Teil 1 Datenerhebungsmaßnahmen mit besonderen Mitteln und Methoden

I. Allgemeines

Die **Beschaffung von Informationen** ist von herausragender Bedeutung für die tägliche Polizeiarbeit. Informationen sind im Bereich der Gefahrenabwehr das Fundament für alle weiteren Eingriffsmaßnahmen. Ob eine (abzuwehrende) Gefahr vorliegt, ist durch Ermittlung des Sachverhaltes, durch Befragung oder Observation/Beobachtung zu klären. Gleiches gilt für die Entscheidung über die Art und Weise der Gefahrenabwehr bzw. Straftatenverhütung. Die Ausermittlung eines in der Vergangenheit liegenden Sachverhaltes ist Hauptzweck des Strafverfahrens und ebenfalls eine der Hauptaufgaben der Polizei. Bereits im Grundstudium, in Niedersachsen also im ersten Studienjahr an der Polizeiakademie, werden die diesbezüglichen „alltäglichen" Standardmaßnahmen, die meist mit einem Eingriff in das Recht auf informationelle Selbstbestimmung (APR-RiS) einhergehen, gelehrt.[1] Mitunter sind jedoch Standardmaßnahmen nicht ausreichend, um den jeweils zu ermittelnden Sachverhalt im erforderlichen Umfang zu erfassen. Ihre Anwendung ist gegebenenfalls, aufgrund ihrer „offenen" Natur, sogar kontraproduktiv. **1**

> **Beispiel:** So erfährt z. B. der Verdächtige/Beschuldigte anlässlich seiner Vernehmung, dass gegen ihn ermittelt wird. Dies könnte er zum Anlass nehmen um Beweise „verschwinden" zu lassen oder Beteiligte zu warnen.

In derartigen Fällen kann es angezeigt sein, „**Maßnahmen mit besonderen Mitteln und Methoden**" – so die Bezeichnung im NPOG (siehe § 30 Abs. 2 Nr. 2 NPOG), die hier auch für die strafprozessualen Maßnahmen verwendet werden soll – anzuwenden. Es handelt sich hierbei um Maßnahmen, die in der Regel verdeckt durchgeführt werden, also als Maßnahmen, die (für den Betroffenen) gar nicht oder jedenfalls nicht als Maßnahme der Gefahrenabwehr oder Strafverfolgung erkennbar sind. Regelmäßig werden bei ihrer Durchführung technische Hilfsmittel eingesetzt. Allen diesen Maßnahmen ist gemein, dass sie intensive Eingriffe in das Recht auf informationelle Selbstbestimmung (das sogenannte APR-RiS) und gegebenenfalls auch andere Grundrechte darstellen. Sie unterliegen dementsprechend erhöhten Anforderungen, sowohl bezüglich der Tatbestandsvoraussetzungen als auch der Form- und Verfahrensvorschriften. **2**

Einige der in NPOG und StPO vorgesehenen Maßnahmen mit besonderen Mitteln und Methoden werden in der Praxis relativ häufig angewandt, andere nur sehr selten. Die folgende Darstellung orientiert sich daher – mit Blick auf den Umfang der Darstellung – an der praktischen Relevanz für den Polizeialltag. **3**

1 Siehe hierzu *König/Roggenkamp*, Eingriffsrecht, Rn. 202 ff.

Vertiefung: So wurden in Niedersachsen im Jahr 2019 insgesamt 1690 Telekommunikationsüberwachungsmaßnahmen nach § 100a Abs. 1 StPO angeordnet (bundesweit 18.225). Im Gegensatz dazu wurde im Jahr 2019 in Niedersachsen keine einzige Online-Durchsuchung nach § 100b Abs. 1 StPO angeordnet oder durchgeführt (bundesweit 32 Anordnungen, davon 12 tatsächliche Durchführungen).[2]

II. Basiswissen

1. Relevante Gesetze und Bestimmungen

4 Die relevanten Eingriffsbefugnisse für die hier gegenständlichen Maßnahmen finden sich etwas verstreut in der StPO (repressive Maßnahmen) sowie dem NPOG (präventive Maßnahmen). Darüber hinaus sind das Telemediengesetz (TMG), das Telekommunikationsgesetz (TKG), das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) sowie die Telekommunikationsüberwachungsverordnung (TKÜV) von besonderer Bedeutung.

5 **a) TMG.** Im Telemediengesetz (TMG) finden sich Regelungen für die **Telemediendienste**. Unter „Telemedien" werden nach der Legaldefinition in § 1 Abs. 1 Satz 1 TMG alle „elektronischen Informations- und Kommunikationsdienste" verstanden, „soweit sie nicht Telekommunikationsdienste nach § 3 Nummer 61 des Telekommunikationsgesetzes, telekommunikationsgestützte Dienste nach § 3 Nummer 63 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind". Diese etwas sperrige und schwer verständliche Legaldefinition hat zur Folge, dass die Zuordnung nicht immer leicht fällt.[3]

6 Jedenfalls zu den Telemediendiensten gehören nach der Gesetzesbegründung (aus dem Jahr 2006) Online-Angebote von „*Verkehrs-, Wetter-, Umwelt- oder Börsendaten, Newsgroups, Chatrooms, elektronische Presse, Fernseh-/Radiotext, Teleshopping*".[4] Mehr oder weniger alle über das Internet abrufbaren Angebote werden zu den Telemedien gezählt.

Vertiefung: Hierzu gehören Shoppingplattformen wie ebay/ebay-kleinanzeigen, zalando, amazon etc. als auch die sozialen Netzwerke wie facebook, instagram & Co. Sie werden auch „**Host-Provider**" genannt.

7 Konkret geregelt werden im TMG insbesondere Fragen der Verantwortlichkeit und Haftung von Telemediendiensteanbietern (§§ 7 – 10 TMG). Die Regelungen zum Datenschutz sowie zu Auskunftsansprüchen finden sich hingegen (seit Ende 2021) im Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG).

8 **b) TKG.** Das Telekommunikationsgesetz (kurz TKG) enthält umfangreiche Regelungen zu Telekommunikationsdiensteanbietern. Unter dem Begriff **Telekommunikationsdienste** versteht der Gesetzgeber ausweislich § 3 Nr. 61 TKG „*in*

2 Zahlen *Bundesamt für Justiz*, Referat III 3, Übersicht Telekommunikationsüberwachung für 2019. Aktuelle Zahlen sowie Zahlen für zurückliegende Jahre sind unter bundesjustizamt.de abrufbar.
3 Ausführlich hierzu *Heckmann*, in: Heckmann, jurisPK-Internetrecht, Kapitel 1, Rn. 49 ff.
4 BT-Drs. 16/3078, S. 13.

der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die – mit der Ausnahme von Diensten, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben – folgende Dienste umfassen: a) Internetzugangsdienste, b) interpersonelle Telekommunikationsdienste und c) Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für den Rundfunk genutzt werden". Stark vereinfacht fallen unter den Begriff der Telekommunikationsdienste die Anbieter von Telefondiensten, Internetzugang sowie andere Kommunikationsdienste wie z. B. SMS, E-Mail und Messengerdienste.

Das **TKG** ist sehr viel umfangreicher und enthält viel mehr Regulierungen als das TMG. Aus polizeilicher Sicht sind hauptsächlich die §§ 170 – 183 TKG von Interesse. Hier finden sich Regelungen darüber, ob und welche Daten ihrer Kunden die Telekommunikationsdiensteanbieter speichern müssen, um hierüber bei Bedarf gegenüber der Polizei und anderen berechtigten Stellen Auskunft geben zu können. Zudem finden sich hier Regelungen zu der Frage, unter welchen Voraussetzungen Telekommunikationsdiensteanbieter eine solche Auskunft überhaupt erteilen dürfen. 9

c) **TKÜV.** Wie die Speicherung zu Zwecken der Auskunftserteilung bzw. Überwachung der Kunden der dazu verpflichteten Telekommunikationsdiensteanbieter technisch und organisatorisch zu erfolgen hat, ist ebenfalls geregelt. Diese Regelungen finden sich nicht im TKG, sondern in einer separaten Verordnung, der „*Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation*" – kurz: Telekommunikations-Überwachungsverordnung bzw. **TKÜV.** 10

> **Vertiefung:** Die technischen Einzelheiten sind in einer technischen Richtlinie der Bundesnetzagentur (der TR TKÜV) festgelegt. Die aktuelle Fassung ist über die Webseite der Bundesnetzagentur abrufbar: www.bundesnetzagentur.de.

d) **TTDSG.** Im Telekommunikation-Telemedien-Datenschutz-Gesetz (kurz **TTDSG**) sind im Jahr 2021 die Datenschutzbestimmungen aus dem TMG und dem TKG in einem Gesetz zusammengefasst worden.[5] Insbesondere finden sich Regelungen zum Umgang der Diensteanbieter mit dem Fernmeldegeheimnis sowie Bestands- und Verkehrsdaten. Aus polizeilicher Sicht sind insbesondere die Regelungen zur Auskunftserteilung über Bestands- und Nutzungsdaten (dazu gleich Rn. 231 ff.) durch Telemediendiensteanbieter in den §§ 22 ff. TTDSG von Interesse. Die entsprechenden Regelungen für Telekommunikationsdiensteanbieter finden sich weiterhin im TKG. 11

2. Relevante Datenarten

Im Mittelpunkt der Maßnahmen mit besonderen Mitteln und Methoden steht die (heimliche) Erhebung personenbezogener Daten. Im Zusammenhang mit Maßnahmen der Telekommunikationsüberwachung haben sich weitere Begrifflichkeiten entwickelt, die **bestimmte Arten von personenbezogenen Daten** 12

5 BT-Drs. 19/27441, S. 2.

betreffen und deren Erläuterung zum Verständnis der entsprechenden Eingriffsbefugnisse hier vorab erfolgen soll.

13 **a) Bestandsdaten.** Die Frage, welcher Person eine bestimmte Telefonnummer zugewiesen ist oder welche Person hinter einer Nutzerkennung (z. B. Accountname eines Instagram oder Twitter-Kontos – auch als „*handle*" bezeichnet) eines Telemediendienstes steht, lässt sich durch Abfrage sogenannter **Bestandsdaten** beim jeweiligen Diensteanbieter in Erfahrung bringen (zu den Voraussetzungen noch unten 341 ff.).

14 Bestandsdaten sind nach der Legaldefinition in § 3 Nr. 6 TKG personenbezogene „Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste".

15 Im § 2 Nr. 2 TTDSG werden Bestandsdaten ähnlich definiert, nämlich als „die personenbezogenen Daten, deren Verarbeitung zum Zweck der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Anbieter von Telemedien und dem Nutzer über die Nutzung von Telemedien erforderlich ist".

16 Es handelt sich vereinfacht ausgedrückt um die personenbezogenen Daten, die der Diensteanbieter (typischerweise) über seinen Nutzer „im Bestand hat", weil er sie im Rahmen des Vertragsschlusses (z. B. Mobilfunkvertrag, Registrierung eines Accounts bei Online-Dienst) abgefragt und (noch) gespeichert hat.

17 Viele „klassische" **Telekommunikationsdiensteanbieter** sind nach § 172 TKG verpflichtet von ihren Kunden bestimmte Bestandsdaten zu erheben, auch wenn sie selbst diese Daten nicht benötigen. Zu diesen Daten gehören z. B. Name, Anschrift, Geburtsdatum, Rufnummer, Gerätenummer eines eventuell mitverkauften Mobilfunkgerätes, vgl. § 172 Abs. 1 Satz 1 TKG. Es kann also erwartet werden, dass die Diensteanbieter Auskunft zu diesen Informationen geben können.

> **Vertiefung:** Angeboten werden müssen, damit § 172 TKG greift, allerdings „**nummerngebundene** interpersonelle Telekommunikationsdienste, **Internetzugangsdienste** oder Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, erbringt und dabei **Rufnummern oder andere Anschlusskennungen vergibt** oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt".

18 Anders stellt sich das bei **Telemediendiensteanbietern** dar. Für diese ist die Erhebung bestimmter personenbezogener Daten gerade nicht verpflichtend. Im Gegenteil: Die Abfrage von Daten ist diesem nur gestattet, wenn sie für die Durchführung des Nutzungsvertrags wirklich benötigt wird (= erforderlich ist). Nach § 19 Abs. 2 TTDSG muss der Anbieter eines Telemediendienstes „*die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym*" ermöglichen, „*soweit dies technisch möglich und zumutbar ist*". Bei kostenpflichtigen Diensten ist die Wahrscheinlichkeit hoch, dass Daten der nach außen unter einem Pseudonym (z. B. Einhorn4711) auftretenden Nutzer (z. B. bei eBay oder Partner-

vermittlungsplattformen) dem Plattformbetreiber vorliegen. Dieser möchte ja im Ernstfall seine Entgelte „eintreiben" können. Bei kostenlosen Plattformen (z. B. soziale Netzwerke, Kleinanzeigen-Online) ist es hingegen vom Einzelfall abhängig, ob die gewünschten Daten vorliegen und im Rahmen einer sog. **Bestandsdatenauskunft** herausgegeben werden können.

> **Vertiefung:** Selbst wenn z. B. im Rahmen einer „Klarnamenspflicht" Daten wie der bürgerliche Name und E-Mailadresse abgefragt werden, heißt das noch nicht, dass diese auch zutreffend sind.

19 **b) Verkehrsdaten.** Im Rahmen der Telekommunikationsüberwachung spielen die sog. **Verkehrsdaten** eine Rolle. Diese werden in § 3 Nr. 70 TKG definiert als „*Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind*". In §§ 9 und 12 TTDSG (lesen!) wird klargestellt, dass Telekommunikationsdiensteanbieter nur bestimmte Verkehrsdaten verarbeiten dürfen, nämlich z. B. „*Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten*" (§ 9 Abs. 1 Nr. 1 TTDSG) sowie „*Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen*" (§ 9 Abs. 1 Nr. 2 TTDSG).

> **Vertiefung:** Kurz: bei Verkehrsdaten handelt es sich um die Einzelheiten von Telekommunikationsvorgängen, also z. B. welche Nummern von einem bestimmten Anschluss angerufen wurden oder in welcher Funkzelle ein Telefon zum Zeitpunkt eines Telefonats „eingeloggt" war.

20 Sobald die Daten nicht mehr (z. B. für Abrechnungszwecke) benötigt werden, muss der Telekommunikationsdiensteanbieter diese löschen. Das folgt aus § 9 Abs. 1 TTDSG unmittelbar, da eine Verarbeitung dieser Daten nur zulässig ist, soweit „*dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen*" bzw. oder zur Störungsbeseitigung (siehe § 12 TTDSG) „*erforderlich ist*". Eine Speicherung „auf Vorrat" ist grundsätzlich (zu den „Vorratsdaten" sogleich unter Rn. 27 f.) unzulässig, vgl. auch § 9 Abs. 1 S. 3 TTDSG.

21 Der Begriff der Verkehrsdaten ist im Bereich der Telemediendiensteanbieter nicht gebräuchlich.

22 **c) Nutzungsdaten (nur Telemediendienste).** Daten, die „*erforderlich*" sind, „*um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen*" werden ausweislich § 2 Nr. 3 TTDSG als **Nutzungsdaten** bezeichnet. Die in § 2 Nr. 3 TTDSG genannten Beispiele – Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien – sind abstrakt gehalten. Welche Daten tatsächlich für die Nutzung eines Telemediendienstes „erforderlich" sind, dürfte vom konkreten Dienst abhängen. Zu den Nutzungsdaten zählen insbesondere die sog. Cookies.[6]

6 *Müller-Broich*, TMG, § 15 Rn. 1.

Vertiefung: Die Zulässigkeit der Verarbeitung der Nutzungsdaten durch die Diensteanbieter richtet sich weitgehend nach den Regelungen der Datenschutzgrundverordnung (DSGVO).[7] Ob und unter welchen Voraussetzungen Behörden gegenüber dem Telemediendiensteanbieter über (diesem vorliegende) Nutzungsdaten Auskunft verlangen können bzw. Diensteanbieter Auskunft geben dürfen, richtet sich nach § 24 TTDSG (iVm. § 100k StPO bzw. § 33c NPOG).[8]

23 Nutzungsdaten sind von besonderer **Sensibilität**, da sie das Verhalten einer Person offenlegen können (Stichwort: gläserner Nutzer). Wird z. B. durch einen Anbieter eines sozialen Netzwerks gespeichert, welche Profile ein bestimmter Nutzer angeschaut/angeklickt hat, welche Seiten er aufgerufen hat und nach welchen Suchbegriffen gesucht wurde, lässt sich bereits aus diesen Informationen ein detailliertes Nutzerprofil erstellen.[9]

24 **d) Standortdaten.** Telekommunikationsdiensteanbieter dürfen unter bestimmten Umständen (siehe §§ 9 Abs. 1 Nr. 1, 13 TTDSG sowie § 176 Abs. 1 Nr. 2 TKG) sogenannte **Standortdaten** erheben und verarbeiten. Unter Standortdaten werden nach der Legaldefinition in § 3 Nr. 56 TKG Daten verstanden, „die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben".

25 **e) Inhaltsdaten.** Die im Rahmen eines Telekommunikationsvorgangs (z. B. Telefonat, Fax, SMS, E-Mail) übermittelten Inhalte werden auch als **Inhaltsdaten** bezeichnet. Diese dürfen von den Telekommunikationsdiensteanbietern grundsätzlich *nicht* erhoben, gespeichert oder verarbeitet werden, vgl. § 3 TTDSG.

26 Inhaltsdaten sind aber im Rahmen einer Telekommunikationsüberwachungsmaßnahme (wesentlicher) Teil der zu überwachenden „Telekommunikation" (zur „**TKÜ**" noch unten unter Rn. 231 ff.). Diese Überwachung und die Aufzeichnung der Inhalte der Telekommunikation muss – bei Vorliegen einer entsprechenden Anordnung – den zuständigen Stellen technisch ermöglicht werden, vgl. z. B. § 100a Abs. 4 StPO iVm. der TKÜV.

27 **f) Sog. Vorratsdaten.** Rechtlich und rechtspolitisch umstritten sind die sog. **Vorratsdaten**, genauer die Speicherung derselben.[10] Nach § 176 TKG (Anm.: in der zu Redaktionsschluss geltenden Fassung) sind bestimmte Telekommunikationsdiensteanbieter – welche genau steht in § 175 TKG – verpflichtet, bestimmte Verkehrsdaten ihrer Kunden für zehn Wochen sowie Standortdaten für vier Wochen zu speichern, obwohl hierfür (noch) gar kein Anlass besteht.

Vertiefung: Die Inhaltsdaten, also z. B. versendete SMS, Telefonate, aufgerufene Webseiten sowie E-Mails etc. dürfen nicht gespeichert werden, § 176 Abs. 5 TKG.

---

7 Vgl. z. B. *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, IT/Datenschutzrecht, § 36 II 1 und 2.
8 Siehe dazu näher z. B. *Ettig*, in: Taeger/Gabel, § 24 TTDSG Rn. 8 ff.
9 Vgl. *Karg*, DuD 2015, 85, 86.
10 Dazu z. B. *Boehm/Andrees*, CR 2016, 146.

Die Daten werden „auf Vorrat" gespeichert, damit sie bei Bedarf durch die Strafverfolgungs- oder Gefahrenabwehrbehörden abgefragt werden können, vgl. § 177 TKG. So werden die Strafverfolgungsbehörden beispielsweise in die Lage versetzt, zu überprüfen, wo sich ein bestimmtes Mobilfunktelefon (und vermutlich auch dessen Besitzer) in den letzten vier Wochen befunden hat oder welche Anschlüsse von diesem angerufen wurden. 28

Eine Abfrage von Vorratsdaten durch staatliche Stellen ist nur unter bestimmten Voraussetzungen zulässig. Zu strafprozessualen Zwecken muss der Verdacht einer „**besonders schweren Straftat**" bestehen, vgl. § 100g Abs. 2 StPO. Das NPOG sieht eine Abfrage von Vorratsdaten nicht vor. Zu Zwecken der Gefahrenabwehr ist also eine Abfrage von Vorratsdaten (für die niedersächsische Polizei) gar nicht möglich. 29

Vertiefung: Die Vereinbarkeit der Regelungen zur Vorratsdatenspeicherung mit dem Grundgesetz und europarechtlichen Vorgaben ist umstritten. Mehrere Verfassungsbeschwerden sind derzeit (Stand 10/2022) beim BVerfG anhängig. Viele Telekommunikationsdiensteanbieter speichern, von der Bundesnetzagentur geduldet, derzeit die Vorratsdaten gar nicht.[11] Aus dem Koalitionsvertrag der seit 12/2021 regierenden Parteien lässt sich zudem ersehen, dass eine grundlegende Reform der Regelungen (wenn nicht sogar Abschaffung) geplant ist.[12] Daher, und auch weil die Einzelheiten der Vorratsdatenspeicherung nicht Gegenstand des Bachelorstudiums sind, sondern im Masterstudiengang vertieft erörtert werden, wird hier[13] nicht näher auf diesen Themenkomplex eingegangen.

I. Relevante Grundrechte

1. Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG

Die hier gegenständlichen Maßnahmen dienen allesamt der Beschaffung personenbezogener Daten und sind daher als Eingriffe in das **Recht auf informationelle Selbstbestimmung** (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG – APR-RiS)[14] zu werten. Der Umstand, dass die Daten in der Regel heimlich und/oder mit Hilfe technischer Mittel erhoben werden veranlasst das BVerfG regelmäßig diese Eingriffe als besonders schwerwiegend einzustufen.[15] An die zu derartigen Eingriffen ermächtigenden Befugnisse werden dementsprechend besonders hohe Anforderungen gestellt.[16] 30

11 Vgl. OVG Nordrhein-Westfalen, Beschluss vom 22.6.2017 – 13 B 238/17 – GSZ 2017, 33 m. Anm. *Löffelmann*.
12 Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP (2021), S. 109.
13 Neuere Lektüre hierzu z. B. *Hammer/Müllmann*, K&R 2020, 103; *Seegmüller*, DRiZ 2020, 398; *Weichert*, vorgänge 2019, Nr. 3, S. 59.
14 Diesbezüglich sei auf die grundsätzlichen Ausführungen in *König/Roggenkamp*, Eingriffsrecht, Rn. 202 ff. verwiesen.
15 Vgl. z. B. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09 – BKA-Gesetz – Rn. 91.
16 Vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09 – BKA-Gesetz – Rn. 101.

2. Art. 13 GG

31 Sofern Informationen aus **Wohnungen** erhoben werden, liegt ein Eingriff in das Wohnungsgrundrecht (Art. 13 Abs. 1 GG) vor.[17] Irrelevant ist es hierbei, ob die Maßnahme heimlich oder offen erfolgt. Ob und in welchem Umfang der Eingriff **verfassungsrechtlich rechtfertigbar** ist, bemisst sich bei technikgestützten Überwachungsmaßnahmen maßgeblich nach den (sehr detailliert formulierten) Absätzen 3 bis 5 des Artikels 13 GG (lesen!). So darf nach Art. 13 Abs. 3 GG zu Zwecken der Strafverfolgung beispielsweise nur eine akustische Überwachung gestattet werden. Eine Befugnisnorm, die zum Zweck der heimlichen Überwachung zu repressiven Zwecken eine optische (Video-)Überwachung gestattete, wäre verfassungswidrig.[18]

3. Art. 10 GG

32 Der Artikel 10 GG spielt bei heimlichen Maßnahmen eine große Rolle. Er enthält die sog. Kommunikationsfreiheiten, namentlich das **Briefgeheimnis**, das **Postgeheimnis** und das **Fernmeldegeheimnis** (auch als **Telekommunikationsgeheimnis** bezeichnet).

33 **a**) **Schutzbereiche.** Geschützt ist – vereinfacht und zusammenfassend gesagt – die individuelle und nicht-öffentliche[19] Kommunikation, die unter Zuhilfenahme Dritter (z. B. Post, Telekommunikationsanbieter, E-Mail-Provider, Messengerdienst) erfolgt, vor (ungewollter) Kenntnisnahme durch den Staat. Brief-, Post- und Fernmeldegeheimnis werden als wesentlicher Bestandteil des Schutzes der Privatsphäre angesehen. Es besteht ein grundrechtlich geschützter Anspruch auf „*Wahrung der **Vertraulichkeit räumlich distanzierter Kommunikation***“.[20]

34 Wird die Vertraulichkeit durch eine staatliche Maßnahme aufgehoben, werden typischerweise personenbezogene Daten erhoben. Gegenüber dem APR-RiS (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) ist Art. 10 GG eine „**speziellere Garantie**“. Das APR-RiS kommt also *nicht* zur Anwendung. Die Maßgaben, die für das APR-RiS gelten, sind jedoch – neben den spezifischen Anforderungen aus Art. 10 GG – anzuwenden.[21]

35 **aa**) **Briefgeheimnis.** Das **Briefgeheimnis** schützt „*den brieflichen Verkehr der Einzelnen untereinander gegen eine Kenntnisnahme der öffentlichen Gewalt von dem Inhalt des Briefes*“[22]. In den sachlichen Schutzbereich fallen Briefe. Ein **Brief** ist jede die mündliche Kommunikation ersetzende, an einen individuellen Empfänger gerichtete, schriftlich fixierte Nachricht, Gedankenäußerung oder Meinung.[23]

---

17 Siehe dazu die grundsätzlichen Ausführungen in *König/Roggenkamp*, Eingriffsrecht, Rn. 227 ff. verwiesen.
18 Vgl. BT-Drs. 13/8651, S. 13.
19 Ausdrücklich BVerfG, Beschluss vom 20.6.1984 – 1 BvR 1494/78 – BVerfGE 67, 157, 171.
20 BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04 – BVerfGE 115, 166, 182.
21 BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13 – Bestandsdatenauskunft II – Rn. 100.
22 BVerfG, Beschluss vom 20.6.1984 – 1 BvR 1494/78 – BVerfGE 67, 157, 171.
23 Vgl. *Hermes*, in: Dreier, GG, Art. 10 Rn. 30.

Vertiefung: Schriftliche Notizen auf Briefpapier sind erst dann „Brief" im Sinne des Art. 10 GG, wenn sie einer anderen Person zukommen sollen. Es kommt also nicht allein auf die äußere Form an.

Für den grundrechtlichen Schutz ist es (anders als bei § 202 StGB) unerheblich, ob ein Brief verschlossen oder unverschlossen ist.[24] **36**

Das Briefgeheimnis schützt einerseits die **Vertraulichkeit des Inhalts** aber auch die Information darüber, an wen Briefe geschickt beziehungsweise von wem Briefe empfangen werden, also die **Umstände** der Briefkommunikation.[25] **37**

Eine maßgebliche Einschränkung des Schutzbereichs erfährt das Briefgeheimnis auf **zeitlicher Ebene**. Es entfaltet keine Wirkung, wenn ein Brief noch nicht abgeschickt wurde. Der Schutz endet zudem in dem Moment, in dem der Empfänger den Brief an sich nimmt (aber noch nicht mit Einwurf in den Briefkasten).[26] **38**

bb) Postgeheimnis. Das **Postgeheimnis** gewährt die Vertraulichkeit aller Transport- und Kommunikationsvorgänge, die durch ein Postunternehmen (z. B. Deutsche Post, PIN, Hermes, UPS, DHL etc.) durchgeführt werden.[27] Es besteht sowohl Schutz vor Offenbarung des konkreten Inhalts einer Sendung als auch der Information darüber, *„wer mit wem [durch die Post] Briefe und Sendungen wechselt"*.[28] **39**

Nach hier geteilter Auffassung ergänzt das Postgeheimnis den Schutz des Briefgeheimnisses, indem es auch die Sendungen erfasst, die keine individuellen Mitteilungen enthalten (z. B. Waren-, Zeitschriften- oder Postwurfsendungen).[29] **40**

Wie das Briefgeheimnis entfaltet sich der Schutz nach Aufgabe beim Postdienstleister und endet mit tatsächlicher Entgegennahme durch den Empfänger. **41**

Vertiefung: Daraus folgt, dass z. B. Sendungen, die in einer **Packstation** oder einem Paketshop lagern (noch) dem Postgeheimnis unterfallen. Gleiches gilt für Sendungen, die bei einem Nachbarn abgegeben und noch nicht vom Empfänger abgeholt wurden.

cc) Fernmeldegeheimnis/Telekommunikationsgeheimnis. Das **Fernmeldegeheimnis**, heutzutage moderner auch als **Telekommunikationsgeheimnis** bezeichnet, schützt *„die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs"*[30]. **42**

---

24 BVerwG, Urteil vom 18.3.1998 – 1 D 88/97 (BDiszG) – zum Postgeheimnis; zustimmend die wohl h. M. vgl. *Ogorek*, in: BeckOK-GG, Art. 10 Rn. 21 m. w. N.
25 BVerfG, Beschluss vom 20.6.1984 – 1 BvR 1494/78 – BVerfGE 67, 157, 172.
26 *Ogorek*, in: BeckOK-GG, Art. 10 Rn. 23 m. w. N. (auch zu engeren Auffassungen).
27 *Ogorek*, in: BeckOK-GG, Art. 10 Rn. 24.
28 BVerfG, Beschluss vom 20.6.1984 – 1 BvR 1494/78 – BVerfGE 67, 157, 171 f.
29 *Funke/Lüdemann*, JuS 2008, 780, 782; a. A. z. B. *Ogorek*, in: BeckOK-GG, Art. 10 Rn. 28.
30 BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04 – BVerfGE 115, 166, 183.

43 Konkret geschützt wird die **Vertraulichkeit der Inhalte** jedweder (nicht öffentlichen) Telekommunikation zwischen mehreren Personen, d. h. sowohl Telefonate als auch SMS, Fax, E-Mail und Messengernachrichten.[31]

Vertiefung: Auf die konkrete Anzahl der an der Kommunikation teilnehmenden Personen kommt es nicht an, solange es sich nicht um einen allgemein zugänglichen Austausch von Nachrichten handelt. So ist auch die Vertraulichkeit der Kommunikation innerhalb einer Whats-App-Chatgruppe von Art. 10 GG erfasst, wenn eine gewisse Auswahl der Teilnehmer stattfindet. Nicht erfasst sind hingegen Unterhaltungen in öffentlich zugänglichen Foren u. ä.[32]

44 Darüber hinaus ist auch die **Vertraulichkeit der Umstände konkreter Telekommunikationsvorgänge** geschützt, also ob, wann und wie oft zwischen zwei Personen „*Telekommunikationsverkehr stattgefunden hat oder versucht worden ist*".[33]

45 Nicht von Artikel 10 GG, sondern vom APR-RiS ist die **Zuordnung einer Telefonnummer** zu einem bestimmten Anschlussinhaber erfasst, da diese keinen Aufschluss über konkrete Telekommunikationsvorgänge liefert. Gleiches gilt für die Ermittlung des **Standorts eines Mobiltelefons** sowie dessen Geräte- oder Kartennummer (z. B. mit Hilfe eines IMSI-Catchers).[34]

Vertiefung: Der Abruf von Bestandsdaten, die anhand **dynamischer IP-Adressen** bestimmt werden, stellt nach dem BVerfG allerdings einen Eingriff in das gegenüber dem APR-RiS speziellere Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG dar.[35] Dies begründet das BVerfG damit, dass „*die Diensteanbieter für die Identifizierung einer dynamischen IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten und dafür auf konkrete Telekommunikationsvorgänge zugreifen müssen.*"[36]

46 In zeitlicher Hinsicht schützt Art. 10 GG grundsätzlich nur die „*laufende Kommunikation*". Das bedeutet, dass Inhalte und Umstände von Telekommunikation (nur) dann und (nur) solange durch Art. 10 GG geschützt sind, wie der Telekommunikationsvorgang andauert.

47 Kommunikationsinhalte und Informationen über Kommunikationsumstände die „*im Herrschaftsbereich des Kommunikationsteilnehmers*" gespeichert bzw. aufbewahrt werden, sind „nur" durch das APR-RiS geschützt.[37] So unterfällt z. B. eine auf einem Handy gespeicherte SMS, Messengernachricht oder E-Mail nicht

---

31 Vgl. BVerfG, Beschluss vom 16.6.2009 – 2 BvR 902/06 – BVerfGE 124, 43, 54.
32 Vgl. BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07 – Online-Durchsuchung – Rn. 293.
33 BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13 – Bestandsdatenauskunft II – Rn. 98 m. w. N.
34 Vgl. BVerfG, Beschluss vom 22.8.2006 – 2 BvR 1345/03 – IMSI-Catcher – Rn. 56 ff.
35 BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13 – Bestandsdatenauskunft II – Rn. 90, 98.
36 BVerfG, Beschluss vom 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13 – Bestandsdatenauskunft II – Rn. 99.
37 BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04 – Leitsatz 1.