Anlage 5: Besondere Vorgaben zu Intensiveingriffen
• Wohnraumüberwachung und Online-Durchsuchung durch den Verfassungsschutz sind nur zur Abwehr einer dringenden bzw. konkretisierten Gefahr für bedeutende Rechtsgüter zulässig • Die Befugnis ist subsidiär für den Fall, dass geeignete polizeiliche Hilfe für das bedrohte Rechtsgut nicht rechtzeitig erlangt werden kann • Die Maßnahmen dürfen sich nicht unmittelbar gegen Dritte richten; unter bestimmten Voraussetzungen dürfen auch die Wohnungen bzw. Informationssysteme Dritter Gegenstand der Maßnahmen sein • Die Anordnung der Maßnahmen darf nur durch eine unabhängige Stelle erfolgen • Jede weitere Nutzung der Daten aus Wohnraumüberwachung und Online-Durchsuchung durch die erhebende Verfassungsschutzbehörde selbst und ihre Übermittlung ist nur zur Abwehr einer den Erhebungsvoraussetzungen entsprechenden Gefahr zulässig

Anforderungen BVerfGE v. 24.5.2022:

Zur Wohnraumüberwachung

Eine präventive Wohnraumüberwachung durch den Verfassungsschutz ist nach der Entscheidung des BVerfG nur **zur Abwehr** einer **dringenden** Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr (vgl. Art. 13 Abs. 4 GG), zulässig. Dabei sind nicht nur an das Ausmaß, sondern auch Wahrscheinlichkeit des Schadenseintritts (Rn. 169) strenge Anforderungen zu stellen (Rn. 177).

Eine dringende Gefahr im Sinne des Art. 13 Abs. 4 GG liegt vor, wenn eine konkrete Sachlage oder ein Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit in allernächster Zukunft einen größeren Schaden verursachen wird. Das Kriterium der Dringlichkeit bezieht sich dabei auf das Ausmaß und die Wahrscheinlichkeit des Schadens (Rn. 297).

Da die Wohnraumüberwachung nur zur Abwehr einer dringenden Gefahr zulässig ist, ist nur eine **subsidiäre Befugnis** für den Fall, dass geeignete polizeiliche Hilfe für das bedrohte Rechtsgut ansonsten nicht rechtzeitig erlangt werden kann, zulässig (vgl. § 9 Abs. 2 Satz 1 BVerfSchG – Rn. 178).

Hinsichtlich des Kreises der betroffenen Personen darf sich die Wohnraumüberwachung **nicht unmittelbar gegen Dritte**, sondern nur gegen diejenigen als Zielperson richten, die für die Gefahr verantwortlich sind. Eine Überwachung der Wohnung eines Dritten kann erlaubt werden, wenn aufgrund bestimmter Tatsachen vermutet werden kann, dass sich die Zielperson dort zur Zeit der Maßnahme aufhält, sie dort für die Beobachtung relevante Gespräche führen wird und eine Überwachung ihrer Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht (mittelbare Maßnahme – Rn. 211 unter Verweis auf BVerfGE 141, 220, 273 f., Rn. 115).

Eine **vorherige Kontrolle durch eine unabhängige Stelle** in Form einer richterlichen Anordnung (vgl. Art. 13 Abs. 4 GG) ist erforderlich (Rn. 214).

Daten aus Wohnraumüberwachungen unterliegen einer **Zweckbindung**:
Jede weitere Nutzung der Daten durch die erhebende (Verfassungsschutz-)Behörde in einem neuen Verfahren – sei es zu dem Zweck der ursprünglichen Datenerhebung oder zu einem anderen Zweck – ist nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechend dringenden Gefahr erforderlich ist (Rn. 228, 271).

Für die Übermittlung nachrichtendienstlich erhobener Daten an eine Gefahrenabwehrbehörde gilt die allgemeine Eingriffsschwelle für heimliche Überwachungsmaßnahmen der Gefahrenabwehrbehörde, also die konkrete bzw. konkretisierte Gefahr und bei einer Wohnraumüberwachung die dringende Gefahr (Rn. 248). Da diese Anforderungen bereits durch die weitere Nutzung durch die erhebende (Verfassungsschutz-)Behörde selbst gelten, muss die Eingriffsschwelle auch für die Übermittlung von Daten an andere Behörden Anwendung finden (vgl. Rn. 226 ff., 270 f.).

Zur Onlinedurchsuchung

Onlinedurchsuchungen sind nach dem BVerfG ebenfalls nur **zur Abwehr einer mindestens konkretisierten Gefahr** zulässig, also wenn bestimmte Tatsachen bereits den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen (Rn. 176 unter Verweis auf BVerfGE 141, 220, 272 f., Rn. 112). Es müssen nach BVerfGE 141, 220, 272 f., Rn. 112 zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen.

An dem betroffenen Geschehen müssten bestimmte Personen beteiligt sein, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme **gezielt** gegen sie eingesetzt und weitgehend auf sie **beschränkt** werden kann (Rn. 176).

Da die Onlinedurchsuchung nur zur Abwehr einer konkretisierten Gefahr zulässig ist, kann sie nur als **subsidiäre Befugnis** für den Fall, dass geeignete polizeiliche Hilfe für das bedrohte Rechtsgut ansonsten nicht rechtzeitig erlangt werden kann, geregelt werden (Rn. 178).

Die Maßnahme darf sich **nicht unmittelbar gegen Dritte** richten, sondern nur gegen diejenigen als Zielpersonen, die für die Gefahr verantwortlich sind. Die Online-Durchsuchung kann auf informationstechnische Systeme Dritter erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort **relevante Informationen speichert** und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Beobachtungsziels **nicht ausreicht** (Rn. 211).

Die Online-Durchsuchung muss durch eine unabhängige Instanz angeordnet werden (Rn. 218). Nach BVerfGE 120, 274, 332 ist grds. richterliche Anordnung notwendig, eine andere Stelle ist dann zulässig, wenn gleiche Gewähr für Unabhängigkeit und Neutralität wie bei Richtern besteht.

Jede **weitere Nutzung** der Daten durch die erhebende (Verfassungsschutz-)Behörde in einem neuen Verfahren ist nur dann zweckentsprechend, wenn sie aufgrund einer zumindest konkretisierten Gefahr erforderlich ist (Rn. 228, 271).

Die Übermittlung personenbezogener Daten, die mittels Online-Durchsuchung gewonnen wurden, an Gefahrenabwehrbehörden ist nur zulässig zur Abwehr einer Gefahr, die den Erhebungsvoraussetzungen entspricht, bei der Online-Durchsuchung also die konkretisierte Gefahr (Rn. 248). Dies muss auch für die Übermittlung an sonstige Stellen gelten, da diese Anforderungen bereits durch die weitere Nutzung durch die erhebende Behörde selbst gelten (vgl. Rn. 226 ff., 270 f.).

<u>Regelungsvorschlag</u>

§/Art. [A] – Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung

(1) [1]Das Landesamt darf zur Abwehr einer dringenden Gefahr für

1. den Bestand oder die Sicherheit des Bundes oder eines Landes,
2. Leib, Leben oder Freiheit einer Person oder
3. Sachen, deren Erhaltung im besonderen öffentlichen Interesse geboten ist,

bei der Erhebung personenbezogener Daten im Schutzbereich von Art. 13 GG [und Art. XX der Landesverfassung] verdeckt technische Mittel einsetzen, um das nichtöffentlich gesprochene Wort abzuhören und aufzuzeichnen sowie Lichtbilder und Bildaufzeichnungen herzustellen.

[2]Werden in Privaträumen Gespräche mit Personen des persönlichen Vertrauens geführt, ist die Maßnahme unzulässig.

[3]Dies gilt nicht, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass

1. *den Gesprächen insgesamt ein höchstvertraulicher Charakter fehlen wird oder*
2. *die Gespräche unmittelbar die Besprechung oder Planung von Straftaten, die sich gegen die in Satz 1 genannten Rechtsgüter richten, zum Gegenstand haben werden.[1]*

[4]Zur Vorbereitung und Durchführung der Maßnahme darf die Wohnung auch ohne Wissen des Inhabers und der Bewohner betreten werden, wenn dies ausdrücklich angeordnet wurde.

[5]Die Maßnahme ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtlos oder wesentlich erschwert wäre und geeignete polizeiliche Hilfe für das betroffene Rechtsgut nicht rechtzeitig erlangt werden kann.

(2) [1]Die Maßnahme darf sich nur gegen eine Person richten, von der auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie für die Gefahr im Sinne des Abs. 1 verantwortlich ist (Zielperson), und nur in deren Wohnung durchgeführt werden.

[2]In der Wohnung einer anderen Person ist die Maßnahme zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. die Zielperson sich dort zur Zeit der Maßnahme aufhält,
2. sich dort für die Erforschung des Sachverhalts relevante Informationen ergeben werden und
3. eine Maßnahme in der Räumlichkeit der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.

(3) Personenbezogene Daten aus Maßnahmen nach Absatz 1 dürfen nur zur Abwehr einer Gefahr im Sinne des Absatzes 1 weiterverarbeitet werden.

(4) Personenbezogene Daten aus Maßnahmen nach Absatz 1, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

§/Art. [B] – Verdeckter Zugriff auf informationstechnische Systeme

(1) Auf informationstechnische Systeme, die der Betroffene in der berechtigten Erwartung von Vertraulichkeit als eigene nutzt und die seiner selbstbestimmten

[1] Zu den Erwägungen hinter der Kernbereichsregelung vgl. Anlage 4.

Verfügung unterliegen, darf das Landesamt zur Abwehr einer konkretisierten Gefahr für die in [A] Abs. 1 Satz 1 genannten Rechtsgüter verdeckt mit technischen Mitteln nur zugreifen, um

1. Zugangsdaten und verarbeitete Daten zu erheben oder
2. zur Vorbereitung einer Maßnahme nach Nr. 1 spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln.

[2] [A] Abs. 1 Satz 2 und 3 gilt entsprechend.

(2) [1]Durch technische Maßnahmen ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden und
3. *Daten, die den Kernbereich privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden.*

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

[3]Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) [1]Die Maßnahme darf sich nur gegen die Zielperson richten und nur durch Zugriff auf deren informationstechnisches System durchgeführt werden.

[2]Der Zugriff auf informationstechnische Systeme anderer ist zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. die Zielperson deren informationstechnisches System benutzt oder benutzt hat,
2. sich dadurch für die Abwehr der Gefahr relevante Informationen ergeben werden und
3. ein Zugriff auf das informationstechnische System der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.

(4) Personenbezogene Daten aus Maßnahmen nach Absatz 1 dürfen nur zur Abwehr einer Gefahr im Sinne des Absatzes 1 weiterverarbeitet werden.

§/Art. [C] – Verfahren bei den Maßnahmen nach [A] und [B]

(1) [1]Der Einsatz technischer Mittel nach den [A] und [B] bedarf einer richterlichen Anordnung.[2]

[2]Bei Gefahr im Verzug kann die Behördenleitung oder ihre Vertretung die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen.

(2) [1]Die Anordnung ist auf höchstens einen Monat zu befristen.

[2]Verlängerungen um jeweils nicht mehr als einen weiteren Monat sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(3) *Anmerkung:*
Hier ist ein Absatz zum Kernbereichsschutz bei Wohnraumüberwachungen einzufügen. Je nachdem, welcher Alternative zum Kernbereichsschutz gefolgt wird (vgl. Anlage 4; S. 5 unten) ist dies

- *der §/Art. C Absatz 3 in Anlage 4 auf Seite 10 (Alternative 1) oder*
- *der §/Art. C Absatz 3 in Anlage 4 auf Seite 16 (Alternative 2)*

(4) *Anmerkung:*
Hier ist ein Absatz zum Kernbereichsschutz beim Verdeckten Zugriff auf informationstechnische Systeme einzufügen.
Je nachdem, welcher Alternative zum Kernbereichsschutz gefolgt wird (vgl. TP 1.5; S. 5 unten) ist dies

- *der §/Art. C Absatz 4 in Anlage 4 auf Seite 11 (Alternative 1) oder*
- *der §/Art. C Absatz 4 in Anlage 4 auf Seite 16f. (Alternative 2)*

(5) [1]§ 4 Abs. 1, 2 Satz 1 und 2 sowie Abs. 3, § 9, § 10 Abs. 2 und 3, § 11 Abs. 1 und 2 sowie § 12 Abs. 1 und 3 G 10 sind entsprechend anzuwenden; für den Verzicht auf die Kennzeichnung bei der Übermittlung sowie das Unterbleiben und die weitere Zurückstellung der Mitteilung an Betroffene gilt Absatz 1 entsprechend.

[2] Alternativ kann die Online-Durchsuchung auch durch eine unabhängige Stelle angeordnet werden, wenn diese die gleiche Gewähr für Unabhängigkeit und Neutralität bietet wie der Richter (BVerfG, Urt. v. 26.4.2022 – Rn. 218 unter Verweis auf BVerfGE 120, 274, 332).

[2]Eine Mitteilung kann auch auf Dauer unterbleiben, wenn überwiegende Interessen eines Betroffenen entgegenstehen oder wenn die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand zu ermitteln ist.

(6) [1]Dient der Einsatz technischer Mittel nach [A] ausschließlich dem Schutz der für den Verfassungsschutz bei einem Einsatz in Wohnungen tätigen Personen, erfolgt die Anordnung abweichend von Abs. 1 durch die Behördenleitung oder ihre Vertretung.

[2]Eine anderweitige Verwendung der hierbei erlangten Erkenntnisse ist nur zulässig, wenn zuvor [die unabhängige Stelle] festgestellt hat, dass die Maßnahme rechtmäßig ist und die Voraussetzungen des [A] Abs. 1 Satz 1 vorliegen; Abs. 1 Satz 2 gilt entsprechend.

[3]Bei der Übermittlung von erhobenen personenbezogenen Daten an andere Stellen finden die Vorschriften des [Übermittlungsvorschriften] entsprechende Anwendung.

[4]Im Übrigen sind die Daten unverzüglich zu löschen.

(7) [1]Zuständig für richterliche Entscheidungen nach den Abs. 1 bis 3 ist [der Richter/das Gericht]; über Beschwerden entscheidet das [Beschwerdegericht].

[2]Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend; die Rechtsbeschwerde ist ausgeschlossen.

Begründung

Der Regelungsvorschlag stützt sich im Wesentlichen auf die bisherigen Vorschriften des BayVSG und passt es an die Vorgaben des BVerfG aus der Entscheidung vom 26.4.2022 an.

Zu [A] – Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung

[A] regelt die Befugnis zum Einsatz des besonderen nachrichtendienstlichen Mittels der technischen Wohnraumüberwachung.

Gemäß [A] Absatz 1 Satz 1 sind diese Mittel nur zur Abwehr einer dringenden Gefahr für hinreichend gewichtige Schutzgüter zulässig. Der Zweck ist auf die Abwehr der dringenden Gefahr begrenzt (vgl. BVerfG, Urt. v. 26.4.2022 – Rn. 301). Eine dringende Gefahr im Sinne des Art. 13 Abs. 4 GG liegt vor, wenn eine konkrete Sachlage oder ein

Verhalten bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit in allernächster Zukunft einen größeren Schaden verursachen wird (vgl. BVerfG, Urt. v. 26.4.2022 – Rn. 297).

Hinreichend gewichtige Schutzgüter in diesem Sinne sind Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes; außerdem Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, wie wesentliche Infrastruktureinrichtungen und sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (BVerfG, Urt. v. 26.4.2022 – Rn. 299).

Da die Eingriffsschwelle an das Vorliegen einer dringenden Gefahr voraussetzt, ist die Wohnraumüberwachung als subsidiäre Befugnis gegenüber polizeilichen Maßnahmen zu regeln. Da es den Verfassungsschutzbehörden an operativen Befugnissen fehlt, käme es andernfalls durch die Informationsübermittlung an die Polizei zu einem erneuten Grundrechtseingriff (BVerfG, Urt. v. 26.4.2022 – Rn.178 ff., 303).

Absatz 2 bestimmt, dass sich die Wohnraumüberwachung nicht unmittelbar gegen Dritte, sondern nur gegen diejenigen Personen richtet, die für die Gefahr im Sinne des Absatzes 1 Satz 1 verantwortlich sind. Er schützt damit unbeteiligte Dritte (BVerfG, Urt. v. 26.4.2022 – Rn. 211 ff.).

In Abweichung davon kann entsprechend der Vorgaben des Bundesverfassungsgerichts nach der Regelung des [A] Absatz 2 Satz 2 die Überwachung der Wohnung eines Dritten erlaubt werden, wenn aufgrund bestimmter Tatsachen vermutet werden kann, dass sich die Zielperson dort zur Zeit der Maßnahme aufhält, sie dort für die Beobachtung relevante Gespräche führen wird und eine Überwachung ihrer Wohnung allein zur Erforschung des Sachverhalts nicht ausreicht (mittelbare Maßnahme – BVerfG, Urt. v. 26.4.2022 – Rn. 211 ff.).

Daten, die aufgrund einer Wohnraumüberwachung erlangt wurden, dürfen nach dem Bundesverfassungsgericht durch die (Verfassungsschutz-)Behörde nur weiter genutzt werden, wenn dies zur Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist (BVerfG, Urt. v. 26.4.2022 – Rn. 228). Dies gilt auch für die Übermittlung dieser Daten zur Gefahrenabwehr und ihre sonstige Weiterverarbeitung (vgl. BVerfG, Urt. v. 26.4.2022 – Rn. 228, 248, 271).

Nach Absatz 4 sind personenbezogene Daten aus optischen Wohnraumüberwachungen von einer Übermittlung an die Strafverfolgungsbehörden ausgeschlossen. Nach der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz erlaubt Art. 13 Abs. 3 GG für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung. Dies darf durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden (so BVerfG, Urt. v.

20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 – BVerfGE 141, 220, Rn. 317). Dies gilt für Nachrichtendienste genauso wie für Polizeibehörden.

Zu §/Art. [B] – Verdeckter Zugriff auf informationstechnische Systeme

[B] regelt die Befugnis zur sogenannten verdeckten Online-Datenerhebung.

Diese ist nach der Entscheidung des BVerfG nur zur Abwehr einer mindestens konkretisierten Gefahr zulässig, also wenn zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die hinreichend gewichtigen Schutzgüter des [A] Abs. 1 Satz 1 bestehen (BVerfG, Urt. v. 26.4.2022 – Rn. 176; BVerfGE 141, 220, 272 f., Rn. 112).

Eine solche ist nach dem BVerfG (Urt. v. 26.4.2022 – Rn. 176; BVerfGE 141, 220, 272 f., Rn. 112) gegeben, wenn bestimmte Tatsachen bereits den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen, das bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahmen gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

Die Verweisung auf [A] Absatz 1 Satz 2 und 3 in Absatz 1 Satz 2 übernimmt die Betretungsbefugnis zur Vorbereitung und die subsidiäre Regelung der Befugnis entsprechend den Vorgaben des Bundesverfassungsgerichts (BVerfG, Urt. v. 26.4.2022 – Rn. 178).

Absatz 2 regelt, dass sicherzustellen ist, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden und Daten, die den Kernbereich privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden (vgl. BVerfG, Urt. v. 26.4.2022 – Rn. 285).

Daten, die aufgrund einer Online-Durchsuchung erlangt wurden, dürfen nach dem Bundesverfassungsgericht durch (die Verfassungsschutzbehörde) nur weiter genutzt werden, wenn dies zur Abwehr einer konkretisierten Gefahr im Sinne des Absatzes 1 erforderlich ist (BVerfG, Urt. v. 26.4.2022 – Rn. 228). Das Gleiche gilt für die Übermittlung dieser Daten an andere Stellen und ihre sonstige Weiterverarbeitung (vgl. BVerfG, Urt. v. 26.4.2022 – Rn. 228, 248, 271).

Zu §/Art. [C] – Verfahren bei den Maßnahmen nach [A] und [B]

[C] regelt die Verfahrensanforderungen an die Maßnahmen nach [A] und [B].

Maßnahmen, die in den Schutzbereich des Wohnungsgrundrechts eingreifen, werden ebenso wie Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme unter Richtervorbehalt gestellt.

Als alternative Regelung ist nach der Rechtsprechung des BVerfG auch zulässig, dass die Online-Durchsuchung durch eine unabhängige Stelle angeordnet werden, solange diese die gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie der Richter (vgl. BVerfG, Urt. v. 26.4.2022 – Rn. 218 unter Verweis auf BVerfGE 120, 274, 332).

Satz 2 regelt die nach Art. 13 Abs. 4 Satz 2 GG zulässige Eilzuständigkeit der Behördenleitung (Präsidentin oder Präsident) und ihrer Vertretung bei Gefahr im Verzug.

Absatz 2 Satz 1 schreibt eine Befristung der Anordnung auf höchstens einen Monat vor. Zwar sind nach dem Wortlaut des Art. 13 Abs. 3 Satz 2 GG nur repressive Maßnahmen der verdeckten akustischen Wohnraumüberwachung zu befristen (vgl. hierzu BVerfGE 109, 279/316). Eine entsprechende verfahrensrechtliche Beschränkung ist im Hinblick auf die hohe Schutzwürdigkeit der betroffenen Grundrechte und die Intensität des Eingriffs auch für die präventive technische Wohnraumüberwachung und die Online-Datenerhebung geboten. Satz 2 erlaubt Verlängerungen um jeweils bis zu einem Monat, solange die Anordnungsvoraussetzungen fortbestehen. Satz 3 verweist hinsichtlich der Prüf-, Kennzeichnungs- und Löschpflichten sowie des Verfahrens auf Vorschriften des Artikel 10-Gesetzes.

Die präventive Wohnraumüberwachung gemäß Art. 13 Abs. 4 GG steht im Gegensatz zur repressiven akustischen Überwachung (Art. 13 Abs. 3 Satz 3 GG) nicht unter einem qualifizierten Richtervorbehalt. Aus der Rechtsprechung des Bundesverfassungsgerichts ergibt sich insoweit nichts Anderes (BVerfGE 109, 279/357 f.).

<u>sonstige Hinweise:</u>

- Zum Schutz Dritter siehe auch Anlage 2.
- Zur unabhängige Vorkontrolle bei Eingriffen in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme; siehe Anlage 4.
- Die Regelungen sind – je nach gewähltem Regelungsmodell – um die Vorschriften für den Kernbereichsschutz bei Wohnraumüberwachung und Online-Durchsuchung zu ergänzen, s. Anlage 4.
- Zur Übermittlung von Daten im Übrigen siehe Anlage 6.