FRIEDRICH NAUMANN
STIFTUNG Für die Freiheit.

DAS DIGITALE BRIEFGEHEIMNIS

Herleitung des Rechts auf Verschlüsselung

Prof. Dr. Dennis-Kenji Kipker

ANALYSE

Impressum

Herausgeberin
Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit
/stiftungfuerdiefreiheit

Autor
Prof. Dr. Dennis-Kenji Kipker

Redaktion
Liberales Institut
der Friedrich-Naumann-Stiftung für die Freiheit

Charlotte Roderfeld,
Referentin für Bürgerrechte und Verwaltungsdigitalisierung

Teresa Widlok,
Leiterin Globale Themen

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand
Mai 2023

Danksagung
Der Verfasser dankt Michael Walkusz (Universität Bremen) für seine fachliche Unterstützung.

ISBN
978-3-948950-37-8

Inhalt

A. Executive Summary

I. Einleitung

Die Diskussionen um verschlüsselte Kommunikation und ein sogenanntes Recht auf Verschlüsselung werden längst nicht mehr nur in Fachkreisen geführt. Durch die flächendeckende Anwendung der technischen Möglichkeiten zur Verschlüsselung von Daten, die fortschreitende Nutzung sozialer Medien sowie zunehmende Erschwernisse für Sicherheitsbehörden bei digitalen Ermittlungen hat die rechtspolitische Debatte in den letzten Jahren eine neue Dynamik bekommen. Die Verschlüsselung von Kommunikation und Inhalten stellt ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Staat, Wirtschaft und Gesellschaft dar. Die Behauptungen, Verschlüsselung führe zu einem erhöhten Gefährdungspotenzial für die Allgemeinheit, weil die Ermittlungsarbeit erschwert werde und Verschlüsselungstechnik werde nur von denjenigen eingesetzt, die „etwas zu verbergen" hätten, greifen zu kurz und missachten die grundrechtlichen Aspekte der Debatte um Verschlüsselung. Das vorliegende Gutachten widmet sich der Frage, inwieweit ein Recht auf Verschlüsselung als Ausformung des digitalen Briefgeheimnisses bereits existiert, unter welchen Umständen es gegebenenfalls eingeschränkt werden kann und was dies für aktuelle rechtspolitische Diskussionen bedeutet.

II. Die Ergebnisse im Überblick

1. Aus dem nationalen Verfassungsrecht ist ein Recht auf Verschlüsselung ableitbar.

2. Aus dem europäischen Verfassungsrecht ist ein Recht auf Verschlüsselung ableitbar.

3. Ein Recht auf Verschlüsselung ergibt sich zwar nicht als solches aus den nationalen und europäischen verfassungsrechtlichen Gewährleistungen. Es kann aber aus der Zusammenschau verschiedener Grundrechte abgeleitet werden. Relevant sind die Grundrechtspositionen, die die digitale Datenverarbeitung und -übermittlung zum Gegenstand haben. Das sind im Grundgesetz im Wesentlichen: das Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (GVIiS) nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Das Recht auf Verschlüsselung ist Grundvoraussetzung für die Ausübung dieser Grundrechte und essenzieller Bestandteil der Ausübung zahlreicher weiterer Grundrechte, die inhaltlich die Privat- und Intimsphäre betreffen. Auf europäischer Ebene ergibt sich ein entsprechendes Recht insbesondere aus Art. 7 GRCh (Achtung des Privat- und Familienlebens) und Art. 8 GRCh (Schutz personenbezogener Daten). Sie schützen umfassend die Vertraulichkeit und Integrität der digitalen Datenverarbeitung, was den Rückschluss auf ein Recht auf verschlüsselte Kommunikation ermöglicht.

4. Bei einer Ableitung eines Rechts auf Verschlüsselung aus verschiedenen verfassungsrechtlichen Gewährleistungen auf nationaler und europäischer Ebene ergibt sich im chronologischen Kommunikationsablauf ein nahezu lückenloser Grundrechtsschutz. Der Kommunikationsvorgang selbst, also Inhalte, Umstände/Metadaten und Verkehrsdaten, ist vom Schutzbereich des Art. 10 Abs. 1 GG umfasst. Auch der vorgelagerte Schritt, nämlich das Generieren der noch unverschlüsselten Inhalte, die im Anschluss (verschlüsselt) übermittelt werden sollen, fällt darunter. Geschützt sind damit sowohl die Transport- als auch die Inhaltsverschlüsselung. Das subsidiäre GVIiS als besondere Ausprägung des Allgemeinen Persönlichkeitsrechts schützt hingegen keinen Kommunikationsvorgang, sondern schützt vor dem staatlichen Zugriff auf IT-Systeme, durch den ein substanzieller Einblick in wesentliche Teile der Lebensgestaltung einer Person möglich wäre (z.B. Computer, Smartphones und elektronische Terminkalender). Weil sich Dateninhaber durch Verschlüsselung vor einem solchen Zugriff schützen können, muss das Recht auf Verschlüsselung auch in den Schutzbereich des GVIis fallen. Auf europäischer Ebene sind ebenfalls sämtliche Verarbeitungsschritte von der Erhebung über die Übermittlung bis hin zur Speicherung eines Datums umfasst.

5. Ein Recht auf Verschlüsselung besteht aus einer aktiven sowie aus einer passiven Dimension. Damit ist es nicht nur Abwehrrecht gegenüber staatlichem Handeln umfasst, sondern kann für den Staat auch (weit gefasste) Handlungspflichten auslösen, um der Umsetzung von Datenverschlüsselung als Methode zur Ausübung effektiven Grundrechtsschutzes gerecht zu werden. Aus Art. 10 GG lässt sich die staatliche Verpflichtung ableiten, effektive Maßnahmen zur Gewährleistung von Verschlüsselung zu realisieren. Dieser Pflicht kann der Staat beispielsweise durch gezielte Informationsmaßnahmen und -kampagnen für Bürgerinnen und Bürger nachkommen, damit diese Verschlüsselung umsetzen können. Zudem muss der Staat Datensätze seiner Bürgerinnen und Bürger verschlüsseln, um sie vor dem Zugriff Dritter zu schützen. Durch entsprechende Regelungen im StGB ist der Staat seiner Verpflichtung, rechtswidrige Maßnahmen Privater zu regulieren bzw. sanktionieren, nachgekommen. § 165 Abs. 2 TKG, wonach Telekommunikationsanbieter angemessene technische und organisatorische Vorkehrungen gegen schädliche Einwirkungen treffen müssen, erfüllt die staatliche Schutzpflicht in Bezug auf die Verpflichtung privater Telekommunikationsanbieter. Durch die Schutzpflicht kann dem Recht auf Verschlüsselung im Ergebnis zu einer besseren Wirksamkeit in der Praxis verholfen werden.

6. Ein Recht auf Verschlüsselung existiert nicht grenzenlos, d.h. es ist im Rahmen der verfassungsrechtlichen Interessenabwägung zu im Einzelfall höherrangigen Zwecken beschränkbar.

7. Eine solche theoretische Einschränkbarkeit eines Rechts auf Verschlüsselung bedeutet jedoch keine beliebige Einschränkbarkeit. Sowohl die nationalen wie auch die europäischen verfassungsrechtlichen Voraussetzungen verlangen hier deutlich qualifizierte Maßstäbe und u.a. eine klare und verhältnismäßige gesetzliche Ermächtigungsgrundlage. Die Grenze für Eingriffe stellt der Kernbereich der privaten Lebensgestaltung dar. Qualifizierte Anforderungen sind insbesondere bei verschlüsselten Daten notwendig, weil ein Eingriff in solche ungleich höher wiegt als ein Eingriff in nur unverschlüsselte Daten.

8. Die häufig im Überwachungskontext zitierte politische Aussage „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" greift inhaltlich zu kurz, da sie die vorgenannten qualifizierten Rechtfertigungsvoraussetzungen für den Eingriff in ein Recht auf Verschlüsselung nicht angemessen wiedergibt, sondern suggeriert, dass Verschlüsselung und deren (technische) Einschränkbarkeit generell gleichrangig nebeneinanderstünden, was nicht der Fall ist.

9. Aktuelle gesetzgeberische Vorhaben und behördliche Maßnahmen aus dem Sicherheitsbereich genügen diesen strengen Anforderungen zur Einschränkbarkeit eines Rechts auf Verschlüsselung nicht immer, so beispielsweise im Hinblick auf den Entwurf der CSA-Verordnung durch die Europäische Kommission.

10. Ein Recht auf Verschlüsselung ist in vielen Fällen einfachgesetzlich reguliert, und das sowohl im europäischen wie auch im nationalen Recht. Zu berücksichtigen ist jedoch, dass die Verschlüsselung häufig nicht unmittelbar in den Gesetzen genannt wird, sondern Gegenstand technischer und organisatorischer Maßnahmen und Vorkehrungen (TOM bzw. TOV) oder beispielhaft als ein mögliches Verfahren zur Herstellung von Datensicherheit genannt ist. Betroffen sind dabei sowohl das öffentliche Recht, wie auch das Strafrecht und das Zivilrecht. Insbesondere in letztgenanntem ist es möglich, die Umsetzung von Verschlüsselung auch auf vertraglicher Grundlage individuell zwischen den Parteien eines Rechtsgeschäfts zu regeln.

B. Thematische Einführung

Die rechtspolitische Diskussion über Beschränkungen der Möglichkeiten von Bürgerinnen und Bürgern, verschlüsselt miteinander zu kommunizieren, wird bereits seit geraumer Zeit geführt. Im Vordergrund der Betrachtung steht dabei das Spannungsverhältnis zwischen dem Bedürfnis nach vertraulicher Kommunikation, die vor unbefugtem Zugriff geschützt ist, einerseits, und andererseits das Interesse des Staates, aber auch von Unternehmen aus der Privatwirtschaft, persönliche Daten zu ihren Zwecken zu erheben und auszuwerten. Mit der Zunahme der Vernetzung, Anforderungen wie *„Privacy by Design"*, *„Privacy by Default"* und *„Security by Design"* und der technischen Möglichkeit, Verschlüsselungstechnik im Alltag z.B. bei Messenger-Diensten ohne technische Vorkenntnisse einsetzen zu können, haben sich die Möglichkeiten zum Zugriff auf die Inhalte privater Kommunikation von Nutzenden elektronischer Kommunikationsdienste deutlich reduziert. Damit wird gleichsam dem IT-Schutzziel der „Vertraulichkeit" von Daten Rechnung getragen. Nichtsdestotrotz ist hierdurch die öffentlich geführte Debatte um den Einsatz von Verschlüsselungstechnik keineswegs obsolet geworden, ganz im Gegenteil: Der mehr und mehr flächendeckende und technisch erleichterte Einsatz von Verschlüsselung wird zunehmend als innenpolitisches Problem für den Staat begriffen. Deshalb überrascht es nicht, dass die *„Cybersicherheitsstrategie für Deutschland"* (CSS) aus dem Jahr 2021 die Thematik u.a. unter der Überschrift *„Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung gewährleisten"* aufgreift.[1]

So wird einerseits betont, dass sichere Verschlüsselung ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Staat, Wirtschaft und Gesellschaft darstellt. Andererseits würden jedoch ebenso Kriminelle Verschlüsselung nutzen, um Straftaten vorzubereiten und durchzuführen. Verschlüsselte Kommunikation stellt laut der CSS deshalb eine technische Hürde dar, um auf Kommunikationsinhalte zuzugreifen und diese zu analysieren. Verschlüsselung hat deshalb auch zur Folge, dass den Sicherheitsbehörden eingeräumte rechtliche Möglichkeiten zur Telekommunikationsüberwachung (TKÜ) und deren technische Durchführbarkeit auseinanderfallen. Die CSS formuliert es drastisch: *„Die Verschlüsselung macht den Zugang zu Kommunikationsinhalten und deren Analyse im Rahmen einer rechtmäßig angeordneten TKÜ, die insbesondere bei schwersten Straftaten und der organisierten Kriminalität eine zentrale Erkenntnisquelle für die Ermittlungsbehörden darstellt, äußerst schwierig oder gar praktisch unmöglich."*[2] Daher gelte es umso mehr, einen Ausgleich zwischen diesen offensichtlich widerstreitenden Interessen auf durch Verschlüsselung geschützte vertrauliche Kommunikation und staatlichen Sicherheitsinteressen bedingenden Datenzugriff auf verschlüsselte Kommunikation herbeizuführen. Diese Erkenntnis ist nicht nur in Deutschland, sondern inzwischen auch in der Europäischen Union gereift. So wurde im Dezember 2020 eine Entschließung angenommen, die sich ebenso mit dem Thema *„Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung"* befasst.[3]

1 BMI, Cybersicherheitsstrategie für Deutschland 2021, S. 101 f.,
abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf.
2 BMI, Cybersicherheitsstrategie für Deutschland 2021, S. 101,
abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf.
3 „Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung",
abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf.

Auch hier wird auf den Widerstreit zwischen privaten und öffentlichen Interessen beim Einsatz von Verschlüsselung hingewiesen und betont, dass immer mehr Kommunikationskanäle und Datenspeicherdienste standardisiert Ende-zu-Ende-verschlüsselt sind. Dies gelte sowohl für Messaging Apps wie auch für Online-Plattformen.[4] Wie auch die Bundesregierung verweist die EU auf die Zunahme von Gefahren im Cyberraum, die ein effektives staatliches Handeln erforderlich machen. Genannt werden als widerstreitende öffentliche Interessen beispielhaft Terrorismus, organisierte Kriminalität, der sexuelle Missbrauch von Kindern insbesondere im digitalen Raum und *„Cyberstraftaten"*.[5] Deshalb sei es notwendig, das „richtige Gleichgewicht" in der Berücksichtigung der verschiedenen Interessen herzustellen: So müsse die Privatsphäre und Sicherheit der Kommunikation durch Verschlüsselung geschützt werden und den zuständigen Behörden in den Bereichen Sicherheit und Strafjustiz müsse ermöglicht werden, einen rechtmäßigen Zugang zu ebenjenen Daten für legitime und klar definierte Zwecke zu erhalten. Dies müsse unter Einhaltung der Grundsätze der Notwendigkeit, Verhältnismäßigkeit und Subsidiarität geschehen.[6] Dass es sich bei derlei Erwägungen nicht bloß um abstrakte verfassungsrechtliche Diskussionen handelt, wird aktuell und regelmäßig deutlich: So beispielsweise anhand der politischen Debatte um die Vorratsdatenspeicherung und verschiedene Alternativen wie „Quick Freeze"[7], den Vorstoß der EU-Kommission für den CSAM-Act[8] sowie den europaweiten strafrechtlichen Ermittlungen, die infolge einer technischen Kompromittierung des ehemaligen Anbieters für verschlüsselte Kommunikation „EncroChat" eingeleitet wurden[9].

Die vielfältigen und widerstreitenden Interessen in der bereits seit Jahren geführten Debatte um den Einsatz von Verschlüsselung durch Private spiegeln sich ebenso in den zahllosen Vorschlägen zum Umgang des Staates mit Verschlüsselung als Ausprägung der rechtspolitischen Diskussion zum Thema wider: So reichen die entsprechenden Vorschläge von einem Verschlüsselungsverbot[10], der Pflicht zur Schlüsselherausgabe (*„Key Escrowing"*, siehe z.B. § 8 Abs. 3 S. 1 TKÜV), der Umgehung/Brechung von Verschlüsselungen (z.B. mit Hilfe der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) § 100a Abs. 1 S. 2, S. 3 StPO, § 1 Abs. 1 G10 i.V.m. §§ 3, 5, 8, 11 Abs. 1a G10, § 34 BNDG, § 51 Abs. 2 BKAG, § 72 Abs. 3 ZFdG) über die Verpflichtung von Telekommunikationsanbietern zur Verschlüsselung (Art. 40 Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation – EKEK) bis hin zu einem gänzlichen Ver-zicht auf Regelungen zum Umgang mit Verschlüsselung („Eingriff" verstanden als Verstoß gegen den Schutzauftrag des Staates im Hinblick auf entsprechende grundrechtliche Schutzpflichten)[11]. Aus dieser Komplexität und Vielschichtigkeit von Argumentation, Anforderungen, Maßnahmen sowie Restriktionen wird schnell deutlich, dass es bei der juristischen Beurteilung von Verschlüsselung nicht nur die zwei Dimensionen der Erleichterung staatlicher Ermittlungen im Cyberspace und einem erhöhten Gefährdungspotenzial für die Allgemeinheit gehen kann, soweit die digitale staatliche Informationssammlung durch den Einsatz von Verschlüsselungsmethoden behindert wird. Ebenso wenig kann das in diesem Kontext oftmals hervorgebrachte Argument, dass Verschlüsselungstechnik nur von Personen eingesetzt wird, die „etwas zu verbergen haben" bzw. „Straftaten begehen wollen", überzeugen.[12] Dieses Argument hat gegenwärtig auch dadurch erheblich an Tragweite verloren, da Verschlüsselungstechnik nicht nur von einer Vielzahl der Kommunizierenden bereits genutzt wird, sondern auch weil Kommunikationsdienste zur Verschlüsselung ihrer übermittelten Nachrichten gesetzlich verpflichtet sind.

Das nachfolgende Rechtsgutachten hat deshalb auch nicht die Beurteilung der Rechtmäßigkeit staatlicher Informationsbeschaffung an sich zum Gegenstand, sondern setzt sich ausschließlich mit der Frage auseinander, welche jeweils unterschiedliche juristische Wertung für die staatliche Beschaffung verschlüsselter Daten in Abgrenzung zur staatlichen Beschaffung unverschlüsselter Daten vorzunehmen ist. Zweifellos gilt dabei der generelle Leitsatz, den das Bundesverfassungsgericht (BVerfG) bereits im Jahr 2008 in seiner Entscheidung zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht bzw. Computer-Grundrecht) zum Ausdruck gebracht hat und der verdeutlicht, dass ein staatlicher Zugriff auf verschlüsselte Daten weitaus höherer Maßstäbe zur verfassungsrechtlichen Rechtfertigung verglichen mit dem Zugriff auf unverschlüsselte Daten bedarf:

„Schließlich ist zu berücksichtigen, dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechnologie zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff unterlaufen. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs."[13]

---

4 „Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung", S. 3, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf.

5 „Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung", S. 3, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf.

6 „Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung", S. 4, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf.

7 Referentenentwurf des Bundesministeriums der Justiz: Entwurf eines Gesetzes zur Einführung einer Sicherungsanordnung für Verkehrsdaten in der Strafprozessordnung, abrufbar unter: https://cdn.netzpolitik.org/wp-upload/2022/10/2022-10-25_BMJ_RefE_Sicherungsanordnung-StPO.pdf.

8 „Regulation Proposal on Child Sexual Abuse Material" (CSAM), Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern, 2022/0155(COD), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0209&from=DE.

9 Siehe zur kritischen Auseinandersetzung mit dem Thema Kipker, „Juristisches Neuland – Der Fall EncroChat: Rechtliche Probleme bei digitalen Ermittlungen", c't Ausgabe 9/2022, S. 174 sowie Kipker/Bruns, „EncroChat und die‚Chain of Custody'", MMR 2022, 363.

10 *Dietrich*, GSZ 2021, 1, 4.

11 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 116 ff.

12 So jedoch z.B. die zurzeit geführte Debatte um „EncroChat", indem argumentiert wird, dass der Kommunikati-onsdienst von vornherein darauf ausgerichtet gewesen ist, die Begehung von Straftaten zu erleichtern bzw. zu ermöglichen. Siehe in diesem Zusammenhang SPIEGEL TV vom 15.3.2021, „Entschlüsselt: Das geheime Tagebuch der Organisierten Kriminalität", abrufbar unter: https://www.spiegel.de/panorama/justiz/spiegel-tv-vom-15-03-2021-entschluesselt-das-geheime-tagebuch-der-organisierten-kriminalitaet-a-763ec429-299b-432d-8a85-61de9fa384de.

13 BVerfG NJW 2008, 822, 830, Rn. 236 (GVIiS-Urteil).

C. Verständnis und Zuordnung der Begrifflichkeiten

Generell kann unter Verschlüsselung ein technisches Verfahren verstanden werden, um die Lesbarkeit von in Daten enthaltenen Informationen zu verhindern bzw. zumindest signifikant zu erschweren. (Unbefugten) Dritten soll es auf diese Weise praktisch unmöglich gemacht werden, Zugang zu den verschlüsselten Informationen zu erlangen, selbst wenn diese über beträchtliche technische Ressourcen verfügen und mit dem Verfahren vertraut sind. Gleichzeitig ist zu gewährleisten, dass sich sowohl die Ver- wie auch die Entschlüsselung von Daten für Berechtigte mit bekanntem Schlüssel als möglichst effizient gestaltet, um die Praktikabilität und damit die Anwendbarkeit des Verfahrens zu sichern.[14]

Zu unterscheiden ist zwischen der Transportverschlüsselung sowie der Inhaltsverschlüsselung. Die Transportverschlüsselung ist bei Kommunikationsvorgängen relevant und betrifft Daten, die über Webverbindungen von einem Datenträger zum nächsten gesendet werden.[15] Im Rahmen der Transportverschlüsselung wird der Nachrichtenkanal, also die Kommunikation zwischen dem Nachrichtensender und dem Provider verschlüsselt. Der Provider leitet die verschlüsselte Nachricht weiter zu ihrem Empfänger bzw. an dessen Provider (sog. „Punkt-zu-Punkt-Verschlüsselung", P2PE bzw. auch als „Leitungsverschlüsselung" bezeichnet). Unter dem Gesichtspunkt der Cybersicherheit ist die Transportverschlüsselung jedoch suboptimal, denn sie bietet zwar den Schutz vor einem Abhören der Datenleitung, jedoch wird die Nachricht auf ihren Zwischenstationen, so beispielsweise auf dem Server des Providers, entschlüsselt. Damit haben bei einer Hintereinanderschaltung verschlüsselter Leitungen alle Zwischenempfänger Zugang zum Klartext einer Nachricht. Moniert wird dabei insbesondere auch, dass sich hierdurch ein technisches Missbrauchspotenzial durch den Provider selbst ergebe.[16] In der juristischen Literatur wird teilweise noch vertreten, dass sich die Transportverschlüsselung als *„Stand der Technik"* etabliert hat.[17] Mittlerweile jedoch dürfte davon auszugehen sein, dass sich die *„Ende-zu-Ende-Verschlüsselung"* (E2EE) mehr und mehr als Standard durchsetzt, so zum Beispiel für E-Mails mit OpenPGP und S/MIME sowie bei Messengern mit dem Signal-Protokoll. Zumindest aber der BGH sieht E2EE im elektronischen Anwaltspostverkehr noch nicht als erforderlich an.[18] Im Sinne einer E2EE kann auch Art. 40 Abs. 1 EKEK verstanden werden, indem von angemessenen und verhältnismäßigen technischen und organisatorischen Maßnahmen die Rede ist, die den Stand der Technik berücksichtigen, worunter laut dem Wortlaut der Vorschrift auch der Einsatz von Verschlüsselungstechnologie fällt. Auch § 19 Abs. 4 TTDSG schreibt den Anbietern von Telemedien gesetzlich vor, die Datensicherheit durch technisch-organisatorische Vorkehrungen sicherzustellen. Hier ist ebenso der Stand der Technik zu berücksichtigen. § 19 Abs. 4 S. 3 TTDSG fordert gar explizit die Anwendung eines *„als sicher anerkannten Verschlüsselungsverfahrens"*.

Die Ende-zu-Ende-Verschlüsselung als Unterfall der *„Inhaltsverschlüsselung"*[19] hat sowohl die Verschlüsselung von Daten während eines Kommunikationsvorgangs wie auch im „ruhenden" Zustand auf einem Endgerät zum Gegenstand. Entscheidender Faktor dabei ist, dass das Datum selbst in seinem Inhalt verschlüsselt wird,[20] sodass die in ihm enthaltene Nachricht lückenlos vom Sendezeitpunkt bis zum Empfangszeitpunkt verschlüsselt bleibt. Beschrieben wird die E2EE als essenzieller Schutz für die Privatsphäre des Anwenders, da der Diensteanbieter im Falle einer alleinigen Transportverschlüsselung immer noch alle auf dem Server gespeicherten Nachrichten mitlesen kann.[21]

Neben den verschiedenen Verschlüsselungstechniken ist überdies die begriffliche Abgrenzung der zu verschlüsselnden Datentypen relevant, da hieraus unterschiedliche verfassungsrechtliche Schutzbereichsanforderungen abgeleitet werden können, so umfasst die Schutzbereichsgewährleistung z.B. des Art. 8 GRCh nur die Verarbeitung, also jeder beliebige Vorgang im Zusammenhang mit Daten (z.B. Erhebung, Benutzung, Veränderung, Weitergabe, Löschung etc.)[22], von personenbezogenen Daten. Zentral ist in diesem Zusammenhang die Legaldefinition zum personenbezogenen Datum in Art. 4 Nr. 1 DSGVO, dergemäß sind *„personenbezogene Daten"*

13 BVerfG NJW 2008, 822, 830, Rn. 236 (GVIiS-Urteil).
14 BSI, Datenverschlüsselung, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datenverschluesselung/datenverschluesselung_node.html.
15 *Gasteyer/Säljemar*, NJW 2020, 1768, 1771.
16 BSI, Verschlüsselt kommunizieren im Internet, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/verschluesselt-kommunizieren_node.html.
17 *Gasteyer/Säljemar*, NJW 2020, 1768, 1772.
18 BGH BeckRS 2021, 9686, Rn. 8: „Das Erfordernis einer Ende-zu-Ende-Verschlüsselung ergebe sich auch nicht mittelbar aus dem gesetzlichen Erfordernis eines sicheren Übertragungswegs. Dies wäre nur der Fall, wenn allein die Ende-zu-Ende-Verschlüsselung diese Voraussetzungen erfüllte. Die Architektur des besonderen elektronischen Anwaltspostfachs sei jedoch sicher im Rechtssinne. Hierbei orientiere sich der Senat an dem von beiden Parteien eingereichten Gutachten, das das beA einer ausführlichen, qualifizierten und nachvollziehbaren Risikobewertung unterzogen habe."
19 *Wurm*, Die DSGVO und die E-Mail-Verschlüsselung, eRecht24, abrufbar unter: https://www.e-recht24.de/artikel/datenschutz/11284-dsgvo-und-e-mail-verschluesselung.html.
20 *Gasteyer/Säljemar*, NJW 2020, 1768, 1772.
21 *Scherschel*, WhatsApp verschlüsselt konsequent: Privatsphäre für eine Milliarde Nutzer, c't Ausgabe 9/2016, S. 16, abrufbar unter: https://www.heise.de/select/ct/2016/9/1461921496355024; siehe auch: BSI, E-Mail Verschlüsselung, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesselt-kommunizieren/E-Mail-Verschluesselung/e-mail-verschluesselung_node.html;
sowie DSK, Orientierungshilfe zu Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Stand 16. Juni 2021,
abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.
22 *Gersdorf* in: BeckOKInfo&MedienR, Art. 8 GRCh, Rn. 18; *Jarass* in: Jarass, GRCh, Art. 8, Rn. 9; Kingreen in: Cal-liess/Ruffert, EUV/AEUV, Art. 8 GRCh, Rn. 13 alle mit Bezug auf Art. 2 lit. b der Datenschutz-RL oder Art. 4 Nr. 2 DS-GVO. Siehe auch Wissenschaftliche Dienste des Deutschen Bundestags, Ausarbeitung „‚Chatkontrolle' – Ana-lyse des Verordnungsentwurfs 202/0155 (COD) der EU-Kommission", Az. WD 10 – 3000 – 026/22, S. 9.

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person[23] […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.[24] Die definitorische Abgrenzung zwischen einem personenbezogenen und einem nichtpersonenbezogenen Datum ist vielschichtig, einzelfallabhängig und nicht immer zweifelsfrei möglich, da hierbei auch Datensparsamkeitstechniken wie Anonymisierung, Pseudonymisierung oder die Generierung von synthetischen Daten eine Rolle spielen. Insoweit wird auf die einschlägige rechtswissenschaftliche Literatur zum Thema verwiesen. Juristisch ist für die Beurteilung des Personenbezugs überdies irrelevant, ob das Datum besonders sensible Informationen enthält, allein der personale Bezug ist für die Einstufung als personenbezogenes Datum entscheidend.[25]

D. Verfassungsrechtliche Gewährleistungen und Grenzen eines „Rechts auf Verschlüsselung“

I. Grundrechtsdogmatik und Grundrechtsfunktionen

Die rechtswissenschaftliche Untersuchung auf Bestehen eines verfassungsrechtlich gewährleisteten „Rechts auf Verschlüsselung“ orientiert sich an der klassischen juristischen Prüfreihenfolge, die sowohl für die nationalen Grundrechte als auch für die GRCh gilt.[26] Unterschieden wird dabei zwischen dem Schutzbereich, dem Eingriff und der verfassungsrechtlichen Rechtfertigung.

Im Schutzbereich wird im ersten Schritt analysiert, ob ein staatlich beeinträchtigtes Verhalten inhaltlich von einem Grundrecht umfasst ist[27] – dies in sachlicher[28] und persönlicher[29] Hinsicht. Dabei gilt, dass mehrere Grundrechte durch die Ausübung eines Verhaltens gleichzeitig parallel betroffen sein können. In diesem Fall kann ein spezielleres Grundrecht das allgemeinere verdrängen.[30] Beispielsweise ist bei dem Versand einer Nachricht und deren anschließender Speicherung auf einem Datenträger zwischen einer Betroffenheit des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG und des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu differenzieren.

Im Rahmen des Eingriffs wird geprüft, ob der Schutzbereich eines Grundrechts, dessen Eröffnung zuvor bejaht wurde, durch eine staatliche Maßnahme auch tatsächlich beeinträchtigt ist.[31] Der Eingriff umfasst nach einem modernen verfassungsrechtlichen Verständnis nicht nur rechtliche, sondern auch rein faktische Auswirkungen, die auch nur mittelbar dem Staat zugerechnet werden können – eine staatliche Intention ist ebenfalls nicht erforderlich.[32] Falls ein Eingriff in mehrere Grundrechte parallel vorliegt, muss dieser für jedes einzelne Grundrecht an sich verfassungsrechtlich gerechtfertigt sein. Dabei kann ein Eingriff auch in einem Unterlassen einer staatlichen Pflicht bestehen.[33] Der Eingriff scheidet aus, falls der Grundrechtsberechtigte auf die Wahrnehmung seines Grundrechts verzichtet.[34]

Die verfassungsrechtliche Rechtfertigung ist der dritte Prüfschritt. So ist der staatliche Eingriff in ein Grundrecht dann nicht rechtswidrig, wenn er verfassungsrechtlich gerechtfertigt ist. Hierbei gilt der Vorbehalt des Gesetzes i.V.m. mit den kollidierenden Grundrechten anderer.[35] Überdies müssen die staatliche Befugnisnorm, die zum Eingriff ermächtigt, und der rechtlich darauf basierende Einzelakt den verfassungsrechtlichen Maßstäben genügen. Dazu gehört, dass beide als aus dem Rechtsstaatsprinzip folgende Anforderung verhältnismäßig sind. Hierfür müssen sie einen legitimen Zweck verfolgen, zur Erreichung dieses Zweckes geeignet sein, im Sinne der Erforderlichkeit das mildeste verfügbare gleicheffektive Mittel darstellen und angemessen sein. Im letztgenannten Prüfungspunkt der Angemessenheit findet eine Abwägung der sich gegenüberstehenden verfassungsrechtlichen Positionen statt.[36] Zu berücksichtigen sind das Übermaß- und das Untermaßverbot.

---

23 EuGH Rs. C-291/12, Rn. 26.
24 EuGH Rs. C-291/12, Rn. 27.
25 *Gersdorf* in: BeckOKInfo&MedienR, Art. 8 GRCh, Rn. 16.
26 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 14; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh, Rn. 46.
27 *Dreier* in: Dreier, GG, Vor Art. 1, Rn. 119 f.
28 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 19 ff.; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh, Rn. 47 ff.
29 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 22 f.; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh, Rn. 51 ff.
30 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 16 ff.
31 *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh, Rn. 55.
32 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 28 f.
33 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 29.
34 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 35.
35 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 38; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh, Rn. 61.
36 BVerfGE 90, 145, 185; *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh, Rn. 65 ff.

Dogmatisch ist bei einer verfassungsrechtlichen Betrachtung zwischen den unterschiedlichen Schutzdimensionen der Grundrechte zu unterscheiden. Das Grundrecht ist in seiner Funktion als sog. *„Abwehrrecht“* dann einschlägig, wenn der Staat in den Schutzbereich eingreift und diesen mithin verkürzt, indem er grundrechtliche Positionen einschränkt. In ihrer Funktion als Abwehrrecht verpflichten die Grundrechte den Staat mithin zur Achtung von Grundrechten durch das Unterlassen von Eingriffen.[37] Diese essenzielle Grundrechtsfunktion ist für die Regelung des Staat-Bürger-Verhältnisses zentral.[38] Durch die Abwehrrechte erhält jeder einzelne Staatsbürger die effektive Möglichkeit, in Form eines Unterlassungsanspruches[39] vom Staat verursachte Störungen zu beseitigen[40]. Dennoch bleiben Eingriffe im Rahmen der zuvor skizzierten verfassungsrechtlichen Rechtfertigung weiterhin zulässig.[41]

Grundrechte können den Staat jedoch auch zu einem aktiven Handeln verpflichten – diese Grundrechtsfunktion wird durch die sog. *„Schutzpflicht“* erfüllt.[42] Einschlägig ist die staatliche Schutzpflicht dann, wenn der grundrechtliche Schutzbereich von Personen ohne staatliches Handeln[43] dermaßen stark verkürzt ist, dass ein Unterlassen des Staates in Form des eigentlich notwendigen aktiven Gegenwirkens einem Eingriff und damit im Ergebnis einem Verstoß gegen das Untermaßverbot gleichkäme.[44] In der Regel erfolgt die Erfüllung der staatlichen Schutzpflicht durch den Erlass entsprechender Rechtsvorschriften,[45] so beispielsweise zur Strafbarkeit von Computersabotage oder dem Ausspähen von Daten. Jedoch verfügt der Staat über einen weit gefassten Einschätzungsspielraum zur Gestaltung der konkreten Art und Weise des aktiven Grundrechtsschutzes.[46] Das Untermaßverbot hat (anders als das *„Übermaßverbot“*) zwei unterschiedliche Dimensionen: So dürfen einerseits die Rechte der zu schützenden Person durch ein staatliches Unterlassen nicht maßlos beeinträchtigt sein, andererseits dürfen die Rechte der durch eine staatliche Maßnahme infolge der Schutzbereichsverkürzung verpflichteten Person ebenso nicht maßlos beeinträchtigt sein. Der staatliche Einschätzungs- und Handlungsspielraum befindet sich inmitten dieses Konflikts widerstreitender Interessen.

II. Ableitung aus dem nationalen Verfassungsrecht

Im Folgenden wird untersucht, ob ein *„Recht auf Verschlüsselung“* aus den nationalen deutschen verfassungsrechtlichen Gewährleistungen ableitbar ist und falls ja, in welchen Inhalten und Dimensionen sich ein solches Recht manifestieren könnte.

Dabei gilt der Grundsatz, dass alle nationalen Grundrechte grds. gleichzeitige parallele rechtliche Wirkung entfalten, soweit diese einen inhaltsgleichen Schutzbereich abdecken und nicht von einem spezielleren Grundrecht verdrängt werden oder ein Grundrecht einen nach seinem Sinngehalt stärkeren Sachbezug aufweist.[47]

Ausdrücklich enthält das Grundgesetz in seinem Wortlaut kein *„Recht auf Verschlüsselung“*, jedoch wird ein solches im Folgenden aus der Zusammenschau bestehender einschlägiger Grundrechte abgeleitet. Relevant in diesem Zusammenhang sind alle Grundrechtspositionen, die die (digitale) Datenverarbeitung und Datenübermittlung zum Gegenstand haben, so das Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (GVIiS). Dabei zu berücksichtigen ist nicht nur die Frage, in welchem Umfang der Schutzbereich der Grundrechte neben unverschlüsselter auch verschlüsselte Kommunikation umfasst, sondern auch, ob und in welchem Umfang ein Recht auf Verschlüsselung verfassungsrechtlich legitimierbar eingeschränkt werden kann.

1. Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG

a) Abwehrrecht: Schutzbereich

Das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG umfasst in seinem Schutzbereich die private oder öffentliche passwort-/schlüsselzugängliche Fernkommunikation und ist *lex specialis* zum Grundrecht auf informationelle Selbstbestimmung.[48] Inhaltlich ist die verschlüsselte Fernkommunikation unstreitig von Art. 10 Abs. 1 GG umfasst.[49] Dies lässt sich u.a. daraus ableiten, dass das Grundrecht in seinem Wesen nicht danach unterscheidet, ob Kommunikationsinhalte verständlich sind oder nicht.[50] Selbst wenn der Inhalt einer Kommunikation verschlüsselt ist, kann überdies für die mit der Kommunikation unerlässlich verbundenen Verkehrsdaten weiterhin ein Schutzbedarf bestehen.[51] Im Ergebnis bedeutet die Ausdehnung des Schutzbereichs des Fernmeldegeheimnisses auf unverschlüsselte wie verschlüsselte Kommunikation gleichermaßen, dass erst auf der Ebene des

37 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 3.
38 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 1.
39 *Sachs* in: Sachs, GG, Vor Art. 1, Rn. 42.
40 *Remmert* in: Dürig/Herzog/Scholz, GG, Art. 19 Abs. 2, Rn. 43.
41 *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 51 GRCh, Rn. 29.
42 BVerfGE 39, 1.
43 BVerfGE 125, 39, 78.
44 BVerfGE 88, 203, 254
45 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 5.
46 BVerfGE 77, 170, 214 f.; 115, 118, 159 f.
47 *Jarass* in: Jarass/Pieroth, GG, Vor Art. 1, Rn. 16 ff.
48 BVerfG NJW 2000, 55, 56.
49 *Dietrich*, GSZ 2021, 1, 2; *Gersdorf* in: BeckOKInfo&MedienR, Art. 10 GG, Rn. 17; *Jarass* in: Jarass/Pieroth, GG, Art. 10, Rn. 12 a. E.; *Ogorek* in: BeckOKGG, Art. 10 Rn. 13 a. E.; *Löwer* in: v. Münch/Kunig, GG, Art. 10, Rn. 12.
50 BVerfGE 106, 28.
51 *Durner* in: Dürig/Herzog/Scholz, GG, Art. 10, Rn. 112.

Grundrechtseingriffes erkennbar ist, ob ein verschlüsseltes Datum kommuniziert wurde. Auch kann im Hinblick auf den Schutzbereich des Art. 10 Abs. 1 GG die Argumentation nicht durchgreifen, dass die Nutzung verschlüsselter Kommunikation per se den Verdacht eines strafbaren Verhaltens nahelege. Denn nur weil sich ein Grundrechtsberechtigter durch technische Maßnahmen in einem überdurchschnittlichen Maß vor einem Eingriff in seine verfassungsrechtlich geschützten Positionen schützt, wäre es sachwidrig, ihm aus diesem Grunde eine zentrale grundrechtliche Gewährleistung abzuerkennen. Anderenfalls würde dies einem Verbot zur Selbsthilfe gleichkommen, seine eigenen Grundrechte effektiv wahrzunehmen.[52] Der Besitz und die Verwendung eines speziell für die verschlüsselte Kommunikation entwickelten Mobilendgeräts begründet deshalb keinen Tatverdacht zur Begehung von Straftaten.[53] Denn wenn man diesen bejahen würde, müsste man bei der gegenwärtig standardisiert verwendeten E2E-Verschlüsselung alle Nutzer von Messenger-Diensten unter einen Generalverdacht stellen. An dieser Stelle kann juristisch auch eine Parallele zum Briefgeheimnis gezogen werden: Wenn verschlossene Briefe der Kenntnisnahme durch Dritte entzogen sind, muss dies konsequenterweise auch für verschlüsselte Nachrichten gelten.[54] Für die Eröffnung des Schutzbereichs kommt es überdies grds. nicht darauf an, welches technische Verschlüsselungsverfahren verwendet wird, welchen Grad von Sicherheit dieses bietet und ob es dem aktuellen Stand der Technik entspricht.

Gleichwohl existiert keine technisch absolut und unangreifbar sichere Verschlüsselungsmethode – genauso können Verschlüsselungsmechanismen umgangen werden, wie die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) belegt. Die entsprechenden gesetzlichen Erlaubnistatbestände zur Kompromittierung digitaler Kommunikation legen jedoch nahe, dass an ein solches staatliches Handeln qualifizierte tatbestandliche Anforderungen in den entsprechenden einfachgesetzlichen Befugnisgrundlagen anzulegen sind. Hieraus ergibt sich folglich, dass der Gesetzgeber erkannt hat, dass verschlüsselte Kommunikation gegenüber unverschlüsselter Kommunikation im Sinne des Schutzbereichs einen höheren inhaltlichen Stellenwert besitzt, sodass eine Ausspähung an dieser Stelle nicht nur eine höhere Eingriffsqualität hat, sondern auch höheren rechtlichen Anforderungen im Rahmen der verfassungsrechtlichen Rechtfertigung genügen muss.[55]

Charakteristisch für den Schutzbereich von Art. 10 Abs. 1 GG ist, dass nicht die Kommunikationsmöglichkeit an sich verfassungsrechtlich geschützt wird – verstanden als Gewährleistung der Existenz der Fernkommunikation durch entsprechende Anlagen – sondern der Kommunikationsvorgang selbst geschützt ist, soweit er spezifische Übermittlungsrisiken mit sich bringt.[56] Umfasst sind daher Inhalte, Umstände/Metadaten[57] und Verkehrsdaten[58]. Es spielt dabei keine Rolle, ob die Kommunikationsdaten personenbezogen sind.

Im Rahmen der Eröffnung des Schutzbereichs des Fernmeldegeheimnisses ergibt sich eine Besonderheit bei der Abgrenzung von P2PE und E2EE. So ist die Verwendung einer Transportverschlüsselung unproblematisch vom Schutzbereich des Art. 10 Abs. 1 GG umfasst: Da bei diesem technischen Verfahren der Kommunikationskanal geschützt bzw. verschlüsselt wird, findet mit einem Eingriff in die Transportverschlüsselung gleichzeitig auch ein Eingriff in den geschützten Kommunikationsvorgang statt. Bei der Verwendung einer Inhaltsverschlüsselung stellen sich jedoch rechtliche Abgrenzungsfragen zum GVIiS – dabei ist zwischen unterschiedlichen Fallkonstellationen zu unterscheiden: Problemlos ist der Schutzbereich des Art. 10 Abs. 1 GG eröffnet, wenn ein bereits verschlüsseltes Datum übermittelt wird, da sich dieses auf dem Kommunikationsweg befindet. Abgrenzungsprobleme ergeben sich aber möglicherweise dann, wenn ein zur Übermittlung bestimmtes Datum zwar verschlüsselt werden soll, die Ermittlungs- bzw. Sicherheitsbehörde auf ebenjenes Datum aber noch vor der Verschlüsselung und dem Beginn des technischen Übermittlungsvorgangs zugreift. In Abgrenzung des Fernmeldegeheimnisses zum GVIiS ist für diesen Fall zu beachten, dass die bloße Verschlüsselung ohne eine Datenübertragung gerade nicht vom technischen Übermittlungsrisiko betroffen ist. Damit würde in der zeitlichen Abfolge an dieser Stelle (noch) nicht der Kommunikationsvorgang, sondern der Schutzbereich der digitalen Datenverarbeitung bzw. -speicherung adressiert, der eigentlich nicht dem Fernmeldegeheimnis unterfällt. Eine solche *„Aufsplittung"* von technisch eigentlich fließend ineinander übergehenden Vorgängen führt juristisch aber zu einer nur schwer vertretbaren Voranstellung von Eingriffs- und Schrankenfragen vor den dogmatisch zuvor zu prüfenden Schutzbereich, denn im Ergebnis ist es wie eingangs festgestellt für die Eröffnung des Schutzbereichs des Fernmeldegeheimnisses unschädlich, ob das zu übermittelnde Datum vor dem technischen Übermittlungsvorgang verschlüsselt wurde oder nicht.[59] Der Zweck des verschlüsselten Datums ist die sich unmittelbar daran anschließende Kommunikation und damit der Schutz des Inhalts der Nachricht, sodass der Schutzbereich des Fernmeldegeheimnisses bei einem technisch derart zusammenhängenden Vorgang eröffnet ist.[60] Soweit daher der Kommunikationsbezug gegeben ist, kann die Bestimmung und der eventuelle Wechsel des Schutzbereichs nicht damit begründet werden, dass der Eingriff an chronologisch im Zeitablauf anderer Stelle erfolgt – vor, während oder nach Abschluss des Kommunikationsvorganges. Eine andere rechtliche Auffassung hätte an dieser Stelle erhebliche Wertungswidersprüche zur Folge, denn ansonsten wäre es staatlichen Einrichtungen freigestellt, selbst

52 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 132.
53 *Kipker/Bruns*, MMR 2022, 363, 364.
54 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 135.
55 Hierzu vertiefend im Folgenden unter C. / II. / 1. / c). Beispielhaft äußern sich die erhöhten Rechtfertigungsvoraussetzungen deutlich in diesen sicherheitsbehördlichen Ermächtigungsgrundlagen: § 100a Abs. 1 S. 2, S. 3 StPO; § 1 Abs. 1 G10 i.V.m. §§ 3, 5, 8, 11 Abs. 1a G10; § 34 BNDG; § 51 Abs. 2 BKAG; § 72 Abs. 3 ZFdG.
56 *Jarass* in: Jarass/Pieroth, GG, Art. 10, Rn. 12.
57 BVerfGE 113, 348, 364 f.; 115, 166, 183; 120, 274, 307.
58 *Jarass* in: Jarass/Pieroth, GG, Art. 10, Rn. 8.
59 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 130.
60 BVerfG NJW 2006, 976, 978, Rn. 68.

die Rechtfertigungsvoraussetzungen für ihre Eingriffe in verschlüsselte Kommunikation zu bestimmen, indem sie je nach Sachlage die für sie günstigste technisch-zeitliche Konstellation ermitteln und zur Begründung bzw. verfassungsrechtlichen Rechtfertigung heranziehen. Dabei zeigt regelmäßig auch die Praxis, dass eine echte zeitliche Zäsur zwischen Verschlüsselung und Beginn der Übermittlung lebensfremd ist.

Gestützt wird diese Auslegung durch die Rechtsprechung des Bundesverfassungsgerichts, indem dieses feststellt, dass die Durchführung einer Quellen-TKÜ mit einem Eingriff in Art. 10 GG verbunden ist.[61] Bei der Quellen-TKÜ handelt es sich um eine Ermittlungsmaßnahme zur Umgehung von Verschlüsselung, bei der die behördliche Kenntnisnahme der Nachricht durch einen Eingriff in ein IT-System vor oder nach der Verschlüsselung, folglich vor Übermittlung oder nach Empfang, erfolgt. Wenn an dieser Stelle verfassungsrechtlich von einem untrennbaren Zusammenhang zwischen Verschlüsselung und Übermittlung der Nachricht ausgegangen wird, kann von einer prozesstechnischen und rechtlichen Zäsur mithin nicht gesprochen werden. Auch nach dieser Auffassung umfasst das Fernmeldegeheimnis mithin bereits verschlüsselte und noch nicht übermittelte Nachrichten, sodass auch die Inhaltsverschlüsselung umfasst ist.[62]

Im Ergebnis ist die verschlüsselte Kommunikation somit vollumfänglich vom Schutzbereich des Fernmeldegeheimnisses gem. Art. 10 Abs. 1 GG geschützt.

b) Eingriffsdogmatik

Ein Eingriff in das Fernmeldegeheimnis liegt in jeder Kenntnisnahme, Aufzeichnung und Verwertung geschützter Kommunikationsdaten,[63] mithin in jeder entsprechenden Datenverarbeitung[64]. Dabei ist jede einzelne Verarbeitung als einzelner Eingriff zu bewerten. Aus dieser rechtlichen Erkenntnis ergibt sich auch, dass die Quellen-TKÜ als Eingriff zu qualifizieren ist. Ebenso erfasst ist das Entschlüsseln kryptografisch gesicherter Kommunikationsinhalte als von der Erhebung getrennter Vorgang.[65] Weiterhin liegt unstreitig ein Eingriff vor, wenn der Staat Verschlüsselungsverfahren verbietet bzw. ihren Einsatz beschränkt.[66] Dabei ist nicht von Belang, ob der Staat die Kommunikationsdaten unmittelbar verarbeitet oder sich unter Behelf von Gesetzeszwang hierzu eines privaten Dritten bedient wie beispielsweise bei der Herausgabe von Verkehrs- und Bestandsdaten von Telekommunikationsdiensteanbietern.[67] Im Ergebnis können mögliche staatliche Eingriffe in das Fernmeldegeheimnis mit Blick auf ein Recht auf Verschlüsselung in einem absoluten/relativen Verschlüsselungsverbot, der Anordnung zur Herausgabe von Schlüsseln („*Key Escrowing*“) und der Umgehung/Brechung von Verschlüsselungen (z.B. mittels technischen Ermittlungswerkzeugen, die durch ZITiS bereitgestellt werden) zu sehen sein. Im Rahmen der erläuterten Grundrechtsdogmatik ist es jedoch ebenso möglich, Eingriffe gegen Telekommunikationsdiensteanbieter in einer Pflicht zur Verschlüsselung zu sehen und im Hinblick auf das Untermaßverbot selbst bei einer staatlichen Vernachlässigung des Themas „*Verschlüsselung*“ von einer Eingriffsqualität im Sinne eines Unterlassens auszugehen.

c) Verfassungsrechtliche Rechtfertigung des Eingriffs in die verschlüsselte Datenübermittlung

Für Art. 10 Abs. 1 GG gilt gem. Art. 10 Abs. 2 S. 1 GG ein einfacher Gesetzesvorbehalt. In diesem Sinne gelten die rechtlich üblichen Maßstäbe, die bei einem staatlichen Eingriff in das Fernmeldegeheimnis an die verfassungsrechtliche Rechtfertigung anzulegen sind: So bedarf es einer rechtlichen Eingriffslegitimation durch die Legislative bzw. auch in der Form von untergesetzlichen Rechtsverordnungen und Satzungen. Überdies müssen das Bestimmtheits- und Zitiergebot, die Wesenserhaltsgarantie und der rechtsstaatliche Grundsatz der Verhältnismäßigkeit eines jeden staatlichen Handelns beachtet werden. Besonderheit für Art. 10 GG sind die Zweckbindung[68], Kennzeichnung[69], Vernichtung[70], Unterrichtung[71] sowie der Richtervorbehalt bei besonders einschneidenden Ermittlungsmaßnahmen (z.B. heimliche Überwachung, vorsorgliche Speicherung)[72]. Die Grenze für Eingriffe ist der Kernbereich privater Lebensgestaltung.[73] Im Hinblick auf verschlüsselte Daten hat das BVerfG festgestellt, dass der staatliche Zugriff auf diese ein höheres Gewicht hat und somit zu seiner verfassungsrechtlichen Legitimation im Vergleich zu unverschlüsselten Daten qualifizierte Anforderungen erfordert. So ist nach Auffassung des Gerichts zu berücksichtigen, „*dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechnologie zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff unterlaufen. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs*“.[74]

Im rechtspolitischen Diskurs wird regelmäßig vertreten, dass starke Verschlüsselungsmechanismen seitens Privater den Staat in seinen digitalen Ermittlungsmöglichkeiten

61 BVerfG NJW 2008, 822, 826, Rn. 190.
62 Selbst bei gegenteiliger Auffassung wäre für die entsprechende Verschlüsselung hilfsweise der Schutzbereich des GVIiS eröffnet.
63 BVerfGE 100, 313, 366; 125, 260, 310.
64 Vgl. *Gersdorf* in: BeckOKInfo&MedienR, Art. 10 GG, Rn. 27.
65 *Durner* in: Dürig/Herzog/Scholz, GG, Art. 10, Rn. 157; *Ogorek* in: BeckOKGG, Art. 10, Rn. 50.
66 *Dietrich*, GSZ 2021, 1, 2 f.; Hermes in: Dreier, GG, Art. 10, Rn. 53; *Martini* in: v. Münch/Kunig, GG, Art. 10, Rn. 31; Ogorek in: BeckOKGG, Art. 10, Rn. 53;
67 BVerfGE 107, 299, 313; 124, 43, 58.
68 BVerfGE 125, 260, 317.
69 BVerfGE 100, 313, 360 f.
70 BVerfGE 100, 313, 362.
71 BVerfGE 100, 313, 361.
72 BVerfGE 120, 274, 331.
73 BVerfGE 113, 348, 391 f.
74 BVerfG NJW 2008, 822, 830, Rn. 236.

behinderten. Diskutiert werden deshalb Ansätze zum möglichst praxisgerechten Umgang mit Verschlüsselungstechnik, um bei gleichzeitig bestehender Verschlüsselungsmöglichkeit staatliche Zugriffsbefugnisse auf die verschlüsselten Informationen weiterhin bestehen zu lassen (*„Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung"*). Hierunter fällt auch die Diskussion um eine Schlüsselherausgabepflicht,[75] der jedoch mit erheblichen juristischen Bedenken entgegenzutreten ist. Soweit es Beschuldigte in einem Strafverfahren anbelangt, würde ein solches staatliches Begehren bereits gegen die Selbstbelastungsfreiheit verstoßen. Auch Dritte wie beispielsweise Systemadministratoren, denen unter Umständen der Schlüssel bekannt ist und die als Zeugen zu qualifizieren wären, müssen den Schlüssel nicht aktiv beschaffen, da sich ihre Aussage ausschließlich auf bereits vorhandenes Wissen beschränkt, nicht jedoch die aktive Beschaffung von zusätzlichem Wissen umfasst.[76] Für die Telekommunikationsdiensteanbieter hat der Gesetzgeber zumindest bereits in § 8 Abs. 3 S. 1 TKÜV eine Pflicht zur Schlüsselherausgabe begründet, soweit TK-Dienste verschlüsselt angeboten werden. Eine solche gesetzliche Regelung ist jedoch kritisch zu würdigen: So entstehen durch die Aufhebung für die Telekommunikation angewendeter Schutzvorkehrungen nicht nur zusätzliche IT-Sicherheitsrisiken, sondern Betroffene könnten sich bei Kenntnis einer solchen gesetzlichen Möglichkeit ebenso alternativer Kommunikationsmethoden bedienen, womit bereits die Effektivität der Regelung in § 8 Abs. 3 S. 1 TKÜV in Frage zu stellen sein dürfte. Überdies ist anzumerken, dass die vorgenannte Pflicht zur Schlüsselherausgabe nicht für Over-the-Top-Dienste (OTT-Dienste) gilt, die von den Netzinfrastrukturanbietern entkoppelt sind. Dabei hat eine Studie der Bundesnetzagentur (BNetzA) aus dem Jahr 2021 noch gezeigt, dass sich OTT-Dienste *„rasant"* verbreiten und von Nutzern oftmals parallel verwendet werden. Hierzu gehören zuvorderst WhatsApp (96%), Facebook Messenger (42%), Instagram Direct Messages (30%), Skype (18%) und Snapchat (12%).[77] Nicht zuletzt sprechen erhebliche psychologische Gründe im Sinne eines Einschüchterungseffekts gegen staatliche Zugriffsmöglichkeiten auf eine verschlüsselte Kommunikation, denn hierdurch wird im Ergebnis das Bewusstsein der Kommunizierenden gestärkt, noch leichter überwacht werden zu können, womit die Persönlichkeitsentfaltung in der Kommunikation beeinträchtigt wird.[78] Daher dürften umfassende und weitreichende staatliche Pflichten zur Schlüsselherausgabe, die sich beispielsweise auch gegen OTT-Dienste richten, verfassungsrechtlich kaum zu rechtfertigen sein.

d) Dimensionen eines Rechts auf Verschlüsselung als staatliche Schutzpflicht

Im Rahmen der Grundrechtsfunktionen[79] wurde bereits dargelegt, dass die Grundrechte den Staat auch zu einem aktiven Handeln verpflichten können – man spricht hier von sog. *„Schutzpflichten"*,[80] die sich in ihrem Umfang und in ihrer konkreten Ausgestaltung am Untermaßverbot orientieren müssen[81]. Hierbei verfügt der Staat über eine weit gefasste Einschätzungsprärogative.[82] Fraglich ist deshalb, ob als weitere Dimension aus den nationalen verfassungsrechtlichen Gewährleistungen auch eine aktive Schutzpflicht dergestalt resultieren kann, dass einerseits eine Verpflichtung für staatliche Einrichtungen besteht, Behördendaten zu verschlüsseln und andererseits eine Pflicht des Staates besteht, Anbieter von TK-Diensten gesetzlich zu einer Datenverschlüsselung zu verpflichten. Insbesondere für die staatliche Datenverarbeitung gilt, dass durch die Behörden eine Vielzahl auch sensibler Bürgerdaten verarbeitet wird, außerdem unterliegen diese ebenso den Pflichten zur Datensicherheit u.a. aus Art. 32 DS-GVO.

Grundsätzlich ist Art. 10 GG geeignet, aktive Pflichten des Staates zu begründen.[83] Dabei ist zu berücksichtigen, dass eine drohende Gefahr durch Überwachungs- bzw. Abhörmaßnahmen durch unbefugte Dritte ein erhebliches Schadenspotenzial für die vertrauliche Kommunikation birgt. Überdies ist zur Risikobeurteilung die potenzielle Schadenshöhe in Relation zur Schadenseintrittswahrscheinlichkeit zu setzen: So besteht bei digitaler Kommunikation stets eine nicht unerhebliche Wahrscheinlichkeit des unbefugten Abfangens bzw. Mitlesens von Nachrichten, sodass jede elektronische Kommunikation stets einer qualifizierten Gefährdungslage unterliegt. Die staatlichen Schutzdimensionen stellen sich für Art. 10 GG deshalb wie folgt dar:

→ In jedem Falle besteht die Verpflichtung der Exekutive, auch jenseits der Gesetzgebung effektive Maßnahmen zur Gewährleistung von Verschlüsselung zu realisieren. Da zur Umsetzung von Verschlüsselung vor allem auch der Bürger selbst gefordert ist, sind staatliche Informationsmaßnahmen und -kampagnen notwendig. Hierzu gehört z.B. die Aufgabe des BSI, im Rahmen der Verbraucherinformation gem. § 3 Abs. 1 Nr. 14a BSIG Leitfäden und Hinweise zur fachgerechten Umsetzung von Datenverschlüsselung zur Verfügung zu stellen. [84]

→ Überdies besteht eine aktive Pflicht der Hoheitsträger – insbesondere der Behörden – entsprechende Datensätze zu verschlüsseln, da ein unbefugter Zugriff durch Dritte eine erhebliche Bedrohung für die allgemeine Sicherheit

75 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 293 ff.
76 Siehe in diesem Zusammenhang auch §§ 95 Abs. 1, 103 Abs. 1 StPO.
77 Bundesnetzagentur, Nutzung von Online-Kommunikationsdiensten in Deutschland: Ergebnisse der Verbrau-cherbefragung 2021, abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/OnlineKom/befragung_lang21.pdf.
78 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 278.
79 Siehe Gliederungspunkt C. / I.
80 BVerfGE 39, 1.
81 BVerfGE 88, 203, 254.
82 BVerfGE 77, 170, 214 f.; 115, 118, 159 f.
83 BVerfG NJW 2007, 3055, 3055, Rn. 13.
84 Siehe beispielhaft BSI, Basistipps zur IT-Sicherheit: Datenverschlüsselung, abrufbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Datenverschluesselung/datenverschluesselung_node.html.

und für betroffene Personen darstellt. Soweit personenbezogene Daten verarbeitet werden, lässt sich eine allgemeine Verpflichtung zur Verschlüsselung insbesondere sensibler Datenbestände bereits aus Art. 5 Abs. 1 lit. f, 32 Abs. 1 lit. a Alt. 2 DSGVO ableiten. Zur technischen Umsetzung der Verschlüsselung stellte das Verwaltungsgericht Frankfurt a.M. im Zusammenhang mit der Kommunikation mit dem Bundesamt für Wirtschaft – auch im Rahmen von Art. 32 DSGVO – wie folgt fest: *„Daraus ist im vorliegenden Bereich wegen seiner Sensibilität zu schließen, dass eine unverschlüsselte elektronische Kommunikation nicht zulässig wäre, woraus freilich noch nicht folgt, dass eine Transportverschlüsselung nicht ausreichend sei.“*[85] Im Leitsatz stellt das Gericht fest, dass *„gegenwärtig eine Ende-zu-Ende-Verschlüsselung ausreichend“* sei.[86]

→ Den Staat trifft eine aktive Pflicht zur Regulierung bzw. Sanktionierung rechtswidriger Maßnahmen Privater, wodurch die Vertraulichkeit der Kommunikation beeinträchtigt wird. Insbesondere geht es hier um die gesetzliche Beschränkung von Störern.[87] Im Bereich des materiellen Strafrechts ist dies durch die Regulierung entsprechender Vorschriften erfolgt, so § 202a StGB (Ausspähen von Daten), § 202b StGB (Abfangen von Daten) und § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses).

→ Eine mögliche staatliche Verpflichtung von privaten TK-Anbietern, Verschlüsselung zu realisieren, muss differenziert betrachtet werden, denn das Untermaßverbot hat für den Bereich der staatlichen Schutzpflichten anders als das Übermaßverbot zwei Dimensionen: So dürfen die Rechte der zu schützenden Person nicht maßlos durch eine Unterlassung beeinträchtigt sein. Mit Blick hierauf ergibt sich infolge des raschen technischen Wandels regelmäßiger Anpassungsbedarf. Auf der Kehrseite dürfen die Rechte der durch das staatliche Handeln verpflichteten (juristischen) Person nicht im Übermaß beeinträchtigt werden. Zu berücksichtigen ist dabei auch, dass die Umsetzung von Verschlüsselungstechnik in standardisierten kommerziellen Kommunikationslösungen mittlerweile immer weniger aufwändig und vielfach zum Standard geworden ist. Im Hinblick auf die Wahrnehmung der Schutzpflicht liegt der staatliche Gestaltungsspielraum zwischen diesen beiden Dimensionen. Damit stellt sich die Frage, ob bei einer Nicht-Verpflichtung der TK-Anbieter zur Verschlüsselung ein so niedriges Sicherheitsniveau in der Kommunikation der Nutzenden entsteht, dass von einem erheblichen Untermaß an staatlicher Sicherheitsverantwortung gesprochen werden kann. Zu berücksichtigen ist hierbei, ob die zu treffende Maßnahme die staatliche Sicherheit bezweckt, ob die Maßnahme zur Gewährleistung der Datensicherheit geeignet bzw. förderlich ist, keine milderen bzw. effektiveren Mittel zur Verfügung stehen und die beabsichtigte Maßnahme die widerstreitenden Interessen in einen gerechten Ausgleich bringt, mithin also angemessen ist. Dabei gilt, dass das Fernmeldegeheimnis ein in einer demokratischen Gesellschaft notwendiges und essenzielles Kommunikationsgrundrecht darstellt, das auch das Teilen und Bilden von Meinungen prägt und somit von sensibler Vertraulichkeit gekennzeichnet ist.[88] Diesem Gedanken hat der Staat in § 165 Abs. 2 TKG einfachgesetzlich Rechnung getragen: So ist derjenige Anbieter, der ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, dazu verpflichtet, angemessene technische und organisatorische Vorkehrungen gegen schädliche Einwirkungen zu treffen. Zum Schutz vor unerlaubten Zugriffen sind insbesondere Verschlüsselungsmaßnahmen vorzusehen. Durch die Schaffung ebensolcher Vorgaben hat der Gesetzgeber unter Berücksichtigung des vorgenannten Verständnisses des Untermaßverbotes zum gegenwärtigen Zeitpunkt seine verfassungsrechtlichen Schutzpflichten erfüllt. Eine weitergehende Verpflichtung beispielsweise zu E2EE lässt sich zum gegenwärtigen Zeitpunkt hingegen (noch) nicht ableiten.[89]

Im Ergebnis lässt sich damit im Hinblick auf die Dimension eines Rechts auf Verschlüsselung als staatliche Schutzpflicht Folgendes feststellen: In seinem Handeln muss der Staat das Bedürfnis und die Notwendigkeit von Verschlüsselung aktiv berücksichtigen. Dabei findet die Verschlüsselung in einfachgesetzlichen Vorschriften zurzeit vor allem als angemessene technisch-organisatorische Sicherheitsmaßnahme Berücksichtigung bzw. wird beispielhaft als ein mögliches Verfahren zur Herstellung von Datensicherheit genannt. Eine noch weitergehende Verpflichtung des Staates ließe sich als aktive Dimension nur dann begründen, wenn man durch die bisherigen Regelungen das Untermaßverbot als verletzt ansieht. Dies ist jedoch nach gegenwärtigem technischen Entwicklungsstand juristisch nur schwer begründbar. Ein weiteres Argument, das dabei gegen die Verletzung des Untermaßverbotes spricht, ist die Tatsache, dass es aktuell auf dem IT- und Kommunikationsmarkt eine Vielzahl an Produkten gibt, die bereits E2EE als Standard implementiert haben, dies gilt insbesondere für standardisierte Messenger- und Videochat-Lösungen. Der nach wie vor intensiv genutzte E-Mail-Verkehr findet hingegen immer noch weitestgehend unverschlüsselt statt – auch aus dieser Tatsache lässt sich jedoch nicht die Verletzung des Untermaßverbotes herleiten, da die Möglichkeit zur Umsetzung von Mailverschlüsselung technisch sowohl theoretisch wie auch praktisch gegeben ist.

85 VG Frankfurt, Beschluss vom 15. Juli 2022 – 5 L1281/22.F, Juris-Rn. 19.
86 VG Frankfurt, Beschluss vom 15. Juli 2022 – 5 L1281/22.F, Leitsatz.
87 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 327.
88 *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 334.
89 So ebenfalls *Dietrich*, GSZ 2021, 1, 3 f. mit einer Auflistung beispielhafter Vorschriften.

2. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (GVIiS)

a) Abwehrrecht: Schutzbereich

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (GVIiS, synonym auch als „Computer-Grundrecht" bzw. „IT-Grundrecht" bezeichnet) wird aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitet und stellt damit eine besondere Ausprägung des Allgemeinen Persönlichkeitsrechts (APR) dar. Das BVerfG argumentierte anlässlich seiner Schaffung im Jahr 2008, dass der bislang vor allem durch Art. 10 Abs. 1 GG (Fernmeldegeheimnis) und Art. 13 Abs. 1 GG (Unverletzlichkeit der Wohnung) vermittelte sowie durch das ebenfalls aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitete Grundrecht auf informationelle Selbstbestimmung mit Blick auf die rasch fortschreitende technische Entwicklung und die damit verbundene extensive digitale Datenspeicherung lückenhaft sei.[90] Damit ist das GVIiS subsidiär zu den inhaltlichen Garantien des Art. 10 Abs. 1 GG und des Art. 13 Abs. 1 GG.[91] Charakteristisch für das GVIiS ist der Grundgedanke, den Computer zunehmend als „ausgelagertes Gedächtnis" zu begreifen. Vor allem auch die Corona-Pandemie hat seit März 2020 gezeigt, dass die Nutzung von Informations- und Kommunikationssystemen (IuK-Systemen) wichtiger denn je für die Persönlichkeitsentfaltung des Einzelnen ist, gleichzeitig aber auch mit steigenden und neuartigen Gefährdungen für die Persönlichkeit verbunden sein kann. Die Ausforschung von IuK-Systemen ermöglicht weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer vollständigen Profilbildung, die weit über die bloße Auswertung von Verkehrsdaten hinausgeht. Eine weitere Feststellung des BVerfG war darüber hinaus, dass wenn ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert wird, mit dieser Infiltration bereits die entscheidende Hürde genommen ist, um das System insgesamt auszuspähen. Das BVerfG begründete seine Entscheidung seinerzeit damit, dass die durch die mit der Infiltration des IT-Systems bedingte Gefährdung weit über die hinausgeht, die mit einer bloßen Überwachung der laufenden Kommunikation verbunden ist. Insbesondere können nach Auffassung des Gerichts auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen.[92] In der Rechtswissenschaft jedoch ist die Notwendigkeit der Einrichtung des GVIiS durchaus umstritten.[93]

Sachlich ist das Grundrecht dann einschlägig, wenn der staatliche Zugriff auf ein IT-System gegeben ist, sodass dessen Nutzung überwacht wird oder Daten abgeschöpft werden. Zentrale Anforderung in dem Zusammenhang: Durch die Infiltration des IT-Systems und dessen technischer Vernetzung ist es möglich, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.[94] In der bundesverfassungsgerichtlichen Entscheidung zur Herleitung des GVIiS werden als Beispiele Computer, Smartphones und elektronische Terminkalender genannt.[95] Demgegenüber soll das Grundrecht dann nicht einschlägig sein, wenn im Sinne einer *„Negativdefinition"* digital verarbeitete Daten einen lediglich punktuellen Bezug zu einem bestimmten Lebensbereich aufweisen. Als Beispiel nennt das BVerfG in diesem Zusammenhang *„nicht vernetzte elektronische Steuerungsanlagen der Haustechnik"*.[96] Für diesen Fall soll vielmehr der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung betroffen sein. Im Hinblick auf das Alter der Entscheidung aus dem Jahr 2008 und der mittlerweile allgegenwärtigen vernetzten Haustechnik in Form des *„Smart Home"* vermag diese Argumentation mittlerweile nicht mehr zu überzeugen, denn auch in heutigen und dem Stand der Technik entsprechenden Haussteuerungsanlagen kann sich die Persönlichkeitsentfaltung detailliert und in verschiedensten programmierten Parametern sowie in der damit verbundenen Sensorik und in Speicherdaten widerspiegeln. Damit wird die Grenzziehung zwischen dem GVIiS und dem Grundrecht auf informationelle Selbstbestimmung zunehmend weniger trennscharf.[97] Zur Abgrenzung zwischen den zwei Grundrechten hilfreicher ist daher eine *„Negativdefinition"*, die auch schon das BVerfG in seiner Entscheidung vorgenommen hat: *„Allerdings bedarf nicht jedes informations-technische System, das personenbezogene Daten erzeugen, verarbeiten oder speichern kann, des besonderen Schutzes durch eine eigenständige persönlichkeitsrechtliche Gewährleistung. Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält […], unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren."*[98]

Charakteristisch für die Einschlägigkeit des GVIiS als Grundrecht zum Schutz gegen eine umfassende digitale Ausforschung ist mithin, dass die betroffene Person das IT-System *„als eigenes"* nutzt. Das setzt voraus, dass sie zumindest eine teilweise Verfügungsgewalt über das System hat.[99]

90 BVerfGE 120, 274, 302 ff.
91 BVerfGE 120, 274, 302.
92 BVerfG NJW 2008, 822, 825, Rn. 188.
93 So z.B. kritisiert von *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 23 m.w.N.
94 BVerfGE 120, 274, 314.
95 BVerfG NJW 2008, 822, 827, Rn. 203.
96 BVerfG NJW 2008, 822, 827, Rn. 202.
97 So im Ergebnis auch *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 25.
98 BVerfG NJW 2008, 822, 827, Rn. 202.
99 *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 26.

Das GVIiS schützt insbesondere die Vertraulichkeit und Integrität der Nutzerdaten. Dabei gilt der Schutz unabhängig davon, ob im Sinne der aus dem Allgemeinen Persönlichkeitsrecht folgenden Sphärentheorie die Intim-, Privat- oder Sozialsphäre betroffen ist. Die Integrität als Schutzziel der IT-Sicherheit adressiert vor allem auch die Sicherheit eines IT-Systems im Vorfeld einer staatlichen Überwachung und ist dann beeinträchtigt, wenn durch den Zugriff auf ein System dessen Leistungen, Funktionen und Speicherinhalte extern genutzt werden können.[100] Zu beachten ist dabei, dass es sich bei der Kompromittierung der Integrität einerseits und dem Zugriff auf vertrauliche Daten andererseits um zwei Eingriffe in das GVIiS handelt, wobei die Kompromittierung der Integrität der Datenerhebung aus dem IT-System regelmäßig vorausgeht.[101] Explizit bezieht das BVerfG in den technischen Schutzumfang des GVIiS auch die Verschlüsselung von Daten ein.[102] Insoweit kann verfassungsrechtlich auch hieraus ein *„Recht auf Verschlüsselung“* abgeleitet werden. Das BVerfG betont in dem Zusammenhang insbesondere, dass eine heimliche technische Infiltration die längerfristige Überwachung der Nutzung des IT-Systems ermöglicht, wodurch der entsprechende Grundrechtseingriff *„von besonderer Schwere“* ist.[103] Hieraus folgt, dass der staatliche Eingriff in verschlüsselte Kommunikation einem deutlich höheren verfassungsrechtlichen Rechtfertigungsdruck unterliegt, als dies bei unverschlüsselter Kommunikation der Fall ist, da sich der Bürger im Fall der Verschlüsselung selbstbestimmt dazu entschieden haben dürfte, dem Schutz seiner digitalen Privatsphäre durch zusätzliche technische Maßnahmen ein besonderes Gewicht beizumessen. In seiner Stoßrichtung schützt das GVIiS mithin umfassende persönlichkeitswiderspiegelnde digitale Datenbestände, die gerade nicht auf einer Kommunikation beruhen müssen.[104] Auch in Abgrenzung sowohl zum Fernmeldegeheimnis als auch zum Grundrecht auf informationelle Selbstbestimmung bezweckt das GVIiS in seinem sachlichen Schutzbereich folglich den Schutz von verschlüsselten Inhaltsdaten – die Transportverschlüsselung (P2PE) ist somit bereits von ihrer Begriffsnatur her nicht vom GVIiS umfasst. Ebenfalls deutlich wird damit, dass aufgrund der notwendigen technischen Differenzierung unterschiedlicher Datenverarbeitungsschritte durchaus ein verfassungsrechtlicher Bedarf zur Schaffung des GVIiS bestand, dem das BVerfG in seinem entsprechenden Urteil nachgekommen ist.

Die den umfassenden digitalen Schutzinteressen Rechnung tragende Argumentationslinie des BVerfG, insbesondere auch die Verschlüsselung von Daten in den Schutzbereich des GVIiS aufzunehmen, wird ebenfalls durch die rechtswissenschaftliche Literatur gestützt. So wird beispielsweise festgestellt, dass sich ein Dateninhaber durch die Verschlüsselung zusätzlich vor einem unbefugten Zugriff schützt – dieser Datenzugriff ist vom gleichen Schutzgehalt umfasst, den auch das GVIiS schützt.[105] Ebenso wird argumentiert, dass die Verschlüsselung demselben Zweck dient wie die inhaltliche Stoßrichtung des GVIiS: der Gewährleistung von Vertraulichkeit und Integrität der Daten. Damit setzt die Verschlüsselung die originäre Zielsetzung der Ableitung des GVIiS aus dem APR um, denn jede Person muss berechtigt bleiben, ihre grundrechtlich geschützten Werte auch selbst effektiv schützen zu dürfen.[106] Ähnliches stellt auch Dietrich fest: *„Die Nutzung von Verschlüsselungstechniken kann zudem dem Schutz des allgemeinen Persönlichkeitsrechts i. S. v. Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG unterfallen. Das vom BVerfG aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung vermittelt dem Grundrechtsträger das Recht, über die Verwendung seiner personenbezogenen Daten grundsätzlich selbst zu entscheiden. Dies umfasst zweifellos das Recht, solche Daten zu verschlüsseln.“* Darüber hinaus hat das BVerfG in seiner Entscheidung zur *„Online-Durchsuchung“* dem allgemeinen Persönlichkeitsrecht den Teilgehalt eines Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme entnommen. Geschützt ist dabei das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Die Vertraulichkeits- und Integritätserwartung lässt sich insbesondere über Verschlüsselungsmechanismen erreichen. Sie bilden die entscheidende technische Hürde gegen Ausspähung, Überwachung oder Manipulation. Mit Blick auf die zunehmende Digitalisierung des Alltags und faktisch bestehenden Grenzen eines staatlich vermittelten Schutzes vor Bedrohungen im *„World Wide Web“* muss der Einzelne berechtigt sein, die Vertraulichkeit und Integrität seiner informationstechnischen Systeme selbst in die Hand zu nehmen. *„Der Einsatz von Verschlüsselung unterfällt demgemäß dem Schutzbereich von Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG.“*[107]

b) Eingriffsdogmatik

Ein Eingriff in das GVIiS ist sowohl nach klassischem Eingriffsbegriff, d.h. final, unmittelbar und imperativ, wie auch rein faktisch und mittelbar möglich. Hierbei ist auf die Verarbeitung eines Datums innerhalb des IT-Systems abzustellen. Auch die versuchte Brechung der Integrität eines informationstechnischen Systems stellt einen Eingriff dar. Beschlagnahmen[108] sind gleichermaßen erfasst wie offene und verdeckte Zugriffe[109]. Jede Einzelmaßnahme zur technischen Kompromittierung ist dabei rechtlich als einzelner Eingriff in die Integrität des IT-Systems zu qualifizieren.

---

100 *Lang* in: BeckOKGG, Art. 2, Rn. 124.
101 *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 28.
102 BVerfG NJW 2008, 822, 830, Rn. 236: „Schließlich ist zu berücksichtigen, dass der geregelte Zugriff unter anderem darauf angelegt und dazu geeignet ist, den Einsatz von Verschlüsselungstechnologie zu umgehen. Auf diese Weise werden eigene Schutzvorkehrungen des Betroffenen gegen einen von ihm nicht gewollten Datenzugriff unterlaufen. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht des Grundrechtseingriffs.“
103 BVerfG NJW 2008, 822, 827, Rn. 234.
104 *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 23 f.
105 *Eisenberg* in: Beweisrecht der StPO, III. Beschaffung durch einzelne verdeckte Maßnahmen, Rn. 2541.
106 *Gerhards*, Grundrecht auf Verschlüsselung?, 183.
107 *Dietrich*, GSZ 2021, 1, 2.
108 *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 40.
109 *Hornung*, CR 2008, 299, 303.

c) Verfassungsrechtliche Rechtfertigung des Eingriffs in die verschlüsselte Datenspeicherung

Wie bereits für die verschlüsselte Kommunikation dargelegt,[110] gilt auch für die durch das GVIiS geschützte verschlüsselte Datenspeicherung, dass ein Eingriff in diese den verfassungsrechtlichen qualifizierten Rechtfertigungsvoraussetzungen genügen muss. Für Eingriffe in das GVIiS gilt der Gesetzesvorbehalt[111] und es müssen in der entsprechenden Ermächtigungsgrundlage Anlass, Zweck und Grenzen bestimmt sein.[112] Für Eingriffe in die verschlüsselte Datenspeicherung gelten infolge der gegenüber unverschlüsselten Datenbeständen erhöhten Eingriffsintensität gesteigerte Anforderungen an die Rechtfertigung. Das aus dem Rechtsstaatsprinzip folgende Verhältnismäßigkeitsgebot staatlichen Handelns verlangt hier, dass der Eingriff in das GVIiS in der Angemessenheit nur mit Kollisionen mit herausragend wichtigen Schutzgütern wie Leib, Leben, Freiheit oder einer Bedrohung für die Grundlagen des Staates zu rechtfertigen ist.[113] Diese strengen verfassungsrechtlichen Voraussetzungen gelten ebenfalls für ein Tätigwerden der Nachrichtendienste, soweit diese Eingriffe in verschlüsselte Kommunikation vornehmen.[114] Grenze staatlichen Eingriffshandelns ist stets der Kernbereich privater Lebensgestaltung.[115] Überdies müssen die angeordneten Maßnahmen aufgrund ihrer Schwergewichtigkeit dem Vorbehalt richterlicher Anordnung (Richtervorbehalt) unterliegen.[116]

Weitere konkretisierende Hinweise zur genauen Ausgestaltung der verfassungsrechtlichen Rechtfertigung von Eingriffen in die verschlüsselte Datenspeicherung stellt das BVerfG nicht zur Verfügung. Jedoch lassen sich zur Bestimmung gesetzlicher Schwellenwerte bereits bestehende gesetzliche Grundlagen zur Umgehung von Verschlüsselung beispielhaft heranziehen, um mögliche Rahmenbedingungen der konkreten Ausgestaltung zu ermitteln. So verweisen die Befugnisgrundlagen zum Eingriff in verschlüsselte Kommunikation in § 100a Abs. 1 S. 2, S. 3 StPO, § 72 Abs. 3 ZFdG auf qualifizierte Katalogstraftaten und herausgehobene tatbestandliche Erfordernisse, die erfüllt sein müssen. §§ 3, 5, 8, 11 Abs. 1a G10, § 34 BNDG, § 51 Abs. 2 BKAG verweisen in diesem Zusammenhang auf staatsgefährdende Sachverhalte. Für die Durchführung des Eingriffs in verschlüsselte Kommunikation sind strenge formelle Vorschriften zu beachten. Überdies ist die genaue Bezeichnung des Adressaten der Überwachungsmaßnahme notwendig und es gilt der Richtervorbehalt.

Unter dem Gesichtspunkt der hohen verfassungsrechtlichen Anforderungen an die Rechtfertigung von Grundrechtseingriffen in die verschlüsselte Kommunikation werden im rechtswissenschaftlichen Diskurs ebenso Ausführungen zu absoluten/relativen Verschlüsselungsverboten sowie zur Schlüsselherausgabepflicht getätigt: So sei das gesetzliche Verbot jeglichen Einsatzes von Verschlüsselungstechniken als schwerster denkbarer Grundrechtseingriff zu qualifizieren und deshalb unverhältnismäßig. So fehle es bereits an der Geeignetheit der staatlichen Maßnahme, die Erfüllung des staatlichen Sicherheitsauftrags zu fördern, denn Verschlüsselungssoftware wäre trotz eines Verbotes in Deutschland weiterhin anderenorts auf der Welt verfügbar. Außerdem sei nicht sinnvoll überprüfbar, ob Verschlüsselungssoftware trotz gesetzlicher Verbote weiterhin eingesetzt werde.[117] Richtigerweise führt Dietrich sodann weiter aus, dass auch für gesetzliche Beschränkungen unterhalb der Schwelle des Verschlüsselungsverbots wie z.B. für den Einbau von *„Backdoors"* in der Verschlüsselungstechnik der Nachrichtenübermittlung erhebliche verfassungsmäßige Zweifel bestehen müssen. So zeige sich bei Abwägung der gegenüberzustellenden verfassungsrechtlichen Positionen, dass einem Eingriff von großer Streubreite, der die Kompromittierung der Vertraulichkeit der Kommunikation aller Bürgerinnen und Bürger betrifft, kaum bzw. allerhöchstens punktuell nennenswerte Sicherheitsgewinne gegenüberstehen.[118] Überdies wird durch ein derartiges staatliches Vorgehen die Verschlüsselungstechnik nachhaltig geschwächt und es werden neue Vektoren für Cyberangriffe eröffnet.

Im Ergebnis gelten für den Eingriff in das GVIiS und damit gleichsam für den Eingriff in ein Recht auf verschlüsselte Datenspeicherung tatbestandlich erheblich einengende Voraussetzungen, damit ein solcher Eingriff unter Abwägung der widerstreitenden verfassungsrechtlichen Positionen verhältnismäßig ist. Zusammenfassend ist der Eingriff in das Grundrecht nur zulässig unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes, soweit tatsächliche Anhaltspunkte für eine konkrete Gefahr vorhanden sind, ausschließlich zum Ziel des Schutzes eines überragend wichtigen Rechtsguts, unter dem Vorbehalt richterlicher Anordnung sowie unter Treffen von Vorkehrungen zur Vermeidung von Eingriffen in den Kernbereich privater Lebensgestaltung durch Ermächtigungsgrundlagen, welche der Normenbestimmtheit und Normenklarheit für den Einzelfall genügen. Die verfassungsrechtliche Eingriffsschwelle für eine Überwachung zugangsgesicherter TK-Inhalte ist damit außerordentlich hoch, selbst wenn sie zum Zeitpunkt der Überwachung noch nicht übermittelt werden bzw. bereits übermittelt wurden und technisch beim Empfänger angelangt sind.

3. Weitere grundrechtliche Ableitungen eines Rechts auf Verschlüsselung

Ein Recht auf Verschlüsselung lässt sich nicht nur aus dem Fernmeldegeheimnis und dem GVIiS ableiten, sondern auch

110 Siehe bereits unter C. / II. / 1. / c).
111 BVerfGE 120, 274, 315.
112 *Gersdorf* in: BeckOKInfo&MedienR, Art. 2 GG, Rn. 94.
113 BVerfGE 120, 274, 328.
114 Vgl. BVerfGE 120, 274, 331.
115 BVerfGE 120, 274, 335.
116 BVerfG NJW 2008, 822, 832; Rn. 257.
117 *Dietrich*, GSZ 2021, 1, 4 f.
118 *Dietrich*, GSZ 2021, 1, 4 f.

aus zahlreichen weiteren Grundrechten, auf die zumindest hilfsweise zurückgegriffen werden kann. Dies kann dann der Fall sein, falls ein IT-System lediglich einen punktuellen Bezug zu einem bestimmten Lebensbereich aufweist, so beispielsweise ein USB-Stick, eine Festplatte, eine Digitalkamera, ein digitales Diktiergerät oder ein SSD-Speichermedium. Denkbar ist außerdem, dass nur einzelne Daten, die sich zwar auf eine natürliche Person beziehen, aber nicht von deren eigenem IT-System extrahiert wurden, betroffen sind. Durch diese Möglichkeit weiterer grundrechtlicher Ableitung eines Rechts auf Verschlüsselung lässt sich ein möglichst lückenloser Schutzbereich eines verfassungsrechtlich verankerten allgemeinen Rechts auf Verschlüsselung generieren, der zwar im Ergebnis unterschiedlichen verfassungsrechtlichen Rechtfertigungsvoraussetzungen genügen muss, aber im sachlichen Schutzbereich durchaus vergleichbare Gewährleistungen aufweist.

Das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist in seinem sachlichen Anwendungsbereich betroffen, wenn personenbezogene Daten verarbeitet werden, die weder von einem Telekommunikationsvorgang, noch – in Abgrenzung zum GVIiS – von einem quantitativ anspruchsvollen und die Persönlichkeit widerspiegelnden und damit technisch hinreichend komplexen IT-System stammen. Vom Schutzbereich des Grundrechts umfasst sind alle Daten, unabhängig vom Sinngehalt.[119]

Die Berufsausübungsfreiheit gem. Art. 12 Abs. 1 S. 2 GG ist inhaltlich relevant für den Schutz von vertraulichen Geschäftsgeheimnissen.[120]

Das Grundrecht auf Unverletzlichkeit der Wohnung gem. Art. 13 Abs. 1 GG umfasst Informationen, die während eines Eindringens in die Wohnung erlangt werden.[121] Mit einem Bezug zur Cybersicherheit, Integrität und Vertraulichkeit von Daten können hierzu z.B. persönliche Fotos, vertrauliche ausgedruckte Dokumente oder verschriftlichte Passwortlisten gehören. Die Beschlagnahme von Gegenständen wie beispielsweise Festplatten mit verschlüsselten Daten wird hingegen durch andere grundrechtliche Gewährleistungen geschützt.[122] Hier ist vor allem die Eigentumsfreiheit gem. Art. 14 Abs. 1 GG zu nennen, in deren Schutzbereich ebenjene Beschlagnahme fällt.[123] Falls die Daten auf beschlagnahmten Datenträgern in einem zweiten Verfahrensschritt entschlüsselt werden, ist dies als gesonderter Grundrechtseingriff zu bewerten, der den strengen Rechtfertigungsvoraussetzungen des GVIiS[124] oder zumindest des Grundrechts auf informationelle Selbstbestimmung genügen muss, falls der Datenträger nur einen begrenzten Lebensausschnitt digital abbildet.

4. Ergebnis: Ableitbarkeit eines Rechts auf Verschlüsselung aus dem nationalen Verfassungsrecht

Wie gezeigt wurde, lässt sich aus der Gesamtheit der in diesem Abschnitt genannten Grundrechte

- → Fernmeldegeheimnis
- → Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
- → Grundrecht auf informationelle Selbstbestimmung
- → Berufsausübungsfreiheit
- → Grundrecht auf Unverletzlichkeit der Wohnung
- → Eigentumsfreiheit

nach deutschen verfassungsrechtlichen Maßstäben ein in seinem Schutzbereich insgesamt nahezu lückenloses Recht auf Verschlüsselung ableiten. Obwohl die Verschlüsselung von Daten somit verfassungsrechtlich bislang als durchgängige inhaltliche Gewährleistung nicht ausdrücklich vorgesehen ist, so ergibt sie sich zumindest mittelbar bzw. in der Auslegung über den zeitlichen Verlauf von Datenverarbeitung und Datenkommunikation aus der kombinierten Zusammenschau bestehender grundrechtlicher Maßstäbe.[125] Gleichwohl gilt, dass auch ein Recht auf verschlüsselte Kommunikation nicht grenzenlos ist, sondern durch staatliches Eingriffshandeln legitimerweise beschränkt werden kann. An ein solches Handeln jedoch sind hohe verfassungsrechtliche Rechtfertigungsvoraussetzungen anzulegen. Das gilt insbesondere dann, wenn der Eingriff in ein verschlüsseltes Dateisystem erhebliche Teile der Persönlichkeit des durch den Eingriff Betroffenen zu offenbaren droht. Die vielfach geführte (politische) Argumentation *„Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“*[126] greift deshalb zu kurz, da sie Schutzbereich und Eingriffsrechtfertigung gleichsetzt, obwohl bei weit auszulegendem Schutzbereich und hohen verfassungsrechtlichen Hürden in seinen Eingriff an dieser Stelle keine Gleichwertigkeit der verfassungsrechtlichen Interessen ohne Weiteres und pauschal unterstellt werden kann.

119 BVerfGE 65, 1, 45.
120 BVerfGE 115, 205, 229.
121 BVerfGE 109, 279, 374.
122 BVerfGE 113, 1, 29; 113, 29, 45.
123 BVerfG NJW 2009, 281, 282.
124 Siehe dazu schon unter C. / II. / 2. / c).
125 So auch *Dietrich*, GSZ 2021, 1, 2; *Gerhards*, (Grund-)Recht auf Verschlüsselung?, 123 ff.
126 Anstelle vieler *Feld/Kliss*, „Verschlüsselte Kommunikation: Eine Hintertür für die Ermittler?“, Tagesschau.de vom 13.11.2022, abrufbar unter: https://www.tagesschau.de/inland/eu-messenger-sicherheit-101.html.

III. Ableitung aus dem europäischen Verfassungsrecht

Die Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta, GRCh) gehört neben dem EUV[127] und dem AEUV[128] zum EU-Primärrecht und gilt gem. Art. 6 EUV als unmittelbares Recht in den EU-Mitgliedstaaten.[129] Die Grundrechte aus der GRCh gelten grds. parallel neben den nationalen Grundrechten aus dem GG.[130] Dabei ist zu berücksichtigen, dass im Kollisionsfall das Unionsrecht gegenüber dem nationalen Recht grds. Anwendungsvorrang hat.[131] Allerdings bindet die GRCh die Mitgliedstaaten *„ausschließlich bei der Durchführung des Rechts der [Europäischen] Union"*, Art. 51 Abs. 1 GRCh. Die Grundrechte der Charta gelten folglich lediglich für Sachverhalte, bei denen das Unionsrecht relevant ist.[132] Da jedoch das Überwachungsrecht nicht vollständig unionsrechtlich determiniert ist (z.B. das Recht des Verfassungsschutzes), ist die GRCh als verfassungsrechtlicher Prüfmaßstab nur anzuwenden, wenn europäische Verordnungs- oder Richtlinienangelegenheiten betroffen sind.[133] Hierdurch wird die rechtliche Bedeutung der GRCh für einen erheblichen Teil der staatlichen Eingriffe in digitale Daten und geschützte digitale Kommunikation relativiert, da viele Überwachungsmaßnahmen beispielsweise im nachrichtendienstlichen Bereich oder zur Gefahrenabwehr nach wie vor mitgliedstaatlich geregelt sind.[134] Überdies zielt das Unionsrecht nicht auf eine Einheitlichkeit des Grundrechtsschutzes ab, sondern will vielmehr eine *„Grundrechtsvielfalt"* zulassen, was ebenso für weit gefasste Anwendungsbereiche nationalen Verfassungsrechts in Abgrenzung zur GRCh spricht.[135] Jedoch verfolgt die GRCh gerade auch das Ziel, im Bereich des Schutzes der Vertraulichkeit der Kommunikation die europäischen Grundrechte zu stärken. Dies muss insbesondere vor dem Hintergrund berücksichtigt werden, dass die Grundrechtsrechtsprechung des EuGH im Vergleich zu den nationalen, mitgliedstaatlichen verfassungsrechtlichen Gewährleistungen bislang verhältnismäßig konturlos ist.

Wie schon für die im Rahmen des nationalen Verfassungsrechts getroffenen Feststellungen gilt auch für die GRCh, dass diese kein explizites und ausdrücklich verankertes Recht auf Verschlüsselung enthält. Ein solches Recht kann jedoch ebenso wie für das deutsche Grundgesetz aus der Gesamtheit der bestehenden, in diesem Kontext inhaltlich relevanten Grundrechte der Charta abgeleitet werden. Für die in diesem Zusammenhang geltende rechtliche Prüfdogmatik wird entsprechend auf die vorangehenden Ausführungen verwiesen.[136] Für die Ableitung eines Rechts auf Verschlüsselung sind insbesondere Art. 7 GRCh (Achtung des Privat- und Familienlebens) und Art. 8 GRCh (Schutz personenbezogener Daten) relevant.

1. Achtung des Privat- und Familienlebens gem. Art. 7 GRCh

Das europäische Grundrecht auf Achtung des Privat- und Familienlebens aus Art. 7 der GRCh bezweckt in seinem Kern-Gewährleistungsgehalt den Schutz der Privat- und Intimsphäre.[137] Vom Schutzgehalt auch umfasst ist die Fernkommunikation als Übermittlungsvorgang von Daten.[138] Die Fernkommunikation beginnt hierbei mit dem Absenden der Nachricht vom System des Senders und endet mit der endgültigen Speicherung auf dem Datenträger des Empfängers. Zur Eröffnung des Schutzbereichs ist zumindest ein Dritter in der Form eines Kommunikations-Providers notwendig, da hierdurch das übermittlungsspezifische Risiko des technischen Abhörens geschaffen wird, das gerade erhöhte Risiken der Fernkommunikation gegenüber dem Präsenzdialog mit sich bringt.[139] Die der Kommunikation zugrunde gelegte Technik spielt keine Rolle – umfasst sind damit Telefongespräche ebenso wie die Kommunikation über das Internet, z.B. per E-Mail.[140] Der Inhalt der Fernkommunikation ist irrelevant – ebenso ist nicht notwendig, dass dieser verständlich oder überhaupt einer Kenntnisnahme zugänglich ist.[141] Insoweit sind die sachlichen Anforderungen durchaus mit den Schutzbereichsgewährleistungen des Art. 10 GG vergleichbar.[142] Im Ergebnis dürfte aufgrund dieser gefährdungsspezifischen Stoßrichtung der inhaltlichen Gewährleistungen des Art. 7 GRCh auch ohne Weiteres die verschlüsselte, fernübertragene Kommunikation vom Schutzbereich des europäischen Grundrechts auf Achtung des Privat- und Familienlebens umfasst sein.

Ein Eingriff in den Schutzbereich von Art. 7 GRCh liegt vor, wenn während des Übermittlungsvorganges auf Inhalte und Kommunikationsdaten zugegriffen wird.[143]

Zu beachten ist, dass soweit personenbezogene Daten vorliegen, Art. 8 GRCh als *lex specialis* der grundrechtliche Prüfmaßstab ist. Zu berücksichtigen ist in diesem Kontext ebenso der spezielle qualifizierte Eingriffsvorbehalt nach Art. 8 Abs. 2 GRCh.[144]

---

127 Vertrag über die Europäische Union (EUV), abrufbar unter: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0020.02/DOC_1&format=PDF.
128 Vertrag über die Arbeitsweise der Europäischen Union (AEUV), abrufbar unter: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:de:PDF.
129 *Jarass* in: Jarass, GRCh, Einleitung: Grundlagen und Bedeutung der Grundrechte, Rn. 9.
130 BVerfG NJW 2020, 300, 301, Rn. 43 ff. (Recht auf Vergessen I).
131 EuGH, Rs. 6/64, 1251, 1269 ff. (Costa/ENEL), bestätigt durch Solange-Rechtsprechung des BVerfG.
132 BVerfG NJW 2003, 1499, 1500, Rn. 88, 90.
133 So z.B. für die europäisch determinierte Vorratsdatenspeicherung (VDS) oder den Vorstoß der EU-Kommission für einen „Regulation Proposal on Child Sexual Abuse Material" (CSAM). Näher hierzu Vasel, ZRP 2022, 191. Siehe im Hinblick auf die VDS aktuell auch EuGH NJW 2022, 3135. Mit Blick hierauf sind Verstöße gegen Art. 7, 8 und 11 der GRCh zu rügen.
134 So auch *Durner* in: Dürig/Herzog/Scholz, GG, Art. 10, Rn. 43.
135 *Durner* in: Dürig/Herzog/Scholz, GG, Art. 10, Rn. 43.
136 Siehe dazu im Detail C. / I.
137 *Gersdorf* in: BeckOKInfo&MedienR, Art. 7 GRCh, Rn. 21.
138 *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 7 GRCh, Rn. 10.
139 Bernsdorff in: Meyer/Hölscheidt, GRCh, Art. 7, Rn. 20; *Gersdorf* in: BeckOKInfo&MedienR, Art. 7 GRCh, Rn. 35.
140 Wissenschaftliche Dienste des Deutschen Bundestags, Ausarbeitung „Chatkontrolle' – Analyse des Verordnungsentwurfs 202/0155 (COD) der EU-Kommission", Az. WD 10 – 3000 – 026/22, S. 7.
141 EuGH C-293/12 und C-594/12 (verbunden), 17, Rn. 49 f.
142 Siehe hierzu im Detail C. / II. / 1. / a).
143 EuGH C-362/14, 26, Rn. 94; *Gersdorf* in: BeckOKInfo&MedienR, Art. 7 GRCh, Rn. 38 f.
144 Siehe zur Abgrenzung vertiefend den nachfolgenden Prüfungspunkt dieses Rechtsgutachtens.

2. Schutz personenbezogener Daten gem. Art. 8 GRCh

Das Grundrecht aus Art. 8 GRCh bezweckt den umfassenden Schutz speziell von personenbezogenen Daten. Soweit dabei personenbezogene Daten in einem Kommunikationsvorgang betroffen sind,[145] gilt der Prüfmaßstab des Art. 8 GRCh als *lex specialis*[146], wird aber sowohl vom EuGH[147] als auch vom BVerfG[148] regelmäßig mit Art. 7 GRCh nebeneinander angewandt. Sind in einem Kommunikationsvorgang hingegen keine personenbezogenen Daten betroffen, ist der Schutzbereich des Art. 7 GRCh einschlägig, der allgemein das Recht auf vertrauliche Kommunikation schützt. Falls weder personenbezogene Daten verarbeitet werden noch ein Kommunikationsvorgang stattfindet, ist ebenso Art. 7 GRCh anwendbar, da seine Schutzbereichsgewährleistungen auch das allgemeine Recht auf Privatsphäre umfassen.

Der Schutzbereich von Art. 8 GRCh ist weit auszulegen.[149] In Entsprechung zum nationalen Verfassungsrecht tangiert er deshalb verschiedene digitale Gewährleistungen des Grundgesetzes. Dazu gehört das Fernmeldegeheimnis, aber auch das Grundrecht auf informationelle Selbstbestimmung und das spezielle GVIiS. Je nach konkretem Datenverarbeitungszuschnitt kann ebenso der Kontext der Berufsausübungsfreiheit betroffen sein, der im deutschen Verfassungsrecht durch das Grundrecht nach Art. 12 Abs. 1 GG bzw. im europäischen Kontext gem. Art. 15 GRCh garantiert wird. Damit lässt sich aus Art. 8 GRCh ebenso ein Schutz von Daten mit Geschäftsbezug ableiten. Im Rahmen seines sachlichen Gewährleistungshorizonts ist Art. 8 GRCh nicht nur ein Abwehrrecht, sondern begründet – wenngleich mit erheblicher Einschätzungsprärogative verbunden – staatliche Schutzpflichten auch gegenüber Privaten durch die Gesetzgebung.[150]

Ein Eingriff in den Schutz personenbezogener Daten ist in jeder entsprechenden Datenverarbeitung zu sehen.[151]

Die Rechtfertigung für den Grundrechtseingriff unterliegt den üblichen rechtsstaatlichen Voraussetzungen im Sinne eines hinreichend bestimmten Gesetzes mit Bezug zu einem legitimen Zweck unter Beachtung des Grundsatzes der Verhältnismäßigkeit, vgl. Art. 52 GRCh (Tragweite und Auslegung der Rechte und Grundsätze). Konkretisierende Anforderungen an die Rechtfertigung von Grundrechtseingriffen enthalten Art. 8 Abs. 2 und Abs. 3 GRCh.[152] Im Rahmen der Angemessenheits-Abwägung sind der betroffene Bereich, das Wesen des fraglichen durch die Charta gewährleisteten Rechts, Art und Schwere des Eingriffs und dessen Zweck[153] sowie das Gewicht der entgegenstehenden Grundrechte und auch – soweit vorhanden – Sekundärrecht maßgeblich. Stets gilt der Vorrang der unmittelbaren und offenen vor der mittelbaren und verdeckten Datenerhebung.[154] Daraus lässt sich ebenfalls ableiten, dass Eingriffe in verschlüsselte Kommunikation, denen oftmals ein verdeckter Charakter innewohnt, auch nach europäischem Recht nur in absoluten Ausnahmefällen zu rechtfertigen sein werden. Eine Massendatenerhebung über einen erheblichen Zeitraum ohne Kenntnis der Betroffenen und ohne das Bestehen erheblicher Verdachtsgrade, wie es z.B. im Rahmen der europäischen EncroChat-Ermittlungen der Fall gewesen ist, dürfte damit europarechtswidrig sein. Bei der Interessenabwägung zur Legitimation des Eingriffs ist außerdem zu beachten, dass sich der Eingriff nur auf die absolut notwendigste Datenverarbeitung beziehen darf,[155] womit ein außerordentlich strenger Rechtfertigungsmaßstab anzulegen ist, soweit vertrauliche personenbezogene Daten erhoben werden. So muss ebenfalls bedacht werden, dass jede Erleichterung einer Verschlüsselung zugunsten der staatlichen Überwachung auch immer zwangsläufig eine Erleichterung eines unberechtigten Zugriffs mit sich bringt und sich damit noch gravierender auf das Schutzinteresse der Betroffenen auswirkt.[156] Zudem darf auch die Fehleranfälligkeit einer solchen zusätzlich eingebauten Maßnahme nicht außer Acht gelassen werden. Eine Fehlerquote von nur einem Tausendstel kann bei täglich 100 Mrd. verschickten Nachrichten mehrere Millionen Nachrichten täglich betreffen, wodurch die ohnehin schon weite Streubreite eines solchen Eingriffs, bei welchem zwangsläufig auch immer harmlose Kommunikation betroffen wird,[157] weiterhin breit intensiviert wird.[158]

Prominente Orientierungspunkte zum Umgang mit diesen europarechtlichen Erwägungen gibt überdies die Rechtsprechungslinie des EuGH zur Speicherung von Vorratsdaten. Hier wurde bei-spielsweise festgestellt, dass die anlasslose Speicherung von Kommunikationsdaten über sechs Monate unverhältnismäßig ist.[159] Außerdem bestimmte das Gericht, dass die VDS ebenfalls im Sinne des Verhältnismäßigkeitsgrundsatzes geografisch sinnvoll begrenzt nur zur Bekämpfung schwerster, die nationale Sicherheit gefährdender Kriminalität zulässig[160] und ansonsten unverhältnismäßig ist.[161]

---

145 *Augsberg* in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, Art. 8 GRCh, Rn. 1.
146 *Bernsdorff* in: Meyer/Hölscheidt, GRCh, Art. 8, Rn. 13.
147 EuGH NVwZ 2014, 435.
148 BVerfG NJW 2020, 314, 322 f., Rn. 99.
149 Wissenschaftliche Dienste des Deutschen Bundestags, Ausarbeitung „Chatkontrolle' – Analyse des Verordnungsentwurfs 202/0155 (COD) der EU-Kommission", Az. WD 10 – 3000 – 026/22, S. 9.
150 *Franzen* in: Franzen/Gallner/Oetker, EurArbR, Art. 8 GRCh, Rn. 4; *Gersdorf* in: BeckOKInfo&MedienR, Art. 8 GRCh, Rn. 12; *Jarass* in: Jarass, GRCh, Art. 8 Rn. 3; *Johlen* in: Stern/Sachs, GRCh, Art. 8, Rn. 22; *Streinz* in: Streinz, EUV/AEUV, Art. 8 GRCh, Rn. 6.
151 *Gersdorf* in: BeckOKInfo&MedienR, Art. 8 GRCh, Rn. 18; *Johlen* in: Stern/Sachs, GRCh, Art. 8, Rn. 33.
152 Vgl. *Gersdorf* in: BeckOKInfo&MedienR, Art. 8 GRCh, Rn. 23 ff.
153 EuGH C-293/12 und C-594/12 (verbunden), 18, Rn. 47.
154 *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 8 GRCh, Rn. 17.
155 EuGH NVwZ 2014, 709, 712, Rn. 51 ff.
156 *Zurawski*, ZD-Aktuell, 01240.
157 *Montag*, becklink 2023186.
158 *Woerlein*, ZD-Aktuell, 01251.
159 EuGH C-293/12 und C-594/12 (verbunden), 18, Rn. 51 ff.
160 EuGH NJW 2021, 531, 538, Rn. 136 ff.
161 EuGH EuZW 2022, 536.

3. Ergebnis: Ableitbarkeit eines Rechts auf Verschlüsselung aus dem europäischen Verfassungsrecht

Art. 7 und Art. 8 der GRCh schützen umfassend die Vertraulichkeit und Integrität der digitalen Datenverarbeitung – in der Zusammenschau unabhängig davon, ob personenbezogene Daten verarbeitet werden oder nicht. Im chronologischen Nutzungsverlauf der Daten sind grundrechtlich ebenfalls sämtliche Verarbeitungsschritte von der Erhebung über die Übermittlung bis hin zur Speicherung eines Datums umfasst. Nur wenige Konkretisierungen jedoch enthält sowohl die Rechtsprechung des EuGH als auch die GRCh selbst in Bezug auf ein konkretes Recht zur Verschlüsselung. Dennoch ist es juristisch ohne Weiteres vertretbar, von einem Recht auf vertrauliche Kommunikation auch im weitergehenden Sinne auf ein Recht auf verschlüsselte Kommunikation zu schließen. Dies wird einerseits bedingt durch den weit gefassten Schutzbereich insbesondere von Art. 8 GRCh und der regelmäßig nebeneinander erfolgenden Prüfung von Art. 7 GRCh, anderseits aber auch durch die technische Notwendigkeit, dass eine vertrauliche Kommunikation unterschiedliche Stufen bis hin zur verschlüsselten Kommunikation umfassen kann. Art. 7 GRCh bestimmt dies mittelbar, indem der Schutzbereich auch dann eröffnet ist, wenn es sich um nicht verständliche Kommunikationsinhalte handelt. Nicht zuletzt wird durch die detaillierten Rechtfertigungsvoraussetzungen des Art. 8 GRCh deutlich, dass Eingriffe in vertrauliche Datenbestände nur in absoluten Ausnahmefällen möglich sein sollen. Das muss umso mehr dann gelten, wenn der Nutzer eines digitalen Endgeräts bzw. Speichermediums die Vertraulichkeit seiner Daten mit dem Einsatz von Verschlüsselung in besonderem Maße und für jeden zugreifenden Dritten sichtbar herausgestellt hat.

E. Einfachgesetzliche Gewährleistungen eines „Rechts auf Verschlüsselung“ und praktische Umsetzung verfassungsrechtlicher Vorgaben

Das verfassungsrechtlich sowohl im nationalen wie auch im europäischen Rahmen gewährleistete Recht auf Verschlüsselung gilt auch für den einfachgesetzlichen Rahmen und findet sich hier entweder konkret benannt oder als verfassungskonforme Auslegung von unbestimmten Rechtsbegriffen im Technikrecht wieder. Letzteres ist vor allem dann der Fall, wenn gesetzliche Vorgaben angemessene technische und organisatorische Maßnahmen bzw. Vorkehrungen (TOM bzw. TOV) nach dem „Stand der Technik“ voraussetzen. Im Folgenden findet sich eine Auflistung relevanter europäischer und nationaler Rechtsvorschriften, die die Verschlüsselung bzw. angemessene technische und organisatorische Anforderungen zur Voraussetzung einer sicheren Datenhaltung machen.

RECHTSVORSCHRIFT:	AUSZUG:
Europäische Union (EU)	
DSGVO – 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) Art. 32 Abs. 1, lit. a	**Artikel 32** **Sicherheit der Verarbeitung** (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten

EKEK – Richtlinie (EU) 2018/1972 über eur. Kodex elektronischer Kommunikation

Art. 40 Abs. 1

→ Umgesetzt in § 165 Abs. 2 S. 1 + S. 2 TKG als Pflicht für Betreiber öffentlich zugänglicher Telekommunikationsdienste, in § 19 Abs. 4 TTDSG, in § 8c Abs. 1, Abs. 2 BSIG (s.u.)

Artikel 40
Sicherheit von Netzen und Diensten

(1) [1]Die Mitgliedstaaten stellen sicher, dass die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste angemessene und verhältnismäßige technische und organisatorische Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten ergreifen. [2]Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist. [3]Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Verschlüsselung, zu ergreifen, um Auswirkungen von Sicherheitsvorfällen auf Nutzer und auf andere Netze und Dienste zu vermeiden und so gering wie möglich zu halten.

ePrivacy-Richtlinie – Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

Art. 4 Abs. 1, Abs. 3, UAbs. 3

Art. 4
Sicherheit der Verarbeitung

(1) [1]Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. [2]Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.
[…]
(3)
[…]
[3] [1]Der Anbieter braucht die betroffenen Teilnehmer oder Personen nicht von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn er zur Zufriedenheit der zuständigen Behörde nachgewiesen hat, dass er geeignete technische Schutzmaßnahmen getroffen hat und dass diese Maßnahmen auf die von der Sicherheitsverletzung betroffenen Daten angewendet wurden. [2]Diese technischen Schutzmaßnahmen verschlüsseln die Daten für alle Personen, die nicht befugt sind, Zugang zu den Daten zu haben.

Funkanlagen-Richtlinie – Richtlinie 2014/53/EU über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG

Art. 3 Abs. 3 lit. e

Artikel 3
Grundlegende Anforderungen

(3) Funkanlagen müssen in bestimmten Kategorien oder Klassen so konstruiert sein, dass sie die folgenden grundlegenden Anforderungen erfüllen:
[…]
e) Sie verfügen über Sicherheitsvorrichtungen, die sicherstellen, dass personenbezogene Daten und die Privatsphäre des Nutzers und des Teilnehmers geschützt werden.

NIS-Richtlinie — Richtlinie (EU) 2016/1148
über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

Art. 7 ff.

Artikel 7
Nationale Strategie für die Sicherheit von Netz- und Informationssystemen

(1) [1]Jeder Mitgliedstaat legt eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen fest, in der die strategischen Ziele und angemessene Politik- und Regulierungsmaßnahmen bestimmt werden, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen erreicht und aufrechterhalten werden soll, und die mindestens die in Anhang II genannten Sektoren und die in Anhang III genannten Dienste abdeckt. [2]Die nationale Strategie für die Sicherheit von Netz- und Informationssystemen behandelt insbesondere die folgenden Aspekte:

a) die Ziele und Prioritäten der nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
[…]

NIS-Richtlinie — ebd.

Art. 14 Abs. 1

Artikel 14
Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) [1]Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. [2]Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

NIS-Richtlinie — ebd.

Art. 16 Abs. 1 lit. a

Artikel 16
Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

(1) [1]Die Mitgliedstaaten stellen sicher, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie im Rahmen der Bereitstellung der in Anhang III aufgeführten Dienste innerhalb der Union nutzen, zu bewältigen. [2]Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, wobei Folgendem Rechnung getragen wird:

a) Sicherheit der Systeme und Anlagen

Bundesrepublik Deutschland

BSI-Gesetz (BSIG)

§ 8c Abs. 1, Abs. 2 Nr. 1

→ Umsetzung Art. 40 Abs. 1 EKEK-RL
→ Umsetzung Art. 16 Abs. 1 lit. a NIS-RL

§ 8c
Besondere Anforderungen an Anbieter digitaler Dienste

(1) [1]Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. [2]Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

(2) [1]Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. 2Dabei ist folgenden Aspekten Rechnung zu tragen:

1. der Sicherheit der Systeme und Anlagen

Bürgerliches Gesetzbuch (BGB)

§ 327e Abs. 3 S. 1 Nr. 2 (sowie sonstiges Gewährleistungsrecht)

§ 327e
Produktmangel
[…]
(3) [1]Das digitale Produkt entspricht den objektiven Anforderungen, wenn
[…]
2. es eine Beschaffenheit, einschließlich der Menge, der Funktionalität, der Kompatibilität, der Zugänglichkeit, der Kontinuität und der Sicherheit aufweist, die bei digitalen Produkten derselben Art üblich ist und die der Verbraucher unter Berücksichtigung der Art des digitalen Produkts erwarten kann,

---

De-Mail-Gesetz (De-Mail-G)

§ 5
Postfach- und Versanddienst
[…]
(3) Der Postfach- und Versanddienst hat die Vertraulichkeit, die Integrität und die Authentizität der Nachrichten zu gewährleisten. Hierzu gewährleistet der akkreditierte Diensteanbieter, dass

1. die Kommunikation von einem akkreditierten Diensteanbieter zu jedem anderen akkreditierten Diensteanbieter über einen verschlüsselten gegenseitig authentisierten Kanal erfolgt (Transportverschlüsselung) und

2. der Inhalt einer De-Mail-Nachricht vom akkreditierten Diensteanbieter des Senders zum akkreditierten Diensteanbieter des Empfängers verschlüsselt übertragen wird.

Der Einsatz einer durchgängigen Verschlüsselung zwischen Sender und Empfänger (Ende-zu-Ende-Verschlüsselung) bleibt hiervon unberührt.

§ 5 Abs. 3
Strafgesetzbuch (StGB)

§ 202a Abs. 1

§ 202a
Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Strafgesetzbuch (StGB)

§ 202b

§ 202b
Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Strafgesetzbuch (StGB)

§ 206 Abs. 1

§ 206
Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Telekommunikationsgesetz (TKG)

§ 165 Abs. 2 S. 1, S. 2

→ Umsetzung Art. 40 Abs. 1 EKEK

§ 165
Technische und organisatorische Schutzmaßnahmen
[...]
(2) [1]Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und

2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.

[2]Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung, zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei diesen Maßnahmen ist der Stand der Technik zu berücksichtigen.

Telekommunikation-Telemedien-Datenschutz-Gesetz
(TTDSG)

§ 19 Abs. 4 S. 1, S. 2, S. 3

→ Umsetzung Art. 40 Abs. 1 EKEK

§ 19
Technische und organisatorische Vorkehrungen
[...]
(4) [1]Anbieter von Telemedien haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und

2. diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.

[2]Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. [3]Eine Vorkehrung nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens.

Telekommunikations-Überwachungsverordnung
(TKÜV)

§ 8 Abs. 3 S. 1

§ 8
Übergabepunkt
[...]
(3) [1]Wenn der Verpflichtete die ihm zur Übermittlung anvertraute Telekommunikation netzseitig durch technische Maßnahmen gegen unbefugte Kenntnisnahme schützt oder er bei der Erzeugung oder dem Austausch von Schlüsseln mitwirkt und ihm dadurch die Entschlüsselung der Telekommunikation möglich ist, hat er die für diese Telekommunikation angewendeten Schutzvorkehrungen bei der an dem Übergabepunkt bereitzustellenden Überwachungskopie aufzuheben.

Über den Autor

Prof. Dr. Dennis-Kenji Kipker

ist Professor für IT-Sicherheitsrecht an der Hochschule Bremen sowie Gastprofessor an der privaten, durch die Soros Foundation begründeten Riga Graduate School of Law in Lettland. Hier forscht er zu Themen an der Schnittstelle von Recht und Technik in der Cybersicherheit, im Datenschutz und zu digitaler Resilienz im Kontext globaler Krisen mit einem Forschungsschwerpunkt insbesondere im chinesischen IT-Recht. Beratend ist er außerdem als Legal Advisor des VDE, CERT@VDE tätig und arbeitet im Policy-Bereich als Mitglied des Vorstandes der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) in Berlin zu den Maßgaben künftiger IT-Regulierung in Deutschland und der EU. Als Geschäftsführer des Beratungsunternehmens "Certavo" in Bremen setzt er sich überdies für die Entwicklung und Umsetzung pragmatischer Lösungen zur digitalen Compliance-Konformität und IT-Strategieplanung von Unternehmen ein und übernimmt in dieser Funktion regelmäßig Beratungs- und Gutachtenaufträge für verschiedene deutsche und europäische Institutionen, so beispielsweise für Bundesministerien und die Europäische Kommission. Kipker ist Begründer und Herausgeber der Zeitschrift "International Cybersecurity Law Review" bei Springer, sowie Mitherausgeber der Zeitschriften "Multimedia-Recht" und "Recht Digital", außerdem des juristischen Kommentars "Recht der Informationssicherheit" sowie des Rechtshandbuchs Cybersecurity im Münchener Verlag C.H. Beck. Als Publizist und Autor schreibt er regelmäßig Gastbeiträge für verschiedene Medien zu den Themen Sicherheit, digitale Resilienz, geopolitische IT-Strategie und digitale Bürgerrechte und verfasst einmal im Monat die "Datenkolumne" für die Bremer Tageszeitung Weser-Kurier sowie die IT-Kolumne "Perspektiven" im Berliner Tagesspiegel. Seit 2022 leitet Kipker den Präsidiumsarbeitskreis "Digitalisierung" der Gesellschaft für Informatik.