



Sachverhalt¹

– Online-Durchsuchung –

Der Landtag des Bundeslandes L beschließt eine Änderung des Gesetzes über den Verfassungsschutz (LVSG). Diese Änderung ermächtigt die Verfassungsschutzbehörden in § 5 Abs. 2 Nr. 11 LVSG zu zwei Arten von Ermittlungsmaßnahmen: zum einen zum heimlichen Zugriff auf informationstechnische Systeme (Alt. 1); zum anderen zum Ausspähen des Speichers des informationstechnischen Systems (Alt. 2). Unter einem heimlichen Zugriff auf ein informationstechnisches System ist eine technische Infiltration zu verstehen, die über die Installation eines Spähprogramms erfolgt (Staatstrojaner). Das Ausspähen des Speichers des informationstechnischen Systems ermöglicht es, die Speichermedien des informationstechnischen Systems durchzusehen. Eine inhaltliche Begrenzung der Datenerhebung ist nicht vorgesehen. Der Zugriff auf einen laufenden Kommunikationsvorgang wird nicht ermöglicht.

Ausschließlich bei Verdacht auf Begehung einer schweren Straftat i. S. d. des § 100a Abs. 2 StPO sollen die Verfassungsschutzbehörden befugt sein, die Maßnahmen durchzuführen. Die Anordnung derartiger Maßnahmen liegt im alleinigen Ermessen der Verfassungsschutzbehörden.

A, die ihren Computer für berufliche und private Zwecke nutzt, ist der Ansicht, dass § 5 Abs. 2 Nr. 11 LVSG nicht mit dem Grundgesetz zu vereinbaren sei. Sie erhebt daher ein halbes Jahr nach Inkrafttreten der Änderung des LVSG formgerecht Verfassungsbeschwerde; es ist davon auszugehen, dass die Verfassungsbeschwerde von allgemeiner Bedeutung ist.

Aufgabe: Beurteilen Sie die Erfolgsaussichten der Verfassungsbeschwerde der A.

¹ In Anlehnung an BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274.



Gliederung

– Online-Durchsuchung –

A.	Zulässigkeit der VB	1
I.	Parteifähigkeit	1
II.	Beschwerdegegenstand	1
III.	Beschwerdebefugnis.....	1
1.	Eigene Betroffenheit.....	2
2.	Gegenwärtigkeit	2
3.	Unmittelbarkeit.....	2
IV.	Erschöpfung des Rechtswegs	3
V.	Grundsatz der Subsidiarität.....	3
VI.	Ordnungsmäßigkeit des Antrags und Frist	4
VII.	Zwischenergebnis	4
B.	Begründetheit der VB	4
I.	Verletzung von Art. 13 Abs. 1 GG	4
1.	Schutzbereich	4
2.	Zwischenergebnis	6
II.	Verletzung von Art. 10 Abs. 1 GG	6
1.	Schutzbereich	6
III.	Verletzung von Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG	7
1.	Schutzbereich	7
2.	Eingriff.....	12
3.	Rechtfertigung.....	12
a)	Bestimmtheitsgebot	13
b)	Verhältnismäßigkeitsgrundsatz	13
c)	Kernbereichsschutz	14
d)	Richtervorbehalt	15
4.	Zwischenergebnis	15
C.	Endergebnis	16



Lösung

– Online-Durchsuchung –

Die Verfassungsbeschwerde (VB) der A gegen § 5 Abs. 2 Nr. 11 LVSG hat gem. Art. 93 Abs. 1 Nr. 4a GG i. V. m. §§ 13 Nr. 8a, 23, 90 ff. BVerfGG Aussicht auf Erfolg, wenn sie zulässig und begründet ist.

A. Zulässigkeit der VB

Die VB der A müsste zulässig sein.

I. Parteifähigkeit

A müsste parteifähig sein. Parteifähig ist jedermann (Art. 93 Abs. 1 Nr. 4a GG, §§ 13 Nr. 8a, 90 Abs. 1 BVerfGG), d. h. jede:r Träger:in von Grundrechten oder grundrechtsgleichen Rechten. Als natürliche Person ist A grundrechtsberechtigt und damit ebenso parteifähig.

II. Beschwerdegegenstand

Zudem müsste ein tauglicher Beschwerdegegenstand vorliegen. Gem. Art. 93 Abs. 1 Nr. 4a GG, §§ 13 Nr. 8a, 90 Abs. 1 BVerfGG kann Beschwerdegegenstand jeder Akt der öffentlichen Gewalt sein. Damit sind Maßnahmen der Legislative, der Exekutive und der Judikative gemeint. A wendet sich gegen § 5 Abs. 2 Nr. 11 LVSG. Diese landesgesetzliche Regelung stellt einen Legislativakt dar und ist somit ein tauglicher Beschwerdegegenstand.

III. Beschwerdebefugnis

Fraglich ist, ob A beschwerdebefugt ist. Gemäß Art. 93 Abs. 1 Nr. 4a GG, §§ 13 Nr. 8a, 90 Abs. 1 BVerfGG muss der:die Beschwerdeführende behaupten, in einem der dort genannten Rechte verletzt zu sein. Das ist der Fall, wenn der:die Beschwerdeführende zumindest möglicherweise in einem der dort genannten Rechte verletzt ist, wenn also eine entsprechende Verletzung nicht von vornherein und unter allen denkbaren Gesichtspunkten ausgeschlossen ist. Indem § 5 Abs. 2 Nr. 11 LVSG den heimlichen Zugriff der Verfassungsschutzbehörde auf informationstechnische Systeme sowie das Ausspähen derer Datensysteme ermöglicht, könnte A in ihren Grundrechten aus Art. 10 Abs. 1, 13 Abs. 1 und 2 Abs. 1 i. V. m. 1 Abs. 1 GG verletzt sein.



Der:die Beschwerdeführende muss jedoch auch selbst, gegenwärtig und unmittelbar betroffen sein.

1. Eigene Betroffenheit

Die Bestimmung des § 5 Abs. 2 Nr. 11 LVSG erfasst potentiell jede:n, bei dem:der die entsprechenden Verdachtsgründe auftreten. A als Trägerin der genannten Grundrechte ist folglich Adressatin der Norm und somit selbst betroffen.

2. Gegenwärtigkeit

Überdies müsste A auch gegenwärtig betroffen sein. Bei einer Rechtsnorm liegt Gegenwärtigkeit dann vor, wenn sie im Gesetzblatt verkündet wurde. Dies ist hier der Fall. A ist somit auch gegenwärtig betroffen.

3. Unmittelbarkeit

Problematisch erscheint hier jedoch die unmittelbare Betroffenheit der A. Die unmittelbare Betroffenheit ist dann ausgeschlossen, wenn Beschwerdegegenstand ein Gesetz ist und dieses Gesetz nicht selbst eine bestimmte Rechtsfolge herbeiführt, sondern erst noch durch einen zusätzlichen Akt vollzogen werden muss.²

Hier sieht § 5 Abs. 2 Nr. 11 LVSG vor, dass die Verfassungsschutzbehörde die beanstandeten Maßnahmen (Infiltration, Alt. 1; Ausspähen, Alt. 2) unter bestimmten Voraussetzungen ergreifen darf. Das angegriffene Gesetz muss daher erst noch durch weitere Akte vollzogen werden. Daher fehlt es an der unmittelbaren Betroffenheit der A.

Eine Ausnahme von dem Erfordernis der Unmittelbarkeit gilt jedoch bei Straf- und Ordnungswidrigkeitsgesetzen. Hier muss der:die Einzelne nicht abwarten, bis eine Entscheidung gegen ihn:sie ergeht.³ Eine solche Ausnahme liegt hier jedoch nicht vor.

Eine weitere Ausnahme von dem Erfordernis der Unmittelbarkeit besteht, wenn der:die Betroffene von dem Vollzugsakt keine Kenntnis erlangen kann.⁴

² Vgl. BVerfG, Beschl. v. 19.12.1951 – 1 BvR 220/51 = BVerfGE 1, 97, (102 f.).

³ Vgl. BVerfG, Urt. v. 27.10.1998 – 1 BvR 2306/96, 1 BvR 2314/96, 1 BvR 1108/97, 1 BvR 1109/97 = BVerfGE 98, 295 (296).

⁴ Vgl. BVerfG, Beschl. v. 14.07.1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 = BVerfGE 100, 313 (354).



So ist es im vorliegenden Fall: Es liegt in der Natur der Sache, dass der:die Betroffene einer heimlichen Maßnahme in der Regel keine Kenntnis davon haben wird. Dadurch aber kann der:die Betroffene sich gegen diese Vollzugsmaßnahmen auch nicht effektiv zur Wehr setzen, sodass es ihm:ihr unzumutbar ist, im Hinblick auf seine:ihre Grundrechtsverletzung mangels Unmittelbarkeit nicht gegen das zugrundeliegende Gesetz und mangels Kenntnis nicht gegen die Vollzugsakte vorgehen zu können. Stattdessen muss es dem:der Betroffenen in diesem Fall erlaubt sein, sich trotz fehlender unmittelbarer Betroffenheit gegen das ermächtigende Gesetz zur Wehr zu setzen.

IV. Erschöpfung des Rechtswegs

Ein Rechtsweg unmittelbar gegen formelle Gesetze ist nicht eröffnet, sodass eine vorherige Rechtswegerschöpfung nicht erforderlich ist (vgl. § 93 Abs. 3 BVerfGG).

V. Grundsatz der Subsidiarität

Der VB der A könnte jedoch der Grundsatz der Subsidiarität entgegenstehen. Dieser in neuerer Rspr. des BVerfG⁵ in sinngemäßer Anwendung des § 90 Abs. 2 BVerfGG⁶ entwickelte und in ständiger Rspr. des BVerfG⁷ vertretene Grundsatz verlangt, dass der:die Beschwerdeführer:in über das Gebot der Rechtswegerschöpfung im engeren Sinne hinaus die ihm:ihr zur Verfügung stehenden und zumutbaren Möglichkeiten ergreift, um eine Korrektur der geltend gemachten Grundrechtsverletzungen zu erreichen oder eine Grundrechtsverletzung zu verhindern.

⁵ BVerfG, Beschl. v. 18.12.1985 – 2 BvR 1167/84, 2 BvR 1185/84, 2 BvR 1636/84, 2 BvR 308/85, 2 BvQ 18/84 = BVerfGE 71, 305 (334 ff.).

⁶ So zu § 90 Abs. 2 S. 2 BVerfGG BVerfG, Urte. v. 23.04.1991 – 1 BvR 1170/90, 1 BvR 1174/90, 1 BvR 1175/90 = BVerfGE 84, 90 (116); In BVerfG, Urte. v. 24.04.1991 – 1 BvR 1341/90 = BVerfGE 84, 133 (144), wird § 90 Abs. 2 S. 2 BVerfGG sogar direkt angewendet.

⁷ BVerfG, Urte. v. 02.12.1986 – 1 BvR 1509/83 = BVerfGE 74, 69 (74 ff.); vgl. auch BVerfG, Urte. v. 26.01.1988 – 1 BvR 1561/82 = BVerfGE 77, 381 (400 ff.); BVerfG, Urte. v. 14.06.1988 – 1 BvR 95/88 = BVerfGE 78, 290 (301 ff.); BVerfG, Urte. v. 01.02.1989 – 1 BvR 1290/85 = 79, 275 (278 f.); siehe dazu näher *Detterbeck*, DÖV 1990, 558; *Gersdorf*, Jura 1994, 398.



Vorliegend handelt es sich aber um eine Sache von allgemeiner Bedeutung im Sinne des § 90 Abs. 2 S. 2 BVerfGG. Mithin steht der Grundsatz der Subsidiarität der Zulässigkeit der VB nicht entgegen.⁸

VI. Ordnungsmäßigkeit des Antrags und Frist

Die VB ist schriftlich (§ 23 Abs. 1 S. 1 BVerfGG), mit Begründung (§§ 23 Abs. 1 S. 2, 92 BVerfGG) und fristgerecht (§ 93 Abs. 3 BVerfGG) zu erheben. Laut Sachverhalt hat A die VB formgerecht und binnen eines halben Jahres nach Inkrafttreten des Gesetzes fristgerecht erhoben.

VII. Zwischenergebnis

Die VB der A ist zulässig.

B. Begründetheit der VB

Fraglich ist, ob die VB der A auch begründet ist. Dies ist der Fall, wenn der:die Beschwerdeführer:in durch § 5 Abs. 2 Nr. 11 LVSG in einem seiner:ihrer Grundrechte verletzt ist, vgl. § 95 BVerfGG.

I. Verletzung von Art. 13 Abs. 1 GG

Möglicherweise ist A durch § 5 Abs. 2 Nr. 11 LVSG in ihrem Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG verletzt. Das ist der Fall, wenn § 5 Abs. 2 Nr. 11 LVSG einen verfassungsrechtlich nicht gerechtfertigten Eingriff in den Schutzbereich des Grundrechts darstellt.

1. Schutzbereich

Dazu müsste zunächst der (sachliche) Schutzbereich des Grundrechts, in dessen (persönlichen) Schutzbereich als Jedermann-Grundrecht die A unproblematisch fällt, eröffnet sein. Wichtigstes Merkmal der Wohnung im Sinne von Art. 13 Abs. 1 GG ist zum einen die Abschottung gegenüber der allgemeinen Zugänglichkeit und zum anderen die Nutzung als Stätte privaten

⁸ Vgl. auch *Morgenthaler*, in: Epping/Hillgruber, BeckOK Grundgesetz, 48. Edition Stand: 15.08.2021, Art. 93 Rn. 73, der zusätzlich noch einen schweren und unabwendbaren Nachteil des Beschwerdeführers, wie bspw. einen intensiven Grundrechtseingriff voraussetzt, was hier aber gegeben wäre.



Lebens und Wirkens. Art. 13 Abs. 1 GG schützt also alle Räume, in denen Menschen ihr privates Leben gestalten.

Umstritten ist, ob Betriebs- und Geschäftsräume zum Schutzbereich der Unverletzlichkeit der Wohnung gehören. Der Zusammenhang des Art. 13 Abs. 1 GG mit der Privatheit könnte zunächst dafürsprechen, diese Räume vom Schutzbereich auszuklammern.

Das BVerfG hat jedoch Betriebs- und Geschäftsräume unter bestimmten Voraussetzungen in den Schutzbereich des Art. 13 Abs. 1 GG einbezogen.⁹ Es kann jedoch im vorliegenden Fall dahinstehen, ob auch das Büro der A vom Schutzbereich des Art. 13 Abs. 1 GG erfasst ist, da sie laut Sachverhalt auch privat einen Computer nutzt, der von einer Online-Durchsuchung betroffen sein könnte.

Es ist jedoch fraglich, ob ein Computer mit Internetzugang, der sich in einer Wohnung befindet, selbst vom Schutzbereich des Art. 13 Abs. 1 GG umfasst ist. Das BVerfG ist der Ansicht, dass Art. 13 Abs. 1 GG dem:der Einzelnen keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines:ihres informationstechnischen Systems vermittelt, auch wenn sich dieses System in einer Wohnung befindet.¹⁰ Denn der Eingriff kann unabhängig vom Standort erfolgen, sodass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insb. für mobile informationstechnische Systeme wie etwa Laptops, Netbooks, Smartphones oder Tablet-PCs.

⁹ Vgl. BVerfG, Beschl. v. 13.10.1971 – 1 BvR 280/66 = BVerfGE 32, 54 (68 ff.); BVerfG, Beschl. v. 26.05.1976 – 2 BvR 294/76 = BVerfGE 42, 212 (219); BVerfG, Beschl. v. 24.05.1977 – 2 BvR 988/75 = BVerfGE 44, 353 (371); BVerfG, Beschl. v. 16.06.1987 – 1 BvR 1202/84 = BVerfGE 76, 83 (88); BVerfG, Beschl. v. 27.05.1997 – 2 BvR 1992/92 = BVerfGE 96, 44 (51); BVerfG, Urt. v. 17.02.1998 – 1 BvR 1/91 = BVerfGE 97, 228 (265); BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (309).

¹⁰ Vgl. BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (310); Kluckert, in: Epping/Hillgruber, BeckOK Grundgesetz, 48. Edition Stand: 15.08.2021, Art. 13 Rn. 10.



2. Zwischenergebnis

Der Inhalt des Computers der A wird somit nicht durch Art. 13 Abs. 1 GG geschützt. § 5 Abs. 2 Nr. 11 LVSG berührt damit bereits nicht den Schutzbereich dieses Grundrechts und verletzt es folglich nicht.

Anmerkung: Eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, kann an Art. 13 Abs. 1 GG zu messen sein, wenn und soweit Mitarbeiter:innen der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren. Ebenso liegt der Fall, wenn ein infiltrierte System genutzt wird, um die als Wohnung geschützten Räumlichkeiten akustisch oder optisch zu überwachen (z. B. durch Einschalten einer in den Computer eingebauten Webcam).

II. Verletzung von Art. 10 Abs. 1 GG

Möglicherweise ist jedoch durch § 5 Abs. 2 Nr. 11 LVSG das Fernmeldegeheimnis der A aus Art. 10 Abs. 1 GG verletzt.

1. Schutzbereich

Auch hierzu müsste zunächst der (sachliche) Schutzbereich des Grundrechts, in dessen (persönlichen) Schutzbereich als Jedermann-Grundrecht die A unproblematisch fällt, eröffnet sein. Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger:innen mit Hilfe des Telekommunikationsverkehrs.¹¹ Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart und welche Ausdrucksform genutzt werden. Der Schutzbereich des Art. 10 Abs. 1 GG erstreckt sich daher auch auf die Kommunikationsdienste des Internets (Chats, E-Mails, etc.).

Vom Schutzbereich des Art. 10 Abs. 1 GG erfasst sind jedoch nicht die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines:einer Kommunikationsteilnehmenden gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das

¹¹ Ogorek, in: Epping/Hillgruber, BeckOK GG, 48 Edition, Stand: 15.08.2021, Art. 10 Rn. 36.



TK-Geheimnis abgewehrt werden sollen, nicht fort. Mithin ist, entsprechend der bundesverfassungsgerichtlichen Rechtsprechung, zu differenzieren, ob eine Speicherung im eigenen oder in einem fremden Herrschaftsbereich erfolgt.¹² Werden die Daten im eigenen Herrschaftsbereich abgespeichert, so ist nach dem BVerfG der Anwendungsbereich des Art. 10 Abs. 1 GG nicht eröffnet, bei Speicherung in einem fremden Herrschaftsbereich hingegen greift der Schutz des Art. 10 Abs. 1 GG ein.¹³

Anmerkung: Das bedeutet auch, dass Daten, die in einer sog. „Cloud“ gespeichert sind, für die der:die Kommunikationsteilnehmende also eigene Schutzvorkehrungen gerade nicht treffen kann und zu deren Abruf er:sie gerade wieder auf Mittel der räumlich distanzierten Kommunikation angewiesen ist (Verbindungsaufbau zum Cloud-Server), sehr wohl dem Schutz des Art. 10 Abs. 1 GG unterfallen können.¹⁴ Sie müssen also genau danach differenzieren, wo die Daten wie gespeichert sind.

Auf Grundlage des § 5 Abs. 2 Nr. 11 LVSG wird ein Ausspähen des Zielrechners dergestalt ermöglicht, dass dessen Speichermedien inspiziert werden können, jedoch keine Einsichtnahme oder ein Abhören des Echtzeitkommunikationsprozesses stattfinden kann. Mithin ist vorliegend der eigene Herrschaftsbereich betroffen und der Schutzbereich des Art. 10 Abs. 1 GG folglich nicht eröffnet.

III. Verletzung von Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG

Durch § 5 Abs. 2 Nr. 11 LVSG ist jedoch möglicherweise das vom BVerfG aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme¹⁵ verletzt.

1. Schutzbereich

Dazu müsste jedoch zunächst der (sachliche) Schutzbereich dieses Jedermann-Grundrechts, in dessen (personellen) Schutzbereich A unzweifelhaft fällt, eröffnet sein.

¹² Vgl. BVerfG, Urt. v. 02.03.2006 – 2 BvR 2099/04 = BVerfGE 115, 166 (183 ff.); BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (307 f.).

¹³ Ebd.

¹⁴ Vgl. Ogorek, in: Epping/Hillgruber, BeckOK GG, 48. Edition, Stand 15.08.2021, Art. 10 Rn. 41 f.

¹⁵ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (302 ff.).



Um dem nach Auffassung des BVerfG lückenhaften Schutz des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), des Telekommunikationsgeheimnisses des Art. 10 Abs. 1 GG und der Unverletzlichkeit der Wohnung des Art. 13 Abs. 1 GG zu begegnen, hat das BVerfG auf Grundlage des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** (GGVIS) entwickelt.¹⁶ Das GGVIS ist nach bundesverfassungsgerichtlicher Rechtsprechung **subsidiär** dort anzuwenden, wo die genannten Grundrechte Schutzlücken hinterlassen.¹⁷

Mithin ist bei der Bestimmung des sachlichen Schutzbereiches des GGVIS eine Abgrenzung zu den spezielleren Vorschriften vorzunehmen, um auf diese Weise die zu schließenden Lücken zu definieren.

Art. 13 Abs. 1 GG entfaltet lediglich einen raumbezogenen Schutz und hinterlässt daher regelmäßig dort Schutzlücken, wo sich ein Zugriff auf informationstechnische Systeme ereignet, die sich außerhalb des geschützten Wohnraums befinden.¹⁸

Der Sachverhalt macht keine Angaben dazu, ob und inwieweit A ihren Computer auch außerhalb des von Art. 13 Abs. 1 GG geschützten Bereiches nutzt. In Zeiten, in denen ein Großteil der Bürger:innen über einen Laptop oder ein vergleichbares transportables Gerät verfügt, ist eine Nutzung außerhalb des Wohnraums gleichwohl jedenfalls nicht ausgeschlossen. Hierzu könnte überdies angenommen werden, dass der (räumliche) Schutzbereich des Art. 13 Abs. 1 GG nicht eröffnet ist, insofern der Staatstrojaner unbeschadet der Privatheit Wirkung entfaltet – also gegenstandsbezogen und nicht raumbezogen ist. Dies gilt zumindest, solange mittels desselben nicht auf Mikro und Kamera des Geräts zugegriffen werden kann und dadurch eine Überwachung von Vorgängen in der Wohnung ermöglicht wird.¹⁹

Daneben erstreckt sich der Schutz des Art. 10 Abs. 1 GG, wie bereits oben erwähnt, nicht auf die nach Abschluss eines Kommunikationsvorgangs im alleinigen Herrschaftsbereich ei-

¹⁶ Ebd.

¹⁷ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (302).

¹⁸ Gersdorf, in: Gersdorf/Paál, Beck-OK Informations- und Medienrecht, 32. Edition, Stand: 01.05.2021, Art. 2 GG, Rn. 23.

¹⁹ Vgl. BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (310); Kluckert, in: Epping/Hillgruber, BeckOK Grundgesetz, 48. Ed. 15.08.2021, Art. 13 Rn. 10.



nes: einer Kommunikationsteilnehmenden gespeicherten Kommunikationsinhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann.²⁰ Auch ist der Schutzbereich des Art. 10 Abs. 1 GG nur auf Kommunikationsinhalte bzw. Umstände eines konkreten Kommunikationsvorganges bezogen; nicht geschützt ist hingegen der Zugriff auf Inhalte und Umstände außerhalb eines laufenden Kommunikationsvorganges. Die daraus resultierende Schutzlücke wird durch das GGVIS geschlossen.²¹ Nach der Rechtsprechung des BVerfG findet das GGVIS im Verhältnis zu Art. 10 Abs. 1 GG dann keine subsidiäre, sondern vielmehr simultane Anwendung, wenn der staatliche Zugriff während einer laufenden Kommunikation erfolgt.²² Mit Blick auf Art. 10 Abs. 1 GG vermag das GGVIS überdies eine dritte Lücke zu schließen, die abermals daraus resultiert, dass Art. 10 Abs. 1 GG lediglich Kommunikationsinhalte bzw. Umstände des Kommunikationsvorganges schützt – das GGVIS geht darüber hinaus und schützt auch persönliche Datenbestände, die nicht auf einer Kommunikation mit Dritten beruhen.²³

Vorliegend ist, wie bereits geprüft, Art. 10 Abs. 1 GG nicht einschlägig, da es um den Zugriff auf Speichermedien geht, die vom eigenen Herrschaftsbereich der A umfasst sind. § 5 Abs. 2 Nr. 11 Alt. 2 LVSG ermächtigt einerseits zum heimlichen Zugriff auf informationstechnische Systeme – hierbei handelt es sich um eine vorgelagerte Maßnahme für die sich daran anschließende (Haupt-)Maßnahme: dem Ausspähen des Speichers des informationstechnischen Systems, mithin zum Ausspähen gespeicherter Kommunikationsinhalte und sonstiger dateiförmig gespeicherter Inhalte, welche mit Blick auf das zuvor Gesagte vom Schutz des GGVIS umfasst sind.

Ferner ist das GGVIS gegenüber dem Recht auf informationelle Selbstbestimmung abzugrenzen. Aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist vom BVerfG 1983 das allgemeine Persönlichkeitsrecht entwickelt worden, womit insbesondere der Schutz der Privatsphäre und das Recht auf informationelle Selbstbestimmung gewährleistet werden soll.²⁴ Letzteres umfasst

²⁰ BVerfG, Urte. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (307 f.); Gersdorf, in: Gersdorf/Paal, Beck-OK Informations- und Medienrecht, 32. Edition, Stand: 01.05.2021, Art. 2 GG, Rn. 23.

²¹ Gersdorf, in: Gersdorf/Paal, Beck-OK Informations- und Medienrecht, 32. Edition, Stand: 01.05.2021, Art. 2 GG, Rn. 24.

²² BVerfG, Urte. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (340).

²³ BVerfG, Urte. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (302).

²⁴ Vgl. das sog. Volkszählungsurteil des BVerfG – BVerfGE 65, 1; vertiefend Gersdorf, in: Gersdorf/Paal, Beck-OK Informations- und Medienrecht, 32. Edition, Stand 01.05.2021, Art. 2 GG, Rn. 16 ff.

auch ein Recht auf Selbstbewahrung, im Rahmen dessen dem:der Einzelnen ein räumlich und thematisch selbstbestimmter Bereich verbleiben soll, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll.²⁵ Damit stellen Erhebung, Speicherung, Verarbeitung und Weitergabe persönlicher oder personenbezogener Daten jeweils einen einzelnen Eingriff mit jeweils grundsätzlich abgestufter Intensität dar,²⁶ wobei letztlich ein nichtpersonenbezogenes Datum schwer vorstellbar ist.²⁷

Diese anerkannten Ausprägungen des allgemeinen Persönlichkeitsrechts genügen jedoch aus der Sicht des BVerfG dem besonderen Schutzbedürfnis des:der Nutzenden eines informationstechnischen Systems nicht in ausreichendem Maße.²⁸ Eine Person, die auf ein informationstechnisches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des:der Betroffenen über einzelne Datenerhebungen weit hinaus.²⁹ Laut dem BVerfG besteht die Schutzlücke folglich darin, dass in das Grundrecht auf informationelle Selbstbestimmung in Form der Datenerhebung nur in äußerst geringer Intensität eingegriffen wird, während die Auswirkung auf den:die Grundrechtsträger:in schon eine überaus große ist, da auch ohne weitere Eingriffe in dieses Grundrecht in Form der Datenverarbeitung u.Ä.

²⁵ Vgl. BVerfG, Beschl. v. 15.01.1970 – 1 BvR 13/68 = BVerfGE 27, 344 (350 ff.); BVerfG, Beschl. v. 24.05.1977 – 2 BvR 988/75 = BVerfGE 44, 353 (372 f.); BVerfG, Beschl. v. 26.04.1994 – 1 BvR 1689/88 = BVerfGE 90, 255 (260); BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96 = BVerfGE 101, 361 (382 f.); BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = 120, 274 (311).

²⁶ St. Rspr. vgl. etwa BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 = BVerfGE 65, 1 (43); BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05 = BVerfGE 130, 151 (184).

²⁷ Vgl. BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83 = BVerfGE 65, 1 (45); BVerfG, Beschl. v. 13.06.2007 – 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05 = BVerfGE 118, 168 (185); BVerfG, Urt. v. 11.03.2008 – 1 BvR 2074/05, 1 BvR 1254/07 = BVerfGE 120, 378 (398 f.); BVerfG, Beschl. v. 24.01.2012 – 1 BvR 1299/05 = BVerfGE 130, 151 (183 f.).

²⁸ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (311 ff.); gegen die Auffassung des BVerfG, der Schutz des Grundrechts auf informationelle Selbstbestimmung sei lückenhaft, u. a. Gersdorf, in: Gersdorf/Paal, Beck-OK Informations- und Medienrecht, 32. Edition, Stand 01.05.2021, Art. 2 GG, Rn. 23.

²⁹ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (313).



umfassende Informationen erlangt werden.³⁰ Formelhaft könnte man sagen, dass das Grundrecht auf informationelle Selbstbestimmung „kleine Eingriffe mit großer Wirkung“ nicht adäquat erfassen können soll.

Die Entwicklung des GGVIS aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG durch das BVerfG soll diese Lücke schließen und damit einen umfassenden Schutz gewährleisten. Bei der Abgrenzung zwischen dem GGVIS und dem Grundrecht auf informationelle Selbstbestimmung ist folglich mit Blick auf die Rechtsprechung des BVerfG ein quantitativer Aspekt zu berücksichtigen. So bietet das Grundrecht auf informationelle Selbstbestimmung Schutz vor dem Zugriff auf einzelne persönliche Daten, das GGVIS dagegen schützt vor dem Zugriff auf einen umfassenden Datenbestand, der in einem informationstechnischen System gespeichert ist.³¹ Geschützt wird also das Vertrauen des Nutzers, dass die Vielzahl der auf seinen Speichermedien gelagerten Daten vertraulich bleibt.

A benutzt sowohl beruflich als auch privat Computer, also informationstechnische Systeme, die ggf. insbesondere nach Maßgabe des § 5 Abs. 2 Nr. 11 Alt. 1 LVSG dem Zugriff durch den Verfassungsschutz ausgesetzt sein könnten. Mithin ist auch insoweit der Schutzbereich eröffnet.

Außerdem bietet das Grundrecht auf informationelle Selbstbestimmung nach Ansicht des BVerfG keinen Schutz vor Maßnahmen im Vorfeld der Ausspähung, also etwa vor der bloßen Infiltration des Systems. Diese alleine bewirkt nämlich noch keine Erhebung, geschweige denn eine Speicherung, Verarbeitung oder Weitergabe von personenbezogenen Daten.³² Doch bestehe mit Blick auf die grundrechtliche Sensibilität der Installation einer Ausspähungssoftware bereits zu diesem Zeitpunkt ein Bedürfnis nach umfassendem Schutz.³³ Im vorliegenden Fall birgt schon die Maßnahme nach § 5 Abs. 2 Nr. 11 Alt. 1 LVSG eine solche Bedrohung.

³⁰ Zur Kritik hierzu m. w. N.: *Gersdorf*, in: *Gersdorf/Paal*, Beck-OK Informations- und Medienrecht, 32. Edition, Stand: 01.05.2021, Art. 2 GG, Rn. 23.

³¹ *Gersdorf*, in: *Gersdorf/Paal*, Beck-OK Informations- und Medienrecht, 32. Edition, Stand: 01.05.2021, Art. 2 GG, Rn. 24.

³² BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (313). Gegen die Auffassung des BVerfG, der Schutz der Integrität sei nicht in das Grundrecht auf informationelle Selbstbestimmung einzubetten, u. a. *Gersdorf*, in: *Gersdorf/Paal*, Beck-OK Informations- und Medienrecht, 32. Edition, Stand: 01.05.2021, Art. 2 GG, Rn. 23.

³³ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (311 ff.).



Auch diese Schutzlücke zu schließen ist ein dogmatischer Grund der Entwicklung des GGVIS, welches schon die Integrität des informationstechnischen Systems schützt.

2. Eingriff

Ferner müsste ein Eingriff in den Schutzbereich des Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG vorliegen. Nach dem sog. klassischen Eingriffsbegriff müsste es sich um eine finale, unmittelbare, rechtsförmige und zwangsweise durchsetzbare staatliche Maßnahme handeln. Darunter fallen Maßnahmen wie die Erhebung, Speicherung, Verwertung und Weitergabe personenbezogener Daten (ESVW) sowie dazu vorgelagerte Maßnahmen, die der ESVW dienen.

Ein Eingriff liegt somit in doppelter Hinsicht vor: Die Infiltration des Systems (1. Alt.) ermächtigt final zu einem heimlichen Zugriff auf informationstechnische Systeme und stellt mithin einen Eingriff im Sinne einer vorgelagerten Maßnahme in die Integrität des informationstechnischen Systems dar. Das Ausspähen des informationstechnischen Systems (Alt. 2) gestattet den Zugriff auf Speichermedien, die dem Herrschaftsbereich der A unterfallen und stellt folglich einen Eingriff in Form der ESVW in die geschützten Datenbestände der A dar.

Anmerkung: Die folgenden Ausführungen nehmen keine Differenzierung zwischen Alt. 1 und 2 des § 5 Abs. 2 Nr. 11 LVSG vor, da die Infiltration (Alt. 1) des Systems das Ausspähen (Alt. 2) erst ermöglicht und hinsichtlich beider dadurch zwangsläufig miteinander verbundenen Alternativen die Argumentation konvergiert.

3. Rechtfertigung

Fraglich ist, ob der Eingriff gerechtfertigt ist. Das Recht auf freie Entfaltung der Persönlichkeit (und somit auch das GGVIS) ist begrenzt durch die Rechte anderer, die verfassungsmäßige Ordnung und das Sittengesetz (sog. Schrankentrias des Art. 2 Abs. 1 GG). Zur verfassungsmäßigen Ordnung i. S. d. Vorschrift gehören alle formell und materiell verfassungsgemäßen Gesetze (die beiden anderen Elemente der Schrankentrias – Sittengesetz, Rechte anderer – kommen hier nicht in Betracht).

Es stellt sich also die Frage, ob § 5 Abs. 2 Nr. 11 LVSG formell und materiell verfassungsgemäß ist. Bedenken gegen die formelle Verfassungsmäßigkeit bestehen mangels entgegenstehender Angaben im Sachverhalt nicht.



a) Bestimmtheitsgebot

Im Datenschutzrecht ist es erforderlich, dass Erhebungszweck und die einzelnen Schritte der Datenverarbeitung klar aus der Eingriffsnorm hervorgehen.

Indem § 5 Abs 2 Nr. 11 LVSG auf den Straftatenkatalog des § 100a StPO verweist, wird dem Bestimmtheitsgrundsatz hinreichend entsprochen.

b) Verhältnismäßigkeitsgrundsatz

Überdies müsste § 5 Abs. 2 Nr. 11 LVSG den sich aus dem Rechtsstaatsprinzip bzw. dem Wesen der Grundrechte³⁴ selbst ergebenden Verhältnismäßigkeitsgrundsatz wahren. Die Norm müsste hierzu einen legitimen Zweck verfolgen, geeignet, erforderlich und zumutbar sein.

Aufgrund des breiten und umfassenden Eingriffes in das GGVIS, dem aufgrund der Heimlichkeit der Maßnahme noch eine zusätzliche Intensivität verliehen ist, kommt als legitimer Zweck nur der Schutz eines überragend wichtigen Rechtsgutes in Betracht.

§ 5 Abs. 2 Nr. 11 LVSG verfolgt das Ziel, durch Infiltration und Ausspähen eine jeweils konkrete Gefahr für ein überragend wichtiges Rechtsgut (hier nach Maßgabe des § 100a StPO) abzuwenden. Dies stellt ein legitimes Ziel dar. Auch ist § 5 Abs. 2 Nr. 11 LVSG zur Zweckerreichung geeignet. Ein mildereres, gleich effektives Mittel ist nicht ersichtlich; insbesondere werden von den vergleichbaren Maßnahmen der StPO – die ohnehin lediglich im Strafverfahren greifen – nicht alle Konstellationen des LVSG erfasst. Mithin ist auch die Erforderlichkeit gegeben.

Es stellt sich jedoch die Frage, ob der Eingriff auch verhältnismäßig im engeren Sinne (also zumutbar) ist. Die Online-Durchsuchung stellt einen schwerwiegenden Eingriff dar, da der auf einem Computer gespeicherte Datenbestand weitreichende Rückschlüsse auf die Persönlichkeit des:der Betroffenen ermöglicht.

Ein solcher Eingriff ist nur zumutbar, wenn die Ermächtigungsgrundlage ihn davon abhängig macht, dass bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend

³⁴ Vgl. BVerfG, Beschl. v. 15. 12.1965 – 1 BvR 513/65 = BVerfGE 19, 342 (348 f.); Grzeszick, in: Maunz/Dürrig, Grundgesetz-Kommentar, 94. EL Januar 2021, Art. 20 Rn. 108.



wichtiges Rechtsgut hinweisen.³⁵ Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist mithin verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.

Vorliegend soll eine Befugnis der Verfassungsschutzbehörden zur Durchführung einer Maßnahme nach § 5 Abs. 2 Nr. 11 LVSG nur bei Verdacht auf Begehung einer schweren Straftat i. S. d. § 100a Abs. 2 StPO gegeben sein. § 100a Abs. 2 StPO enthält einen Katalog von Straftatbeständen, welche die soeben genannten überragend wichtigen Rechtsgüter in erheblichem Maße berühren und daher gewissermaßen exemplarisch für die Anforderungen des BVerfG herangezogen werden können. Hinsichtlich dieser Begrenzung der Befugnis auf den Verdacht der Begehung von Kapitaldelikten ist die Zumutbarkeit zu bejahen.

c) Kernbereichsschutz

Eine weitere Anforderung an die Verfassungsmäßigkeit eines Eingriffes in das GGVIS ist das Vorliegen kernbereichsschützender Regelungen.³⁶ Dies folgt aus dem vor staatlichen Eingriffen stets entzogenen Menschenwürdekern des GGVIS, der dem:der Einzelnen stets einen Kernbereich privater Lebensgestaltung garantiert.³⁷ Dieser Schutz des „Kernbereich[s] privater Lebensgestaltung beansprucht gegenüber allen Überwachungsmaßnahmen Beachtung“³⁸; bei deren Durchführung muss „dem Kernbereichsschutz 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.

³⁵ BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 (220).

³⁶ BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 (220); Gersdorf, in: Gersdorf/Paal, Beck-OK Informations- und Medienrecht, 32. Edition Stand 01.05.2021, Art. 2 GG, Rn. 29.

³⁷ BVerfG, Urt. v. 03.03.2004 – 1 BvR 2378/98, 1 BvR 1084/99 = BVerfGE 109, 279 (313 f.).

³⁸ BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 (277).



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.“³⁹

Vorliegend sind keine derart ausgestalteten Regelungen ersichtlich; Datenzugriff und -verwertung werden nicht durch besondere Verfahren geschützt. § 5 Abs. 2 Nr. 11 LVSG ist mithin bereits in Ermangelung kernbereichsschützender Regelungen materiell verfassungswidrig.

d) Richtervorbehalt

„Die heimliche Infiltration eines informationstechnischen Systems ist [überdies] grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.“⁴⁰ Der Gesetzgeber darf eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein:e Richter:in.⁴¹

§ 5 Abs. 2 Nr. 11 LVSG enthält keine Regelungen, nach denen die betreffenden Maßnahmen nur auf Anordnung durch eine:n Richter:in oder eine vergleichbare unabhängige Kontrollinstanz durchgeführt werden können. Vielmehr steht die Durchführung der entsprechenden Maßnahmen im alleinigen Ermessen der Verfassungsschutzbehörden. Insofern ist § 5 Abs. 2 Nr. 11 LVSG materiell verfassungswidrig.

Anmerkung: Die Ausführungen zu Kernbereichsschutz und Richtervorbehalt gelten ebenso für die übrigen genannten Grundrechte, mithin Art. 10 GG, Art. 13 GG und – sofern dafür Anhaltspunkte im Sachverhalt vorhanden sind, gegebenenfalls auch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung).

4. Zwischenergebnis

§ 5 Abs. 2 Nr. 11 LVSG verstößt gegen Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und ist mithin materiell verfassungswidrig

³⁹ BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 = BVerfGE 141, 220 (278); siehe auch BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274 (337).

⁴⁰ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274, Ls. 3.

⁴¹ BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07 = BVerfGE 120, 274, (332).



C. Endergebnis

Die Verfassungsbeschwerde der A hat somit Aussicht auf Erfolg.