

**Ausarbeitung**

# Zugriff auf vernetzte Geräte

Verfassungsrechtliche Aspekte

**Zugriff auf vernetzte Geräte**
Verfassungsrechtliche Aspekte

Aktenzeichen: WD 3- 3000 - 191/19
Abschluss der Arbeit: 29.08.2019
Fachbereich: WD 3: Verfassung und Verwaltung

## 1. Einleitung

Die Möglichkeiten des Zugriffs von Strafverfolgungsbehörden auf sogenannte „Smart-Home-Geräte“ nach aktueller Rechtslage wurden in der Ausarbeitung der Wissenschaftlichen Dienste des Deutschen Bundestages zum Thema „Zugriff auf vernetzte Geräte zum Zwecke der Strafverfolgung. Strafverfahrensrechtliche Rahmenbedingungen“ (WD 7 - 3000 - 119/19) dargestellt. Darüber hinaus wirft der Zugriff auf vernetzte Geräte zahlreiche verfassungsrechtliche Fragen auf. Im Folgenden wird zunächst auf die Unterschiede der Intensität des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung im Vergleich zur akustischen Wohnraumüberwachung eingegangen (2.). Anschließend wird auf den gebotenen Schutz des Kernbereichs privater Lebensführung eingegangen (3.). Ferner werden die Anforderungen erläutert, die sich aus der Rechtsprechung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung ergeben (4.).

## 2. Eingriffsintensität im Vergleich zur akustischen Wohnraumüberwachung

§ 100c Strafprozessordnung (StPO) befugt zur akustischen Wohnraumüberwachung zum Zwecke der Strafverfolgung, jedoch nicht zur Manipulation von Geräten der betroffenen Personen.[1] Der Zugriff auf vernetzte Geräte berührt dagegen stets die **Vertraulichkeit und Integrität informationstechnischer Systeme** betroffener Personen, deren verfassungsrechtlicher Schutz nach der Rechtsprechung des Bundesverfassungsgerichts aus dem **Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG**) folgt.[2] Erfasst sind insbesondere Systeme, die „in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.“[3]

Darüber hinaus besitzen viele vernetzte Geräte sowohl Mikrofone als auch Kameras. Mithin könnte ein Echtzeitabruf von **Audio-, Foto- und Videoaufnahmen** erfolgen. **Art. 13 Abs. 3 GG** begrenzt die Zulässigkeit von Eingriffen in die Unverletzlichkeit von Wohnungen zu **Strafverfolgungszwecken auf akustische Überwachungsmaßnahmen**[4]**,** wie dies in § 100c StPO vorgesehen ist. Im Umkehrschluss dazu schließe die Verfassung nach der Rechtsprechung des Bundesverfassungsgerichts eine **optische Wohnraumüberwachung zur Gefahrenabwehr** nach **Art. 13 Abs. 4 GG** nicht grundsätzlich aus.[5] Der **kombinierte Abruf von Ton- und Bildaufnahmen** greife jedoch **regelmäßig stärker** in die informationelle Selbstbestimmung und die Unverletzlichkeit der Wohnung ein als eine rein akustische Wohnraumüberwachung und bedürfe daher einer **besonderen Rechtfertigung**.[6]

---

1 WD 7 - 3000 - 119/19, S. 12.

2 BVerfGE 120, 274 (313).

3 BVerfGE 120, 274 (314).

4 Gornig, in von Mangoldt/Klein/Starck, GG, Bd. 1, 7. Aufl. 2018, Art. 13 Rn. 96; Papier, in: Maunz/Dürig, Grundgesetz-Kommentar, Stand: 86. EL Januar 2019, Art. 13 Rn. 73.

5 BVerfGE 141, 220 (296 f.).

6 BVerfGE 141, 220 (296).

„Dementsprechend sind die Anforderungen an die Geeignetheit, Erforderlichkeit und Angemessenheit bei der Anordnung der Maßnahmen für jede der Überwachungsformen eigens und gegebenenfalls auch mit Blick auf deren Verbindung zu prüfen. Dabei reicht es für die zusätzliche Anordnung einer optischen Überwachung regelmäßig nicht, auf bloße Erleichterungen für die Zuordnung von Stimmen zu verweisen, sondern bedarf es gewichtiger, für den Erfolg der Überwachung maßgeblicher eigener Gründe. Diesen Anforderungen kann und muss im Rahmen der Gesetzesanwendung Rechnung getragen werden.“[7]

### 3. Schutz des Kernbereichs privater Lebensführung

**Rechtsgrundlagen** für Eingriffe in das Allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) einschließlich aller seiner besonderen Ausprägungen sowie in die Unverletzlichkeit der Wohnung (Art. 13 GG) müssen den absoluten Schutz des Kernbereichs privater Lebensführung sicherstellen.[8]

Das Bundesverfassungsgericht hat in seiner Entscheidung zum Großen Lauschangriff zum Kernbereichsschutz bei akustischen Wohnraumüberwachungen **zum Zwecke der Strafverfolgung** instruktiv ausgeführt: Eine zeitliche und räumliche **„Rundumüberwachung“** sei regelmäßig schon wegen der großen Wahrscheinlichkeit der Erfassung höchstpersönlicher Gespräche unzulässig.[9] Auch eine Art der Überwachung, die zu einer nahezu **lückenlosen Registrierung** aller Bewegungen und Lebensäußerungen des Betroffenen führen und so zur Grundlage für ein Persönlichkeitsprofil werden könnten, verletzten nach Ansicht des Bundesverfassungsgerichts die Menschenwürde.[10]

Überwachungsmaßnahmen in Privatwohnungen dürfen nur vorgenommen werden, soweit keine hinreichenden äußeren Anzeichen für die wahrscheinliche Erfassung absolut geschützter Gespräche bestehen. Dabei dürfe nicht etwa erst in den absoluten Kernbereich privater Lebensgestaltung eingegriffen werden, um festzustellen, ob die Informationserhebung diesen Bereich betrifft.[11]

Auch bei danach zulässigen Wohnraumüberwachungen sei **größtmögliche Zurückhaltung** geboten. „So kann es der Schutz des Art.1 Abs. 1 GG erforderlich machen, bei dem Abhören einer Privatwohnung auf eine nur automatische Aufzeichnung der abgehörten Gespräche zu verzichten, um jederzeit die Ermittlungsmaßnahme unterbrechen zu können. Sollte im Rahmen einer Wohnraumüberwachung eine Situation eintreten, die dem unantastbaren Kernbereich privater Lebensgestal-

---

7 BVerfGE 141, 220 (297).

8 St. Rspr. des Bundesverfassungsgerichts, vgl. BVerfGE 6, 32 (41); 54, 143 (146); 80, 367 (373); 109, 279 (323); 112, 304 (309 ).

9 BVerfGE 109, 279 (323).

10 BVerfGE 109, 279 (323).

11 BVerfGE 109, 279 (323).

tung zuzurechnen ist, muss die Überwachung abgebrochen werden. Dennoch erfolgte Aufzeichnungen sind zu vernichten. Die Weitergabe und Verwertung der gewonnenen Informationen sind untersagt."[12]

Diese Grundsätze gelten nach der Entscheidung des Bundesverfassungsgerichts zu Vorschriften des Bundeskriminalamtsgesetzes (a.F.) auch für Überwachungsmaßnahmen **zum Zwecke der Gefahrenabwehr**.[13] Der Schutz des Kernbereichs privater Lebensgestaltung bilde eine strikte, nicht frei durch Einzelfallerwägungen überwindbare Grenze, die **nicht durch Abwägung mit den Sicherheitsinteressen** nach Maßgabe des Verhältnismäßigkeitsgrundsatzes **relativiert werden darf**.[14] Dem Kernbereichsschutz müsse auf zwei Ebenen Rechnung getragen werden: „Zum einen sind auf der **Ebene der Datenerhebung** Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zum anderen sind auf der **Ebene der nachgelagerten Auswertung und Verwertung** die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren."[15]

### 4. Rechtsprechung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Eine Vorratsdatenspeicherung von Daten von vernetzten Geräten greift auch in Art. 10 Abs. 1 GG ein. Dieser schützt sowohl die Vertraulichkeit der Inhalte von Telekommunikation als auch der näheren Umstände des Kommunikationsvorgangs.[16] In seinem Urteil vom 2. März 2010[17] hat das Bundesverfassungsgericht erläutert, unter welchen Maßgaben eine Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG vereinbar sein kann[18]:

Die Speicherung dürfe nicht direkt durch den Staat, sondern nur durch eine Verpflichtung privater Diensteanbieter verwirklicht werden.[19] Damit werde gewährleistet, dass die Daten dem Staat nicht unmittelbar als Gesamtheit zur Verfügung stehen. Die anlasslose Speicherung der Telekommunikationsverkehrsdaten müsse eine Ausnahme bleiben und dürfe nur in einem engen zeitlichen

12 BVerfGE 109, 279 (324 m.w.N. zur Rspr. des BVerfG).

13 BVerfGE 141, 220 – zu Wohnraumüberwachung nach § 20h BKAG a.F. siehe insb. S. 295 ff.

14 BVerfGE 141, 220 (278).

15 BVerfGE 141, 220 (278 f.) (Hervorhebung nur hier).

16 BVerfGE 125, 260 (309).

17 BVerfGE 125, 260.

18 Vgl. dazu schon die Ausarbeitungen der Wissenschaftlichen Dienste des Deutschen Bundestages, Zulässigkeit einer Vorratsdatenspeicherung in Deutschland nach der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs; WD 3 - 3000 - 088/15 und Rechtlicher Rahmen für eine Regelung der Vorratsdatenspeicherung durch den deutschen Gesetzgeber, WD 3 - 3000 - 071/15.

19 BVerfGE 125, 260 (321).

Rahmen erlaubt werden.[20] Eine Speicherungsdauer von sechs Monaten liege an der Obergrenze dessen, was unter Verhältnismäßigkeitserwägungen rechtfertigungsfähig sei.[21]

Weiter fordert das Gericht **hinreichend anspruchsvolle und normenklare Regelungen** zur Datensicherheit, zur Begrenzung der Datenverwendung zur Transparenz sowie zum Rechtsschutz:[22]

Eine Vorratsdatenspeicherung erfordere ein besonders hohes Maß an **Datensicherheit**.[23] Dabei könne der Gesetzgeber die Aufgabe der technischen Konkretisierung des vorgegebenen Maßstabs auch einer Aufsichtsbehörde übertragen. Er habe jedoch sicherzustellen, dass die jeweiligen Telekommunikationsanbieter nicht unkontrolliert die Entscheidungen über Art und Maß der Schutzvorkehrungen treffen.

Die **Verwendung der Daten**[24] sei nur für überragend wichtige Aufgaben des Rechtsgüterschutzes zulässig. Für die Strafverfolgung bedeute dies, dass ein Abruf zumindest den durch bestimmte Tatsachen begründeten Verdacht einer auch im Einzelfall schwerwiegenden Straftat voraussetze. Für die Gefahrenabwehr gelte, dass ein Abruf der vorsorglich gespeicherten Daten nur bei Vorliegen einer durch bestimmte Tatsachen hinreichend belegten, konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden dürfe. Diese Anforderungen seien auch auf die Nachrichtendienste zu übertragen, da es auch insoweit um eine Form der Gefahrprävention gehe. Der Verhältnismäßigkeitsgrundsatz gebiete zudem ein grundsätzliches Übermittlungsverbot für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen.

Zu den **Transparenzanforderungen**[25] gehöre auch der Grundsatz der Offenheit der Erhebung und Nutzung personenbezogener Daten. Eine Verwendung der Daten ohne Wissen des Betroffenen sei nur dann zulässig, wenn andernfalls der Zweck der Untersuchung, dem der Datenabruf diene, vereitelt würde. Der Gesetzgeber könne dies für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste grundsätzlich annehmen. Im Rahmen der Strafverfolgung komme auch eine offene Erhebung und Nutzung der Daten in Betracht. In diesem Bereich dürfe eine heimliche Verwendung der Daten nur erfolgen, wenn sie im Einzelfall erforderlich und richterlich angeordnet sei. Erfolge die Datenverwendung heimlich, sei eine nachträgliche Benachrichtigung vorzusehen. Ausnahmen bedürften der richterlichen Kontrolle.

---

20 BVerfGE 125, 260 (323 f.).

21 BVerfGE 125, 260 (322).

22 BVerfGE 125, 260 (Ls. 2).

23 BVerfGE 125, 260 (325 ff.).

24 BVerfGE 125, 260 (327 ff.).

25 BVerfGE 125, 260 (334 ff.).

Die Übermittlung und Nutzung der gespeicherten Daten sei zur **Gewährleistung effektiven Rechtsschutzes**[26] grundsätzlich unter Richtervorbehalt zu stellen. Sofern dies nicht möglich sei, müsse eine nachträgliche gerichtliche Kontrolle eröffnet werden. Insbesondere vor dem Hintergrund der Verpflichtung des Staates, dem Einzelnen die Entfaltung seiner Persönlichkeit zu ermöglichen und ihn vor Persönlichkeitsrechtsgefährdungen durch Dritte zu schützen, sei zudem die Schaffung wirksamer Sanktionen für den Fall von Rechtsverletzungen erforderlich. Der Gesetzgeber besitze diesbezüglich jedoch einen weiten Gestaltungsspielraum.

Weniger strenge verfassungsrechtliche Anforderungen gelten laut Bundesverfassungsgericht für eine nur mittelbare Verwendung der vorsorglich gespeicherten Daten in Form von **behördlichen Auskunftsansprüchen** gegenüber Diensteanbietern hinsichtlich der **Anschlussinhaber bestimmter, bereits bekannter IP-Adressen**.[27] Systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen seien auf der Grundlage solcher Auskünfte nicht möglich.

***

26 BVerfGE 125, 260 (337 ff.).

27 BVerfGE 125, 260 (340 ff.).