auch die Schranken des Persönlichkeitsrechts (Schrankentrias) näher untersucht. Anhand der beiden konkreten Beispiele soll eine verfassungsrechtliche Rechtfertigung unternommen werden, die insbesondere berücksichtigt, ob und welche Gefährdungen im Informationszeitalter für Grundrechte erwachsen, die unterhalb bzw. jenseits des klassischen (finalen) Eingriffsbegriffs und des ähnlich schwerwiegenden faktischen Eingriffs liegen.

¹⁴ BGBl. 2005 I, S. 1841.

¹⁵ *Calliess*, DVBl. 2003, 1096 ff.

¹⁶ *Hassemer*, Vorgänge, 2002 (Heft 3), 10 (11).

¹⁷ *Hoffmann-Riem*, ZRP 2002, 497 (498).

¹⁸ *Kloepfer*, Verfassungsrecht, Bd. I, § 1, Rn. 95.

Abstrakter formuliert geht es in dieser Arbeit darum, wie viel Sicherheit die (Handlungs-) Freiheit verträgt, damit nach wie vor eine freiheitlich-demokratische Grundordnung auf der Grundlage des Grundgesetzes fortbesteht. Es geht um die möglichst präzise Kennzeichnung und angemessene Auflösung des Spannungsverhältnisses zwischen staatlichem Schutzauftrag und Freiheits-Grundrechten der jeweiligen Grundrechtsträger.¹⁹

Die Entwicklung im Bereich der Informationstechnologie bewirkte einen grundlegenden Wandel der Gesellschaft in Bezug auf die Akzeptanz und in Bezug auf die Lebensgewohnheiten der Bevölkerung. Es ist kaum ein Lebensbereich vor dem Durchdringen mit Technik verschont geblieben.²⁰ Die Folge dieses immensen Einflusses von Technik auf den Alltag ist, dass durch die von den technischen Geräten generierten Daten Schlussfolgerungen auf die Nutzer gezogen werden können. Aus den Daten, die Mobiltelefone technisch bedingt generieren, können in der Verknüpfung mit den Standortdaten Bewegungsprofile erstellt werden. Aber auch für die Exekutive sind die Auswirkungen der technischen Entwicklungen²¹ im Bereich der Informationstechnologien beträchtlich. Die fortschreitende Technisierung der Exekutive ermöglicht es, in bestimmten Bereichen Entscheidungen zu automatisieren. Diese möglich erscheinende Automatisierung²² von Verwaltungsentscheidungen rührt aber auch von einem gewissen Rationalisierungsdruck auf die öffentliche Verwaltung infolge von Sparzwängen.²³ Die Interessen, Daten, die für einen ursprünglich anderen Zweck erhoben wurden, auch für andere Zwecke zu nutzen, belegt ein Beispiel aus dem europäischen Ausland. In Spanien werden beispielsweise die Standortdaten von Handynutzern für eine Volkszählung genutzt.²⁴ Dieses Beispiel zeigt einerseits die Begehrlichkeiten des Staates an derartigen Daten für seine Zwecke. Gleichzeitig ist es auch ein Beispiel dafür, welche Risiken eine solche Datenerhebung und Datenverknüpfung in sich bergen kann. Sofern in dem Beispielfall die Standortdaten nicht technisch korrekt gegen unbefugten Zugriff gesichert sind, können Dritte hieraus Rückschlüsse ziehen. Dass sich hieraus Gefährdungen des allgemeinen Persönlichkeitsrechts durch die Verknüpfung von Daten ergeben können, hat das Bundesverfassungsgericht

¹⁹ *Di Fabio*, NJW 2008, 421 ff.

²⁰ *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 7.

²¹ Zu Risiken für das Persönlichkeitsrecht durch technische Entwicklungen: *Hansen/Thomsen*, DuD 2010, 283 ff.

²² *Braun Binder*, NVwZ 2016, 960 (963).

²³ *Herold*, DöV 2020, 181.

²⁴ *Sperlich*, heise online vom 21.11.2019, <https://www.heise.de/newsticker/meldung/Volkszaehlung-Behoerde-trackt-Handys-von-Millionen-Spaniern-4594157.html> (Stand: 21.11.2019).

schon im Mikrozensusbeschluss²⁵ und in der Entscheidung zur Volkszählung²⁶ hervorgehoben. Ein anderes Beispiel, aus der sich eine Grundrechtsgefährdung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergeben kann, ist die Videoüberwachung im öffentlichen Raum. Sofern die Daten dieser Kameras gespeichert werden und mit anderen Daten verknüpft werden, können hieraus weitergehende Aussagen möglich werden. In der Literatur wird darauf hingewiesen, dass für die Wahrnehmung von der freiheitlich-demokratischen Grundordnung garantierten Freiheit schon das Gefühl des Überwachtwerdens eine einschüchternde Wirkung erzeugen könne.²⁷ *Di Fabio* spricht davon, dass im Zeitalter der Digitalisierung Grundrechte gewissermaßen dauergefährdet seien.²⁸ Hinter diesem diffusen Eindruck des Überwachtwerdens durch Kameras im öffentlichen Raum steht die durch Mitglieder der Vereinigung der deutschen Staatsrechtslehrer seit dem Jahr 1981 diskutierte Frage des Verhältnisses zwischen Recht und Technik und der Gestaltung desselben durch den Gesetzgeber.²⁹ Die Fortschritte der technischen Entwicklungen bewirken einerseits erweiterte Handlungsoptionen für die Nutzer der Geräte bzw. Technologien. Sie bergen aber auch vielfältige Gefahren und Risiken, die sich nicht unmittelbar hieraus selbst erkennen lassen, sondern erst als eine Folgewirkung ergeben können. Derjenige, der durch eine Kamera im öffentlichen Raum gefilmt wird, wird keine unmittelbare Beeinträchtigung seiner Handlungsfreiheit erkennen können. Möglicherweise wird er die Folgen erst dann wahrnehmen, wenn er bei der Kontrolle am Flughafen zu einer „Sonderkontrolle“ gebeten wird, weil er im System als „Gefährder“ registriert ist, weil er auf dem Heimweg einen oder mehrere Kriminalitätsschwerpunkte durchquert hat und dabei von Kameras aufgenommen und diese Daten gespeichert wurden. Sofern die Kameras im öffentlichen Raum nicht nur Personen als Gesamtheit, sondern einzelne körperliche Merkmale, z.B. Gesichtsaufnahmen, erfassen und verarbeiten können, kann dieser technische Detaillierungsgrad dazu führen, dass in der Folge weitere Beeinträchtigungen des Persönlichkeitsrecht dieser Person zu befürchten sind.³⁰ Die

²⁵ BVerfG, Beschl. v. 16.07.1969, Az. 1 BvL 19/63 = BVerfGE 27, 1 ff.

²⁶ BVerfGE 65, 1 ff.

²⁷ Moser-Knierim, Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr, 2014, S. 131, 159.

²⁸ *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, S. 32 ff.

²⁹ Eichenberger/Novak/Kloepfer, VVDStRL 40, S. 7 ff.; Ipsen/Murswiek/Schlink, VVDStRL 48, S. 177 (190).

³⁰ Kuppjuweit, Testphase für Gesichtserkennung am Südkreuz ist gestartet, Tagesspiegel vom 1.8.2017, abrufbar unter: <https://www.tagesspiegel.de/berlin/neue-ueberwachungskameras-in-berlin-testphase-fuer-gesichtserkennung-am-suedkreuz-ist-gestartet/20120258.html> (Stand: 23.11.2019); Lauer, Erst mal verdächtig, Die Zeit Nr. 33/2017 vom 2.8.2017, abrufbar unter: <http://www.zeit.de/2017/32/gesichts-erkennung-ue->

technischen Entwicklungen in der Informationstechnologie und deren Auswirkungen auf das Recht scheinen durch ein Paradoxon³¹ gekennzeichnet zu sein: je mehr und je schneller die technische Entwicklung voranschreitet, desto mehr fachlich-technisches Wissen hat eine Gesellschaft. Gleichzeitig scheint der Gesetzgeber jedoch wenig Wissen über die Folgen oder Risiken zu haben, um die Grundrechte seiner Bürger effektiv schützen zu können. Für die Legislative ist dieses Wissen jedoch unbedingt notwendig, damit sie die Rechtsprechung des Bundesverfassungsgerichts aus den Entscheidungen zur Rasterfahndung³², zum G 10³³, zum BKAG³⁴ sowie zur Volkszählung³⁵ im Rahmen der Austarierung der Balance zwischen Sicherheit und Freiheit umsetzen kann. Die Schwierigkeit für den Gesetzgeber besteht einerseits darin, dass die technische Entwicklung der Informationstechnologie seit den 1980er Jahren bis heute sehr schnell vorangeschritten ist. Darüber hinaus kann der Gesetzgeber auch nur begrenzte Prognosen über die Wirkungen auf die Grundrechtsgefährdung des allgemeinen Persönlichkeitsrechts erstellen, da ihm sicheres Wissen über künftige Ereignisse oder künftige Möglichkeiten von Technologien fehlt. *Ossenbühl*³⁶ beschreibt dieses Dilemma zutreffend mit dem Auseinanderklaffen des Erkennens eines Regelungsbedarfs einerseits und dem Regelungspotential andererseits. *Jaeckel*³⁷ sieht in diesem Zusammenhang kognitive Abhängigkeiten des Staates von naturwissenschaftlichem Spezialwissen. Der Gesetzgeber muss einerseits den Zeitpunkt erkennen, wann er einschreiten muss, damit das Verhältnis zwischen Freiheit und Sicherheit noch ausgewogen ist. Er muss aber auch erkennen, welches Potential seine Regelung bezogen auf die mögliche Beeinträchtigung hat, da der Gesetzgeber entscheiden muss, wo er Regelungsbedarf sieht und wo dies aus seiner Sicht nicht erforderlich ist. Hierbei kann er einerseits auf technische Regelwerke verweisen.³⁸ Die grundlegenden Weichenstellungen muss der Staat jedoch selbst treffen.³⁹ Welche

[berwachung-bundes-polizei-berlin-test](#) (Stand: 4.2.2018); *Kurz*, De Maiziére plant flächendeckende Gesichtserkennung trotz hoher Fehlerquoten am Südkreuz, abrufbar unter: <https://netz-politik.org/2017/de-maiziere-plant-flaechendeckende-gesichtserkennung-trotz-hoher-fehlerquoten-am-sued-kreuz/> (Stand: 4.2.2018); *Schindler*, ZD-Aktuell 2019, 06071; eingehend: *Stettner*, Sicherheit am Bahnhof, 2017, S. 21.

³¹ *Ipsen/Murswiek/Schlink*, VVDStRL 48, S. 177 (208); *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 10.

³² BVerfGE 125, 320.

³³ BVerfGE 143, 1.

³⁴ BVerfGE 141, 220.

³⁵ BVerfGE 65, 1.

³⁶ *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 11 ff.

³⁷ *Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, S. 221 ff.

³⁸ *Jaeckel*, Gefahrenabwehrrecht und Risikodogmatik, S. 225 ff.

³⁹ *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 26.

Auswirkungen seine Regelungen in Bezug auf die Gefährdung des Persönlichkeitsrechts haben, wenn der Gesetzgeber beispielsweise die Videoüberwachung des öffentlichen Raumes unter Nutzung von biometrischen Auswertungsmöglichkeiten erlaubt, ist auch durch die gegensätzlichen Zustände von Technik und Recht gekennzeichnet. Das Recht will durch Transparenz Rechtsfrieden, d.h. Stabilität erreichen. Technik ist eher durch Innovation, Veränderung, d.h. von Dynamik gekennzeichnet. Es deutet sich die Erkenntnis an, dass das Recht der Technik nicht den Weg bereiten kann, sondern ihr tendenziell nachfolgt.⁴⁰

In Art. 158 Abs. 2 WRV⁴¹ wird der Schutz der Wissenschaft, Kunst und Technik besonders hervorgehoben. Das Wort „Technik“ findet man im Grundgesetz hingegen vergebens, weshalb in der Literatur⁴² kritisiert wird, dass das Grundgesetz eher keine Affinität zur Technik aufweise, obgleich die Wissenschaftsfreiheit gemäß Art. 5 Abs. 3 S. 1 GG besonders geschützt wird. Der technische Fortschritt ist u.a. auch deshalb möglich, weil die Freiheit der Forschung und Lehre gemäß Art. 5 Abs. 3 S. 2 GG garantiert wird. Gleichwohl entbindet diese Freiheit als Rahmenbedingung für die technische Evolution nicht von der Treue zur Verfassung und damit zur normativ geprägten Grundordnung i.S.d. GG. Entscheidend ist vielmehr der Umstand, dass sich der Staat seinen Schutzpflichten für die Grundrechte im Allgemeinen und für das allgemeine Persönlichkeitsrecht im Speziellen nicht entziehen kann, denn in besonderen Konstellationen können sich die objektiven Schutzpflichten zu gerichtlich durchsetzbaren Schutzansprüchen der Grundrechtsträger verdichten.⁴³ Der Gesetzgeber muss sich daher fragen, welche Risiken sich für das allgemeine Persönlichkeitsrecht beim Einsatz von bestimmten Technologien ergeben und ob es für diese Grundrechtsgefährdung hinreichende Anhaltspunkte in Form von konkreten wissenschaftlich gesicherten Erkenntnissen gibt.⁴⁴ Bei seiner Entscheidung über einen deregulierten Technikeinsatz oder das Ergreifen von bestimmten Schutzmaßnahmen darf der Gesetzgeber auf veränderte Bedrohungslagen für die Gesellschaft insgesamt, wie sie beispielsweise durch terroristische Anschläge oder etwaige Planungen einhergehen, reagieren und für den Zeitraum der Bedrohungslage, entsprechend verhältnismäßig ausgestalten.

⁴⁰ *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 12.

⁴¹ Art. 158 Abs. 2 WRV lautet: „Den Schöpfungen deutscher Wissenschaft, Kunst und Technik ist durch zwischenstaatliche Vereinbarung auch im Ausland Geltung und Schutz zu verschaffen.“

⁴² *Murawiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985, S. 22; *Isensee*, DöV 1983, 565 (569).

⁴³ *Isensee*, in: *Isensee/Kirchhof* (Hrsg.) HdbStR, Bd. V, 3. Aufl., 2007, § 111, Rn. 86 ff.; *Murawiek*, Die staatliche Verantwortung für die Risiken der Technik, 1985, S. 88 ff.

⁴⁴ *Ossenbühl*, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 15.

Der Staat ist zur Gefahrenabwehr und damit zur Gewährleistung von Sicherheit befugt.⁴⁵ Keinesfalls darf er jedoch die Balance zwischen Sicherheit und Freiheit grundsätzlich verschieben.⁴⁶ Eine besondere Herausforderung für den Gesetzgeber ist hierbei, dass die technische Entwicklung zunehmend schneller und komplexer erfolgt, als die Erkenntnisse über die Folgen von Risiken von Techniken erlangt werden.⁴⁷ Insofern stehen gerade Informationstechnologien zunehmend im Spannungsfeld zum Schutz des allgemeinen Persönlichkeitsrechts sowie dem hieraus abgeleiteten Recht auf informationelle Selbstbestimmung sowie des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Im Hinblick auf die Akteure aus dem Bereich der Sicherheitsbehörden bedeutet dies, dass sie ihr Handeln bei Inanspruchnahme von Ermächtigungen einerseits am Ziel der Maßnahme ausrichten müssen und andererseits jeweils die Auswirkungen bei der Inanspruchnahme der gesetzlichen Ermächtigung den Grundrechtsschutz, insbesondere des allgemeinen Persönlichkeitsrechts, beachten müssen. Dies können sie jedoch nur dann erfolgreich umsetzen, wenn der Gesetzgeber zuvor bei der Normierung von Eingriffsbefugnissen die Abwägung zwischen staatlicher Gewährleistung von Sicherheit und Freiheit in ausgewogener Balance in den jeweiligen Eingriffsbefugnissen geregelt hat. Für den Fall, dass dies nicht oder nicht in ausreichendem Maße geschehen ist, ist es die Aufgabe der Judikative, die aus dem Gleichgewicht geratene Balance zwischen Sicherheit und Freiheit wieder neu auszurichten. Die Beispiele der Rechtsprechung⁴⁸ belegen, dass der Judikative hier eine wesentliche Rolle zukommt, um spätestens nachgelagert nach dem Vollzug ordnungsbehördlicher Maßnahmen die objektiv-rechtliche Gewährleistungsfunktion der Grundrechte rechtsstaatlich zu sichern. Hierbei hat primär die Legislative Eingriffsschwellen für Eingriffe in das Persönlichkeitsrecht zu definieren und für Maßnahmen, die durchgeführt werden sollen, ohne dass eine konkrete Gefahr vorliegt (sog. Vorfeldmaßnahmen), entsprechende Schutzmechanismen zur Gewährleistung des objektiv-rechtlichen Gehalts des Persönlichkeitsrechts vorzusehen. Rapide technische Entwicklungen, wie sie in den letzten zwanzig Jahren eingetreten sind, und deren zukünftige Gestaltung können bei den Antworten auf gegenwärtige verfassungsrechtliche Fragen die Geltung der Grundrechte stärken, aber auch schwächen.⁴⁹

⁴⁵ Köck, AöR 121 (1996), 1 (14); Demmer, Vorbeugende Gefahrenabwehr im Wirtschaftsverwaltungsrecht durch akkreditierte Zertifizierung, 2014, S. 16.

⁴⁶ BVerfGE 115, 320, siehe 1. Teil, B, III, 1, a, jj; Schröder, JA 2016, 641 (648).

⁴⁷ Ossenbühl, Die Not des Gesetzgebers im naturwissenschaftlich-technischen Zeitalter, S. 11 (20).

⁴⁸ Siehe 1. Teil, B, III, 1 bis 3.

⁴⁹ Härtel, LKV 2019, 49 (50).