§ 24.4 Vertraulichkeit und Integrität informationstechnischer Systeme

Notwendiges Vorwissen: Prüfung eines Freiheitsgrundrechts, Recht auf freie Entfaltung der Persönlichkeit, Grundrecht auf informationelle Selbstbestimmung

Lernziel: Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme verstehen und von anderen Gewährleistungen abgrenzen können

Für dieses Kapitel gibt es frei zugängliche interaktive Übungen. Halte einfach deine Smartphone-Kamera vor den Kasten mit den Punkten (QR-Code).

Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (teilweise etwas unpräzise als „Computergrundrecht" bezeichnet) wurde vom BVerfG als Ausformung des Persönlichkeitsrechts vor dem Hintergrund neuer Persönlichkeitsgefahren formuliert.[1] Es schützt davor, dass digitale Endgeräte heimlich überwacht werden. Das BVerfG hielt den Schutz bestehender Grundrechte nicht für ausreichend, da so viele private Aspekte unserer Persönlichkeit auf Smartphones oder Computern zu finden sind, dass eine Überwachung sehr viel über die betroffene Person aussagt.

i Weiterführendes Wissen

Das BVerfG hielt es für notwendig, die Dogmatik weiter zu entwickeln, weil digitale Endgeräte omnipräsent sind. Faktisch ist ein großer Bereich gesellschaftlicher Teilhabe nur über digitale Kommunikation möglich. Gusy spricht hier anschaulich von einer „Informations- und Kommunikationsgesellschaft"[2]. Dass ein erhöhter Schutzbedarf besteht, war auch in der Literatur unumstritten, allerdings war unklar, ob hierfür tatsächlich ein neues Grundrecht notwendig war. Teilweise wurde die informationelle Selbstbestimmung als ausreichend empfunden, da es letztendlich auch um den Schutz (einer größeren Menge) Daten gehe.[3] Wegen der ebenfalls bestehenden Schwächen der informationellen Selbstbestimmung wurde auch eine Anknüpfung an das

1 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 168 = BVerfGE 120, 274 – Online-Durchsuchung.

2 Gusy, DuD 2009, 33 (41).

3 Eifert, NVwZ 2008, 521 (522).

https://doi.org/10.1515/9783110765533-048

Persönlichkeitsrecht unter Einbeziehung von Art. 8 EMRK vorgeschlagen.[4] Andererseits könnte das neue Grundrecht auch so gelesen werden, dass eine rein abwehrrechtliche Perspektive der sonstigen digitalen Grundrechte nicht ausreicht und es auch darum gehen muss, die Vertraulichkeit und Integrität der Systeme einer privaten Kommunikationsinfrastruktur freiheitsfördernd zu gestalten.[5] Gerade die informationelle Selbstbestimmung ist – trotz Ansätzen zu einem Systemdatenschutz – auf die selbstbestimmte Kontrolle einzelner Datenverarbeitungen gerichtet.[6] Wenn auf ein informationstechnisches System zugegriffen wird, ist nicht nur eine Vielzahl unterschiedlicher Datenbestände einsehbar, sondern gleichzeitig (zum Beispiel durch den Zugriff auf Passwörter) der Zugriff auf externe Datenspeicher möglich.[7] Dieses Gefährdungspotential lässt sich nur mit dem Grundrecht auf informationelle Selbstbestimmung nicht abbilden.

A. Schutzbereich

I. Sachlicher Schutzbereich

Das Grundrecht bezieht sich auf **Systeme**, die so viele personenbezogene Daten der betroffenen Person enthalten, dass ein Zugriff auf das System einen Einblick in wesentliche Teile der Lebensgestaltung oder sogar ein aussagekräftiges Bild der Persönlichkeit der Person ermöglicht.[8] Hierbei muss das System als eigenes genutzt werden, sodass eine gewisse Vertraulichkeits- und Integritätserwartung der Nutzer:in besteht.[9] Geschützt wird also nicht nur das System selbst, sondern vor allem das **Vertrauen** darauf, dass ein eingesetztes System so funktioniert, wie es von der Nutzer:in erwartet werden kann.[10] In den Schutz einbezogen sind auch Daten, die zwar auf externen Servern („Cloud“) gespeichert werden, aber nur über das Gerät zugänglich sind.

Beispiel: Geschützt sind der eigene Laptop, das eigene Tablet oder das persönliche Smartphone. Nicht geschützt wären öffentlich zugängliche Computer in der Universität. Auch Smart-Home Geräte können darunter fallen, wenn sie im WLAN hängen.

4 Wegener/Muth, Jura 2010, 847 (849).
5 Gusy, DuD 2009, 33 (37).
6 Hoffmann-Riem, JZ 2008, 1009 (1015).
7 Hoffmann-Riem, JZ 2008, 1009 (1016).
8 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 205 = BVerfGE 120, 274 – Online-Durchsuchung.
9 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 208 = BVerfGE 120, 274 – Online-Durchsuchung.
10 Hoffmann-Riem, JZ 2008, 1009 (1012).

Wichtig für die Eröffnung des Schutzbereiches ist der Zugriff auf das System über das Internet (zum Beispiel durch einen „Staatstrojaner“ als verwendete Spähsoftware). Wenn die staatlichen Sicherheitsbehörden manuell in die Wohnung eindringen würden, um händisch Spähsoftware auf dem Computer der Zielperson zu installieren, wären eher das Persönlichkeitsrecht in der Dimension des Privatsphärenschutzes und der Schutz der Wohnung aus Art. 13 GG relevant.[11]

i **Weiterführendes Wissen**

Weitgehend ungeklärt ist die Reichweite des Schutzes gegenüber Privaten.[12] Die Frage wird umso drängender im Angesicht einer Netz-, Soft- und Hardwareinfrastruktur, die weitgehend von global agierenden, durch Geschäftsgeheimnisse notorisch intransparenten Konzernen zur Verfügung gestellt wird.

II. Persönlicher Schutzbereich

Das Grundrecht findet auf alle natürlichen Personen Anwendung, da es aus dem Recht auf freie Entfaltung der Persönlichkeit hergeleitet wird. Auch eine Anwendung auf juristische Personen ist denkbar, ggf. mit einem abgemilderten Schutz, da hier die Aspekte der Menschenwürde nicht betroffen sein können.

B. Eingriff

Ein Eingriff in den Schutzbereich liegt schon dann vor, wenn eine entsprechende Spähsoftware („Trojaner“) auf dem Gerät installiert ist und noch keine Daten abgegriffen worden sind. Bereits jetzt ist die **Integrität** des Gerätes betroffen, da schon zu diesem Zeitpunkt beliebige Daten ausgelesen oder sogar verändert/gelöscht werden können.[13] Im Gegensatz zu anderen Beeinträchtigungen digitaler Grundrechte ist der **heimliche** Eingriff hier der Normalfall. Das führt unter anderem zu den besonders hohen Anforderungen an die Rechtfertigung.

11 Gusy, DuD 2009, 33 (39).
12 Hoffmann-Riem, JZ 2008, 1009 (1019).
13 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 242 = BVerfGE 120, 274 – Online-Durchsuchung.

C. Rechtfertigung

I. Einschränkbarkeit

Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme kann wegen der Herleitung aus Art. 2 I GG durch ein Gesetz beschränkt werden. Es handelt sich lediglich um einen einfachen Gesetzesvorbehalt.[14]

II. Grenzen der Einschränkbarkeit

Ein Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme kann gerechtfertigt werden, solange die gesetzliche Grundlage bestimmte Anforderungen erfüllt. Auch hier steht das BVerfG in seiner Tradition, gegenüber staatlicher Überwachung formelle Anforderungen und äußere Grenzen zu definieren.[15]

Die gesetzliche Grundlage muss dem Bestimmtheitsgebot entsprechen.[16] Insbesondere müssen die tatbestandlichen Voraussetzungen der Eingriffsgrundlage klar herausgestellt werden.[17] Gerade hier ist eine sorgfältige Beachtung des Bestimmtheitsgebotes besonders wichtig, da die Eingriffe heimlich erfolgen und wenigstens die Möglichkeit des Eingriffs bekannt sein soll. Ein Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist nur zum Schutz **besonders hochwertiger Rechtsgüter** möglich, für deren Gefährdung tatsächliche Anhaltspunkte bestehen.[18]

Beispiel: Hochwertige Rechtsgüter, die den Eingriff in ein informationstechnisches System rechtfertigen würden, wären zum Beispiel Leib, Leben, Freiheit der Person oder solche Güter der Allgemeinheit, die staatliche Existenzgrundlagen sichern (kritische Infrastruktur).

Ein **heimlicher** Zugriff auf private Endgeräte ist nicht nur besonders **umfangreich** hinsichtlich der erlangten Daten, er gefährdet auch die Integrität des Rechners, da bestehende Sicherheitslücken ausgeweitet und die Dateien selbst durch

---

14 Siehe zur Einschränkbarkeit von Grundrechten Milas, § 6, in diesem Lehrbuch.

15 Wegener/Muth, Jura 2010, 847 (848).

16 Siehe zu dieser und anderen Grenzen der Einschränkbarkeit von Grundrechten Milas, § 7, in diesem Lehrbuch.

17 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 216 = BVerfGE 120, 274 – Online-Durchsuchung.

18 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 252 = BVerfGE 120, 274 – Online-Durchsuchung.

den Staat verändert werden könnten.[19] Deshalb steht der Eingriff unter **Richter:innenvorbehalt**.[20] Der Richter:innenvorbehalt wird hier vor allem mit der Hochwertigkeit des betroffenen Rechtsguts, der Heimlichkeit der Maßnahme sowie mit der Schaffung vollendeter Tatsachen, wofür Rechtsschutz typischerweise nicht rechtzeitig möglich ist, begründet.[21]

Ein Eingriff in den Kernbereich der Lebensgestaltung (Intimsphäre) muss durch den Staat von Anfang an vermieden werden.[22] Sofern diese Daten unabsichtlich erhoben werden, muss durch geeignete Verfahren garantiert werden, dass eine anschließende Löschung möglich ist.[23]

i Weiterführendes Wissen

Hier besteht folglich das Dilemma, dass die Daten erst sicher der Intimsphäre zugeordnet werden können, wenn sie durch die Behörden ausgewertet wurden und somit bereits erhoben sind. Allerdings bleibt es laut BVerfG bei dem Vorrang der Nichterhebung. Deshalb muss im Sinne des „zweistufigen Schutzkonzeptes“[24] gezielt nach Anhaltspunkten gesucht werden, ob die Intimsphäre berührt sein könnte.

D. Konkurrenzen

Art. 10 GG ist immer dann einschlägig, wenn der Staat den Kommunikations**vorgang** selbst überwacht. Der Schutz reicht jedoch nicht so weit, dass auch die auf dem Endgerät gespeicherten Daten erfasst würden.[25]

19 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 242f = BVerfGE 120, 274 – Online-Durchsuchung.
20 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 261 = BVerfGE 120, 274 – Online-Durchsuchung.
21 Gusy, DuD 2009, 33 (40).
22 Siehe zum Sphärenkonzept Valentiner, § 18.2 A. I. 1., in diesem Lehrbuch.
23 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 283ff. = BVerfGE 120, 274 – Online-Durchsuchung.
24 Hoffmann-Riem, JZ 2008, 1009 (1021).
25 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 187 = BVerfGE 120, 274 – Online-Durchsuchung.

Maximilian Petras

Weiterführendes Wissen

Ein Sonderproblem besteht hier bei der sogenannten „Quellen-Telekommunikationsüberwachung". Hier wird in das zur Kommunikation benutzte Gerät eingedrungen, weil die über das Internet verschickten Datenpakete verschlüsselt sind und von den Sicherheitsbehörden nicht gelesen werden können. In diesem Fall müsste auch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme greifen.[26]

Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist gegenüber dem Schutz der Wohnung aus Art. 13 GG spezieller, sofern nicht die komplette Wohnung sondern lediglich der in der Wohnung stehende Computer überwacht wird. Darüber hinaus werden gerade kleine Geräte wie Laptops oder Smartphones nicht ständig in der Wohnung gelagert, sodass sie grundlegend geschützt werden müssen.[27] Wenn allerdings über das Gerät eine Überwachung der Wohnung erfolgt (Kamera oder Mikrofon werden eingeschaltet), stellt das einen eigenständigen Eingriff in Art. 13 GG dar, der auch hieran gemessen werden muss.[28]

Das Recht auf freie Entfaltung der Persönlichkeit in Ausformung des Schutzes der **Privatsphäre** hilft ebenfalls nicht weiter, da die auf einem Endgerät gespeicherten Daten allen möglichen Sphären zugerechnet werden können.[29]

Ebenfalls tritt das **Grundrecht auf informationelle Selbstbestimmung** wegen der besonders großen Menge betroffener Daten und des speziell gelagerten Zugriffes hinter dem hier einschlägigen Grundrecht zurück.[30]

E. Europäische und internationale Bezüge

Ein den Gehalt dieses Grundrechts erfassendes ähnliches Grundrecht auf GRCh- oder EMRK-Ebene gibt es nicht. Am ehesten würde der Schutz durch Art. 7, 8 GRCh garantiert werden, sowohl in Bezug auf die gespeicherten Daten als auch hinsichtlich ihres Privatsphärenbezuges. Gleiches gilt für Art. 8 EMRK.

26 Hoffmann-Riem, JZ 2008, 1009 (1022).
27 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 196 = BVerfGE 120, 274 – Online-Durchsuchung.
28 Hoffmann-Riem, JZ 2008, 1009 (1021).
29 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 199 = BVerfGE 120, 274 – Online-Durchsuchung.
30 BVerfG, Urt. v. 27.2.2008, Az.: 1 BvR 595/07, Rn. 202 = BVerfGE 120, 274 – Online-Durchsuchung.

Zusammenfassung: Die wichtigsten Punkte

- Das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ schützt persönliche digitale Endgeräte.
- Für die Rechtfertigung eines Eingriffes müssen zahlreiche Verfahrensvorkehrungen eingehalten werden.

Weiterführende Studienliteratur

- Bernhard Wegener/Sven Muth, Das „neue Grundrecht“ auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Jura 2010, S. 847–852

Maximilian Petras