Entscheidungsbesprechung

BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19[1]

Trojaner I – der präventive Einsatz von Telekommunikationsüberwachungs- und Quellen-Telekommunikationsüberwachungsmaßnahmen

1. Art. 10 Abs. 1 GG schützt vor den spezifischen Gefahren, die mit einer räumlich distanzierten Kommunikation einhergehen, und gewährleistet insoweit eine Privatheit auf Distanz. […]. Im Lichte seiner Entwicklungsoffenheit [erfasst] das Grundrecht auch […] mithilfe von Telekommunikationstechniken über Distanz transportierte Daten.

2. Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht) schützt insbesondere vor heimlichen Zugriffen durch eine Online-Durchsuchung, ist hierauf aber nicht beschränkt (Anschluss an BVerfGE 120, 274).

   a) Schutzgegenstand sind IT-Systeme, die aufgrund ihrer technischen Funktionalität allein oder durch ihre technische Vernetzung Daten einer betroffenen Person in einem Umfang und einer Vielfalt vorhalten 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.

   b) […] Das IT-System-Grundrecht schützt nicht nur die Vertraulichkeit der Daten, die durch Datenerhebungsvorgänge verletzt wird, sondern verlagert diesen Schutz nach vorne. Denn bereits mit dem Zugriff auf ein IT-System entsteht eine besondere Gefährdungslage für die dort erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten. Der Gewährleistungsgehalt des IT-System-Grundrechts geht […] über den Schutz personenbezogener Daten hinaus und vermittelt einen insoweit vorgelagerten Schutz der Persönlichkeit.

3. Darf die Überwachung und Aufzeichnung laufender Telekommunikation auch in der Weise erfolgen, dass mit technischen Mitteln in von Betroffenen genutzte IT-Systeme eingegriffen wird (Quellen-Telekommunikationsüberwachung), begründet dies sowohl einen Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis als auch in das IT-System-Grundrecht. Solche Maßnahmen sind an beiden Grundrechten zu messen (Abweichung von BVerfGE 141, 220).

4. Den im präventiven Bereich erforderlichen Rechtsgüterschutz kann der Gesetzgeber auch in der Weise sicherstellen, dass er an hinreichend gewichtige Straftaten anknüpft. Er kann ihn aber auch unabhängig vom Gewicht der Straftat […] dergestalt sicherstellen, dass er eine hinreichende Qualifizierung als terroristische Straftat im Einzelfall vorsieht.

(Amtliche Leitsätze, gekürzt durch *Verf.*)

*Carolin Kemper, Potsdam**

* Postdoctoral Researcher in der Forschungsgruppe Technology Regulation am Hasso-Plattner-Institut in Potsdam.
[1] Die Entscheidung ist veröffentlicht in NJW 2025, 3424.

I. Einleitung

Staatliche Überwachungsmaßnahmen beschäftigen das BVerfG regelmäßig[2] und lösen meist verfassungsgerichtliche Kritik aus. Der Trojaner-I-Beschluss stellt eine Ausnahme dar: Das BVerfG befand die gesetzliche Grundlage für Überwachungseingriffe für verfassungsmäßig.[3] Teilweise wies es die Verfassungsbeschwerde bereits als unzulässig zurück.

Zentraler Gegenstand des Beschlusses sind die Befugnisse des nordrhein-westfälischen Polizeigesetzes in § 20c PolG NRW zur Telekommunikationsüberwachung (TKÜ) und zur sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Während die TKÜ mithilfe des Anbieters von Telekommunikationsdiensten, d.h. z.B. der Telekom, durchgeführt wird, ist die Quellen-TKÜ notwendig, wenn die Zielperson verschlüsselt kommuniziert. In diesem Fall muss das betroffene Gerät (typischerweise ein Smartphone) infiltriert werden, um die Kommunikation mitzeichnen zu können. Es handelt sich daher um „staatliches Hacking".[4] Im Gegensatz zur Online-Durchsuchung, die es Polizeibehörden erlaubt, IT-Systeme zu durchforsten, erlaubt die Quellen-TKÜ lediglich die Aufzeichnung laufender Kommunikationsvorgänge.

Der Trojaner-I-Beschluss steht in engem Zusammenhang mit dem zeitgleich ergangenen Trojaner-II-Beschluss, bei dem sich der *Erste Senat* mit der strafprozessualen Seite der „Staatstrojaner"-Problematik befasst. Allerdings beanstandete er die strafprozessualen Grundlagen der Telekommunikationsüberwachung (§ 100a StGB) und der Online-Durchsuchung (§ 100b StPO).[5] Die „Neuerungen" der beiden Trojaner-Entscheidungen beziehen sich vor allem auf die Erweiterung des Schutzgehalts des Fernmeldegeheimnisses in Art. 10 Abs. 1 GG und die Schärfung des Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG), das das BVerfG nunmehr als „IT-System-Grundrecht" bezeichnet. Außerdem klärt das BVerfG das Verhältnis der konkurrierenden Grundrechte sowie die Anforderungen an die verfassungsrechtliche Rechtfertigung von TKÜ- und Quellen-TKÜ-Maßnahmen. Dabei distanziert es sich an einigen Stellen von der „Online-Durchsuchung"-Entscheidung aus dem Jahr 2008.[6]

Der Trojaner-I-Beschluss ist vor allem für die Rechts*wissenschaft* bedeutend – praktisch finden Infiltrationen wie die Quellen-TKÜ dagegen relativ selten statt: Im Jahr 2023 wurde die Maßnahme 130 Mal angeordnet und kam in 68 Fällen zum Einsatz.[7]

II. Sachverhalt

Die Beschwerdeführenden sehen ihre Grundrechte durch § 20c PolG NRW verletzt. Diese Rechtsgrundlage, die seit 2018 besteht, ermöglicht Polizeibehörden die Datenerhebung durch die Überwachung der laufenden Telekommunikation. § 20c Abs. 2 PolG NRW ermöglicht zudem die Überwachung durch Infiltration zur Umgehung von Verschlüsselung.

Die Maßnahme sei laut Gesetzgebung notwendig zur Abwehr von Gefahren durch Terrorismus, aber auch zur Bekämpfung von Alltagskriminalität, die „zunehmend organisiert begangen werde".[8] Denn Telekommunikation findet heutzutage meist verschlüsselt statt, z.B. mit Apps wie WhatsApp oder

[2] Siehe z.B. BVerfGE 120, 274 ff.; 125, 260 ff.

[3] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 84 ff.

[4] Vgl. hierzu bspw. *Derin/Golla*, NJW 2019, 1111 ff.; *Kipker*, ZRP 2016, 88 ff.; *Wischmeyer*, Informationssicherheit, 2023, S. 279 ff.

[5] Vgl. BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23 (Trojaner II), Rn. 179 ff.

[6] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 110, 121; vgl. auch Rn. 138.

[7] *Meister*, netzpolitik.org v. 5.8.2025 (26.2.2026).

[8] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 5.

Signal, die standardmäßig alle Nachrichten verschlüsseln und dadurch den sicherheitsbehördlichen Zugriff auf die Inhalte vereiteln. Daher müsse der Zugriff im Rahmen der Quellen-TKÜ auch „an der ‚Quelle' der Kommunikation erfolgen, an der die kommunizierten Inhalte noch nicht verschlüsselt oder wieder unverschlüsselt vorliegen – also vor Beginn der Verschlüsselung beim Sendegerät oder nach der Entschlüsselung beim Empfangsgerät".[9] Die Polizei darf daher nach § 20c Abs. 2 PolG NRW mit technischen Mitteln, d.h. mit „Staatstrojaner"-Software, in das IT-System eingreifen, um ausschließlich die laufende Kommunikation zu überwachen.

Gesetzliche Voraussetzung für die Überwachungsmaßnahmen ist entweder eine gegenwärtige Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib oder Leben einer Person oder die konkrete Wahrscheinlichkeit einer terroristischen Straftat in absehbarer Zeit (§ 20c Abs. 1 S. 1 PolG NRW). Die Quellen-TKÜ erfordert zusätzlich, dass der Eingriff in das IT-System „notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen" (§ 20c Abs. 2 S. 1 Nr. 2 PolG NRW). Nach § 20c Abs. 4 S. 1 PolG NRW müssen die Maßnahmen durch ein Amtsgericht angeordnet werden.

Die Beschwerdeführenden rügen Eingriffe in ihre Grundrechte aus Art. 2 Abs. 1 GG i.V.m. Art. 2 Abs. 1 GG durch § 20c PolG NRW, u.a. weil sie selbst bereits durch (Klima-)Aktivismus polizeilich auffällig geworden seien oder Kontakt mit Personen oder Gruppen hätten, die in Verfassungsberichten als extremistisch eingestuft sind.[10] Dadurch seien sie potenzielle Ziele von Überwachungsmaßnahmen nach § 20c PolG NRW. Alle Beschwerdeführenden führen an, dass sie Telekommunikationsanschlüsse sowie internetfähige IT-Systeme nutzen.[11]

III. Entscheidung und rechtliche Begründung des Gerichts

Die Verfassungsbeschwerde war nur teilweise zulässig, insoweit aber unbegründet.

1. Zulässigkeit

Das BVerfG wies die Verfassungsbeschwerde teilweise als unzulässig ab, u.a. weil die Beschwerdeführenden ihre Beschwerdebefugnis nicht hinreichend darlegt hätten.[12] Dies betrifft vor allem die Frage einer staatlichen Schutzpflicht in Bezug auf das IT-System-Grundrecht und inwiefern staatliches „Hacking" – und insbesondere das Zurückbehalten von Schwachstellen in IT-Systemen – zum Schutz der Allgemeinheit einzuschränken sei.[13] Das BVerfG beanstandet, dass die Beschwerdeführenden unzureichende Ausführungen zum Normkomplex des Datenschutz- und Cybersicherheitsrechts gemacht hätten.[14] Diese Handhabung kritisierte *Nicolas Ziegler* als „übermäßige Strenge […], die im Ergebnis zu einem Rechtsschutzdefizit" führe.[15]

[9] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 10.
[10] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 14 ff.
[11] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 20.
[12] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 51 ff.
[13] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 52.
[14] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 53.
[15] *Ziegler*, NVwZ 2025, 1803 (1808).

2. Grundrechtseingriffe durch die TKÜ in das Fernmeldegeheimnis (Art. 10 Abs. 1 GG)

Das BVerfG erweitert den Schutzgehalt des Fernmeldegeheimnisses umfassend auf die Vertraulichkeit jeglicher unkörperlicher Kommunikationsübertragung.[16] Dabei verweist es auf die veränderten technischen Gegebenheiten, insbesondere Kommunikationsdienste des Internets, d.h. beim Surfen, dem Hoch- und Herunterladen von Daten oder den Datenaustausch über sog. Cloud-Dienste.[17] Vom Schutz erfasst seien auch Rohdaten.[18]

> „Maßgeblich ist dabei, dass das Fernmeldegeheimnis einen Ausgleich für den technisch bedingten Verlust an Beherrschbarkeit der Privatsphäre schafft, der für über Distanz transportierte Daten insbesondere bei Nutzung von Übertragungsmedien Dritter zwangsläufig entsteht".[19] „Denn […] Grundrechtsträger [sind] schutzbedürftig, da sie auf eine für sie nicht beherrschbare und dem möglichen Zugriff Dritter ausgesetzte Übermittlung von potentiell persönlichkeitsrelevanten Daten auf Distanz angewiesen sind, gleichzeitig aber eine berechtigte Vertraulichkeitserwartung hinsichtlich der kommunizierten Inhalte und Umstände des Datentransports haben".[20]

Die grundrechtstypische Gefährdungslage bestehe daher lediglich *während* der Übertragung; gespeicherte Daten fallen (nach wie vor) nicht in den Schutzbereich.[21]

Das Fernmeldegeheimnis in Art. 10 Abs. 1 GG hat sich mit dem Trojaner-I-Beschluss zu einem umfassenden Recht auf „Privatheit auf Distanz" entwickelt, das bspw. auch Lokalisationsdaten und automatisierte Backups vor staatlichem Mitzeichnen schützen kann.[22] Dieser geschützte Freiheitsraum ist in der Informationsgesellschaft notwendig, da sich auch beim „bloße[n] ‚digital[n] Selbstgespräch', also [dem] Speichern und Abrufen von Daten in Cloud-Speichern"[23] eine vulnerable Lage ergibt – immerhin handelt es sich bei Cloud-Speichern um Computer anderer Personen, sodass Daten in den Herrschaftsbereich einer anderen Person übermittelt werden.[24] Die reine Maschine-zu-Maschine-Kommunikation ist dagegen nicht von Art. 10 Abs. 1 GG erfasst.[25]

Dieser weite Schutzbereich des Art. 10 Abs. 1 GG adressiert nunmehr umfassend das Übermittlungsrisiko von Informationstechnik und schließt damit eine Lücke, die das systembezogene IT-System-Grundrecht nicht abdeckt.[26]

3. Grundrechtseingriffe durch die Quellen-TKÜ

Statt bislang lediglich einen Eingriff in das Fernmeldegeheimnis – wie bei der klassischen TKÜ – anzunehmen, änderte das BVerfG seine Rechtsprechung und sieht nun auch das IT-System-Grundrecht

[16] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 87 f.
[17] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 89, 91.
[18] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 92.
[19] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 90.
[20] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 91.
[21] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 88.
[22] *Ziegler*, NVwZ 2025, 1803 (1804).
[23] *Ziegler*, NVwZ 2025, 1803 (1804).
[24] Vgl. zu „Datenbesitz" *Hoeren*, MMR 2019, 5 ff.; *Martini u.a.*, MMR-Beilage 2021, 3 (13 ff.).
[25] Vgl. genauer *Ziegler*, NVwZ 2025, 1803 (1805).
[26] *Ziegler*, NVwZ 2025, 1803 (1804 f.).

als verletzt an.[27] Damit ist die Quellen-TKÜ nicht mehr als ein funktionelles Äquivalent zur TKÜ, sondern als eingeschränkte Online-Durchsuchung zu verstehen.[28]

Der Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG ergibt sich dem BVerfG nach durch die Überwachung und Aufzeichnung laufender Kommunikationsvorgänge.[29] Die Quellen-TKÜ erforderte jedoch ebenfalls, dass Polizeibehörden das IT-System der zu überwachenden Person *infiltrieren*. Die Maßnahme verkürze „den Gewährleistungsgehalt des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht)".[30] Prägend sei die *Systembezogenheit*: Ähnlich wie Art. 13 GG die Wohnung als Privatraum schützt,[31] solle das IT-System-Grundrecht die Privatheit im Rahmen von IT-Nutzung gewährleisten. IT-Systeme böten einen „virtuellen Raum der Bewahrung und Entfaltung der eigenen Persönlichkeit".[32] Dadurch ermöglichten sie es, „einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[33]

Schutzziele seien sowohl die Vertraulichkeit als auch die Integrität, sodass mit der Infiltration „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen" ist.[34] Ein Eingriff in das IT-System-Grundrecht liege bereits vor, wenn „Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können".[35] Folglich ist – wie nun klar gestellt wird – der Schutz des IT-System-Grundrechts nicht rein funktional auf die Vertraulichkeit, sondern auch auf Manipulation ausgerichtet.[36] Entscheidend für diesen Schutz ist ausdrücklich die *Vertraulichkeitserwartung* der Grundrechtsträger, sodass sich der Schutz auf die „abstrakt-systembezogene Vertraulichkeitserwartung im Vorfeld konkreter Datenerhebungen" bezieht und das „auf [ein] System insgesamt bezogen[e] Gefährdungspotenzial" in den Blick nimmt.[37] Ein Eingriff scheidet daher aus, wenn das überwachte IT-System nicht als eigenes genutzt wird – in diesem Fall lehnt das BVerfG eine berechtigte Vertrauenserwartung ab.[38]

Die Eingriffsintensität der Maßnahmen ergibt sich dem BVerfG zufolge nicht nur aus der Quantität der Daten, sondern auch aus der Qualität (z.B. bei einem umfassenden Einblick in die Persönlichkeit).[39] Entscheidend sei zudem, ob private Dritte an der Überwachung beteiligt seien.[40] Damit nimmt das BVerfG indirekt Bezug auf private Softwareangebot zur Infiltration von IT-Systemen, wie bspw. „Pegasus" der NSO Group, die u.a. durch ihren Einsatz zu Überwachung von Journalistinnen und Journalisten bekannt wurde.[41]

---

[27] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 93 ff.; vgl. dagegen noch BVerfGE 120, 274 (309 Rn. 190) sowie *Martini/Fröhlingsdorf*, NVwZ-Extra 24/2020, 3 ff. Siehe ferner *Ziegler*, NVwZ 2025, 1803 (1806) m.w.N.

[28] *Ziegler*, NVwZ 2025, 1803 (1807).

[29] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 94.

[30] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 95.

[31] Diesen Vergleich zieht auch BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 115.

[32] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 101.

[33] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 97.

[34] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 99 mit Verweis auf BVerfG 120, 274 (314).

[35] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 99.

[36] Für einen funktionalen Bezug zur Vertraulichkeit bspw. *Skistims*, Smart Homes, 2016, S. 214 f.

[37] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 100. Diese Vertraulichkeitserwartung sei auch nicht durch die allgegenwärtige Überwachung, auch durch Private, hinfällig, a.a.O., Rn. 113.

[38] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 104.

[39] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 97.

[40] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 114.

[41] Vgl. hierzu *Reuter/Beckedahl*, netzpolitik.org v. 20.7.2021 (26.2.2026).

Da die Quellen-TKÜ darauf ausgelegt sei, IT-Systeme zu infiltrieren und damit die Vertraulichkeitserwartung der Nutzenden in die Vertraulichkeit und Integrität zu verletzen, sei es konsequent, neben dem Eingriff nach Art. 10 Abs. 1 GG wegen der Überwachung der *laufenden* Kommunikation auch einen *systembezogenen* Schutz durch das IT-System-Grundrecht anzunehmen.[42]

Das BVerfG folgert hieraus, dass beide Grundrechte in Idealkonkurrenz stünden und parallel anwendbar seien.[43] Es erkennt das IT-System-Grundrecht als „eigenständige[n] Freiheitsbereich mit festen Konturen" an.[44] Das Fernmeldegeheimnis gehe zwar grds. als besonderes Freiheitsrecht dem allgemeinen Persönlichkeitsrecht vor; doch seien die betroffenen Schutzgehalte im Fall der Quellen-TKÜ nicht kongruent, sodass das IT-System-Grundrecht eine Schutzlücke schließe.[45] Das BVerfG betont insoweit die „unverzichtbare Bedeutung" von IT-Systemen „für die persönliche Lebensführung".[46] In der Folge lehnt das BVerfG die funktionale Äquivalenz der Quellen-TKÜ gegenüber der traditionellen TKÜ ab, da ein Eingriff in das IT-System erfolge – auch dann, wenn nur die laufende Kommunikation überwacht wird.[47]

Der Trojaner-I-Beschluss schärft daher die Dogmatik des „IT-System-Grundrechts" sowie dessen Gewährleistungsgehalt.[48] Außerdem stellt das BVerfG das Verhältnis des Art. 10 Abs. 1 GG zum IT-System-Grundrecht klar, wie *Nicolas Ziegler* zusammenfasst:

> „Entweder ein System kommuniziert und Art. 10 I GG schützt, oder die Daten ruhen, dann schützt das IT-System-Grundrecht."[49]

4. Rechtfertigung der Grundrechtseingriffe

Zu Beginn der Ausführungen zur Rechtfertigung der Grundrechtseingriffe betont das BVerfG, dass „keine kategorische Abstufung zwischen Eingriffen in das IT-System-Grundrecht und in das Fernmeldegeheimnis" stattfinde, sondern die konkreten Umstände (u.a. die konkret betroffenen Daten und die Heimlichkeit der Maßnahme) entscheidend seien.[50] Entscheidend sei zunächst die *Eingriffsschwelle* (der Anlass der Überwachung) und das zu schützende Rechtsgut.[51] Dabei gelte: Je geringer die Anforderungen an die Eintrittswahrscheinlichkeit sind (z.B. statt einer konkreten nur eine „konkretisierende" Gefahr), desto höherrangiger müsse das zu schützende Rechtsgut sein.[52] Außerdem sei das *Eingriffsgewicht* der konkreten Maßnahme zu berücksichtigen:

---

[42] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 103.

[43] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 105 ff.

[44] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 108.

[45] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 106 f., vgl. auch Rn. 112. Das BVerfG distanziert zugleich von seiner Online-Durchsuchung-Entscheidung aus dem Jahr 2008 (BVerfGE 120, 274), BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 110.

[46] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 113.

[47] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 117 ff.

[48] Vgl. auch *Ziegler*, NVwZ 2025, 1803 (1805).

[49] *Ziegler*, NVwZ 2025, 1803 (1806)

[50] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 124.

[51] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 126.

[52] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 126. Vgl. zum sog. „Je-desto-Grundsatz" auch *Korte/Drittrich*, JA 2017, 332 ff.

„Je tiefer Überwachungsmaßnahmen in das Privatleben hineinreichen und berechtigte Vertraulichkeitserwartungen überwinden, desto strenger sind die Anforderungen an ihre Rechtfertigung."[53]

§ 20c PolG NRW ermöglicht Überwachungsmaßnahmen unterhalb der konkreten Gefahr, allerdings nur zur Abwehr besonderer, gegenwärtiger Gefahren oder zur Verhütung terroristischer Straftaten.[54] Die zu schützenden Rechtsgüter sind daher besonders hochrangig.[55]

Den legitimen Zweck, die Geeignetheit und die Erforderlichkeit der Überwachungsmaßnahmen nach § 20c PolG NRW zweifelt das BVerfG daher nicht an und verweist u.a. auf terroristische und organisierte Kriminalität.[56] Unproblematisch sei es, dass das (präventive) Polizeigesetz an die Verhütung von Straftaten anknüpft, da dies ebenfalls Teil des präventiven Rechtsgüterschutzes sei.[57] § 20c PolG NRW qualifiziere die Straftaten näher, da es sich um *terroristische* Straftaten (definiert in § 8 Abs. 4 PolG NRW) handeln muss.[58] Die Zulässigkeit des in § 8 Abs. 4 PolG NRW genannten Straftatenkatalogs bestätigt das BVerfG, da dieser hinreichend eingeschränkt sei.[59]

IV. Relevanz für die Fallbearbeitung

Die Trojaner-I-Entscheidung ist für die Fallbearbeitung vor allem deshalb bedeutsam, weil sie die Schutzgehalte des Fernmeldegeheimnisses sowie des IT-System-Grundrechts genauer ausleuchtet und zeitgemäß interpretiert. Dabei löst das BVerfG die sorgfältige Trennung des einfachen Rechts zwischen Quellen-TKÜ und Online-Durchsuchung weitestgehend auf.[60]

Die Ausführungen zur Rechtfertigung der Überwachungsmaßnahmen verdeutlichen die dogmatische Herangehensweise bei der Abwägung von Grundrechtseingriffen zum Schutz anderer Rechtsgüter. Dabei kommt im Polizeirecht insbesondere dem Je-Desto-Grundsatz hohe Bedeutung zu: Je größer der Schaden bzw. je höherrangiger das zu schützende Rechtsgut, desto geringere Anforderungen können an die Wahrscheinlichkeit der Gefahrverwirklichung gestellt werden. Dies ist v.a. im Bereich der Terrorabwehr, bei der die Tatsachenlage typischerweise im Gefahrenvorfeld zu verorten ist, relevant, um Gefahrenabwehrmaßnahmen zu rechtfertigen.

Klausurrelevant dürften zudem die Anforderungen an Straftatenkataloge im präventiven Kontext sein: Eine „binäre Etikettierung bestimmter Straftaten als terroristisch"[61] reicht nicht aus. Da jedes Bundesland über eigene Rechtsgrundlagen verfügt, ergibt sich viel Prüfungsbedarf.

[53] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 126.

[54] Vgl. auch *Ziegler*, NVwZ 2025, 1803 (1807).

[55] Vgl. auch BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 131, vgl. auch genauer zu besonders gewichtigen Rechtsgütern Rn. 135.

[56] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 129.

[57] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 136.

[58] Vgl. BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 138 f.

[59] BVerfG, Beschl. v. 24.6.2025 – 1 BvR 2466/19 (Trojaner I), Rn. 141 ff. Demgegenüber kritisierte der *Erste Senat* den Straftatenkatalog in § 100a Abs. 2 StPO: BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23 (Trojaner II), Rn. 179 ff.

[60] *Ziegler*, NVwZ 2025, 1803 (1808).

[61] *Ziegler*, NVwZ 2025, 1803 (1808).