GESELLSCHAFT
FÜR FREIHEITSRECHTE

02. JULI 2026 | RECHTSGUTACHTEN

STAATLICHER UMGANG MIT IT-SCHWACHSTELLEN UND SPYWARE

VERFASSUNGSRECHTLICHE ANFORDERUNGEN UND GRENZEN

GESELLSCHAFT
FÜR FREIHEITSRECHTE

IMPRESSUM

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin
Telefon 030 549 08 10 – 0
Fax 030 549 08 10 – 99
info@freiheitsrechte.org
PGP/GPG Key ID FA2C23A8

Kontoverbindung
IBAN: DE 88 4306 0967 1182 9121 00
BIC: GENODEM1GLS
GLS Gemeinschaftsbank eG

Vertreten durch den Vorstand des Vereins
Prof. Dr. Nora Markard
Prof. Dr. Boris Burghardt
Dr. John Philipp Thurn
Prof. Dr. Dana-Sophia Valentiner
Felix Reda
Prof. Dr. Leonie Steinl LL.M.

V.i.S.d.P.
Malte Spitz
Boyenstr. 41
10115 Berlin

Autor:innen
Prof. Dr. Thomas Wischmeyer
Dr. Paul Friedl

Titelbild
unsplash.com | Philipp Katzenberger

Layout
Bernhard Leitner

Inhaltsverzeichnis

Executive Summary **6**

Gutachten **12**

A. Einführung 12

B. Verfassungsrechtliche Determinanten staatlichen Schwachstellenmanagements 17

I. Betroffene Grundrechte 17

1. Anwendbare Grundrechtsordnung 18

2. IT-System-Grundrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG 20

3. Telekommunikationsgeheimnis, Art. 10 GG 22

4. Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG 23

5. Weitere Grundrechte der IT-Nutzenden 25

6. Grundrechte der Hersteller 26

II. Eingriffsschwere und Bedeutung der staatlichen Kenntnis und Nutzung von IT-Schwachstellen 27

III. Verfassungsrechtliche Grundlagen einer gesetzlichen Pflicht zum Schwachstellenmanagement 31

1. Schwachstellenmanagement und grundrechtliche Schutzpflichten 31

2. Schwachstellenmanagement und Grundsatz der Wesentlichkeit 37

3. Schwachstellenmanagement und Verhältnismäßigkeit staatlichen Schwachstellenerwerbs und -nutzung 40

IV. Verfassungsrechtliche Mindestanforderungen 43

1. Formell-gesetzliche Regelung 43

a) Formell-gesetzliche Verankerung 43

b) Regelungsumfang der formell-gesetzlichen Verankerung 44

2. Regelungsadressaten und Regelungsgegenstand 46

3. Abwägungsprozess 48

a) Abwägungspflicht 48
b) Abwägungsbelange 49
4. Regel-Ausnahme-Verhältnis 50
5. Entscheidungszuständigkeit und -prozess 50
6. Entscheidungsfolgen 51
7. Aufsicht und Kontrolle 52
8. Schutzmaßnahmen 55
V. Weitere Anforderungen an eine sachgerechte Ausgestaltung 56
1. Entscheidungszuständigkeit 56
a) Struktur des Entscheidungskörpers 57
b) Mögliche Ausgestaltungen 58
2. Entscheidungsprozess 60
3. Transparenz- und Berichtspflichten 62
VI. Inanspruchnahme externer Überwachungskapazitäten 63
1. Dienstleistungsbasierte Überwachung („Commercial Surveillance Vendors") 63
a) Strukturen und Praxen dienstleistungsbasierter Überwachung 64
b) Risiken dienstleistungsbasierter Überwachung 65
c) Verfassungsrechtliche Bewertung 68
d) Verfassungsrechtliche Vorgaben und sachgerechte Ausgestaltung 72
2. Zusammenarbeit mit ausländischen Sicherheitsbehörden 76

C. Kompetenzrechtlicher Rahmen 78
I. Kompetenz der Europäischen Union 78
1. Kompetenztitel 79
a) Art. 114 Abs. 1 Satz 2 AEUV 79
b) Art. 16 Abs. 2 UAbs. 1 Satz 2 AEUV 81
c) Justizielle und polizeiliche Zusammenarbeit 81
d) Zwischenergebnis 83
2. Kompetenzgrenzen 83
3. Ergebnis 86
II. Vorgaben des Unionsrechts 86
1. NIS-2-Richtlinie 87
2. ePrivacy-Richtlinie 89

3. DSGVO 91
4. JI-Richtlinie 93
5. Cyber Resilience Act 94
6. Cybersecurity Act 95
7. Ergebnis 96
III. Kompetenzverteilung im Bundesstaat 96

Regelungsvorschlag 102

Literatur 107

Das Gutachten "Staatlicher Umgang mit IT-Schwachstellen und Spyware. Verfassungsrechtliche Anforderungen und Grenzen" wurde von der Gesellschaft für Freiheitsrechte e.V. in Auftrag gegeben und ohne inhaltliche Weisungen erstellt. Es gibt die Bewertung der Autoren wieder.

Executive Summary

Deutsche Version

Sog. *zero-day vulnerabilities* – IT-Sicherheitslücken, die den betroffenen Herstellern noch unbekannt sind – bergen regelmäßig massive Freiheits- und Sicherheitsrisiken: Sie öffnen Angriffswege, über die feindliche Akteure deutsche Politiker:innen oder Unternehmen ausspionieren können, über die Journalist:innen oder Oppositionelle im In- und Ausland überwacht werden können und über die kritische Infrastruktur sabotiert und lahmgelegt werden kann. Um diese Gefahren einzudämmen, gebietet es die Informationssicherheit, solche Sicherheitslücken im Falle ihrer Entdeckung umgehend an die betroffenen Hersteller zu melden, damit diese sie schließen können.

Dennoch entscheiden sich auch staatliche Behörden nicht immer für die Offenlegung derartiger Schwachstellen. Denn auch sie können ein Interesse an der Geheimhaltung der Schwachstellen haben: Polizei und Nachrichtendienste machen von *zero-day vulnerabilities* Gebrauch, um Verdächtige und andere Zielpersonen abzuhören. Militärs und Sicherheitsbehörden nutzen sie für offensive Cyberoperationen. Erhält der Staat Kenntnis von einer *Zero-Day*-Schwachstelle, kann sich für ihn also ein Zielkonflikt auftun: einerseits sollte er die Schwachstelle zum Schutz von Bevölkerung, Behörden und Wirtschaft möglichst schnell an die Hersteller melden. Andererseits kann die Schwachstelle für Sicherheitsbehörden ein wertvolles Gut in der Ausübung ihrer gesetzlichen Aufgaben darstellen.

Das Grundgesetz gebietet, dass dieser Zielkonflikt vom Gesetzgeber durch ein formelles Parlamentsgesetz aufgelöst wird, das sowohl den staatlichen Umgang mit unbekannten IT-Schwachstellen wie auch die Verwendung externer Spyware verbindlich regelt. Das ergibt sich eindeutig aus der Entscheidung „IT-Sicherheitslücken“ des Bundesverfassungsgerichts (2021) sowie der übrigen einschlägigen verfassungsgerichtlichen Rechtsprechung.

Ein solches Gesetz fehlt in Deutschland bislang. Damit verletzt der Gesetzgeber gegenwärtig seine verfassungsrechtliche Pflicht, das IT-System-Grundrecht zu schützen.

Inhaltlich lässt sich der gebotene Regelungsgehalt in verfassungsrechtlich zwingende Mindestanforderungen und darüber hinausreichende Regelungsempfehlungen aufgliedern.

Verfassungsrechtlich zwingend geboten ist zunächst, dass Entscheidungen über die Offenhaltung unbekannter IT-Schwachstellen nur im Rahmen eines strukturierten Verfahrens getroffen werden, in dem Gefahren und potenzieller Nutzen der Schwachstelle gegeneinander abgewogen werden. Außerdem muss das Gesetz vorsehen, dass IT-Schwachstellen im Regelfall offengelegt werden und nur ausnahmsweise temporär geheim gehalten werden dürfen. Es muss bestimmen, welche Institution für die Entscheidung zuständig ist, und die Grundzüge des Verfahrens festlegen. Wird eine Schwachstelle nicht offengelegt, sind zusätzlich Maßnahmen zur Mitigierung der damit einhergehenden Informationssicherheitsrisiken zu erwägen und eine periodische Neuevaluierung der Schwachstelle sicherzustellen. Geheim gehaltene Schwachstellen sind durch effektive Maßnahme der Informationssicherheit gegen Verlust und Diebstahl zu sichern. Schließlich muss das Gesetz eine unabhängige Kontrollinstanz einrichten, die über hinreichende Informationen, Expertise und Ressourcen verfügt, um die getroffenen Entscheidungen effektiv überprüfen zu können.

Bei der Ausgestaltung im Detail hat der Gesetzgeber Spielräume. Was die organisatorische Verankerung des Entscheidungsprozesses und das konkret zu durchlaufende Verfahren angeht, erscheint es jedoch sinnvoll, dies nicht einer einzelnen Behörde zu überlassen, sondern einem überbehördlichen und interministeriellen Gremium zu übertragen, das im Grundsatz konsensual entscheidet und über ein hinreichend ausgestattetes Sekretariat verfügt. Was Aufsicht und Kontrolle angeht, bietet sich aus verfassungsrechtlichen Gesichtspunkten eine umfassende objektive Rechtskontrolle an, durch die alle Entscheidungen über die Geheimhaltung einer Schwachstelle unabhängig überprüft werden können. Weitere

Regelungsaspekte können und sollten auf eine Rechtsverordnung ausgelagert werden.

Darüber hinaus muss der Gesetzgeber auch den staatlichen Umgang mit Überwachungskapazitäten regeln, die dem Staat von Dritten – konkret: kommerziellen Spyware-Anbietern und befreundeten Nachrichtendiensten – zur Verfügung gestellt werden. Denn auch diese Aktivitäten sind aus grundrechtlicher Sicht hochsensibel. Zudem droht sonst das Leerlaufen bzw. die Umgehung der verfassungsrechtlichen Pflicht zum Schwachstellenmanagement. Der Gesetzgeber muss dabei sicherstellen, dass staatliche Behörden nicht auf Überwachungskapazitäten zugreifen, die inakzeptable Risiken für grundrechtlich geschützte Freiheiten und Sicherheiten schaffen. Beim Ankauf von kommerzieller Spyware kann dies neben einer dem Schwachstellenmanagement vergleichbaren Pflicht zur Anbieter- und Produkt-Bewertung nur durch flankierende Schutzregelungen, etwa zur vertraglichen Weitergabe von Datensicherheitsanforderungen, garantiert werden. Auch ein White-Listing-Modell oder ein gänzliches Verbot des Rückgriffs auf kommerzielle Spyware sind denkbar.

Zur Umsetzung dieser Regelungen ist der Bundesgesetzgeber auch kompetenziell befugt. Weder kommt der Europäischen Union insoweit eine ausschließliche Regelungskompetenz zu, noch wird ein nationales Regelungsvorhaben durch bestehendes Unionsrecht substanziell beschränkt. Innerhalb Deutschlands ist der Bund allerdings unmittelbar nur zur Regelung der eigenen Bundesbehörden befugt. Was den Umgang mit IT-Schwachstellen oder Spyware durch Landesbehörden angeht, kommen nur begrenzte Kooperationsregelungen in Betracht.

English version

So-called *zero-day vulnerabilities* – IT security flaws unknown to the vendors whose products they affect – pose serious risks to both civil liberties and public security. They create attack vectors that hostile actors can use to spy on German politicians and businesses, to surveil journalists and dissidents at home and abroad, and to sabotage critical infrastructure. Basic information security principles therefore require that such vulnerabilities, once discovered, be reported promptly to the affected vendors for patching.

State authorities, however, do not always choose to disclose what they find. They have their own reasons to keep vulnerabilities secret: law enforcement and intelligence agencies exploit zero-day vulnerabilities to intercept the communications of suspects and other surveillance targets, while military and security agencies deploy them in offensive cyber operations. When the state learns of a zero-day vulnerability, it thus faces a dilemma: disclosure protects the public, government, and economy, but the vulnerability may also be operationally valuable to security agencies carrying out their statutory functions.

Germany's Constitution, the *Grundgesetz*, requires the legislature to resolve this dilemma through a formal act of parliament that establishes binding rules for both the state's handling of unknown IT vulnerabilities and its use of third-party spyware. This obligation follows directly from the Federal Constitutional Court's 2021 decision on IT Security Vulnerabilities („*IT-Schwachstellen*“) and the broader body of relevant constitutional case law. Germany currently has no such legislation. That gap means the legislature is in breach of its constitutional duty; most importantly, its duty to protect the fundamental right to the integrity and confidentiality of IT systems.

The content that legislation must cover falls into two categories: constitutionally mandatory requirements and politically advisable recommendations that go beyond them.

On the mandatory side, any decision to retain an unknown vulnerability rather than disclose it must be made through a structured procedure that weighs

the operational value of keeping it secret against the security risks of doing so. The legislation must establish a presumption in favour of disclosure: vulnerabilities may be withheld only temporarily and only in exceptional circumstances. It must designate a responsible decision-making body and set out the core elements of the procedure. Where a vulnerability is withheld, the legislation must require that steps be taken to mitigate the resulting information security risks and that the decision be revisited periodically. Withheld vulnerabilities must be protected against loss or theft through robust information security measures. The framework must also provide for independent oversight with the information, expertise, and resources needed to scrutinise decisions effectively.

Beyond these requirements, the legislature has room to make its own choices about the details of the process. With respect to the institutional hosting of the decision-making process and the specific procedure to be followed, it appears sensible not to leave this to a single authority, but rather to assign it to a cross-agency and interministerial body that decides on a consensual basis as a matter of principle and that has an adequately resourced secretariat at its disposal. On oversight and review, constitutional considerations favor a comprehensive review of legality, allowing every decision to withhold a vulnerability to be scrutinized independently. The remaining regulatory details can and should be left to secondary legislation..

The legislature must also regulate the state's use of surveillance capabilities supplied by third parties – commercial spyware vendors and allied foreign intelligence services. For these activities, too, are highly sensitive from a fundamental-rights perspective. Moreover, without such regulation, the constitutional duty to manage vulnerabilities would risk being rendered ineffective or circumvented. In doing so, the legislature must ensure that state authorities do not draw on surveillance capabilities that create unacceptable risks to constitutionally protected freedoms and securities. For commercially procured spyware, that means not only a vendor and product assessment process comparable to the vulnerability management framework, but also accompanying safeguards – such as contractual data

security requirements imposed on suppliers. A whitelist model or an outright ban on commercial spyware would equally be worth considering.

The federal legislature has the authority to enact these legislative projects. The EU holds no exclusive competence in this area, and existing EU law does not substantially constrain national action. Within Germany, however, the federation's direct legislative authority extends only to its own federal agencies; separate cooperative arrangements would be needed to cover how *Länder* authorities handle vulnerabilities and spyware.

Gutachten

A. Einführung

In der vernetzten Gesellschaft von heute stellt die Gewährleistung eines angemessenen Informationssicherheits-Niveaus eine Grundbedingung des sicheren und verlässlichen Freiheitsgebrauchs dar. Informationssicherheit gewährleistet, dass Privatpersonen, aber auch Journalist:innen und sonstige professionelle Geheimnisträger vertraulich und ohne Angst vor Überwachung kommunizieren können, dass Betreiber kritischer Infrastrukturen, vom Krankenhaus bis zum Stromnetzbetreiber, ihre Versorgungsaufgaben zuverlässig erfüllen können und dass Unternehmen sicher und geschützt vor Cyberangriffen wirtschaften können. Dementsprechend ist heute weitgehend unbestritten, dass es sich bei der Gewährleistung eines angemessenen Maßes an Informationssicherheit um eine Staatsaufgabe von grundlegender Bedeutung handelt.

Vor diesem Hintergrund mag es widersprüchlich wirken, dass der Staat selbst teils erhebliche Informationsunsicherheit erzeugt und aufrechterhält. Genau dies ist aber der Fall, wenn staatliche Stellen, insbesondere Sicherheitsbehörden, unbekannte IT-Schwachstellen (sog. *Zero-Days*) nicht an die betroffenen Hersteller melden, um deren Behebung zu ermöglichen, sondern sie geheim halten, um sie für eigene Operationen (bspw. Überwachungsmaßnahmen) nutzen zu können.

Der Wunsch staatlicher Akteure, über entsprechendes geheimes Schwachstellen-Wissen zu verfügen, kann dabei durchaus nachvollziehbar sein: Unter den Bedingungen weitgehend verschlüsselter Kommunikationsinfrastrukturen können die hierdurch eröffneten Angriffsvektoren eines der wenigen Mittel darstellen, um kriminelle Akteure zu identifizieren und zu überwachen.

Die durch die Offenhaltung von Schwachstellen ausgelösten Freiheits- und Sicherheitsrisiken sind gleichwohl massiv. Hält der Staat eine Schwachstelle offen, kann er nämlich gewöhnlich nicht sicherstellen, dass diese nicht zugleich oder zu einem späteren Zeitpunkt zu illegitimen, illegalen oder kriminellen Zwecken eingesetzt wird. Schließlich handelt es sich oftmals um dieselben Schwachstellen, die Cyberkriminelle zur Erpressung von Unternehmen mittels *Ransomware* einsetzen, die ausländische staatliche Akteure zur Durchführung von Angriffen auf kritische Infrastrukturen nutzen oder die autoritäre Regime verwenden, um Oppositionelle zu überwachen.

Der Staat befindet sich mithin in einem Zielkonflikt: Er muss einerseits effektive Gefahrenabwehr und Strafverfolgung gewährleisten, muss andererseits aber auch die IT-Sicherheit und die damit verbundenen Freiheitsrechte schützen. Der Ausbau offensiver Cyberkapazitäten des BKA und der Bundespolizei (auch bekannt als „*hack backs*“), wie er im „Gesetz zur Stärkung der Cybersicherheit“ vorgeschlagen wird, das voraussichtlich noch 2026 vom Bundestag verabschiedet wird,[1] würde diese bestehende Konfliktlage weiter verschärfen.

Ein Mittel zur strukturierten Auflösung dieses Zielkonflikts liegt in der Implementierung eines sog. Schwachstellen-Managements. Dabei handelt es sich um ein formelles, oftmals gesetzlich geregeltes Verfahren, in dem staatliche Behörden unter Abwägung der widerstreitenden Belange darüber entscheiden, ob eine spezifische Schwachstelle geheim gehalten oder aber an den betroffenen Hersteller gemeldet wird. Öffentlich wurden derartige

---

[1] Bundesregierung, *Entwurf eines Gesetzes zur Stärkung der Cybersicherheit* (21.05.2026), § 41a BPolG-E und § 68d BKAG-E, abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/cyberabwehr-RefE.pdf?__blob=publicationFile&v=4.

Prozesse beispielsweise in den USA,[2] Großbritannien[3] und Australien[4] etabliert.[5] Auch in anderen Ländern sollen vergleichbare Prozesse in bestimmten Behörden eingerichtet worden sein, ohne dass aber genauere Informationen über diese Verfahren öffentlich bekannt wären.[6]

Auch in Deutschland betreiben Sicherheitsbehörden nach eigenen Angaben innerbehördliches Schwachstellenmanagement.[7] Gesetzliche Vorgaben dazu, wie derartige Verfahren ausgestaltet sein müssen, gibt es bisher aber keine. Das scheint nicht nur angesichts der bestehenden Opazität dieser Verfahren und der eingangs dargestellten hohen Grundrechtsrelevanz der Frage problematisch: In seinem „*IT-Sicherheitslücken*"-Beschluss von Juni 2021 stellte das Bundesverfassungsgericht nämlich fest, dass das Grundgesetz eine „Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits"

---

[2] Siehe *Vulnerabilities Equities Policy and Process for the United States Government* (*U.S. VEP*) (15.11.2017), abrufbar unter https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[3] Government Communications Headquarters (GCHQ), *The Equities Process* (2018) abrufbar unter https://www.gchq.gov.uk/information/equities-process.

[4] Australian Signals Directorate, *Responsible Release Principles for Cyber Security Vulnerabilities* (2019) abrufbar unter https://www.asd.gov.au/sites/default/files/2022-03/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf.

[5] Dem U.S.-amerikanischen *Vulnerabilities Equities Process* (VEP) kommt, da es sich bei ihm nach allgemeiner Lesart um den global ersten öffentlich beschriebenen Schwachstellen-Management-Prozess handelt, immer noch diskursprägende Wirkung zu.

[6] Siehe auch Herpig und Schwartz, *The Future of Vulnerabilities Equities Processes Around the World* (4. Januar 2019) abrufbar unter https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world.

[7] Bundesministerium des Innern, für Bau und Heimat, *Cybersicherheitsstrategie für Deutschland 2021*, S. 103 f.

erfordert.[8] Ob die hinter diesem Regelungsauftrag stehende grundrechtliche Schutzpflicht derzeit aber tatsächlich verletzt ist, konnte das Gericht wegen des insofern nicht hinreichend substantiierten Vortrags der Beschwerdeführenden offenlassen.[9] Auch der Gesetzgeber ist dementsprechend bisher noch nicht tätig geworden.

Damit ist weiterhin unklar, ob der Staat verfassungsrechtlich zur gesetzlichen Normierung eines Schwachstellenmanagements verpflichtet ist, ob und, wenn ja, welche Vorgaben sich an dieses Schwachstellenmanagement aus dem „*IT-Sicherheitslücken*"-Beschluss und der weiteren verfassungsgerichtlichen Judikatur ergeben und welche Regelungsspielräume gegebenenfalls bestehen.

Diese Fragen sollen durch das folgende Gutachten beantwortet werden, das sich in drei Teile gliedert: Zunächst wird erörtert, welche verfassungsrechtlichen Determinanten Anforderungen und Vorgaben zu einer gesetzlichen Schwachstellen-Regelung aufstellen (Teil B.). Dazu wird erörtert, inwiefern sich die geheime Bevorratung staatlichen Schwachstellenwissens grundrechtsbeschränkend auswirkt, welche Konfigurationen eines Schwachstellenmanagement-Prozesses deshalb verfassungsrechtlich zwingend erforderlich sind und welche Optionen sich in den verbleibenden Regelungsspielräumen anbieten. Gesondert wird auf die Frage der Inanspruchnahme externer Schwachstellenkenntnis, sowohl von kommerziellen Spyware-Anbietern als auch von befreundeten Drittstaaten, eingegangen. Im zweiten Teil des Gutachtens wird dann erörtert, wer im dreischichtigen Kompetenzgefüge zwischen Europäischer Union, Bund und Ländern kompetenziell zur gesetzlichen Regelung des Schwachstellenmanagements befugt ist (Teil C.). Dabei wird gezeigt, dass Deutschland für die Regelung des Umgangs mit IT-Schwachstellen und Spyware zuständig ist und bestehendes Unionsrecht die nationalen Gesetzgeber in ihrer Regelungsfreiheit nicht wesentlich einschränkt.

---

[8] BVerfG, Beschluss vom 8. Juni 2021, Ls. 2.b) (*IT-Sicherheitslücken*).

[9] BVerfG, Beschluss vom 8. Juni 2021, Rn. 48-66 (*IT-Sicherheitslücken*).

Schließlich wird auf der Grundlage der verfassungsrechtlichen Analyse ein konkreter Vorschlag für die Regelung des Managements für unbekannte Schwachstellen (*Zero-Days*) sowie für die Inanspruchnahme externer Spyware-Kapazitäten durch den Bundesgesetzgeber formuliert (Teil D.).

B. Verfassungsrechtliche Determinanten staatlichen Schwachstellenmanagements

Zunächst ist zu klären, ob und, wenn ja, welche Vorgaben das Grundgesetz an eine Regelung des staatlichen Umgangs mit IT-Sicherheitslücken und externen Spyware-Kapazitäten stellt. Zur Beantwortung dieser Frage wird zunächst dargelegt, welche Grundrechte durch den staatlichen Umgang mit IT-Sicherheitslücken betroffen sind (dazu I.) und wie die Eingriffsschwere der staatlichen Kenntnis und Nutzung von Schwachstellen zu beurteilen ist (dazu II.), bevor erläutert wird, dass eine verfassungsrechtliche Pflicht zur Regelung des Schwachstellenmanagements besteht (dazu III.), die Mindestanforderungen an eine Regelung stellt (dazu IV.), dem Gesetzgeber im Übrigen aber auch gewisse Handlungsspielräume belässt (dazu V.). Der Ankauf von kommerziellen Spyware-Kapazitäten und die Einwerbung derartiger Kapazitäten von befreundeten Drittstaaten werden separat behandelt (dazu VI.).

I. Betroffene Grundrechte

Der behördliche Umgang mit unbekannten IT-Sicherheitslücken kann mit den Gewährleistungsbereichen unterschiedlicher Grundrechte interferieren. Die spezifischen Begründungsstrukturen, Schutzgehalte und Rechtfertigungsanforderungen dieser Grundrechte sind für die verfassungsrechtliche Bewertung des Schwachstellenmanagements daher zentral. Im Folgenden sollen deshalb in einem ersten Schritt die tangierten Grundrechte in ihren Grundzügen kurz vorgestellt werden. Diese überblicksartige Darstellung darf aber nicht darüber hinwegtäuschen, dass die konkret betroffenen Grundrechte sowie die Art und Schwere ihrer Beeinträchtigung immer von dem konkret in den Blick genommenen Sachverhalt abhängen. Ob etwa Art. 10 GG beeinträchtigt ist, hängt davon ab,

ob eine spezifische Schwachstelle auch zur Ausleitung von Kommunikationsdaten genutzt werden kann und ob die konkrete Behörde, die Kenntnis von der Schwachstelle hat, diese auch zur Kommunikationsüberwachung nutzen darf (rechtlich), kann (technisch) und will (faktisch). Überdies dürfen die Divergenzen, die sich bei unterschiedlichen Grundrechtsbetroffenheiten ergeben, nicht überbewertet werden: Auch das Bundesverfassungsgericht operiert insbesondere im Bereich staatlicher Überwachung mit grundrechtsübergreifenden Voraussetzungen.[10]

1. Anwendbare Grundrechtsordnung

Bevor der Blick auf einzelne Grundrechte gelenkt werden kann, muss die Frage nach der anwendbaren Grundrechtsordnung geklärt werden. Finden nur die Grundrechte des Grundgesetzes oder nur diejenigen der Europäischen Grundrechtecharta Anwendung oder gelten gar beide Grundrechtsordnungen parallel?

Nach bundesverfassungsgerichtlicher Rechtsprechung finden die Grundrechte des Grundgesetzes Anwendung, wenn die zu überprüfenden Normen nicht ausschließlich der Umsetzung zwingenden Unionsrechts gelten, d.h. unionsrechtlich vollständig determiniert sind.[11] Dies ist weder für die bereits bestehenden Ermittlungs- und Eingriffsbefugnisse der unterschiedlichen Sicherheitsbehörden der Fall[12] noch würde dies, wie in Teil C. noch dargestellt wird,[13] für eine noch zu schaffende Regelung zum

---

[10] BVerfG, Beschluss vom 24. Juni 2025, Rn. 125 (*Trojaner I*) (m.w.N.).

[11] BVerfGE, Beschluss vom 27. Mai 2020, Rn. 83-84 (*Bestandsdatenauskunft*).

[12] Siehe auch BVerfG, Beschluss vom 24. Juni 2025, Rn. 125 (*Trojaner I*) (PolGNRW); BVerfG, Beschluss vom 24. Juni 2025, Rn. 168 (*Trojaner II*) (StPO); BVerfG, Beschluss vom 8. Oktober 2024, Rn. 77-81 (*BND-Cybergefahren*) (G10-Gesetz); BVerfG, Urteil vom 26. April 2022, Rn. 142-143 (*Bayerisches Verfassungsschutzgesetz*) (BayVfSchG).

[13] Siehe unten C.II.

Schwachstellenmanagement gelten.[14] Dass unionsrechtliche Vorschriften Bezüge zur Frage des Schwachstellenmanagements aufweisen und einzelnen Behörden potenziell schon heute Vorgaben zum Umgang mit IT-Schwachstellen machen,[15] steht dem nicht entgegen.[16]

Auch findet für die hier interessierenden Konstellationen die Europäische Grundrechtecharta keine parallele Anwendung. Nach Art. 51 Abs. 1 GRCh gilt die Charta „für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union". Ob eine solche Durchführung des Unionsrechts vorliegt, beurteilt sich nach der Rechtsprechung des EuGH insbesondere danach, „ob mit der fraglichen nationalen Regelung die Durchführung einer Bestimmung des Unionsrechts bezweckt wird".[17] Dies ist für die hier betroffenen Fallkonstellationen und Rechtsmaterien, wie ebenfalls in Teil C. noch dargestellt wird,[18] nicht der Fall.

Käme es zu einer unionalen Regelung, könnte dies freilich anders zu beurteilen sein

Neben dem Grundgesetz findet weiter immer auch die Europäische Menschenrechtskonvention Anwendung, deren Vorgaben bei der Auslegung und Anwendung der deutschen Grundrechte zu beachten sind.[19]

---

[14] BVerfG, Beschluss vom 8. Juni 2021, Rn. 23 (*IT-Sicherheitslücken*).

[15] Siehe unten C.II.

[16] So auch BVerfG, Beschluss vom 8. Juni 2021, Rn. 23 (*IT-Sicherheitslücken*); siehe auch BVerfG, Urteil vom 26. April 2022, Rn. 142 (*Bayerisches Verfassungsschutzgesetz*); BVerfG, Beschluss vom 24. Juni 2025, Rn. 83 (*Trojaner I*); BVerfG, Beschluss vom 24. Juni 2025, Rn. 168 (*Trojaner II*); BVerfG, Beschluss vom 8. Oktober 2024, Rn. 77-81 (*BND-Cybergefahren*).

[17] EuGH, Urteil vom 10. Juli 2014, Rs. C-198/13, Rn. 37 (*Julian Hernández ua*); EuGH, Urteil vom 22. Janur 2020, Rs. C-177/18, Rn. 59 (*Baldonedo Martín*).

[18] Siehe unten C.II.

[19] BVerfG, Beschluss vom 14. Oktober 2004, Rn. 32 (*EGMR-Entscheidungen*).

2. IT-System-Grundrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Besondere Bedeutung für die Diskussion um staatliches Schwachstellenmanagement hat das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (IT-System-Grundrecht).

Das IT-System-Grundrecht, das vom Bundesverfassungsgericht in der Entscheidung „Online-Durchsuchungen" von 2008 als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts anerkannt wurde,[20] schützt die Vertraulichkeit und Integrität von IT-Systemen, die Daten einer betroffenen Person in einem Umfang und einer Vielfalt vorhalten können, dass ein Zugriff auf das System Einblick in wesentliche Teile der Lebensgestaltung einer Person oder gar ein aussagekräftiges Bild der Persönlichkeit ermöglicht.[21]

Geschützt sind dabei nicht nur die Vertraulichkeit und Integrität der auf einem vom Schutzbereich des Grundrechts erfassten IT-System gespeicherten Daten. Vielmehr verlagert das Grundrecht den Schutz nach vorne auf die „abstrakt-systembezogene Vertraulichkeitserwartung im Vorfeld konkreter Datenerhebungen[, da] bereits mit dem Zugriff auf ein IT-System […] eine besondere Gefährdungslage für die dort erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten" entstehe.[22]

Der Schutzbereich des Grundrechts ist deswegen bereits dann beeinträchtigt, wenn sich Unberechtigte Zugriff auf ein geschütztes IT-System verschaffen; ein tatsächlicher Datenabfluss oder ein Ausspähen ist nicht notwendig.[23]

---

[20] BVerfG, Urteil vom 27. Februar 2008, Rn. 166 ff. (*Online-Durchsuchungen*).

[21] BVerfG, Beschluss vom 24. Juni 2025, Rn. 97 (*Trojaner I*).

[22] BVerfG, Beschluss vom 24. Juni 2025, Rn. 100 (*Trojaner I*).

[23] BVerfG, Beschluss vom 24. Juni 2025, Rn. 100 (*Trojaner I*).

Weitere Voraussetzung ist allerdings stets, dass das betroffene IT-System als eigenes genutzt wird.[24]

Selbst wenn staatliche Maßnahmen auch zum Datenabfluss führen und dadurch weitere Grundrechte, insbesondere Art. 10 GG oder das Grundrecht auf informationelle Selbstbestimmung, betroffen werden, tritt das IT-System-Grundrecht nicht hinter diesen zurück.[25]

Das staatliche Vor- und Geheimhalten von IT-Sicherheitslücken kann – ungeachtet der vom Bundesverfassungsgericht aus dem Grundrecht abgeleiteten konkreten Schutzpflicht –[26] mit der durch das IT-System-Grundrecht geschützten Vertraulichkeits- und Integritätserwartung interferieren. Indem bekannte Schwachstellen nicht geschlossen werden, bleibt eine Gefährdungslage bestehen, die unberechtigte Zugriffe auf informationstechnische Systeme ermöglicht und damit den Schutzbereich des Grundrechts berührt. Voraussetzung ist insofern nur, dass es sich um IT-Sicherheitslücken handelt, die tatsächlich einen weitgehenden Zugriff auf hinreichend persönlichkeitsnahe IT-Systeme (insbesondere PCs und Mobiltelefone) erlaubt. Bei den hier in Rede stehenden Sicherheitslücken, die oftmals sehr weitgehenden bis hin zu Root-Zugriff ermöglichen, wird dies regelmäßig der Fall sein.

---

[24] BVerfG, Beschluss vom 24. Juni 2025, Rn. 104 (*Trojaner I*) (zur Nutzung als eigenes Gerät).

[25] BVerfG, Beschluss vom 24. Juni 2025, Rn. 105-118 (*Trojaner I*) (zum Verhältnis zwischen IT-System-Grundrecht und Art. 10 GG); überholt demnach BVerfG, Beschluss vom 8. Juni 2021, Rn. 27-29 (*IT-Sicherheitslücken*), wo davon ausgegangen wird, dass ein staatlicher Zugriff im Sinne einer Quellen-Telekommunikationsüberwachung nur an Art. 10 GG zu messen wäre.

[26] Dazu sogleich B.III.1.

3. Telekommunikationsgeheimnis, Art. 10 GG

Auch das Telekommunikationsgeheimnis aus Art. 10 GG spielt für die verfassungsrechtliche Bewertung staatlichen Schwachstellenmanagements eine Rolle.

Art. 10 GG schützt die unkörperliche Übermittlung von Informationen mit Hilfe des Telekommunikationsverkehrs, „einerlei, welche Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und welche Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) genutzt werden".[27] Geschützt sind demnach neben der Telefonie oder dem Nachrichtenversand über Mobilfunknetze auch internetbasierte Kommunikationsdienste.[28] Der Schutz umfasst dabei sowohl Kommunikationsinhalte als auch Kommunikationsumstände (etwa Metadaten).[29]

In seiner Entscheidung „Trojaner I" stellte das Bundesverfassungsgericht 2025 fest, dass Art. 10 GG dabei auch dann Anwendung findet, wenn es nicht um die Übermittlung von Informationen an individuelle Empfänger:innen, sondern „andere mithilfe von Telekommunikationstechniken über Distanz transportierte Daten" geht, etwa Daten, die beim Abruf von Webseiten oder bei sonstigem Hoch- oder Herunterladen von Inhalten übermittelt werden.[30]

Im Ergebnis schützt das Telekommunikationsgeheimnis also den gesamten telekommunikativ übermittelten Rohdatenstrom.[31] Nicht umfasst sind allerdings Daten, die außerhalb eines laufenden Kommunikationsvorgangs aus dem Herrschaftsbereich eines Betroffenen abgeschöpft werden.[32] Das

---

[27] BVerfG, Urteil vom 27. Februar 2008, Rn. 182-183 (*Online-Durchsuchungen*).

[28] BVerfG, Urteil vom 27. Februar 2008, Rn. 183 (*Online-Durchsuchungen*).

[29] BVerfG, Beschluss vom 24. Juni 2025, Rn. 88 (*Trojaner I*).

[30] BVerfG, Beschluss vom 24. Juni 2025, Rn. 91 (*Trojaner I*).

[31] BVerfG, Beschluss vom 24. Juni 2025, Rn. 91 (*Trojaner I*).

[32] BVerfG, Beschluss vom 24. Juni 2025, Rn. 88 (*Trojaner I*).

schließt den Zugriff auf Telekommunikationsinhalte von einem infiltrierten Endgerät allerdings nicht aus.[33] Tatsächlich geht das Bundesverfassungsgericht weiter davon aus, dass bereits der Zugriff auf ein IT-System zwecks Überwachung der laufenden Kommunikation von Art. 10 GG erfasst ist.[34]

Analog zur Beeinträchtigung des IT-System-Grundrechts ist deshalb durch das Vor- und Geheimhalten von IT-Sicherheitslücken auch das Telekommunikationsgeheimnis betroffen, da dadurch Zugriffe Dritter auf Inhalte und Umstände laufender Telekommunikation ermöglicht werden, die (im Falle staatlicher Verantwortung) einen Eingriff in Art. 10 GG darstellen. Das deckt sich mit dem Diktum des Bundesverfassungsgerichts, dass Art. 10 GG einen „Auftrag an den Staat [begründet], Schutz auch insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen."[35]

4. Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Drittens berührt das staatliche Bevorraten von IT-Sicherheitslücken in besonderer Weise auch das vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, abgeleitete Recht auf informationelle Selbstbestimmung.[36]

Dieses schützt „die Befugnis Einzelner, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte

---

[33] Siehe nur BVerfG, Beschluss vom 24. Juni 2025, Rn. 94 (*Trojaner I*).

[34] BVerfG, Beschluss vom 24. Juni 2025, Rn. 117 (*Trojaner I*).

[35] BVerfG, Beschluss vom 9. Oktober 2002, Ls. 2 (*Mithörvorrichtung*); BVerfG, Beschluss vom 8. Juni 2021, Ls. 1 (*IT-Sicherheitslücken*); mehr zur damit angesprochenen Schutzpflicht, unten B.III.1.

[36] Grundlegend BVerfG, Urteil vom 15. Dezember 1983 (*Volkszählung*).

offenbart werden”.[37] Es ist grundsätzlich „bei jeder Erhebung, Speicherung, Verwendung oder Weitergabe personenbezogener Daten betroffen”,[38] unabhängig von der Quantität, Qualität, Sensibilität oder dem Speicherort der betroffenen Daten.

Wie das Bundesverfassungsgericht in seiner Entscheidung „Trojaner II” im Juni 2025 klarstellte, schützt das Recht außerdem „nicht nur vor einzelnen Datenerhebungen, sondern auch vor dem Zugriff auf große und dadurch typischerweise besonders aussagekräftige Datenbestände”.[39] Auch das Recht auf informationelle Selbstbestimmung wird deswegen bereits durch die Infiltration eines „aussagekräftigen Datenbestandes”, beispielsweise eines Mobiltelefonspeichers, beeinträchtigt.[40] Zudem wohnt auch dem Recht auf informationelle Selbstbestimmung eine Schutzdimension inne, aus der sich staatliche Schutzpflichten ergeben können.[41]

Geht es um den Zugriff auf ein IT-System zum Zwecke der Datenausspähung, wird das Recht auf informationelle Selbstbestimmung nach der verfassungsgerichtlichen Rechtsprechung aber vom IT-System-Grundrecht verdrängt.[42] Dies gilt allerdings nur, soweit das IT-System-Grundrecht auch tatsächlich Anwendung findet, d.h. es sich insbesondere um ein eigengenutztes, hinreichend qualifiziertes IT-System handelt.[43] Geltung beanspruchen kann das Recht auf informationelle Selbstbestimmung deswegen beispielsweise für auf einem IT-System gespeicherte

---

[37] BVerfG, Beschluss vom 24. Juni 2025, Rn. 223 (*Trojaner II*).

[38] BVerfG, Beschluss vom 24. Juni 2025, Rn. 223 (*Trojaner II*).

[39] BVerfG, Beschluss vom 24. Juni 2025, Rn. 223 (*Trojaner II*).

[40] BVerfG, Beschluss vom 24. Juni 2025, Rn. 223-224 (*Trojaner II*).

[41] BVerfG, Beschluss vom 17. Juli 2013, Rn. 19 f. „Die aus dem Recht auf informationelle Selbstbestimmung folgende Schutzpflicht gebietet es, dafür Sorge zu tragen, dass informationeller Selbstschutz für Einzelne tatsächlich möglich ist.”.

[42] BVerfG, Beschluss vom 24. Juni 2025, Rn. 227-230 (*Trojaner II*).

[43] BVerfG, Beschluss vom 24. Juni 2025, Rn. 230 (*Trojaner II*).

Kommunikationsdaten Dritter, da hier auch Art. 10 Abs. 1 GG als spezielle Garantie nicht betroffen sein kann.[44]

Aus diesem Grund ist denkbar, dass der Zugriff auf ein IT-System bzw. die Ermöglichung von Zugriffen auf IT-Systeme durch das Vorhalten von IT-Sicherheitslücken das Recht auf informationelle Selbstbestimmung beeinträchtigt, wenn auf diesem - wie dies oftmals der Fall sein wird - umfangreich auch Daten Dritter gespeichert sind.

5. Weitere Grundrechte der IT-Nutzenden

IT-Sicherheitslücken und dadurch ermöglichte Angriffe können ganz unterschiedliche Folgen für die betroffenen Individuen oder Einrichtungen zeitigen. Die damit angesprochenen Risiken für die Freiheit und Sicherheit Einzelner[45] können im Einzelfall auch von anderen Grundrechten abgedeckt sein.[46] Führt ein Cyberangriff zum Ausfall zentraler IT-Infrastruktur eines Krankenhauses, kann beispielsweise das Recht auf Leben und körperliche Unversehrtheit aus Art. 2 Abs. 2 Satz 1 GG betroffen sein. Bei Ransomware-Angriffen, bei denen IT-Systeme lahmgelegt oder verschlüsselt werden, um Lösegeld zu erpressen, kann die Eigentumsfreiheit des Art. 14 Abs. 1 GG betroffen sein. Wird die Infiltration eines IT-Endgeräts zur Überwachung des Wohnraums der betroffenen Person ausgenutzt, kommt eine Beeinträchtigung der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG in Betracht.[47]

---

[44] BVerfG, Beschluss vom 24. Juni 2025, Rn. 230 (*Trojaner II*), folgend „Der Schutz aus dem Recht auf informationelle Selbstbestimmung kann insofern allerdings nicht weiter reichen als derjenige aus dem IT-System-Grundrecht".

[45] Siehe auch BVerfG, Beschluss vom 8. Juni 2021, Rn. 37 (*IT-Sicherheitslücken*).

[46] Wischmeyer, Informationssicherheit, 2023, S. 4 f. Umfassend hierzu und insbesondere zur Frage der Beeinträchtigung spezieller Freiheitsrechte durch die bloße Kompromittierung eines IT-Systems auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 131-137, 197-203.

[47] Beispiel nach Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 131

Da es sich um spezielle Freiheitsrechte handelt, wird hier im Regelfall Grundrechtskonkurrenz zum jeweils ebenso beeinträchtigten IT-System-Grundrecht anzunehmen sein.[48]

Freilich wird eine rechtlich relevante Beeinträchtigung dieser Grundrechte regelmäßig erst durch die Ausnutzung einer Sicherheitslücke, nicht bereits durch die bloße Kompromittierung eines IT-Systems erfolgen.[49] Insbesondere was die Frage der verfassungsrechtlichen Zulässigkeit des staatlichen Unterlassens von Schutzmaßnahmen angeht, handelt es sich bei den genannten Beeinträchtigungen also eher um abstrakte Risiken, die zwar in die verfassungsrechtliche Bewertung einzustellen sind, für sich genommen jedoch noch keine konkreten Schutz- oder Handlungspflichten des Staates auszulösen vermögen.

6. Grundrechte der Hersteller

Schließlich kann das Offenhalten von IT-Sicherheitslücken auch Auswirkungen auf die Grundrechte der Hersteller der betroffenen IT-Komponenten haben.

Ob die Nichtmitteilung entdeckter Sicherheitslücken aber in die Berufsfreiheit aus Art. 12 Abs. 1 GG eingreift, scheint fraglich. Hier mangelt es wohl am erforderlichen Berufsbezug bzw. der berufsregelnden Tendenz.

Jedenfalls eine Beeinträchtigung in der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 Satz 1 GG kommt jedoch in Betracht.

---

[48] Siehe oben B.I.2.

[49] Siehe auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 131-137.

II. Eingriffsschwere und Bedeutung der staatlichen Kenntnis und Nutzung von IT-Schwachstellen

Die gesetzgeberische Pflicht zur Regelung des staatlichen Umgangs mit unbekannten IT-Schwachstellen[50] findet ihren Grund letztlich in einer einfachen Einsicht: die Offenhaltung unbekannter IT-Sicherheitslücken zeitigt spezifische grundrechtsbelastende Folgen, die grundrechtlich erheblich ins Gewicht fallen, und von der Ausnutzung einer Sicherheitslücken unabhängig sind. Bereits diese Folgen sind so schwerwiegend, dass sie aus verfassungsrechtlichen Gesichtspunkten parlamentarisch verantwortet werden müssen und damit ein legislatives Einschreiten erforderlich machen.[51]

Zuvörderst ist dabei zu beachten, dass von unbekannten IT-Schwachstellen für Nutzer:innen der betroffenen IT-Infrastruktur regelmäßig schwerwiegendste IT-Sicherheitsrisiken ausgehen.[52] Regelmäßig besteht ein staatliches Interesse an der Offenhaltung gerade solcher Schwachstellen, die besonders weitreichende Zugriffe auf fremde IT-Systeme ermöglichen und daher für Infiltrations- oder Manipulationszwecke geeignet sind. Über derartige Sicherheitslücken ist im Normalfall sowohl die Ausspähung des gesamten Datenbestandes eines infiltrierten Gerätes als auch dessen Veränderung und Manipulation möglich. Möglich ist dann also nicht nur die Ausspähung auch sensibelster Informationen und Aufzeichnungen, wie etwa intimer Chat-Verläufe, Bankdaten oder Gesundheitsinformationen, und damit verbunden schwerste Gefährdungen der Persönlichkeitsrechte der Betroffenen, sondern auch Angriffe wie etwa die Verschlüsselung der vorfindlichen Daten, die im Rahmen von sog. Ransomware-Attacken genutzt werden.[53] Gerade solche leistungsfähigen Schwachstellen sind jedoch nicht

---

[50] Dazu sogleich III.

[51] Zu den verschiedenen Grundlagen dieses Einschreitens, siehe B.III.

[52] Siehe bereits BVerfG, Beschluss vom 8. Juni 2021, Rn. 36-37 (*IT-Sicherheitslücken*).

[53] BVerfG, Beschluss vom 8. Juni 2021, Rn. 37 (*IT-Sicherheitslücken*).

nur für staatliche Stellen von Interesse. Vielmehr stellen sie auch für kriminelle Akteure attraktive Angriffsvektoren dar sowie für ausländische Sicherheitsbehörden, die entsprechende Schwachstellen bekanntermaßen teilweise auch ohne hinreichende rechtliche Grundlage einsetzen. Wirkt der Staat nicht auf die Schließung entsprechender Schwachstellen hin, muss er daher damit rechnen, dass diese von beliebigen Dritten ausgenutzt werden, und Grundrechtsberechtigte hierdurch zu Schaden kommen.[54] Dies gilt insbesondere dann, wenn der Staat die betreffende Schwachstelle nicht selbst entdeckt hat, sondern Kenntnis von Dritten, etwa durch Drittstaaten oder im grauen bzw. schwarzen Markt, erlangt hat.

Eng damit verbunden ist der Umstand, dass Sicherheitslücken oftmals eine unbestimmte Vielzahl von IT-Nutzenden betreffen[55] und ihre Offenhaltung deswegen Risiken von erheblicher Streubreite hervorrufen.[56] Die absolute Mehrheit dieser Betroffenen hat nie und wird nie Anlass zu sicherheitsbehördlichen Maßnahmen geben, sieht sich aber dennoch tiefgreifender Gefährdungen der von ihnen genutzten IT-Infrastruktur ausgesetzt.[57]

Dazu kommt, dass sich Einzelne – Privatpersonen sowie Unternehmen und andere Einrichtungen – gegen *Zero-Day*-Schwachstellen in der Regel nicht selbst schützen können.[58] In jedem Fall bereitet (wirksamer) informationeller

---

[54] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 65 („Kollisionsrisiko").

[55] BVerfG, Urteil vom 27. Februar 2008, Rn. 239-241 (*Online-Durchsuchungen*); BVerfG, Beschluss vom 24. Juni 2025, Rn. 193 (*Trojaner II*).

[56] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 119-120 (Schwächung „auf Vorrat", „größtmögliche Streubreite").

[57] Zu den Kriterien der Anzahl der betroffenen Grundrechtsträger und der Anlassbezogenheit einer Maßnahme BVerfG, Urteil vom 14. Juli 1999, Rn. 219 (*Telekommunikationsüberwachung I*); BVerfG, Urteil vom 2. März 2010, Rn. 210 (*Vorratsdatenspeicherung*); BVerfG, Beschluss vom 27. Mai 2020, Rn. 129 (*Bestandsdatenauskunft II*).

[58] BVerfG, Beschluss vom 8. Juni 2021, Rn. 37 (*IT-Sicherheitslücken*).

Selbstschutz erhebliche Schwierigkeiten und verursacht großen Aufwand und Kosten.[59]

Weiter ist zu berücksichtigen, dass der staatlichen Bevorratung von Kenntnissen über unbekannte IT-Sicherheitslücken ein erhebliches Verlustrisiko anhaften kann, insofern als dass die „zentrale" Speicherung derartiger Informationen für Dritte ein besonders begehrliches Angriffsziel darstellt.[60] Das Risiko, dass geheimes Wissen über IT-Schwachstellen durch Infiltration oder Cyberangriffe an Dritte gelangt, ist, wie die Geschichte zeigt, auch alles andere als theoretisch: 2016 gab beispielsweise die Hacker-Gruppe „Shadow Brokers" bekannt, Zero-Day-Exploits der National Security Agency (NSA) gestohlen zu haben. Kurz darauf wurde einer dieser Exploits in der globalen Ransomware-Kampagne „WannaCry" verwendet, die hunderttausende Computer außer Betrieb setzte und allein beim britischen Gesundheitssystem NHS einen Schaden von knapp 100 Millionen Pfund verursachte.[61]

Darüber hinaus haftet jeder Sicherheitslücke ein Missbrauchsrisiko an: sie erlaubt den über sie verfügenden Sicherheitsbehörden technisch mehr, als ihnen rechtlich gestattet ist.[62] Das betrifft zum einen das technische Potenzial der Sicherheitslücke im Kontext eines geplanten und zulässigen Einsatzes. Denn im Normalfall übersteigt die über eine bestimmte Sicherheitslücken ermöglichte Eingriffsbreite das, was gesetzlich zulässig ist.[63] Zum anderen

---

[59] BVerfG, Urteil vom 27. Februar 2008, Rn. 180 (*Online-Durchsuchungen*); Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 116-117.

[60] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 65-66 („Proliferationsrisiko").

[61] National Health Executive, „*WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled*" (12. Oktober 2018) abrufbar unter https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled.

[62] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 66 („Einsatzrisiko").

[63] Das ist schon deswegen der Fall, weil derartige Zugriffe regelmäßig unbegrenzte Lese- und Schreibrechte für das infiltrierte System beinhalten.

muss aber auch berücksichtigt werden, dass Amtsträger Sicherheitslücken auch für gänzlich unbefugte Einsätze missbrauchen können. Auch dieses Risiko entsteht bereits mit der Kenntnis einer unbekannten und ungeschlossenen Sicherheitslücke und ist von den gesetzlichen Befugnissen zur Nutzung von Sicherheitslücken unabhängig.

Zu diesen konkreten, aus der Kenntnis über die einzelne Sicherheitslücke erwachsenden Gefahren treten strukturelle Risiken hinzu, die in ihrer grundrechtsbeeinträchtigenden Wirkung nicht weniger schwerwiegend sein müssen:

Wie das Bundesverfassungsgericht bereits in der Entscheidung *Online-Durchsuchung* dargestellt hat, lösen *Zero-Day*-Schwachstellen für den Staat einen Zielkonflikt aus: das Interesse an einer möglichst hohen IT-Sicherheit konfligiert mit dem Interesse an der Ausnutzung und dadurch bedingten Geheimhaltung der Sicherheitslücke.[64] Insofern kann der Zielkonflikt „das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist"[65] und dadurch Nutzer:innen in der Wahrnehmung ihrer Freiheitsrechte im digitalen Raum hemmen. Insbesondere für Akteure, die besonders sensible Daten kommunizieren wollen, etwa Oppositionelle, Journalist:innen, aber auch staatliche Einrichtungen, können die damit angesprochenen *chilling effects*[66] spürbar sein.

Die potenzielle Nutzung von unbekannten Sicherheitslücken durch staatliche Behörden setzt weiter auch für Sicherheitsforscher:innen einen Anreiz, identifizierte Schwachstellen den betroffenen Herstellern nicht zu melden, um diese stattdessen an staatliche Abnehmer verkaufen zu können.[67] Als

---

[64] BVerfG, Urteil vom 27. Februar 2008, Rn. 241 (*Online-Durchsuchungen*).

[65] BVerfG, Urteil vom 27. Februar 2008, Rn. 241 (*Online-Durchsuchungen*).

[66] Siehe allgemein zu *chilling effects* auch BVerfG, Urteil vom 2. März 2010, Rn. 212 (*Vorratsdatenspeicherung*).

[67] BVerfG, Beschluss vom 8. Juni 2021, Rn. 42 (*IT-Sicherheitslücken*).

primäre Abnehmer von *Zero-Day*-Exploits sind staatliche Akteure tatsächlich hauptverantwortlich für das Entstehen des Marktes für derartige Sicherheitslücken[68] und tragen damit maßgeblich zur Entstehung und Persistenz erheblicher IT-Sicherheitsrisiken bei.

III. Verfassungsrechtliche Grundlagen einer gesetzlichen Pflicht zum Schwachstellenmanagement

Die verfassungsrechtliche Pflicht zur gesetzlichen Regelung des staatlichen Umgangs mit IT-Sicherheitslücken gründet auf drei parallel gültigen verfassungsrechtlichen Fundamenten: Sie ist erstens zur Erfüllung der aus dem IT-System-Grundrecht und dem Telekommunikationsgeheimnis abgeleiteten staatlichen Schutzpflicht erforderlich (dazu 1.). Sie folgt darüber hinaus aus dem Parlaments- und Wesentlichkeitsvorbehalt (dazu 2.) sowie aus dem Verhältnismäßigkeitsgebot (dazu 3.).

1. Schwachstellenmanagement und grundrechtliche Schutzpflichten

Bereits 2002 urteilte das Bundesverfassungsgericht in seiner Entscheidung zu Mithörvorrichtungen,[69] dass aus Art. 10 GG ein staatlicher Schutzauftrag folge, Telekommunikation vor dem Zugriff privater Dritter zu bewahren.[70] Dieser Schutzauftrag gründe in der besonderen Anfälligkeit von Telekommunikation gegenüber derartigen unbefugten Zugriffen.[71]

In seinem „IT-Sicherheitslücken"-Beschluss vom Juni 2021,[72] der eine 2017 verabschiedeten Ermächtigung zur Quellen-

---

[68] Siehe auch B.VI.1.a).

[69] In den beiden gegenständlichen Verfahren hatten Dritte ein Telefongespräch jeweils über die in handelsüblichen Festnetztelefonen verbauten Freisprechfunktionen mitgehört.

[70] BVerfG, Beschluss vom 9. Oktober 2002, Rn. 21 (*Mithörvorrichtung*).

[71] BVerfG, Beschluss vom 9. Oktober 2002, Rn. 20 (*Mithörvorrichtung*).

[72] BVerfG, Beschluss vom 8. Juni 2021, Rn. 26 ff. (*IT-Sicherheitslücken*).

Telekommunikationsüberwachung (Quellen-TKÜ) im Baden-Württembergischen Polizeigesetz betraf, konkretisierte das Gericht diesen Schutzauftrag sodann zu einer grundrechtliche Schutzpflicht.[73]

Die Beschwerdeführenden hatten hier gerügt, dass die Ermächtigung zum Einsatz der Quellen-TKÜ zur Folge hätte, dass Polizeibehörden ihnen bekannte *Zero-Day*-Schwachstellen nicht den Herstellern melden, sondern diese vielmehr offenhalten würden, um sie zu Infiltrationszwecken auszunutzen.[74] Dies ermögliche auch Angriffe von dritter Seite.[75] Der durch die Befugnis ausgelöste Anreiz, IT-Sicherheitslücken nicht den betroffenen Herstellern zu melden, bedeute deshalb eine Verletzung der aus der objektiv-rechtlichen Dimension des IT-System-Grundrechts abgeleiteten Schutzpflicht des Staates.[76] Diese könne nur durch eine zwingend gesetzlich zu verankernde Begleitregelung zum Schwachstellenmanagement erfüllt werden, die ein geregeltes Verfahren zur Beurteilung von und Entscheidung über *Zero-Day*-Schwachstellen vorsehen müsse.[77]

Das Bundesverfassungsgericht bestätigte diese Argumentation im Wesentlichen und bejahte eine konkrete staatliche Schutzpflicht: Wo staatliche Behörden von einer den Herstellern unbekannten Sicherheitslücken wüssten, sei der Staat verpflichtet, die Nutzer:innen informationstechnischer Systeme vor Angriffen Dritter auf diese Systeme zu schützen.[78] Dies folge aus der Art. 10 Abs. 1 GG und dem hier konkurrierend anzuwendenden IT-System-Grundrecht entspringenden Schutzdimension.[79]

---

[73] BVerfG, Beschluss vom 8. Juni 2021, Rn. 26 (*IT-Sicherheitslücken*).

[74] BVerfG, Beschluss vom 8. Juni 2021, Rn. 4 (*IT-Sicherheitslücken*).

[75] BVerfG, Beschluss vom 8. Juni 2021, Rn. 4 (*IT-Sicherheitslücken*).

[76] BVerfG, Beschluss vom 8. Juni 2021, Rn. 9 (*IT-Sicherheitslücken*).

[77] BVerfG, Beschluss vom 8. Juni 2021, Rn. 10 (*IT-Sicherheitslücken*).

[78] BVerfG, Beschluss vom 8. Juni 2021, Rn. 26 (*IT-Sicherheitslücken*).

[79] BVerfG, Beschluss vom 8. Juni 2021, Rn. 33 (*IT-Sicherheitslücken*).

Diese Schutzdimension gründe auf der Einsicht, dass Bürgerinnen und Bürger zur Wahrnehmung ihrer grundrechtlich geschützten Entfaltungsfreiheit heutzutage auf die Nutzung vernetzter Informationstechnik angewiesen seien und sich den Gefahren dieser Nutzung damit immer weniger entziehen könnten.[80] Deshalb treffe den Staat „eine Pflicht, dazu beizutragen, dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt werden".[81]

Wisse der Staat von Sicherheitslücken, die Herstellern und Nutzer:innen unbekannt seien, „verdicht[e] sich der allgemeine Schutzauftrag zu einer konkreten grundrechtlichen Verpflichtung, die Nutzerinnen und Nutzer informationstechnischer Systeme davor zu schützen, dass Dritte über unbekannte Sicherheitslücken die genutzten Systeme infiltrieren".[82] Diese Schutzpflicht stütze sich auf drei Gründe: Erstens wohnten IT-Sicherheitslücken hohe Gefährdungs- und Schädigungspotenziale inne, und dies nicht nur für die Privatsphäre von Bürgerinnen und Bürgern, sondern etwa auch für Betriebe und den wirtschaftlichen Handel im Allgemeinen.[83] Zweitens könnten sich Einzelne gegen die Gefahren unbekannter Sicherheitslücken in der Regel nicht wirksam schützen.[84] Drittens bestehe in den erfassten Fällen eine besondere Schutzverpflichtung des Staates, weil dieser, im Gegensatz zu den Herstellern und Nutzer:innen der Infrastruktur, Kenntnis von der Schutzlücke habe.[85]

Diese Schutzpflicht schließe zwar die Nutzung von Schutzlücken zu Infiltrationszwecken nicht aus, verlange aber vom Gesetzgeber „eine

---

[80] BVerfG, Beschluss vom 8. Juni 2021, Rn. 33 (*IT-Sicherheitslücken*).

[81] BVerfG, Beschluss vom 8. Juni 2021, Rn. 33 (*IT-Sicherheitslücken*).; umfassend zu den Gründen einer staatlichen Schutzpflicht für die IT-Sicherheit auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 176-185.

[82] BVerfG, Beschluss vom 8. Juni 2021, Rn. 34 (*IT-Sicherheitslücken*).

[83] BVerfG, Beschluss vom 8. Juni 2021, Rn. 36-38 (*IT-Sicherheitslücken*).

[84] BVerfG, Beschluss vom 8. Juni 2021, Rn. 39 (*IT-Sicherheitslücken*).

[85] BVerfG, Beschluss vom 8. Juni 2021, Rn. 40 (*IT-Sicherheitslücken*).

Regelung darüber, wie die Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikations-überwachungen andererseits aufzulösen hat".[86]

Konkret müsse der Behörde „eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine *Zero-Day*-Schutzlücke bekannt wird".[87] Dabei sei „sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an den Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt".[88]

Im Ergebnis ließ das Bundesverfassungsgericht die Beschwerde daran scheitern, dass die Beschwerdeführenden den besonderen verfassungsrechtlichen Darlegungsanforderungen, die zur Substantiierung einer Schutzpflichtverletzung erfüllt werden müssen, nicht genügt hätten.[89] Da nämlich das Bundesverfassungsgericht eine Schutzpflichtverletzung nur dann feststellen könne, „wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben",[90] sei bereits zur Begründung der Möglichkeit einer

---

[86] BVerfG, Beschluss vom 8. Juni 2021, Rn. 44 (*IT-Sicherheitslücken*); siehe auch Rn. 34, 41-43.

[87] BVerfG, Beschluss vom 8. Juni 2021, Rn. 44 (*IT-Sicherheitslücken*).

[88] BVerfG, Beschluss vom 8. Juni 2021, Rn. 44 (*IT-Sicherheitslücken*).

[89] BVerfG, Beschluss vom 8. Juni 2021, Rn. 48-66 (*IT-Sicherheitslücken*).

[90] BVerfG, Beschluss vom 8. Juni 2021, Rn. 50 (*IT-Sicherheitslücken*) (st.Rspr.).

Grundrechtsverletzung erforderlich, „den gesetzlichen Regelungszusammenhang insgesamt zu erfassen", wozu zumindest „die einschlägigen Regelungen des als unzureichend beanstandeten Normkomplexes [...] in Grundzügen dargestellt" werden müssten und begründet werden müsse, „warum vom Versagen der gesetzgeberischen Konzeption auszugehen ist".[91]

Die Beschwerde hätte sich demnach zum einen mit der in der gegenständlichen Ermächtigungsbefugnis enthaltenen Klausel zum „Schutz des eingesetzten Mittels gegen unbefugte Nutzung", und zum anderen mit verschiedenen Regelungen des Polizei-, Datenschutz- und Cybersicherheitsrechts und dem untergesetzlich normierten Meldestandard des IT-Planungsrats[92] auseinandersetzen müssen.[93] Zur Wahrung der Subsidiarität hätten die Beschwerdeführenden außerdem versuchen müssen, Auslegungsfragen bezüglich dieser Regelungen durch die Fachgerichte zu erreichen.[94]

Das Bestehen einer konkretisierten staatlichen Schutzpflicht, die den Staat zur Regelung des Umgangs mit IT-Sicherheitslücken verpflichtet, wurde in den Entscheidungen „Hessentrojaner",[95] „Bayerisches Verfassungsschutzgesetz",[96] „Trojaner I",[97] und „Trojaner II"[98] bekräftigt. Auch in diesen Entscheidungen sah das Gericht allerdings schon das

---

[91] BVerfG, Beschluss vom 8. Juni 2021, Rn. 51 (*IT-Sicherheitslücken*).

[92] IT-Planungsrat, Verbindliches Meldeverfahren zum Informationsaustausch über Cyberangriffe (5.10.2017), abrufbar unter https://www.it-planungsrat.de/fileadmin/beschluesse/2017/Beschluss2017-35_Meldestandards_Anlage1.pdf.

[93] BVerfG, Beschluss vom 8. Juni 2021, Rn. 53-66 (*IT-Sicherheitslücken*).

[94] BVerfG, Beschluss vom 8. Juni 2021, Rn. 67-74 (*IT-Sicherheitslücken*).

[95] BVerfG, Beschluss vom 20. Januar 2022, Rn. 17 (*Hessentrojaner*).

[96] BVerfG, Urteil vom 26. April 2022, Rn. 111 (*Bayerisches Verfassungsschutzgesetz*).

[97] BVerfG, Beschluss vom 24. Juni 2025, Rn. 51-53 (*Trojaner I*).

[98] BVerfG, Beschluss vom 24. Juni 2025, Rn. 108 (*Trojaner II*).

Zulässigkeitserfordernis der hinreichenden Substantiierung einer Schutzpflichtverletzung nicht erfüllt, da die Beschwerdeführenden entsprechend dem benannten Maßstab wiederum nicht hinreichend dargelegt hätten, dass unter Berücksichtigung des gesetzlichen Regelungszusammenhangs vom Versagen der gesetzgeberischen Konzeption auszugehen sein könnte.[99]

Die Zurückhaltung des Bundesverfassungsgerichts ist nicht nur aus prozessualen Gründen nachvollziehbar. Im demokratischen Verfassungsstaat ist es nämlich in erster Linie Sache des Gesetzgebers, Gefahren für die Grundrechte entgegenzuwirken. Dabei kommt ihm grundsätzlich auch ein Einschätzungs-, Wertungs- und Gestaltungsspielraum zu.[100] Allerdings lässt die Tatsache, dass das Bundesverfassungsgericht in ständiger Rechtsprechung eine Schutzpflicht*verletzung* nur dann feststellen will, „wenn Schutzvorkehrungen entweder überhaupt nicht getroffen sind, wenn die getroffenen Regelungen und Maßnahmen offensichtlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder wenn sie erheblich hinter dem Schutzziel zurückbleiben“,[101] die objektiv-rechtliche Verpflichtung des Gesetzgebers, seiner Schutzpflicht nachzukommen, nicht entfallen. Der Gesetzgeber muss also von Verfassungs wegen im Interesse des Grundrechtsschutzes umfassend tätig werden, auch wenn nicht jedes Zurückbleiben hinter den verfassungsrechtlichen Erwartungen unmittelbar justiziabel ist.

Die Tatsache, dass das Bundesverfassungsgericht im *IT-Sicherheitslücken*-Beschluss nicht nur das Vorliegen einer grundrechtlichen Schutzpflicht für die IT-Sicherheit, also eine konkrete objektiv-rechtliche Bindung des parlamentarischen Gesetzgebers bejaht hat, sondern diese Pflicht zugleich

---

[99] BVerfG, Beschluss vom 20. Januar 2022, Rn. 17 (*Hessentrojaner*).; BVerfG, Urteil vom 26. April 2022, Rn. 111 (*Bayerisches Verfassungsschutzgesetz*); BVerfG, Beschluss vom 24. Juni 2025, Rn. 52-53 (*Trojaner I*); BVerfG, Beschluss vom 24. Juni 2025, Rn. 108 (*Trojaner II*).

[100] BVerfG, Beschluss vom 24. März 2021, Rn. 152 (*Klimaschutzgesetz*) (m.w.N).

[101] BVerfG, Beschluss vom 24. März 2021, Rn. 152 (*Klimaschutzgesetz*) (m.w.N).

auf die gesetzliche Verankerung eines Schwachstellenmanagement-Prozesses hin konkretisiert hat,[102] kann und muss daher als explizite Aufforderung an den Gesetzgeber verstanden werden, in diese Richtung tätig zu werden.

Dieser Auftrag ist dringlich, denn die vom Bundesverfassungsgericht für die Erfüllung der Schutzpflicht als potenziell relevant angeführten gesetzlichen Regelungen stellen bei gründlicher Analyse offensichtlich keine den Anforderungen des Gerichts gerecht werdenden Schutzvorkehrungen dar.[103] Auch anderen, teils nach den Entscheidungen *IT-Sicherheitslücken* und *Bayerisches Verfassungsschutzgesetz* in Kraft getretenen Regelungswerken, insbesondere dem überarbeiteten BSI-Gesetz, dem Cyber Resilience Act und dem Cybersecurity Act, lässt sich – wie in Teil C. teils noch gezeigt wird – bisher kein hinreichendes Schutzkonzept entnehmen.[104] Aktuell muss daher konstatiert werden, dass das bestehende gesetzliche Regelwerk zur Erfüllung der aus dem IT-System-Grundrecht abgeleiteten Schutzpflicht wohl tatsächlich gänzlich ungeeignet und völlig unzulänglich ist,[105] und die Erfüllung der Pflicht zur gesetzlichen Regelung des Schwachstellenmanagements weiter aussteht.

2. Schwachstellenmanagement und Grundsatz der Wesentlichkeit

Auch der verfassungsrechtlich begründete Parlamentsvorbehalt und der damit eng verzahnte Grundsatz der Wesentlichkeit sprechen stark für die verfassungsrechtliche Notwendigkeit der gesetzlichen Verankerung des Schwachstellenmanagements.

---

[102] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 189-190.

[103] Vertiefend Wischmeyer, *Informationssicherheitsrecht*, 2023, S. 290-292 („Nebelkerzen"); Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 237-257.

[104] Siehe unten C.II.

[105] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 258 (m.w.N.).

In ständiger Rechtsprechung leitet das Bundesverfassungsgericht aus Rechtsstaatsprinzip und Demokratiegebot die Pflicht des Gesetzgebers ab, „in allen grundlegenden normativen Bereichen die wesentlichen Entscheidungen selbst zu treffen".[106] Der Gesetzgeber ist deswegen insbesondere verpflichtet, „die für die Grundrechtsverwirklichung maßgeblichen Regelungen im Wesentlichen selbst zu treffen und diese nicht dem Handeln und der Entscheidungsmacht der Exekutive zu überlassen".[107] Durch den Parlamentsvorbehalt soll dabei gewährleistet werden, dass grundlegende politische Entscheidungen in einem transparenten, demokratischen Diskurs getroffen werden und dass über Notwendigkeit und Umfang von Grundrechtseingriffen öffentlich Rechenschaft abgelegt wird.[108]

Was dabei als grundrechts-wesentlich gilt und demnach vom Gesetzgeber zu verantworten ist, ist vom Verfassungsgericht nur rudimentär umrissen. Ausschlaggebend ist zunächst „die Bedeutung des Regelungsgegenstandes und die Intensität der durch die Regelung oder aufgrund der Regelung erfolgenden Grundrechtseingriffe".[109] Eine Pflicht zum legislativen Einschreiten „besteht insbesondere in mehrdimensionalen, komplexen Grundrechtskonstellationen, in denen miteinander konkurrierende Freiheitsrechte aufeinander treffen und deren jeweilige Grenzen fließend und nur schwer auszumachen sind".[110] „Wann und inwieweit es einer Regelung durch den Gesetzgeber bedarf, lässt sich [allerdings] nur mit Blick auf den jeweiligen Sachbereich und auf die Eigenart des betroffenen Regelungsgegenstandes bestimmen".[111]

---

[106] BVerfG, Urteil vom 19. September 2018, Rn. 191 (*Zensus 2011*) (st. Rspr.).

[107] BVerfG, Beschluss vom 21. April 2015, Rn. 53 (*Altershöchstgrenzen*) (st.Rspr.).

[108] BVerfG, Beschluss vom 21. April 2015, Rn. 53 (*Altershöchstgrenzen*).

[109] BVerfG, Urteil vom 19. September 2018, Rn. 196 (*Zensus 2011*).

[110] BVerfG, Beschluss vom 21. April 2015, Rn. 53 (*Altershöchstgrenzen*); BVerfG, Urteil vom 19. September 2018, Rn. 194 (*Zensus 2011*).

[111] BVerfG, Urteil vom 19. September 2018, Rn. 193 (*Zensus 2011*) (st. Rspr.).

Die Wesentlichkeit einer Materie entscheidet sodann nicht nur über die Frage, *was* vom Gesetzgeber selbst geregelt werden muss, sondern auch *in welchem Umfang* und *in welcher Bestimmtheit*.[112] Je wesentlicher die zu entscheidenden Fragen, desto umfänglicher und dichter muss die legislative Regelung ausfallen. Nur so ist eine effektive Begrenzung und Steuerung der Verwaltung und eine wirksame Kontrolle durch die Gerichte möglich.[113] Die Komplexität oder Entwicklungsoffenheit eines bestimmten Regelungsbereichs können einer besonders detaillierten legislativen Gestaltung allerdings entgegenstehen.[114]

Anhand dieser Maßstäbe sprechen die folgenden guten Gründe für die Annahme einer grundrechtlichen Pflicht zur gesetzgeberischen Regelung des Umgangs mit IT-Sicherheitslücken:[115] Wie bereits dargestellt hat der Umgang mit IT-Sicherheitslücken umfängliche Auswirkungen auf verschiedene Grundrechte.[116] Das gilt nicht nur für die Nutzung einer Schwachstelle, sondern aufgrund der oben angesprochenen Risiken[117] bereits für die Entscheidung über die Offenhaltung einer Schwachstelle, wie dies auch durch den *IT-Schwachstellen*-Beschluss zum Ausdruck kommt. Bereits diese Entscheidung ist aus den benannten Gründen deswegen schon grundrechtserheblich.

Es handelt sich insofern um eine „mehrdimensionale, komplexe Grundrechtskonstellation", in der die Verwerfungen zwischen den unterschiedlichen konfligieren Grundrechten und Verfassungswerten schwer zu bestimmen sind. Gerade diese Komplexität und Konflikthaftigkeit der betroffenen Grundrechtspositionen legt es nahe, die erforderlichen

---

[112] BVerfG, Urteil vom 19. September 2018, Rn. 196 (*Zensus 2011*) (st. Rspr.).

[113] BVerfG, Urteil vom 19. September 2018, Rn. 196 (*Zensus 2011*) (st. Rspr.).

[114] BVerfG, Urteil vom 19. September 2018, Rn. 196 f. (*Zensus 2011*).

[115] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 195-197.

[116] Siehe oben B.I.

[117] Siehe oben B.II.

Abwägungsentscheidungen dem parlamentarischen Gesetzgeber vorzubehalten. Denn bei der Entscheidung über das Offenhalten oder Melden einer IT-Schwachstelle geht es nicht lediglich um technische oder operative Fragen der Gefahrenabwehr, sondern um grundlegende Wertungsentscheidungen über das Verhältnis zwischen staatlichen Sicherheitsinteressen, der IT-Sicherheit der Allgemeinheit und den Freiheitsrechten der Betroffenen. Solche Entscheidungen berühren zentrale Fragen der Freiheitssicherung im digitalen Raum und bedürfen daher einer demokratisch legitimierten und öffentlich verantworteten Regelung durch den Gesetzgeber.

Hinzu kommt, dass der Umgang mit unbekannten IT-Sicherheitslücken naturgemäß durch strukturelle Intransparenz geprägt ist. Entscheidungen über die Bevorratung, Nutzung oder Offenlegung von Schwachstellen erfolgen regelmäßig innerhalb der Exekutive und unterliegen aufgrund der Geheimhaltungsbedürftigkeit nur sehr eingeschränkter öffentlicher Kontrolle. Gerade unter solchen Bedingungen kommt dem parlamentarischen Gesetzgeber die Aufgabe zu, durch gesetzliche Vorgaben Entscheidungsverfahren, Abwägungskriterien und Kontrollmechanismen festzulegen, um eine rechtsstaatlich hinreichende Begrenzung exekutiver Handlungsspielräume sicherzustellen. Auch diese Aspekte sprechen dafür, dass die maßgeblichen Leitentscheidungen nicht der Verwaltung überlassen werden dürfen, sondern im Wege parlamentarischer Gesetzgebung zu treffen sind.[118]

3. Schwachstellenmanagement und Verhältnismäßigkeit staatlichen Schwachstellenerwerbs und -nutzung

Wie bereits erörtert, kann der staatliche Umgang mit IT-Schwachstellen auf vielfältige Arten (negative) Effekte auf die Ausübung der Grundrechte zeitigen und, sofern die Schwelle zum Grundrechtseingriff erreicht ist, für die

---

[118] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 195-197.

abwehrrechtliche Dimension der Grundrechte relevant sein. Die Ausnutzung von Schwachstellen zu Infiltrationszwecken etwa stellt eindeutig einen Grundrechtseingriff dar. Auch das Ankaufen, Erforschen, Vorhalten oder Teilen von Sicherheitslücken kann aber bereits Grundrechte, insbesondere das IT-System-Grundrecht, beeinträchtigen.

Unabhängig von der Frage, welche dieser Aktivitäten konkret die Schwelle zum Grundrechtseingriff überschreiten, ist mit dieser abwehrrechtlichen Perspektive die Frage nach der Verhältnismäßigkeit Schwachstellen-bezogener staatlicher Handlungen aufgeworfen. Der Grundsatz der Verhältnismäßigkeit wird in entsprechenden Konstellationen insofern auch vom Bundesverfassungsgericht als zentraler Maßstab der Rechtfertigung von Eingriffen in persönlichkeitsrechtsschützende Grundrechte betrachtet.[119] Eine gesetzliche Pflicht zum Schwachstellen-Management würde für alle Schwachstellen-bezogenen staatlichen Aktivitäten einen Beitrag zur Sicherung eben dieser Verhältnismäßigkeit leisten, und könnte in gewissen Situationen sogar unverzichtbar sein.

Dies ergibt sich aus der Funktion des Schwachstellen-Managements für die Verhältnismäßigkeitsprüfung: Zentraler Parameter dieser Prüfung ist zunächst die Schwere des Eingriffs.[120] Wie bereits dargestellt wurde,[121] hat auch das Bundesverfassungsgericht bereits mehrmals betont, dass die Nutzung und damit einhergehende Offenhaltung von IT-Sicherheitslücken die Schwere der durch sicherheitsbehördliche Eingriffsbefugnisse ausgelösten Eingriffe erhöht.[122]

Im Gegenzug würde die gesetzliche Regelung des Umgangs mit IT-Schwachstellen das Gewicht entsprechender Beeinträchtigungen

---

[119] BVerfG, Beschluss vom 24. Juni 2025, Rn. 124 (*Trojaner I*).

[120] BVerfG, Beschluss vom 24. Juni 2025, Rn. 124 (*Trojaner I*).

[121] Siehe B.II.

[122] BVerfG, Urteil vom 27. Februar 2008, Rn. 139-142 (*Online-Durchsuchungen*); BVerfG, Beschluss vom 24. Juni 2025, Rn. 193 (*Trojaner II*) f.

reduzieren. Eine Regelung würde nämlich nicht nur verfahrensmäßig absichern, dass die Nutzbarkeit einer Schwachstelle vor dem Hintergrund ihres Schädigungspotenzials gerechtfertigt werden kann, sondern darüber hinaus auch ein gewisses Maß an Transparenz und aufsichtlicher Kontrolle ermöglichen.[123]

Außerdem stellt das Bundesverfassungsgericht in ständiger Rechtsprechung fest, dass der Verhältnismäßigkeitsgrundsatz bei heimlichen Überwachungsmaßnahmen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtlicher Kontrolle stellt.[124] Wertet man, wie bereits angesprochen,[125] richtigerweise bereits die Entscheidung über die Offenhaltung einer Schwachstelle als grundrechtserheblich, wie dies auch durch den IT-Schwachstellen-Beschluss zum Ausdruck kommt, liegt nahe, diese Anforderungen im Grundsatz auch auf das Schwachstellenmanagement zu übertragen. Weil Transparenz und individuellem Rechtsschutz bei der Offenhaltung von IT-Sicherheitslücken, wie auch beim Einsatz heimlicher Überwachungsmethoden, allerdings enge Grenzen gesetzt sind, kommt der aufsichtlichen Kontrolle insofern besondere Bedeutung zu.[126] Kontrolle ist aber nur möglich, wo über die Verwendung einer Schwachstelle formell entschieden wurde und diese Entscheidung samt der sie bestimmenden Überlegungen protokolliert wurde.[127] Eine solche verbindliche, gleichförmige und gerichtlich überprüfbare Entscheidungs- und Protokollierungspflicht lässt sich indes nicht durch bloße verwaltungsinterne Vorgaben sicherstellen, die die Exekutive jederzeit ändern und der parlamentarischen wie gerichtlichen Kontrolle entziehen könnte. Da es zudem – wie gezeigt – um grundrechtswesentliche Leitentscheidungen geht,

---

[123] Zu den letzten beiden Punkten, siehe auch B.IV.7. und B.V.3.

[124] BVerfG, Urteil vom 20. April 2016, Rn. 134 ff. (*BKA-Gesetz*).

[125] Siehe oben B.III.2.

[126] BVerfG, Urteil vom 20. April 2016, Rn. 140 (*BKA-Gesetz*).

[127] Vgl. auch BVerfG, Urteil vom 20. April 2016, Rn. 141 (*BKA-Gesetz*).

ist der Gesetzgeber gehalten, die maßgeblichen Verfahrens-, Abwägungs- und Kontrollanforderungen selbst zu regeln. Dies kann letztlich nur durch eine gesetzliche Regulierung des Schwachstellenmanagements erreicht werden.

IV. Verfassungsrechtliche Mindestanforderungen

Geht man mit den vorangehenden Überlegungen davon aus, dass sich aus der Verfassung eine gesetzgeberische Pflicht zur Regelung des staatlichen Umgangs mit IT-Schwachstellen ergibt, stellt sich weiter die Frage, wie diese Regelung ausgestaltet werden muss.

Dabei lassen sich aus der verfassungsgerichtlichen Rechtsprechung sowie aus allgemeinen verfassungsrechtlichen Erwägungen bestimmte Mindestanforderungen an die Ausgestaltung einer behördlichen Pflicht zum IT-Schwachstellenmanagement ableiten (dazu sogleich 1.–8.). Für weitere Regelungsaspekte enthält die Verfassung hingegen keine konkreten Vorgaben; insoweit können Anforderungen lediglich aus Gesichtspunkten sachgerechter Ausgestaltung entwickelt werden (dazu II.).

1. Formell-gesetzliche Regelung

a) Formell-gesetzliche Verankerung

Zunächst ist das Schwachstellenmanagement zwingend durch formelles Gesetz zu regeln und darf nicht im Ganzen auf untergesetzliche Normsetzungs- oder Verwaltungsverfahren delegiert werden.

Im IT-Sicherheitslücken-Beschluss hielt das Bundesverfassungsgericht insofern selbst fest: „Die Schutzpflicht schließt hier eine *Verpflichtung des Gesetzgebers* ein, den Umgang der Polizeibehörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, zu regeln".[128]

---

[128] BVerfG, Beschluss vom 8. Juni 2021, Rn. 41 (*IT-Sicherheitslücken*).

Dem kann nicht entgegengehalten werden, dass das Bundesverfassungsgericht in seiner kursorischen, als *obiter dictum* erfolgenden Darstellung relevanter bestehender Regelungen auch auf den vom IT-Planungsrat[129] beschlossenen Meldestandard „Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund" und damit auf eine weder formell- noch materiell-gesetzliche Regelung einging. Zum einen ist nämlich sowohl die Pflicht zur Festlegung von IT-Sicherheitsstandards wie dem Meldestandard als auch deren Bindungswirkung gesetzlich verankert (§ 2 Abs. 1 bzw. Abs. 2 IT-Staatsvertrag). Zum anderen merkte auch das Bundesverfassungsgericht selbst an, dass „näherer Prüfung" bedürfe, „[i]nwieweit der grundrechtlichen Schutzpflicht durch untergesetzlich normierte Mitteilungspflichten genügt werden kann und ob die gesetzliche Verankerung dieser Normierung hier ausreicht".[130] Gleichzeitig verwies es auf die übrigen in Frage kommenden gesetzlich normierten Regelungen.

Im Übrigen leitet sich die Pflicht zur gesetzlichen Verankerung der behördlichen Pflicht zum Schwachstellen-Management auch aus dem Parlaments- und Wesentlichkeitsvorbehalt ab,[131] da die staatliche Entscheidung über die Geheimhaltung oder Offenlegung von IT-Sicherheitslücken, wie oben gezeigt, für den Ausgleich konfligierender Grundrechte und Verfassungsgütern und damit verfassungsrechtlich insgesamt wesentlich ist.

b) Regelungsumfang der formell-gesetzlichen Verankerung

Fraglich ist sodann, welchen Detailgrad die formell-gesetzliche Regelung bzw. Verankerung des Schwachstellenmanagements erreichen muss,

---

[129] Beim IT-Planungsrat handelt es sich um ein Steuerungsgremium von Bund und Ländern, welches die Zusammenarbeit im Bereich der nach Art. 91c GG eingeführten gemeinsamen Informationstechnik koordiniert.

[130] BVerfG, Beschluss vom 8. Juni 2021, Rn. 66 (*IT-Sicherheitslücken*).

[131] Siehe oben B.III.2.

respektive welche Regelungsentscheidungen untergesetzlicher Normgebung oder der behördlichen Praxis überantwortet werden dürfen.

Klar ist zunächst, dass die gesetzliche Regelung mindestens diejenigen Aspekte regeln muss, die vom Bundesverfassungsgericht im IT-Sicherheitslücken-Beschluss explizit als Bestandteile der zu schaffenden gesetzlichen Regelung benannt wurden,[132] d.h. die Bestimmung eines Abwägungsprozesses inklusive der abzuwägenden Belange (dazu 3.) und die Festschreibung eines Regel-Ausnahme-Verhältnisses (dazu 4.).

Weiter gehört es zum Wesentlichen einer Schwachstellen-Regelung, *wen* die Entscheidungspflicht *in welchen Fällen* trifft (Frage der Regelungsadressaten und des Regelungsgegenstandes, dazu 2.) *wer* die Entscheidung über Geheimhaltung oder Offenlegung trifft (Frage der Entscheidungszuständigkeit, dazu)[133] und welche Handlungspflichten die Entscheidung auslösen kann (Frage der Entscheidungsfolgen, dazu 6.). Schließlich muss das Gesetz zumindest auch im Grundsatz Regelungen für den Schutz geheimgehaltener Sicherheitslücken (dazu 7.) und zur Aufsicht und Kontrolle der getätigten Entscheidung (dazu 8.) vorsehen.

Andere Aspekte der materiellen und verfahrensmäßigen Ausgestaltung des Schwachstellen-Managements, etwa spezifischere Vorgaben zur (Standardisierung der) Auswahl, Gewichtung und Relationierung abzuwägender Belange, zur Ausgestaltung des Entscheidungsverfahrens (bspw. Aufgabenverteilung, Sub-Zuständigkeiten) oder zu etwaigen Transparenzpflichten können hingegen an den Verordnungsgesetzgeber delegiert werden.

---

[132] Dazu bereits oben B.III.1.

[133] Was die Frage der Entscheidungsbefugnis angeht, stehen dem Gesetzgeber allerdings verschiedene Regelungsoptionen offen (dazu deswegen auch B.V.1.).

2. Regelungsadressaten und Regelungsgegenstand

Die erste Frage, die eine gesetzliche Regelung zum Schwachstellen-Management beantworten muss, ist jene nach den Regelungsadressaten und dem Regelungsumfang: Welche staatlichen Einrichtungen sollen im Falle der Kenntnis welcher IT-Sicherheitslücken ein geordnetes Verfahren zur Entscheidung über den Umgang mit selbigen durchlaufen?

Der Aspekt der erfassten Einrichtungen lässt sich dabei direkt aus dem IT-Sicherheitslücken-Beschluss ableiten. Dieser begrenzt das Entstehen der staatlichen Schutzpflicht nicht auf bestimmte Behörden;[134] alle denkbaren Behörden und staatlichen Einrichtungen müssen im Falle der Kenntnis einer erfassten Sicherheitslücke das Schwachstellenmanagement-Verfahren durchlaufen.[135]

Erfasst sind allerdings nur *Zero-Day*-Schutzlücken, d.h. Schutzlücken, die Herstellern unbekannt sind. Zwar gehen auch von *N-Day*-Schutzlücken erhebliche Sicherheitsgefahren aus, die sowohl von kriminellen als auch von staatlichen Akteuren genutzt werden.[136] Die spezifischen Gefahren, die das Entstehen einer staatlichen Schutzpflicht nach dem IT-Sicherheitslücken-Beschluss begründen – besonders schwerwiegende Infiltrationsrisiken, keine Möglichkeit des digitalen Selbstschutzes, Handlungsmöglichkeit des Staates bei gleichzeitiger Handlungsunmöglichkeit des betroffenen Herstellers –, liegen so aber nur bei unbekannten Schwachstellen vor.[137] Die

---

[134] BVerfG, Beschluss vom 8. Juni 2021, Rn. 35 (*IT*-Sicherheitslücken) „Werden den staatlichen Behörden Sicherheitslücken bekannt, verdichtet sich der allgemeine Schutzauftrag des Staates zu einer konkreten grundrechtlichen Schutzpflicht".

[135] Freilich kann dieser Schutzauftrag nicht die Regelungskompetenz des Bunds- oder Landesgesetzgebers erweitern, sodass, wie unten noch darzustellen ist (C.III.), der Bund nur zur Verpflichtung der eigenen Behörden gehalten ist.

[136] Siehe auch Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 12.

[137] BVerfG, Beschluss vom 8. Juni 2021, Rn. 35-40 (*IT-Sicherheitslücken*), Rn. 40 „Gerade aus dieser Kenntnis und der gleichzeitigen Unkenntnis des Herstellers und der fehlenden Selbstschutzmöglichkeit der Betroffenen erwächst die besondere Schutzverpflichtung des Staates".

Schwachstelle darf deshalb weder dem Hersteller noch öffentlich bekannt sein.[138]

Das Bundesverfassungsgericht sieht hier auch keinen Unterschied zwischen Schwachstellen, die der Staat selbst entdeckt hat, und solchen, die er von Dritten beschafft hat.[139] Auf spezifische Fragen, die beim Erwerb von Schwachstellen durch private oder staatliche Dritte auftreten, wird unten zurückgekommen.[140]

Weiter ist nach dem Beschluss auch keine Begrenzung der erfassten Sicherheitslücken, beispielsweise nach der Art der betroffenen IT-Infrastruktur, angezeigt. Werden IT-Systeme ausschließlich von staatlichen Einrichtungen in ihrer Funktion als Hoheitsträger genutzt, können diese sich nicht auf Grundrechte berufen, sodass die verfassungsrechtliche Schutzpflicht nicht ausgelöst wird. Deshalb ist denkbar, dass sog. Government off-the-shelf Komponenten (GOTS), d.h. Soft- oder Hardware, die eigens für den staatlichen Einsatz hergestellt wurde, vom Umfang der Schutzpflicht ausgenommen wird. Eine diesbezügliche Ausnahme scheint sich allerdings jedenfalls aus Zweckmäßigkeitserwägungen zu verbieten.[141]

Eine Ausnahme ist allerdings für Schwachstellen zu machen, die dem Staat einzig zum Zwecke der koordinierten Offenlegung im sog. Coordinated

---

[138] Öffentliche Bekanntheit besteht dabei, wenn die Schwachstelle in öffentlich zugänglichen Quellen dokumentiert ist; siehe auch *Vulnerabilities Equities Policy and Process for the United States Government* (*U.S. VEP*) (15.11.2017), abrufbar unter https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF, S. 12.

[139] BVerfG, Beschluss vom 8. Juni 2021, Rn. 40 (*IT-Sicherheitslücken*).

[140] Siehe B.VI.

[141] Auch der VEP bezieht ausdrücklich alle Arten von Hard- und Software ein, *U.S. VEP* (2017) S. 3 „This policy [...] includes Government off-the-shelf (GOTS), Commercial off-the-shelf (COTS), or other commercial information systems (to include open-source software), Industrial Control Systems (ICS) or products, and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).".

Vulnerability Disclosure (CVD)-Verfahren[142] übermittelt wurden. Diese Schwachstellen müssen unmittelbar den betroffenen Herstellern gemeldet werden und dürfen deshalb nicht in den Schwachstellen-Management-Prozess eingespeist werden.[143] Meldende vertrauen hier darauf, dass die Information ausschließlich zur Weiterleitung an die betroffenen Hersteller genutzt wird; eine staatliche Nutzung für eigene Zwecke würde dieses Vertrauen brechen und damit für die gesamtgesellschaftliche IT-Sicherheit zentrale Schwachstellen-Meldungen gefährden. Im Übrigen wäre aufgrund der bestehenden Dritt-Bekanntheit der Schwachstelle ohnehin nicht davon auszugehen, dass der Staat diese erfolgreich für eigene Zwecke ausnutzen könnte.

Auch in Notfällen, in denen eine Verzögerung der Offenlegung der Schwachstelle schwerwiegende Nachteile auslösen würde (bspw. weil die Schwachstelle aktiv von Dritten ausgenutzt wird), muss auf das Verfahren verzichtet und die Lücke umgehend einer Schließung zugeführt werden.[144]

3. Abwägungsprozess

Weiter muss die gesetzliche Regelung die betroffenen Behörden zu einem Abwägungsverfahren verpflichten, in dem Risiken und Nutzen der Geheimhaltung der Schwachstelle zu gewichten und gegenüberzustellen sind.

a) Abwägungspflicht

Das Bundesverfassungsgericht sieht keine Pflicht zur Schließung einer jeden behördlich bekanntgewordenen Sicherheitslücke: „Die grundrechtliche

---

[142] Bei CVD-Verfahren handelt es sich um Prozesse, durch die Sicherheitsforschende entdeckte Schwachstellen zunächst vertraulich den betroffenen Herstellern oder damit betrauten Koordinierungsstellen melden können, damit diese die Behebung der Schwachstelle anleiten können, bevor sie öffentlich bekannt gemacht wird. In Deutschland bietet das BSI einen CVD-Prozess an.

[143] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 18.

[144] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 18; zu weiteren denkbaren Ausnahmen, *U.S. VEP* (2017) S. 10.

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verleiht […] keinen Anspruch darauf, die Quellen-Telekommunikationsüberwachung durch Nutzung unerkannter Sicherheitslücken vollständig zu untersagen. Sie begründet auch keinen Anspruch auf Verpflichtung der Behörde, jede unerkannte Sicherheitslücke sofort und unbedingt dem Hersteller zu melden".[145]

Der Behörde muss aber „eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine *Zero-Day*-Schutzlücke bekannt wird" bei der sicherzustellen ist, „dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt".[146]

Wie auch diese Formulierung des Bundesverfassungsgerichts anzeigt, muss der Abwägungsprozess nur durchlaufen werden, wenn die entdeckende Behörde die Schwachstelle offenhalten will. Die Meldung der Schwachstelle an die betroffenen Hersteller kann die Behörde hingegen eigenverantwortlich veranlassen. Hiermit kommt die Behörde unmittelbar ihrer grundgesetzlich radizierten Schutzpflicht für die IT-Sicherheit nach, was keiner weitergehenden prozeduralen Absicherung bedarf.

b) Abwägungsbelange

Damit sind bereits die wesentlichen Belange angesprochen, die in dieser Abwägung zu berücksichtigen sind. Auf Seiten der betroffenen IT-Nutzenden ist insbesondere „die Gefahr einer weiteren Verbreitung der Kenntnis von [der] Sicherheitslücke" einzustellen. Dient die Schutzpflicht der Abwehr von unberechtigten Zugriffen Dritter, scheint zwingend, dass in die Analyse nicht nur die Gefahr der Verbreitung der *Kenntnis* sondern auch die Gefahr der *Nutzung* der Schwachstelle und das dadurch ermöglichte (grundrechtliche)

---

[145] BVerfG, Beschluss vom 8. Juni 2021, Rn. 42 (*IT-Sicherheitslücken*).

[146] BVerfG, Beschluss vom 8. Juni 2021, Rn. 44 (*IT-Sicherheitslücken*).

Schadenspotenzial sowohl in Umfang als auch in Qualität bestimmt wird. Gegen diese Gefahren soll der „quantitativ und qualitativ" bestimmte Nutzen einer möglichen behördlichen Infiltration der Lücke abgewogen werden.

Die abzuwägenden Faktoren sind gesetzlich vorzustrukturieren;[147] eine detaillierte Bestimmung, inspiriert etwa auch durch vorhandene Prozesse,[148] kann in abgeleiteten Rechtsakten geschehen.

4. Regel-Ausnahme-Verhältnis

Überdies ergibt sich aus dem IT-Sicherheitslücken-Beschluss, dass im Regelfall die Meldung der Sicherheitslücke an den Hersteller erfolgen muss. Nur wenn im Ausnahmefall „das Interesse an der Offenhaltung der Lücke überwiegt", darf die Meldung unterbleiben.[149] Damit wird die prinzipielle Priorität des Schutzes der IT-Sicherheit festgeschrieben, wie sie auch in der Literatur und auch in ausländischen Schwachstellen-Regelungen den Standard darstellt (sog. *Default-to-Disclose*).[150]

5. Entscheidungszuständigkeit und -prozess

Institutionelle Verortung und prozedurale Ausgestaltung des Schwachstellenmanagements haben maßgeblichen Einfluss auf Interpretation und Anwendung der materiell-rechtlichen Vorgaben und damit auch des Grundrechtsschutzes und stellen deshalb wesentliche Elemente

---

[147] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 76.

[148] Für eine Übersicht relevanter Überlegungen, siehe bspw. *U.S. VEP* (2017) Annex B.

[149] BVerfG, Beschluss vom 8. Juni 2021, Rn. 44 (*IT-Sicherheitslücken*).

[150] Beispielsweise im *U.S. VEP* (2017) S. 1 „the primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes.".

dar, die zwingend bereits von der gesetzlichen Regelung zu bestimmen sind.[151]

Aus der Verfassung lassen sich allerdings keine ganz konkreten Vorgaben zu institutionellem Design, Zuständigkeit und Verfahren des einzurichtenden Schwachstellenmanagements ableiten. Mögliche und sinnvolle Regelungsoptionen werden deshalb im Abschnitt zur zweckmäßigen Ausgestaltung vorgestellt.[152]

6. Entscheidungsfolgen

Weiter muss bereits in der gesetzlichen Grundlage des Schwachstellenmanagements festgelegt werden, zwischen welchen Entscheidungsfolgen am Ende des Prozesses ausgewählt werden kann.

Die Offenlegung der Schwachstelle durch Meldung an den Hersteller einerseits und die Geheimhaltung der Schwachstelle andererseits stellen dabei zwar die zwei wichtigsten, nicht aber die einzigen beiden Handlungsmöglichkeiten dar. Wie etwa auch im VEP dargestellt wird, kann der Staat daneben beispielsweise auch 1) Informationen weitergeben, die das Ausnutzungsrisiko mindern können, ohne die konkrete Schwachstelle offenzulegen, 2) die Nutzung der Schwachstelle durch staatliche Stellen in bestimmter Weise einschränken, oder 3) innerstaatliche und/oder ausländische Behörden vertraulich über die Schwachstelle informieren.[153]

Die verschiedenen Handlungsmöglichkeiten sollten in der gesetzlichen Grundlage in hinreichender Bestimmtheit aufgelistet werden.

---

[151] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 77.

[152] Siehe B.V.1.

[153] *U.S. VEP* (2017) S. 1; Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 31-33; beispielsweise kann der Staat Betreiber gefährdeter Infrastruktur vor dem unmitigierten Einsatz bestimmter IT-Infrastruktur warnen, ohne diese oder den Hersteller über die entdeckte Schwachstelle aufzuklären.

Weiter muss auch in der gesetzlichen Grundlage bereits festgelegt werden, dass eine geheim gehaltene Schwachstelle periodisch neu evaluiert werden muss, bis sie letztlich – wie dies für jede Schwachstelle erforderlich ist –[154] gemeldet wird. Der Evalutionsturnus und etwaige Handlungspflichten bei Eintritt von unvorhergesehenen Notfall-Situationen können dabei auch in untergesetzlichen Regelungen festgelegt werden.

Fällt die Entscheidung, wie dies in der Regel der Fall sein muss,[155] gegen die Zurückhaltung der Schwachstelle, muss diese in einem CVD-Prozess an den Hersteller gemeldet werden. Damit sollte das BSI betraut werden, das auch von Privaten zur Durchführung von CVD-Verfahren beauftragt werden kann.[156]

7. Aufsicht und Kontrolle

Wie auch in anderen Bereichen sicherheitsdienstlicher Tätigkeit erfordert das Grundgesetz auch für behördliche Entscheidungen über die Offenhaltung von IT-Schwachstellen angemessene Aufsichts- und Kontrollmechanismen, die von unabhängigen und hinreichend ausgestatteten Organen ausgeübt werden.[157]

Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass die mangelnde Transparenz und weitgehende Begrenzung individuellen Rechtsschutzes im Falle (geheimer) Überwachungsmaßnahmen durch besondere Anforderungen an die unabhängige objektivrechtliche Kontrolle derartiger Maßnahmen kompensiert werden muss.[158] Im Bereich der

---

[154] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 14.

[155] Siehe B.IV.4.

[156] Siehe Bundesamt für Sicherheit in der Informationstechnik, *Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess* (01.12.2022), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf.

[157] Umfassend, Wischmeyer, *Informationssicherheitsrecht*, 2023, S. 302-307.

[158] BVerfG, Urteil vom 19. Mai 2020, Rn. 265 ff. (*BND – Ausland-Ausland-Fernmeldeaufklärung*) (umfassend zu den Anforderungen an Kontrollmechanismen);

nachrichtendienstlichen Aufklärung hat sie außerdem „als Ausgleich für die im Wesentlichen nur finale Anleitung der Überwachungsbefugnisse die gebotene verfahrensmäßige Strukturierung der Handhabung dieser Befugnisse" zu gewährleisten,[159] d.h. als Korrektiv zur besonderen Breite und Unbestimmtheit der Überwachungsmaßnahmen rechtfertigenden Gründe zu fungieren. Nur so könne der Ausfall üblicher rechtsstaatlicher Sicherungen ausgeglichen werden.[160]

Diese Gründe der Erforderlichkeit objektivrechtlicher Kontrollmechanismen greifen auch im Fall des Schwachstellenmanagements: Auch hier besteht im Falle der Geheimhaltung bestehender Sicherheitslücken keine Transparenz, ist im Normalfall kein individueller Rechtsschutz möglich und sind die entscheidungsbestimmenden Parameter – die konfligierenden Ziele der IT-Sicherheit und der sicherheitsdienstlichen Aufklärung – im Wesentlichen nur final bestimmt.

Dies spricht dafür, dass man auch in diesem Bereich hohe Anforderungen an Umfang und Effektivität der Kontrollbefugnisse fordert. Dem wird im Zweifel nur eine umfassende, kontinuierliche objektive Rechtskontrolle gerecht werden,[161] d.h. die (Möglichkeit der) rechtlichen Überprüfung einer jeden Entscheidung über die Offenhaltung einer IT-Sicherheitslücke.

Denkbar scheint deswegen, dass auch hier eine zweiteilige Kontrolle einzurichten ist, wie sie das Bundesverfassungsgericht auch für gewisse Entscheidungen des BND im Bereich der Auslandsaufklärung fordert: Einerseits eine gerichtsähnliche Kontrolle durch einen unabhängigen

---

BVerfG, Beschluss vom 8. Oktober 2024, Rn. 171 (*BND-Cybergefahren*); BVerfG, Urteil vom 20. April 2016, Rn. 140 ff. (*BKA-Gesetz*)

[159] BVerfG, Urteil vom 19. Mai 2020, Rn. 273 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[160] BVerfG, Urteil vom 19. Mai 2020, Rn. 273 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[161] BVerfG, Urteil vom 19. Mai 2020, Rn. 272 ff. (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

Spruchkörper mit formalisiertem Verfahren und wirkungsvoller Einzelfallprüfung. Andererseits eine administrative Rechtskontrolle durch eine unabhängige Verwaltungsinstanz, die auf eigenes Betreiben, stichprobenartig oder auch umfassender Einzelentscheidungen oder auch darunter liegende Handlungsprozesse überprüfen kann.[162]

Hält man eine derart umfassende Kontrolle nicht für erforderlich, kommen auch weniger intensive Kontrollregime in Betracht. Beispielsweise ist denkbar, dass das Kontrollorgan nur Beanstandungsrechte, nicht aber echte Entscheidungs- bzw. Interventionsrechte hat. Eine derart eingeschränkte Kontrolle könnte etwa damit begründet werden, dass sich der Gesetzgeber für die Ausgestaltung des behördlichen Abwägungs- und Beurteilungsprozesses als Gremienentscheidung entscheidet[163] und damit bereits durch den Erstentscheidungsprozess eine gewisse reziproke „Kontrolle" sichergestellt ist. Außerdem unterliegt im Regelfall auch die Ausübung der durch eine Sicherheitslücke erlangten Angriffsfähigkeiten noch einmal der Kontrolle.[164]

Unabhängig von der Frage der konkreten Entscheidungsbefugnisse der Aufsichtsinfrastruktur, muss diese gewissen verfassungsrechtlichen Mindestanforderungen genügen:

Sie muss vollständig unabhängig und mit hinreichenden Ressourcen und Expertise – sowohl im technischen als auch im juristischen Bereich – ausgestattet sein[165] und muss auf Informationen zugreifen können, die eine angemessene Bewertung und Kontrolle der Entscheidungen ermöglichen.

---

[162] BVerfG, Urteil vom 19. Mai 2020, Rn. 272-300 (*BND – Ausland-Ausland-Fernmeldeaufklärung*). (umgesetzt durch den Unabhängigen Kontrollrat); Wischmeyer, *Informationssicherheitsrecht*, 2023, S. 304.

[163] Dazu unten B.V.1.

[164] Etwa durch die Kontrollmechanismen des Unabhängigen Kontrollrats oder auch der Ermittlungsrichter im strafprozessualen Bereich.

[165] BVerfG, Urteil vom 19. Mai 2020, Rn. 285-288 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

Letzteres bedeutet insbesondere, dass alle Entscheidungen hinreichend zu protokollieren sind und die Kontrollinstanz(en) hinreichende Informationen für eine wirksame Ausübung ihrer Befugnisse erhalten.[166]

Ungeachtet möglicher Einschränkungen durch erforderliche Maßnahmen des Geheimnisschutzes,[167] müssen Entscheidungen über die Offenhaltung von IT-Sicherheitslücken außerdem der parlamentarischen Kontrolle unterliegen. So sollten sie in jedem Fall in den Aufsichts- und Beurteilungsbereich des Parlamentarischen Kontrollgremiums aufgenommen werden.[168]

8. Schutzmaßnahmen

Wie bereits erwähnt, bedeutet die staatliche Bevorratung von IT-Schwachstellen auch deswegen ein erhebliches IT-Sicherheits- und Grundrechtsrisiko, weil behördliches Schwachstellenwissen von böswilligen Akteuren gestohlen werden kann.[169]

---

[166] BVerfG, Urteil vom 19. Mai 2020, Rn. 288-295 (*BND – Ausland-Ausland-Fernmeldeaufklärung*); BVerfG, Urteil vom 20. April 2016, Rn. 141 (*BKA-Gesetz*).

[167] BVerfG, Urteil vom 19. Mai 2020, Rn. 296 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).; siehe auch Wischmeyer, *Informationssicherheit*, 2023, S. 307.

[168] Zum Ein- bzw. Ausschluss des Parlamentarischen Kontrollgremiums in geheimhaltungsbedürftige Kontrollmaterien, BVerfG, Urteil vom 19. Mai 2020, Rn. 296-300 (*BND – Ausland-Ausland-Fernmeldeaufklärung*); siehe auch Wischmeyer, *Informationssicherheit*, 2023, S. 306.

[169] Siehe oben B.II.

Aus diesem Grund ist es verfassungsrechtliches Gebot,[170] dass für diese Aufbewahrung am jeweiligen Stand der Technik gemessen besonders hohe Informationssicherheitsstandards gelten.[171]

Allgemein geltende IT-Sicherheitsanforderungen, beispielsweise nach BSIG, Datenschutzrecht oder den jeweils anzuwendenden Polizei- und Nachrichtendienstgesetzen,[172] werden hierfür wohl nicht ausreichend sein.

V. Weitere Anforderungen an eine sachgerechte Ausgestaltung

In dem so vorgezeichneten Rahmen verfassungsrechtlicher Notwendigkeiten bleiben dem Gesetzgeber verschiedene konkrete Ausgestaltungsoptionen. Dies gilt insbesondere, was Design und Auswahl des mit dem Schwachstellenmanagement beauftragten Entscheidungsorgan (dazu 1.), Ausgestaltung des Entscheidungsverfahren (2.) und etwaige Transparenz- und Berichtspflichten (dazu 3.) angeht.

1. Entscheidungszuständigkeit

Institutionelles Design des verfahrensleitenden Körpers und prozedurale Ausgestaltung des Entscheidungsverfahrens stellen zentrale, aber auch besonders diffizile Aspekte einer Schwachstellenmanagement-Regelung dar.

---

[170] Ähnliche Pflichten zur gesetzgeberischen Gewährleistung hoher IT-Sicherheitsstandards hat das Bundesverfassungsgericht beispielsweise auch mit Bezug zur Vorratsspeicherung und Übermittlung von Telekommunikationsverkehrsdaten, BVerfG, Urteil vom 2. März 2010, Rn. 221 ff. (*Vorratsdatenspeicherung*) bzw. BVerfG, Urteil vom 27. Mai 2020, Rn. 188 (*Bestandsdatenauskunft II*) („Untrennbarer Bestandteil der Anordnung einer Speicherungsverpflichtung von Daten wie auch der Öffnung privater Datenbestände ist neben einer den Anforderungen genügenden normenklaren Begrenzung der Datenverwendung auch die verfassungsrechtlich gebotene Gewährleistung der Datensicherheit").

[171] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 76; Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 33-34; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 305-306.

[172] Bspw. § 30 BSIG oder Abschnitt 9 des BKAG.

Hier sollen zunächst Grundfragen zur Struktur des Entscheidungskörpers beantwortet werden, bevor einige denkbare konkrete Ausgestaltungen diskutiert werden.

a) Struktur des Entscheidungskörpers

Analog zu bestehenden nationalen Governance-Systemen, etwa dem *VEP*[173] oder dem *Equities Process* des Vereinigten Königreichs[174], und in Übereinstimmung mit bestehenden Vorschlägen für eine deutsche Ausgestaltung,[175] sollte die Entscheidung über die Offenhaltung einer Schwachstelle nicht innerhalb einer Behörde (weder der „entdeckenden" Sicherheitsbehörde noch einer „unbeteiligten" Drittbehörde[176]) getroffen, sondern behörden- und ressortübergreifend als Stakeholder-Prozess ausgestaltet werden. Dadurch lässt sich sicherstellen, dass die Interessen aller von der Entscheidung betroffenen Akteure berücksichtigt und ihre jeweilige Expertise eingebunden wird.

Organisationell entspricht dies einem Gremienorgan, in dem betroffene Stellen über Vertreter:innen ihre Position in den Abstimmungs- und Entscheidungsprozess einbringen können. Eingebunden werden sollten dabei zumindest leitende Stellen der Bundesministerien des Innern, der Verteidigung, für Wirtschaft und Energie, der Justiz und für Verbraucherschutz, für Digitales und Staatsmodernisierung sowie des BSI, der ZITiS, der Sicherheitsdienste (BfV, BND und MAD), der Polizeien (BKA,

---

[173] *U.S. VEP* (2017) S. 3-5.

[174] Government Communications Headquarters (GCHQ), *The Equities Process* (2018) abrufbar unter https://www.gchq.gov.uk/information/equities-process.

[175] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, S. 76 f.; Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 19 ff.; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 300 ff.

[176] Zu Vorschlägen das Schwachstellenmanagement im Ganzen in einer Behörde, insbesondere dem BSI oder dem ZITiS anzusiedeln, Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 300-302.

BP), der Bundeswehr und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe.

Das Entscheidungsverfahren muss vorbereitet, geleitet und unterstützt werden. Dafür bedarf es einer institutionellen Einbettung und Umrahmung, die derartige Aufgaben übernehmen kann („Sekretariat“).[177] Da für Teile der Unterstützungsarbeit erhebliche IT-sicherheitsbezogene Kenntnisse notwendig sein werden (beispielsweise zur Beantwortung von Fragen über die technische Komplexität der Ausnutzung einer entdeckten Sicherheitslücke oder zur Wahrscheinlichkeit von Patches), ist sicherzustellen, dass ein derartiges Sekretariat auf entsprechende Expertise zugreifen kann. Dies kann durch eigenes, entsprechend befähigtes Personal oder durch eine beratende Einbindung anderer Institutionen, etwa des BSI und ZITis, erreicht werden.

Das Sekretariat muss weiterhin den Dokumentations- und Berichterstattungsaufgaben gerecht werden und sollte im besten Falle auch als institutionelles Gedächtnis fungieren. Zu beachten ist in jedem Falle, dass sich auch in der Leitung, Koordinierung und Unterstützung des Entscheidungsprozesses Eigeninteressen der zuständigen Institution Bahn brechen können; es handelt sich bei der Wahl der zuständigen Institution deshalb um mehr als eine bloß technische Frage.

b) Mögliche Ausgestaltungen

Vor diesem Hintergrund sind verschiedene Institutionen als Sekretariat des Verfahrens denkbar.

Für eine Ansiedlung beim BSI[178] spricht dessen umfassende, insbesondere technische, Expertise in Fragen der IT-Sicherheit. Ihr steht aber entgegen, dass das BSI als „defensive” Behörde seinem gesetzlichen Auftrag nach (nur)

---

[177] Wischmeyer, *Informationssicherheit*, 2023, S. 302.

[178] So vorgeschlagen im *Koalitionsvertrag 2021-2025*, S. 87, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

dem Schutz der IT-Sicherheit dient und politisch als Interessenvertreter der hiermit verknüpften Belange auftritt.[179] Das könnte mit der neutralen Rolle als Verfahrensleiter konfligieren. Außerdem sollte das Vertrauen, auf das das BSI zur Wahrnehmung seiner Aufgaben im IT-Sicherheitsbereich zwingend angewiesen ist, durch eine Flankierung oder Verwässerung dieses gesetzlichen Auftrags nicht in Zweifel gesetzt werden.[180] Letztlich dürfte dies gegen eine Ansiedlung beim BSI sprechen.

Ähnlich ist eine Ansiedlung beim ZITiS zu bewerten. Sie scheint mit dessen Ausrichtung auf die Entwicklung offensiver Cyber-Fähigkeiten inkompatibel, jedenfalls schwer zu vereinbaren.[181]

Für eine Ansiedlung beim Bundeskanzleramt spricht, dass dieses ohnehin in zahlreichen Feldern Koordinierungsaufgaben zwischen den Einzelressorts sowie zwischen Bund und Ländern wahrnimmt und einen „neutralen" Boden für die Einbettung des Entscheidungsprozesses darstellt.[182] Andererseits mangelt es dem Bundeskanzleramt (bislang) an relevanter IT-Sicherheitsbezogener Expertise. Diese könnte jedoch aufgebaut werden.

Für eine Zuständigkeit des Nationalen Cyber-Abwehrzentrum (NCAZ) spricht, dass sich hier schon heute Sicherheitsbehörden und BSI zu Themen der gesamtstaatlichen Cyber-Sicherheit austauschen.[183] Nachteilhaft stellt sich allerdings das Fehlen einer gesetzlichen Grundlage des NCAZ dar. Diese

---

[179] Vgl. auch § 3 Abs. 1 Nr. 18 und Nr. 19 BSIG, nach dem das BSI Sicherheits- und andere Behörden nur unterstützen darf, soweit dies zur Abwehr oder Erforschung von Tätigkeiten, die gegen die IT-Sicherheit gerichtet sind, erforderlich ist.

[180] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 20; Wischmeyer, *Informationssicherheit*, S. 302; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 301.

[181] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 301 f.

[182] Wischmeyer, *Informationssicherheit*, 2023, S. 301 f.

[183] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 303 f.; die acht Kernbehörden des NCAZ sind: MAD, BKA, BSI, BfV, BBK, BND, BPol und das Bundeswehr-Kommando Cyber- und Informationsraum.

könnte im Zuge der gesetzlichen Anordnung eines Schwachstellenmanagements geschaffen werden.

Der Nationale Cyber-Sicherheitsrat (NCSR) scheint demgegenüber eher weniger geeignet, da hier bisher keine Vertreter der Sicherheitsbehörden teilnehmen und die Einbindung von Wirtschaftsverbänden den Geheimnisschutz erschweren würde.

Alternativ zur Angliederung an eine bestehende Institution kommt auch die Schaffung eines neuen Körpers in Betracht.

2. Entscheidungsprozess

Zumindest untergesetzlich sollte auch der Prozess, in dem die Entscheidung über Geheimhaltung oder Offenlegung der Schwachstelle getroffen wird, näher ausgestaltet werden.

Über einige der zu definierenden Verfahrensschritte kann dabei wenig Streit bestehen:

Behörden, die Kenntnis von einer *Zero-Day*-Schwachstelle erhalten, müssen diese, falls sie sie offenhalten wollen, innerhalb kurzer Zeit (bspw. einer Woche) an das Sekretariat melden. Diese Meldung muss eine Beschreibung und (Erst-)Beurteilung der Schwachstelle beinhalten, die zumindest Informationen bzw. Einschätzungen zu den folgenden Aspekten liefert: Art der Erlangung/Herkunft der Schwachstellenkenntnis, Art und Schwere der Schwachstelle (Beschreibung des Angriffsvektors, Grad des ermöglichten Systemzugriffs etc.),[184] Verbreitungsgrad der Schwachstelle bzw. der betroffenen Produkte und Art der betroffenen Produkte bzw. Infrastruktur, Verbreitungsgrad der Schwachstellenkenntnis und Wahrscheinlichkeit der Ausnutzung, Möglichkeit und Wahrscheinlichkeit von Patches (Verfügbarkeit von Maintainern, *End-of-Life*, Erreichbarkeit von Betroffenen etc.),

[184] Beispielsweise bewertet nach dem *Common Vulnerability Scoring System*, siehe FIRST.Org, Inc., *Common Vulnerability Scoring System Version 4.0: Specification Document (Version 1.2)* (2024).

Möglichkeit von Mitigationsmaßnahmen, operativer Nutzen („added value", Verzichtbarkeit der Schwachstelle etc.).[185]

Sodann muss das Entscheidungsverfahren zwar allen beteiligten Behörden hinreichend Zeit zur Analyse und Beurteilung der Schwachstelle lassen, gleichzeitig jedoch auch die zeitnahe Herbeiführung einer Entscheidung im Blick behalten. Angemessen scheinen etwa eine Beurteilungsfrist von einer Woche und ein Tagungs- bzw. Entscheidungsrhythmus von einem Monat.

Im Falle der Entscheidung für die Offenlegung der Schwachstelle, sollte diese dem BSI mitgeteilt werden, damit es im Rahmen seines CVD-Prozesses den betroffenen Hersteller kontaktieren kann.[186]

Im Falle der Entscheidung für die Zurückhaltung der Schwachstelle muss einerseits die Möglichkeit und Erforderlichkeit von Mitigationsmaßnahmen erörtert werden[187] und andererseits die weiterhin sichere und geheime Verwahrung der Schwachstelle sichergestellt werden.[188] Vorkehrungen sollten getroffen werden, die im Falle der unerwarteten Kenntnis Dritter eine schnelle Offenlegung der Schwachstelle oder anderweitige Schutzmaßnahmen ermöglichen.[189] Außerdem muss eine regelmäßige Re-Evaluation der Schwachstelle, etwa jährlich oder halbjährlich, geschehen.[190]

Ein größerer Regelungsspielraum besteht in Bezug auf das Entscheidungsverfahren. Denkbar sind insbesondere konsensorientierte und wahlbasierte Entscheidungsverfahren, wobei bei letzteren verschiedene

---

[185] Erläuternd zu diesen Punkten, Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 23-30 und *U.S. VEP* (2017) S. 13-14.

[186] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 305.

[187] Siehe auch oben B.IV.6.

[188] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 33 f.; siehe bereits B.IV.8.

[189] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 14.

[190] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 305; siehe auch oben B.IV.8.

Entscheidungsquoren möglich sind.[191] Weiter kommen auch Entscheidungsprärogativen (bspw. für die „entdeckende" Behörde), Vetorechte sowie gestaffelte Prozesse in Betracht.[192]

Vergleichbar zum VEP[193] scheint ein konsensorientierter Entscheidungsprozess vorzugswürdig, bei dem Einvernehmen über die Entscheidung angestrebt wird und für die Erreichung einer Entscheidung letztlich auch erforderlich ist.[194] Wahlbasierte Verfahren tragen das Risiko arithmetischer Zufälligkeiten (bspw. zahlenmäßig größere Beteiligung von Sicherheitsbehörden), generieren geringere politische Legitimität und können sachwidrige Entscheidungsdynamiken erzeugen.

3. Transparenz- und Berichtspflichten

Schließlich sollte eine gesetzliche Regelung auch Berichtspflichten zur Schaffung von Transparenz gegenüber der Öffentlichkeit und insbesondere externen Expert:innen festlegen, die eine (grobe) Einschätzung und Bewertung des Beurteilungsverfahrens erlaubt.[195] Derartige Berichte sollten zumindest Informationen über die Zahl der bekannt gewordenen

---

[191] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 23 befürwortet beispielsweise eine Sperrminorität gegen die Geheimhaltung von Schwachstellen von ca. 15%.

[192] Zu letzterem, Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 23.

[193] *U.S. VEP* (2017) 7 f.

[194] Im U.S. VEP-Verfahren wird bei Fehlen des Einvernehmens im Gremium über die durchzuführende Option abgestimmt. Diese Mehrheitsentscheidung kann dann von einer einzelnen beteiligten Behörde angefochten werden. Kommt es zu einer solchen Anfechtung, wird die Entscheidung in höhere Ebenen der U.S. Sicherheitsarchitektur eskaliert. Am Ende dieser Eskalationswege steht die Entscheidung durch den Präsidenten, *U.S. VEP* (2017) 7 f.; im Grundsatz sind solche Eskalationsverfahren, bspw. auch unter sukzessivem Ausschluss bestimmter zuvor beteiligter Akteure, auch im deutschen Gefüge denkbar.

[195] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, S. 34.

Sicherheitslücken und die Anteile der Offenlegung bzw. Geheimhaltung und Mitigierung enthalten.

VI. Inanspruchnahme externer Überwachungskapazitäten

Die Entdeckung von Schwachstellen und *Exploits* und die Entwicklung einsatzfähiger Spionagetools bedürfen einer technischen Expertise, die bei staatlichen Einrichtungen oftmals nur sehr begrenzt vorhanden ist. Auch aus diesem Grund kommt der Inanspruchnahme externer offensiver Cyberkapazitäten, inklusive Spyware-Tools, in der sicherheitsbehördlichen Praxis heute erhebliche Bedeutung zu. Dies betrifft sowohl kommerzielle Anbieter (sog. *Commercial Surveillance Vendors*) als auch Kooperationen mit ausländischen Sicherheits- und Nachrichtendiensten. Schon aus Gründen der Praxisrelevanz darf der Bereich derartiger dienstleistungsbasierter Überwachung deshalb nicht von einer Regelung des Schwachstellenmanagements ausgeschlossen werden. Im Übrigen wäre dies auch verfassungsrechtlich zweifelhaft.[196] Im Folgenden werden zunächst die Inanspruchnahme kommerzieller Anbieter (dazu 1.) und sodann die Nutzung entsprechender Kapazitäten im Rahmen staatlicher Kooperationen (dazu 2.) näher untersucht.

1. Dienstleistungsbasierte Überwachung („Commercial Surveillance Vendors")

Es ist davon auszugehen, dass derzeit der Großteil deutscher Überwachungskapazitäten auf Wissen oder Werkzeugen basiert, die von kommerziellen privaten Spyware-Anbietern stammen.[197] Im Folgenden wird dieser Komplex dienstleistungsbasierter Überwachung kurz dargestellt (dazu a.), bevor sodann die spezifischen Risiken ausgelagerter

---

[196] Siehe unten B.VI.1.c).

[197] Mit dieser Einschätzung für den US-amerikanischen Kontext, Google Threat Analysis Group, *Buying Spying* (2024).

Intrusionsoperationen erörtert werden (dazu b.) und diese in die bestehende verfassungsgerichtliche Judikatur und den übrigen bereits dargestellten verfassungsrechtlichen Rahmen eingeordnet werden (dazu c.). Schließlich werden Anforderungen des Verfassungsrechts und der Zweckmäßigkeit bezüglich der Regulierung dienstleistungsbasierter Überwachung dargestellt (dazu d.).

a) Strukturen und Praxen dienstleistungsbasierter Überwachung

Die Nachfrage nach kommerziellen Überwachungswerkzeugen hat in den letzten zwei Jahrzehnten zum Entstehen eines Milliarden-schweren, allerdings äußerst opaken Spyware-Marktes geführt, der in teils komplexen Lieferketten (sog. *exploitation supply chains*) die Versorgung staatlicher und privater Akteure mit derartigen Tools organisiert.[198] Akteure auf der Anbieterseite sind hier insbesondere private Schwachstellen-Researcher und *Exploit*-Entwickler:innen, die Schwachstellen entdecken und Software zu ihrer Ausnutzung entwickeln, Broker, die derartige Kapazitäten ankaufen und handeln, sowie *Spyware-as-a-Product*- und *Spyware-as-a-Service*-Anbieter, die funktionierende Überwachungs-Gesamtlösungen (vom sog. *delivery mechanism* bis zum Tool für die Analyse der erspähten Daten) vertreiben.[199]

Staatliche Akteure können von diesen Angeboten auf unterschiedliche Art und Weise Gebrauch machen: Einerseits können sie Schwachstellen ankaufen und eigene Werkzeuge zu deren Ausnutzung entwickeln. Dann erlangen sie Wissen von einer Schwachstelle und können bzw. müssen damit das Schwachstellenmanagement-Verfahren durchlaufen. Sie können aber auch *Spying-as-a-service*- oder *Spying-as-a-product*-Kapazitäten ankaufen, die ihnen die Infiltration und Ausspähung von Zielgeräten ermöglichen, ohne dass sie genauere Informationen über die ausgenutzten Schwachstellen oder

---

[198] Für einen sehr guten Überblick über diesen Markt und seine Eigenarten und Dynamiken, siehe DeSombre Bernsen, *Crash (exploit) and burn* (2024) S. 7-20; siehe auch Roberts u.a., *Mythical Beasts and Where to Find Them* (2024).

[199] Kategorisierung nach Google Threat Analysis Group, *Buying Spying* (2024) S. 16-45.

das Design der verwendeten Spionage-Software erhalten.[200] Dann erhalten sie im Grundsatz kein Wissen über die ausgenutzte IT-Schwachstelle, über deren Offenlegung entschieden werden könnte. Damit vergleichbar ist die (wohl deutlich seltenere) Situation, dass staatliche Akteure zwar relevante Informationen über die ausgenutzte Schwachstelle erhalten, dieses aber aufgrund einer Geheimhaltungsvereinbarung (sog. Non-Disclosure-Agreement) nicht weitergeben würden, d.h. entweder schon nicht anderen staatlichen Stellen zur Überprüfung geben, jedenfalls die Schwachstelle aber nicht gegenüber dem Hersteller offenlegen dürfen.

Bezüglich aller Produkte und Dienstleistungen muss festgehalten werden, dass die dahinterstehende Lieferkette in den seltensten Fällen vollständig aufklärbar ist[201] und dass staatliche Käufer selten Exklusivverträge erhalten, d.h. das angekaufte Produkt wird in der Regel gleichzeitig auch noch anderen Käufern angeboten.

b) Risiken dienstleistungsbasierter Überwachung

Der staatliche Ankauf kommerzieller Überwachungstools birgt Gefahren für die IT-Sicherheit wie auch für die Freiheitsrechte Einzelner und staatliche Interessen, die jene, die durch staatliches Wissen von Sicherheitslücken ausgelöst werden teils erheblich übertreffen, mit diesen aber zumindest vergleichbar sind.

Bezieht der Staat Überwachungskapazitäten von Privaten, besteht Gewissheit, dass (auch) andere Akteuren, jedenfalls das verkaufende Unternehmen, von der ausgenutzten Sicherheitslücke wissen und diese ausnutzen können. Dies kann auch autoritäre Staaten, die Überwachungsfähigkeiten gezielt gegen Opposition und Zivilgesellschaft

---

[200] Für ein illustratives Produktangebot der Spyware Firma Intellexa, inklusive enthaltenen Services und Preisen, siehe Google Threat Analysis Group, *Buying Spying* (2024) S. 30-33; darüber hinaus werden auch Abonnement-Lösungen angeboten, bei denen staatliche Käufer bspw. Zugriff auf alle *Exploits* erhalten, die eine Firma in einem bestimmten Zeitraum entdeckt, siehe DeSombre Bernsen, *Crash (exploit) and burn* (2024) S. 12.

[201] Zur Opazität dieser Lieferketten und der verbreiteten Einbindung von Subunternehmern, DeSombre Bernsen, *Crash (exploit) and burn* (2024) S. 16-18.

einsetzen, und selbst kriminelle Akteure, etwa Ransomware-Betreiber, umfassen.[202] Selbst wenn Anbieter angeben, nur an Regierungen oder nur an „westliche" Regierungen zu verkaufen, werden sich solche Zusagen selten sicher verifizieren lassen. Zu berücksichtigen ist dabei auch, dass es sich bei privaten Anbietern um wirtschaftlich handelnde Akteure handelt, die auf Profiterzielung ausgerichtet sind, und hohe Investitionskosten durch noch höhere Einnahmen übertreffen müssen.[203] Aufgrund der Opazität und Komplexität des Marktes lässt sich oftmals außerdem nicht nachverfolgen, woher die Kapazitäten (Schwachstellen, *exploits*) kommen, auf denen ein angebotenes Überwachungstool beruht, und wer noch von diesen Kenntnis hat.

Weiter lässt sich auch der Schutz der eingesetzten Schwachstellen gegen Angreifer:innen nicht kontrollieren oder verifizieren. Die Auslagerung von Spionage-Aktivitäten kreiert daher erhebliche Counterintelligence-Risiken.[204] Bekannt ist nämlich, dass private Spionage-Anbieter regelmäßig von Dritten, inklusive staatlichen Akteuren, u.a. Nordkorea, angegriffen werden.[205] Derartige Counterintelligence-Angriffe können kaum überraschen, handelt es sich bei den ausgelagerten Aktivitäten doch um einige der sensibelsten

---

[202] NSO Group, das Unternehmen hinter der Spyware Pegasus, hatte nach eigenen Angaben neben seinen Kunden in 14 EU-Ländern auch in u.a. Indien, Saudi-Arabien, den Vereinigten Arabischen Emiraten, Kasachstan, Togo, Ruanda und Indonesien staatliche Abnehmer. Die jährlich etwa 12.000 Angriffe galten vor allem Politiker:innen, Oppositionellen, Aktivist:innen, Wissenschaftler:innen und Journalist:innen, siehe Meister, *Staatstrojaner Pegasus wird alle 40 Minuten eingesetzt* (22.06.2022) abrufbar unter https://netzpolitik.org/2022/pega-untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/#2022-06-21_European-Parliament_PEGA_NSO.

[203] Zu den wirtschaftlichen Bedingungen unter denen derartige Unternehmen operieren, siehe DeSombre Bernsen, *Crash (exploit) and burn* (2024) S. 9-12.

[204] Deibert, *The Perils of Privatized Cyberwarfare* (2016) (mit einer kleinen Liste bekannter Fälle); vgl. auch das oben bereits angespochene Proliferationsrisiko, siehe B.II.

[205] DeSombre Bernsen, *Crash (exploit) and burn* (2024) S. 10.

nachrichtendienstlichen, militärischen und polizeilichen Operationen eines Staates überhaupt.[206]

Daneben besteht immer auch die Gefahr, dass die beauftragten Unternehmen geheime Informationen, die ihnen zur Identifizierung von Zielpersonen übermittelt werden,[207] missbrauchen oder an andere Kunden weitergeben,[208] oder sogar Zugriff auf die extrahierten Informationen bekommen.[209] Im Verfahren zwischen *WhatsApp* und dem Spyware Anbieter *NSO Group* sagten Mitarbeiter:innen des Spionage-Unternehmens beispielsweise aus, dass Kunden der *NSO Group* die Telefonnummern der Zielpersonen übermitteln und diese den Infiltrations- und Extraktionsprozess kontrolliert.[210]

Insgesamt werden Transparenz und Möglichkeiten der öffentlichen Kontrolle durch die Auslagerung an den privaten Sektor, der in diesem Bereich ganz besonderen Wert auf Geheimhaltung und Intransparenz legt, geschwächt.[211]

Strukturell nährt die staatliche Nachfrage nach privaten Überwachungswerkzeugen außerdem ein korruptes Ökosystem kommerzieller *threat actors*, die die Sicherheit fundamentalster IT-

---

[206] Deibert, *The Perils of Privatized Cyberwarfare* (2016).

[207] Spyware-Firmen machen regelmäßig keine klaren Aussagen dazu, wieviel Einblick sie in die über ihre Systeme ausgeführten Operationen haben, Deibert, *The Perils of Privatized Cyberwarfare* (2016).

[208] Deibert, *The Perils of Privatized Cyberwarfare* (2016).

[209] European Parliament, *Recommendation*, S. 10.

[210] Weiter ungeklärt ist aber, ob *NSO Group* auch auf die extrahierten Informationen zugreifen konnte; Smally, *Testimony from NSO Group raises questions about its culpability for spyware abuses* (19.11.2024) abrufbar unter https://therecord.media/nso-group-whatsapp-case-documents.

[211] The Citizen Lab, *Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the United Nations Working Group on the Use of Mercenaries* (2026) S. 3.

Infrastruktur global angreifen und IT-Sicherheit universal unterminieren.[212] Daran können auch „no buy"-Listen oder staatliche Sanktionen gegen besonders aggressive Akteure[213] wenig ändern, zumal sanktionierte Firmen versuchen, über Scheinfirmen unentdeckt weiter im Geschäft zu bleiben.[214]

Schließlich legitimiert der Ankauf von privaten Überwachungstools die entsprechenden Märkte für IT-Unsicherheit und trägt zum Verlust der eigenen Reputation und Glaubwürdigkeit und zur Aushöhlung internationaler Cybernormen bei, die dauerhaft das Absinken des globalen IT-Sicherheitsniveaus wie auch die Proliferation illegitimer Überwachungskapazitäten befeuern.[215]

c) Verfassungsrechtliche Bewertung

Der Beschluss des BVerfG zu IT-Sicherheitslücken beschränkt das Bestehen einer Regelungspflicht ausdrücklich auf diejenigen Fälle, in denen staatliche

---

[212] Google Threat Analysis Group, *Buying Spying* (2024) S. 5; Deibert, *The Perils of Privatized Cyberwarfare* (2016) „Outsourcing these operations to the private sector will incentivize a race to discover, acquire, and, crucially, hoard software vulnerabilities not just in modern phones but also in critical infrastructure, ... This arms race will inevitably lead firms to dig deeper into the increasingly invasive internet of things and operational technology infrastructure upon which modern society relies, such as consumer security cameras or Siemens industrial controllers, found throughout sensitive systems, including electrical grids and water treatment plants. The service of one actor's narrow national security interests will spawn an ever-growing collective insecurity for the rest of the globe, at the deepest level of infrastructure on which all of society critically depends"; European Parliament, *Recommendation*, S. 5.

[213] Siehe beispielsweise die Sanktionen der USA gegen die NSO Group, U.S. Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (03.11.2021) abrufbar unter https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[214] Deibert, *The Perils of Privatized Cyberwarfare* (2016); im Jahr 2023 gab das FBI bekannt, herausgefunden zu haben, dass ein Zulieferer als Deckfirma für die von den USA sanktionierte NSO Group agiert habe, siehe Krempl, *Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert* (31.07.2023) abrufbar unter https://www.heise.de/news/Trotz-Verbot-FBI-hat-ueber-Vertragsfirma-NSO-Spyware-finanziert-9231066.html; siehe auch European Parliament, *Recommendation*, 7-8.

[215] Deibert, *The Perils of Privatized Cyberwarfare* (2016) spricht von einem Wettrüsten; The Citizen Lab, *Submission*, S. 5-6.

Behörden selbst Kenntnis von einer bestimmten Schwachstelle haben, unabhängig davon, wie sie diese Kenntnis erlangt haben.[216]

Bei genauerer verfassungsrechtlicher Analyse steht aber fest, dass auch die Auslagerung von Angriffskapazitäten an private Akteure, mit anderen Worten: die Ausnutzung privat bevorrateter Sicherheitslücken, von dieser Regelungspflicht nicht ausgenommen werden kann.

Das lässt sich letztlich schon daraus ableiten, dass die Ziele und die Effektivität staatlichen Schwachstellenmanagements vollständig unterminiert werden könnten, wenn der Staat ohne Beschränkungen auf private Infiltrationskapazitäten zurückgreifen könnte, solange er nur kein Wissen über die dabei verwendeten Schwachstellen erhält.[217] Tatsächlich würde eine derartige Rechtslage Sicherheitsbehörden starke Anreize zum Rückgriff auf private Infiltrationskapazitäten geben und dadurch ein Ausweichen auf strukturell noch gefährlicheres Schwachstellenwissen bzw. die Umgehung des Schwachstellen-Beurteilungsverfahrens befördern.

Auch eine Analyse der spezifisch verfassungsgerichtlichen Argumentation macht deutlich, dass die Einbindung von privaten Spionagekapazitäten nicht von der Beurteilungspflicht ausgenommen werden kann. Denn diese stützt das Verfassungsgericht gerade auf die allgemeine „Pflicht, dazu beizutragen, dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt"[218] wird, die durch das hohe Gefährdungs- und Schädigungspotenzial von Schutzlücken und die fehlende Möglichkeit des Selbstschutzes begründet wird.[219] Außerdem besteht auch in den Fällen der Inanspruchnahme privater Spionagekapazitäten eine

---

[216] BVerfG, Beschluss vom 8. Juni 2021, Rn. 40 (*IT-Sicherheitslücken*).

[217] Deibert, *The Perils of Privatized Cyberwarfare* (2016) „However, it is difficult to see how any internal government VEP can remain effective when the responsibility to discover and stockpile [exploits] to private contractors, effectively placing the inventory and decision-making outside the scope of formal oversight procedures.".

[218] BVerfG, Beschluss vom 8. Juni 2021, Rn. 40 (*IT-Sicherheitslücken*).

[219] BVerfG, Beschluss vom 8. Juni 2021, Rn. 34-39 (*IT-Sicherheitslücken*).

spezifische Verantwortung für den Staat, der, auch wenn er selbst womöglich nicht die Behebung der Schwachstelle anstoßen kann, doch als (potenzieller) Abnehmer deren fortgeführte Offenhaltung erforderlich macht.

Für die Übertragbarkeit des Schutzpflichtenarguments sprechen weiter auch die verfassungsgerichtlichen Vorgaben zur strukturell vergleichbaren Kooperation mit ausländischen Sicherheitsdiensten. In seinem Urteil zur Ausland-Ausland-Fernmeldeaufklärung hat das Bundesverfassungsgericht klargestellt, dass das Grundgesetz Kooperationen mit anderen Nachrichtendiensten zwar nicht grundsätzlich entgegensteht, dass aber „Regelungen zur Kooperation mit ausländischen Nachrichtendiensten [...] grundrechtlichen Anforderungen nur [genügen], wenn sie sicherstellen, dass die rechtsstaatlichen Grenzen durch den gegenseitigen Austausch nicht überspielt werden und die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Kern gewahrt bleibt".[220]

Insbesondere dürften grundrechtliche Standards, etwa Erhebungsverbote, nicht durch die Annahme von Informationen anderer Sicherheitsdienste im Wege eines „Ringtauschs" umgangen werden.[221]

Auf die Überwachungsmöglichkeiten anderer Dienste dürfte deswegen nur zugegriffen, die von diesen erhobenen Daten nur erlangt und genutzt werden,

---

[220] BVerfG, Urteil vom 19. Mai 2020, Ls. 7, Rn. 244 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).; die entsprechenden Regelungen sind in den §§ 13-17 BNDG enthalten; siehe auch BVerfG, Urteil vom 20. April 2016, Rn. 327 (*BKA-Gesetz*) „Die Grenzen der inländischen Datenerhebung und -verarbeitung des Grundgesetzes dürfen durch einen Austausch zwischen den Sicherheitsbehörden nicht in ihrer Substanz unterlaufen werden. Der Gesetzgeber hat daher dafür Sorge zu tragen, dass dieser Grundrechtsschutz durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen ebenso wenig ausgehöhlt wird wie durch eine Entgegennahme und Verwertung von durch ausländische Behörden menschenrechtswidrig erlangten Daten".

[221] BVerfG, Urteil vom 19. Mai 2020, Rn. 248-249 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

wenn entsprechende gesetzliche Grundlagen vorlägen,[222] die „dem solchen Praktiken inhärenten Potential einer Umgehung innerstaatlicher Bindungen [...] und den spezifischen Grundrechtsgefährdungen, die durch die Zusammenarbeit eintreten können, Rechnung" tragen.[223]

Konkret müsste sich deshalb im Vorhinein einer solchen Kooperation beispielsweise vergewissert werden, dass durch den Partnerdienst datenschutzrechtliche Standards und rechtsstaatliche Grundsätze gewahrt würden und müssten solche Vergewisserungen durch „gehaltvolle Zusagen" der Partnerdienste untermauert werden.[224] Auch eine „gerichtsähnliche Vorabkontrolle" könne erforderlich sein.[225]

Verfassungsrechtlich erforderliche Kontrollmechanismen dürften nicht unter Berufung auf die sog. *Third Party Rule*, nach der Informationen von ausländischen Sicherheitsdiensten nicht ohne deren Zustimmung an Dritte weitergegeben werden dürfen, behindert werden.[226] Der Gesetzgeber hätte deswegen sicherzustellen, dass sich die Sicherheitsdienste in ihren Absprachen mit Partnern in jedem Falle die entsprechenden Genehmigungen erteilen ließen, damit sie alle für die Kontrolle relevanten Informationen auch an die entsprechenden Kontrollorgane weitergeben dürften bzw. diese nicht als *Third Party* eingeordnet würden.[227]

---

[222] BVerfG, Urteil vom 19. Mai 2020, Rn. 250 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[223] BVerfG, Urteil vom 19. Mai 2020, Rn. 250 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[224] BVerfG, Urteil vom 19. Mai 2020, Rn. 233-243 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[225] BVerfG, Urteil vom 19. Mai 2020, Rn. 240 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[226] BVerfG, Urteil vom 19. Mai 2020, Rn. 291 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[227] BVerfG, Urteil vom 19. Mai 2020, Rn. 294-295 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

Auch wenn es sich um unterschiedliche Regulierungsfragen handelt: Macht die Verfassung schon an die Überwachungskooperation mit („befreundeten") staatlichen Akteuren derart feinregulatorische Vorgaben, scheint ausgeschlossen, dass sich die Auslagerung von Überwachungsaktivitäten an private und damit nicht grund- und menschenrechtsgebundende Akteure jeglicher verfassungsrechtlichen Einhegung entzieht.

d) Verfassungsrechtliche Vorgaben und sachgerechte Ausgestaltung

Kann mithin die Inanspruchnahme privater Überwachungskapazitäten nicht gänzlich von der Pflicht zum Schwachstellenmanagement ausgenommen werden[228] bzw. unreguliert bleiben, ist damit noch nicht geklärt, wie genau derartige Vorgänge eingehegt werden müssen bzw. welche Regelungsoptionen dem Gesetzgeber hier zur Verfügung stehen. Denkbar sind u.a. die folgenden Regelungsmodelle:

Angesichts der hohen IT-Sicherheits- und Grundrechtsrisiken, die der Rückgriff auf private Spionageunternehmen birgt,[229] ist zunächst denkbar, derartige Kooperationen prinzipiell zu verbieten. Der Staat wäre dann darauf angewiesen, eigene Aufklärungskapazitäten zu entwickeln bzw. diese von Partnerdiensten zu beziehen. Langfristig würde dadurch auch die selbst in Sicherheitskreisen überaus kritisch gesehene Abhängigkeit von privat entwickelten und damit strukturell unsicheren und unkontrollierbaren Spionagewerkzeugen beendet.

Ähnlich prohibitiv wäre eine Regelung, nach der der Staat private Überwachungstools zwar ankaufen darf, auch diese aber dem Schwachstellenmanagement zuführen muss und etwaig die Schwachstelle an den Hersteller offenlegen muss. Effektiv würde das bedeuten, dass der Staat eine Exklusivlizenz an dem entwickelten Produkt erwerben muss. Darauf werden sich Anbieter nur bei entsprechend hohen Preisen einlassen.

---

[228] So aber etwa im Wesentlichen der Fall im Rahmen des *U.S. VEP* (2017) S. 9-10.

[229] Siehe B.VI.1.b).

Weiter käme ein Prüfmodell vergleichbar zu den verfassungsgerichtlich etablierten Anforderungen an die Zusammenarbeit mit fremden Nachrichtendiensten in Betracht.[230] Der Staat müsste dann vor der Zusammenarbeit mit privaten Spyware-Anbietern in einem Due-Diligence-Verfahren gewisse Legalitäts- und Rechtsstaatlichkeitsstandards prüfen. Vergleichbar mit den Anforderungen, die für die Kooperation mit Nachrichtendiensten bestehen, könnte der Staat etwa verpflichtet sein, sich zu vergewissern, dass gewisse datenschutzrechtliche Gewährleistungen, insbesondere solche der Datensicherheit, sowie rechtsstaatliche Grundsätze gewahrt sind.[231] Letztere könnten etwa darin bestehen, dass betroffene Anbieter ihre Produkte nachweislich nicht an autoritäre Regierungen oder „Unrechtsstaaten" verkaufen und hinreichende Gewähr dafür bieten, dass diese auch über andere Wege nicht an solche Akteure gelangen, dass die Produkte nicht gegen geschützte Personengruppen eingesetzt werden und dass von den Anbietern keine (unzumutbaren) Counterintelligence-Risiken ausgehen.[232] Die Einschätzung dürfte freilich nicht dem freien Ermessen der bewertende staatlichen Einrichtungen unterliegen und hätte sich auf „gehaltvolle, realitätsbezogene und aktuelle Informationen zu stützen".[233] Sie müsste mit Auskunftsrechten[234] und effektiven Sanktionsmechanismen

---

[230] Siehe bereits B.IV.7; siehe auch European Parliament, *Recommendation*, S. 22 „companies applying in a public procurement process to be suppliers should undergo a vetting process which includes the company's response to human rights violations committed with their software and whether the technology relies on data gathered in undemocratic and abusive surveillance practices".

[231] BVerfG, Urteil vom 19. Mai 2020, Rn. 231-237 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[232] Handhabbare Standards und Definitionen zu diesen Prinzipien könnten auch aus Executive Order 14093 des ehemaligen US-Präsidenten Joe Biden übernommen werden, Executive Office of the President, *Executive Order 14093 - Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security* (27.03.2023).

[233] BVerfG, Urteil vom 19. Mai 2020, Rn. 241 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[234] BVerfG, Urteil vom 19. Mai 2020, Rn. 237 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

gegenüber den Spyware-Anbietern verstärkt werden. Insbesondere sollten Anbieter im Wege eines „Know Your Vendor"-Verfahrens dazu verpflichtet werden, Zulieferer und Investoren offenzulegen.[235] Weiter müsste die Beurteilung zwingend dokumentiert und damit einer unabhängigen Kontrolle zugänglich gemacht werden.

Prozedural könnte auch ein solches Beurteilungsverfahren im Sinne eines „Spyware Equities Process" ähnlich dem für die Bewertung von Sicherheitslücken vorgeschlagenen Verfahren organisiert werden.[236] Dann müsste die anwerbende oder angesprochene Behörde in einer Vorprüfung die erforderlichen Informationen einholen, um unter den geltenden materiellen Standards eine Ersteinschätzung durchzuführen, die dann dem Gremium zur Entscheidung vorgelegt wird. Wichtig ist dann auch, dass die Überwachung der Anbieter laufend fortgeführt wird.

In jedem Fall sollte die Einhaltung rechtlicher Vorgaben durch das Partnerunternehmen durch vertragliche Abreden abgesichert werden, auch wenn diese natürlich keine Garantie für die tatsächliche Einhaltung liefern. Derartige Abreden könnten auch eine Pflicht enthalten, dass das Tool möglichst so designt und/oder konfiguriert werden muss, dass schon technisch nur möglich ist, was rechtlich auch erlaubt sein kann („rule-of-law-by-design").[237] Auch eine Pflicht zur Verwendung von Nachverfolgbarkeits-Markern ist denkbar, die auf infiltrierten Geräten eine Signatur oder ähnliches technisches Artefakt hinterlassen, mit dem im Nachhinein nachprüfbar ist,

---

[235] Roberts u.a., *Mythical Beasts and Where to Find Them* (2024) S. 23; solche Pflichten sind insbesondere erforderlich, um die Umgehung effektiver Kontrollen durch Scheinfirmen und andere Verschleierungstaktiken zu verhindern; siehe auch Panagiotopoulos, *Policymakers Ignore Spyware Middlemen Driving Global Proliferation* (18.03.2026).

[236] Auch das Europäische Parlament ist der Ansicht, dass der Ankauf von Spyware von einer unabhängigen Kontrollinstanz überprüft werden können muss, European Parliament, *Recommendation*, S. 22 „Concludes that when a Member State has purchased spyware, the acquisition must be auditable by an independent, impartial audit body with appropriate clearance".

[237] Siehe auch European Parliament, *Recommendation*, S. 21-22.

wer den Einsatz der Spyware wann veranlasst hat.[238] In jedem Fall müssen Verträge mit Spyware-Anbietern sicherstellen, dass ankaufende Behörden nicht davon abgehalten werden, andere staatliche Stellen über Anfälligkeiten betroffener Infrastruktur zu informieren; nur so kann sichergestellt werden, dass der Staat zumindest effektive Maßnahmen zum Selbstschutz ergreifen kann.

Flankierende Regelungen, etwa eine gerichtsähnliche Vorabkontrolle oder die Bedingung, dass auf private Spionagesoftware nur zurückgegriffen werden darf, wo dies für die Durchführung gesetzlicher Aufgaben absolut erforderlich ist, sollten den Einsatz weiter absichern. Auch eine Pflicht zur unternehmerseitigen Offenlegung der ausgenutzten Sicherheitslücke(n) ist denkbar.

Alternativ könnten derartige Standards auch in einem Zertifizierungsmodell durchgesetzt werden, in dem Anbieter, bevor sie dem Staat Spyware-Produkte anbieten können, erst eine entsprechende Zertifizierung erhalten müssen, die dann einem regelmäßigen Audit unterzogen wird (sog. *White Listing*). Dies hätte insbesondere den Vorteil, dass Ressourcen in der Evaluation gebündelt würden und ein sichtbarer Marktanreiz für „saubere" Anbieter erzeugt würde. Harte Sanktionen gegen Unternehmen, die gegen vertragliche Abreden oder Gesetzesrecht verstoßen, könnten der derzeit vorherrschenden Kultur der Verantwortungs- und Straflosigkeit entgegenwirken.[239]

Darüber hinaus scheint auch denkbar, die Inanspruchnahme von „Hacking-as-a-Service"-Dienstleistungen, bei denen im Unterschied zum Ankauf von Spionage-Tools Infiltration und Extraktion durch das Drittunternehmen

---

[238] European Parliament, *Recommendation*, S. 21 „a marker needs to be included in the surveillance software so that oversight bodies can unambiguously identify the deployer in the event of suspicion of abuse; the mandatory signature for each spyware deployment should consist of an individual label for the acting authority, the type of spyware used and an anonymised case number".

[239] The Citizen Lab, *Submission*, S. 6-7.

gesteuert und ausgeführt werden, ganz zu verbieten, da die anbietenden Unternehmen bei diesen regelmäßig noch extensiveren Zugriff auf sensible Informationen erhalten bzw. dieser Zugriff jedenfalls noch schwerer verhindert werden kann.[240]

Auch eine anbieterseitige Durchsetzung von materiellen Vorgaben in Gestalt einer direkten Marktregulierung – etwa so, dass nach einem „rule-of-law-by-design"-Ansatz nur solche Technologien verkauft werden dürfen, die hinreichende Gewähr für die Einhaltung eines angemessenen Schutzniveaus bieten (bspw. durch Softwaredesign, Verschlüsselung, Authentifizierungsmechanismen) – kommt in Betracht, bietet sich aber wenn nur auf Unionsebene an.[241]

2. Zusammenarbeit mit ausländischen Sicherheitsbehörden

Es ist davon auszugehen, dass auch ausländische Partnerdienste deutschen Sicherheitsbehörden regelmäßig offensive Cyberkapazitäten zur Verfügung stellen. Wie dies auch für den Rückgriff auf kommerziell angebotene Überwachungsfähigkeiten gilt,[242] darf auch durch derartige Kooperationen Ziel und Wirksamkeit einer Regelung zum Schwachstellenmanagement nicht unterlaufen werden. Regulatorisch bietet sich eine Übertragung der Prüfpflichten an, die das Bundesverfassungsgericht für den Bereich der nachrichtendienstlichen Kooperation in der Fernmeldeaufklärung aufgestellt hat.[243] Wie diese Vorgaben auf die Überprüfung von offensiven

---

[240] European Parliament, *Recommendation*, S. 22.

[241] Dies schlägt auch das EU-Parlament vor, das insofern auch darauf hinweist, dass Bürger:innen in Drittstaaten aufgrund der Dual-Use-Verordnung der EU insofern besseren Schutz genießen als EU-Inländer, European Parliament, *Recommendation*, S. 21-22.

[242] Siehe B.VI.1.

[243] BVerfG, Urteil vom 19. Mai 2020, Rn. 233-242 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

Cyberkapazitäten übertragen werden kann, wurde hier schon im Kontext der Inanspruchnahme kommerzieller Angebote erläutert.[244]

[244] Siehe B.VI.1.d).

C. Kompetenzrechtlicher Rahmen

Wurde in Teil B. herausgearbeitet, dass der deutsche Staat zur Regelung des Schwachstellenmanagements und des Spyware-Ankaufs grundrechtlich verpflichtet ist, stellt sich nun die Frage, ob und in welchem Umfang er, und insbesondere der Bundesgesetzgeber, dazu auch kompetenziell befugt ist.

Mit anderen Worten muss geklärt werden, welche institutionelle Ebene für derartige gesetzliche Regelungen kompetenzrechtlich überhaupt zuständig sind. In Betracht kommt insofern die Europäische Union, auf nationaler Ebene der Bundesgesetzgeber und die Länder. Im Folgenden wird deshalb zunächst geprüft, ob die Europäische Union zur Regelung der hier betroffenen Materien zuständig ist (dazu I.), bevor in einem zweiten Schritt geprüft wird, wem innerhalb des innerdeutschen Kompetenzgefüges die Regelungskompetenz zukommt (dazu III.). Da das Regelungsermessen nationaler Gesetzgeber aufgrund des Vorrangs des Unionsrechts auch durch unionales Sekundärrecht beschränkt sein könnte, muss weiter geprüft werden, ob das Unionsrecht schon heute Anforderungen an nationales Schwachstellenmanagement stellt (dazu II.)

Das Bestehen einer Kompetenz hängt maßgeblich vom genauen Zuschnitt und Inhalt der geplanten Regelung ab. Den folgenden Ausführungen wird insofern der Wunsch nach einer möglichst umfassenden und möglichst viele staatliche Institutionen erfassenden materiellen Regelung der Pflicht zur Implementierung eines Schwachstellenmanagementverfahrens wie auch nach einer Regelung des staatlichen Umgangs mit kommerziellen Spyware-Tools zugrunde gelegt.

I. Kompetenz der Europäischen Union

In Betracht kommt zunächst, dass der Europäischen Union die Kompetenz zur Regelung der genannten Materien zukommt.

1. Kompetenztitel

Nach dem Grundsatz der begrenzten Einzelermächtigung kann die Europäische Union nur tätig werden, sofern ihr in den Verträgen (EUV und AEUV) eine entsprechende Kompetenz zugewiesen wurde.

In Betracht kommen insofern verschiedene kompetenzrechtliche Grundlagen.

a) Art. 114 Abs. 1 Satz 2 AEUV

Gem. Art. 114 Abs. 1 Satz 2 AEUV kann die EU Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten erlassen, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben. Auf der Grundlage dieser Kompetenz ist es der EU mithin gestattet, Hemmnisse für den europäischen Wirtschaftsverkehr abzubauen, um zur Verwirklichung eines europäischen Binnenmarktes beizutragen.[245] Auch wenn Art. 114 AEUV keine allgemeine Regulierungskompetenz begründet, ermöglicht er doch Angleichungsmaßnahmen in einer Vielzahl von Rechtsbereichen[246] und wird von den europäischen Gesetzgebern, größtenteils ohne Widerspruch seitens des EuGH, extensiv ausgelegt.[247] Im Bereich des Informationssicherheitsrechts geht der Unionsgesetzgeber davon aus, dass auch Maßnahmen zur allgemeinen Anhebung der Cybersicherheit, zur Abwehr von Cyberangriffen und auch zur Stärkung des „Vertrauens in den digitalen Binnenmarkt" von Art. 114 AEUV erfasst sein können.[248] So trägt Art. 114 AEUV bspw. auch die Einrichtung der europäischen Agentur für Netz- und Informationssicherheit ENISA[249] sowie die detaillierten Normen der NIS-2-Richtlinie und des Cybersecurity Act

---

[245] Calliess/Ruffert/*Korte* (2022) Art. 114 AEUV Rn. 2, 40.

[246] Grabitz/Hilf/Nettesheim/*Tietje* (September 2025) Art. 114 AEUV Rn. 77-79.

[247] Streinz/*Schröder* (2018) Art. 114 AEUV Rn. 33.

[248] Siehe bspw. ErwG 2, 7 Cybersecurity Act.

[249] EuGH, C-217/04 v. 2.5.2006, Rn. 48 ff. – ENISA.

(CSA), die der Agentur großflächig auch äußerst abstrakte, „marktferne" Kompetenzen, etwa zur Beratung der Mitgliedstaaten im Bereich der Cybersicherheitsforschung, zuschreiben.[250]

Vor diesem Hintergrund liegt es alles andere als fern, dass der Unionsgesetzgeber auch gesetzliche Regelungen zum staatlichen Umgang mit IT-Schwachstellen von Art. 114 Abs. 1 Satz 2 AEUV gedeckt sieht, hat die Vorhaltung solcher Lücken doch Auswirkungen auf das Funktionieren des digitalen Binnenmarkts.[251] Ähnlich verhält es sich mit Regelungen zum Ankauf kommerzieller Spyware-Kapazitäten.[252] Solchen Regelungen kommt technisch betrachtet zudem eine noch stärkere Marktfinalität zu. In beiden Fällen müsste dann aber im Lichte des konkreten Regelungsvorschlags geprüft werden, inwiefern einheitliche Regelungen zum Abbau von Handelshemmnissen in diesem Bereich tatsächlich nötig sind bzw. ob dies tatsächlich mit einer derartigen Regelung bezweckt würde. Das scheint – insbesondere für eine Regelung des Ankaufs von Spyware-Kapazitäten – denkbar, hängt aber auch davon ab, ob sich beweisen lässt, dass aufgrund unterschiedlicher nationaler Regelungen tatsächlich Handelshemmnisse oder Wettbewerbsverzerrungen bestehen und die Maßnahme im Schwerpunkt deren Überwindung dient.[253]

---

[250] Näher dazu Wischmeyer, *Informationssicherheit*, 2023, S. 164 ff. Siehe auch Calliess/Baumgarten, Cybersecurity in the EU, German L. J. 21 (2020), S. 1149 (1164).

[251] Andere Ansicht Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 278.

[252] Das Europäische Parlament scheint davon auszugehen, dass insofern eine EU-Kompetenz besteht, European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)* (P9_TA(2023)0244), S. 18 „the configuration of spyware that is imported into the EU and otherwise placed on the market should be regulated by way of a measure based on Article 114 TFEU"; das Parlament schlägt im Übrigen auch vor, das Anbieten und den Verkauf von Spyware marktseitig direkt zu regulieren; für eine derartige Regelung scheint eine EU-Kompetenz wahrscheinlich, European Parliament, *Recommendation*, S. 21-22 „Emphasises that only spyware that is designed so that it enables and facilitates the functionality of spyware according to the legislative framework as set out in paragraph 32 may be placed on the internal market, developed or used in the Union".

[253] Siehe zu den vom EuGH aufgestellten Maßstäben auch Streinz/*Schröder* (2018) Art. 114 AEUV Rn. 19-33, auch mit einigen instruktiven, wenngleich wenig kohärenten Beispielen.

b) Art. 16 Abs. 2 UAbs. 1 Satz 2 AEUV

Die Kompetenz aus Art. 16 Abs. 2 UAbs. 1 Satz 2 AEUV, die den Schutz personenbezogener Daten betrifft, dürfte demgegenüber nicht einschlägig sein.[254] Denn auch wenn der EuGH über Art. 16 Abs. 2 UAbs. 1 Satz 2 AEUV vermittelte Einbrüche in für die Mitgliedstaaten reservierte Regelungskompetenzen für gewöhnlich nachsichtig betrachtet,[255] lassen sich doch weder Entscheidungen über die Offenhaltung einer Schwachstelle noch über den Ankauf von Spyware im Wesentlichen als Regelungen über die „Verarbeitung von personenbezogenen Daten" verstehen.[256]

c) Justizielle und polizeiliche Zusammenarbeit

In Betracht kommen weiter Kompetenzgrundlagen der Kapitel 4 („Justizielle Zusammenarbeit in Strafsachen") und 5 („Polizeiliche Zusammenarbeit") des Titel 5 des AEUV („Raum der Freiheit, der Sicherheit und des Rechts").[257]

Konkret kann die EU gem. Art. 82 Abs. 1 UAbs. 2 lit. d) AEUV im Bereich der Strafverfolgung Maßnahmen erlassen, um „die Zusammenarbeit zwischen den Justizbehörden oder entsprechenden Behörden der Mitgliedstaaten im Rahmen der Strafverfolgung [...] zu erleichtern", wobei diese nicht zu einer „Angleichung der Rechtsvorschriften der Mitgliedstaaten" führen dürfen.[258] Nach Abs. 2 UAbs. 2 ist hingegen sogar eine solche Angleichung in Form von Mindestvorschriften zulässig, wenn es sich um den Bereich der „Zulässigkeit

---

[254] So auch *Buntrock, Staatlicher Umgang mit IT-Sicherheitslücken, 2025,*, Staatlicher Umgang mit IT-Sicherheitslücken, 2025, S. 278.

[255] Siehe bspw. EuGH, Urteil vom 30.3.2023, C-34/21, Rn. 32 ff. (*Hauptpersonalrat*) (zur Regelung von Online-Unterricht trotz Zuständigkeit der Mitgliedstaaten für die Gestaltung des Bildungssystems)

[256] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 278; auch das EU-Parlament stützt keinen seiner Regelungsvorschläge auf Art. 16 AEUV, European Parliament, *Recommendation*.

[257] Davon scheint auch das EU-Parlament auszugehen, ohne eine genauere Analyse der denkbaren Kompetenztitel anzustellen, European Parliament, *Recommendation*, S. 18.

[258] Streinz/*Satzger* (2018) Art. 82 AEUV Rn. 16 ff.

von Beweismitteln auf gegenseitiger Basis" (lit. a)) oder „sonstige spezifische Aspekte des Strafverfahrens, die zuvor vom Rat durch Beschluss bestimmt worden sind" (lit. c)), handelt. Zwar geht der europäische Gesetzgeber (zweifelhafterweise) davon aus, dass auf die Regelungen nicht nur Maßnahmen zur Festlegung bestimmter Standards der Zusammenarbeit, etwa standardisierter Datenformate, gestützt werden können.[259] Mehr als Mindeststandards für die grenzüberschreitende Anerkennbarkeit von mithilfe von Sicherheitslücken bzw. Spyware erlangten Beweismitteln[260] werden über Art. 82 AEUV allerdings nicht zu erreichen sein.

Gem. Art. 87 Abs. 2 lit. a) AEUV kann die EU im Bereich der polizeilichen Zusammenarbeit Maßnahmen erlassen, die das „Einholen, Speichern, Verarbeiten, Analysieren und Austauschen sachdienlicher Informationen", betreffen. Allerdings werden weder Standards zur Offenlegung oder Geheimhaltung von Sicherheitslücken noch zur Nutzung kommerzieller Spyware-Kapazitäten als Aspekte einer solchen „informationellen Kooperation" zwischen Polizeibehörden betrachtet werden können.[261] Gem. Art. 87 Abs. 2 lit. c) AEUV kann die EU zwar auch „gemeinsame Ermittlungstechniken" regulieren, diese dürfen aber nur die „Aufdeckung schwerwiegender Formen der organisierten Kriminalität" betreffen. Schließlich können bei Einstimmigkeit im Rat gem. Art. 87 Abs. 2 AEUV auch Maßnahmen erlassen werden, die die „operative Zusammenarbeit" von Polizeibehörden betreffen. Das erfasst wohl „jede gemeinsame Abstimmung

---

[259] Auch die PNR-Richtlinie, nach der die Mitgliedstaaten Fluggesellschaften dazu verpflichten müssen, gewisse Passagierdaten auf Vorrat zu speichern, wurde auf Art. 82 Abs. 1 UAbs. 2 lit. d) AEUV gestützt.

[260] Insbesondere einheitliche Mindestanforderungen, unter denen ein mithilfe einer Sicherheitslücke oder Spyware in einem Mitgliedstaat erlangtes Beweismittel in einem anderen Mitgliedstaat verwertbar ist (bspw. Dokumentations-, Integritäts- oder Herkunftsnachweise zur Beweiskette).

[261] Ähnlich Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 279; klassische Beispiele hierfür sind etwa die Fahndungssysteme des Schengener Informationssystems oder das Visa-Informationssystem.

oder Koordination in Bezug auf polizeiliche oder justizielle Maßnahmen auf dem Gebiet der polizeilichen Gefahrenabwehr und der polizeilichen Strafverfolgung",[262] belässt im Einzelnen aber auch einen erheblichen Interpretationsspielraum. Auch in dieser Vorschrift wird man aber keine allgemeine Kompetenz für die Regelung von Anforderungen an Schwachstellenmanagement und Spyware-Ankauf sehen können.[263]

d) Zwischenergebnis

Im Ergebnis kommt also in Betracht, dass eine unionale Regelung zum Schwachstellenmanagement wie auch zum Ankauf von kommerziell vertriebener Spyware auf Art. 114 Abs. 1 Satz 2 AEUV gestützt werden kann. Auf Art. 82 AEUV könnten allenfalls Mindeststandards zur Verwertbarkeit von durch derartige Angriffswege erlangte Beweismittel in der Strafverfolgung, nicht aber eine eigentliche Regelung zum Schwachstellenmanagement gestützt werden. Dabei handelt es sich jeweils um geteilte Zuständigkeiten gem. Art. 4 AEUV, sodass gem. Art. 2 Abs. 2 AEUV die Mitgliedstaaten regelnd tätig werden können, „sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat".

2. Kompetenzgrenzen

Auch die der Union explizit zugewiesenen Kompetenzen stehen aber unter gewissen Vorbehalten bzw. Einschränkungen.

Relevant für die hiesigen Überlegungen ist dabei insbesondere Art. 4 Abs. 2 Satz 2 EUV, wonach die Union „die grundlegenden Funktionen des Staates, insbesondere [...] die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit" zu achten hat. Gem. Art. 4 Abs. 2 Satz 3 EUV fällt deswegen „[i]nsbesondere die nationale Sicherheit [...] weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten".

---

[262] Calliess/Ruffert/*Suhr* (2022) Art. 87 AEUV Rn. 24.

[263] Andere Ansicht Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 280.

Dementsprechend weisen auch bestehende unionale Regelungen im Bereich der IT-Sicherheit Ausnahmeregelungen für den Bereich der „nationalen Sicherheit", teils auch der „öffentlichen Sicherheit" auf.[264] Auch das EU-Parlament gesteht zu, dass der Einsatz von Spyware für Belange der nationalen Sicherheit unional allenfalls „indirekt" reguliert werden dürfte.[265]

Was aber als Regelung der „nationalen Sicherheit" zu betrachten ist, ist bislang nicht abschließend geklärt.[266] Im Grundsatz wird der Begriff enger verstanden als jene der „öffentlichen" oder „inneren Sicherheit".[267] Klar ist auch, dass der EuGH entsprechende Bereichsausnahmen in der Vergangenheit eher eng interpretiert hat, und auch nationale Maßnahmen, die eindeutig Aktivitäten der Nachrichtendienste betreffen, als vom Unionsrecht erfasst ansah.[268] Nach den Worten des EuGH kann auch „die bloße Tatsache, dass eine nationale Maßnahme zum Schutz der nationalen

---

[264] Siehe bspw. Art. 1 Abs. 2 Cybersecurity Act „Von dieser Verordnung unberührt bleiben die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich."; Art. 2 Abs. 7 NIS-2-RL „Diese Richtlinie gilt nicht für Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten."; Art. 1 Abs. 5 Cyber Solidarity Act „Diese Verordnung lässt die grundlegenden staatlichen Funktionen der Mitgliedstaaten, darunter auch die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit, unberührt. Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.".

[265] European Parliament, *Recommendation*, S. 18 „notes that the use of spyware for national security purposes may only be indirectly regulated through, for example, fundamental rights and rules relating to data protection".

[266] European Parliament, *Recommendation*, S. 23; weiterführend *Tzanou/Vogiatzoglou*, European Papers eJournal (18.11.2025); Sandhu, *Squaring the Circle: The CJEU between Fundamental Rights Guardian and Architect of a Security Union*, Verfassungsblog, 2024.12.02.

[267] Siehe auch European Parliament, *Recommendation*, S. 23; Art. 15 der Richtlinie 2002/58 setzt die „nationale Sicherheit" mit der „Sicherheit des Staates" gleich.

[268] Siehe etwa EuGH, Urteil vom 21. Dezember 2016, C-203/15 und C-698/15, Rn. 75 ff. (*Tele2 Sverige*); EuGH, Urteil vom 2. Oktober 2018, C-217/16, Rn. 29 ff. (*Ministerio Fiscal*); EuGH, Urteil vom 6.10.2020, C-623/17, Rn. 44 ff. (*Privacy International*); EuGH, Urteil vom 6.10.2020, C-511/18 u. a., Rn. 99 ff. (*La Quadrature du Net*).

Sicherheit getroffen wurde, nicht dazu führen, dass das Unionsrecht unanwendbar ist und die Mitgliedstaaten von der erforderlichen Beachtung dieses Rechts entbunden werden".[269]

Dennoch spricht einiges dafür, dass unionale Regelungen, die *spezifisch und direkt* den staatlichen Umgang mit IT-Schwachstellen oder kommerzieller Spyware durch Nachrichtendienste, potenziell auch durch Polizeibehörden, regulieren, als Regeln im Bereich der „nationalen Sicherheit" zu gelten haben und damit kompetenzwidrig wären. Dafür spricht zum einen, dass die genannten Urteile eben jeweils nur (negativ) die Bereichsausnahme bzw. Kompetenzzuweisung für Maßnahmen der nationalen Sicherheit in Art. 15 ePrivacy-RL, und damit die Reichweite des Unionsrechts, nicht aber (positiv) die unionalen Gesetzgebungskompetenzen betrafen. Zum anderen, dass der betreffende Rechtsakt, die ePrivacy-RL, zweifellos viele Regelungen erfasst, die eindeutig nicht dem Bereich der nationalen Sicherheit zugeordnet werden können.

Daneben könnte auch Art. 346 Abs. 1 lit. a) AEUV einer unionalen Verpflichtung zum Schwachstellenmanagement bzw. ihrer ausnahmslosen Durchsetzung entgegenstehen.[270] Dieser schreibt vor, dass ein Mitgliedstaat „nicht verpflichtet [ist], Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht".[271] Auch wenn der EuGH in ständiger Rechtsprechung bekräftigt, dass sich aus Art. 346 AEUV „kein allgemeiner, dem Vertrag immanenter Vorbehalt ableiten [lässt], der jede Maßnahme, die im Interesse der öffentlichen Sicherheit getroffen wird, vom Anwendungsbereich des Unionsrechts ausnähme",[272]

---

[269] EuGH, Urteil vom 6.10.2020, C-511/18 u. a., Rn. 44 ff. (*La Quadrature du Net*) (m.w.N.).

[270] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 280 f.

[271] Nach vorherrschender Auffassung in der Literatur betrifft die Norm auch „Auskünfte" gegenüber Einzelnen und der Öffentlichkeit, Calliess/Ruffert/*Wegener* (2022) Art. 346 AEUV Rn. 5 (m.w.N.).

[272] Siehe nur EuGH, Urteil vom 04.03.2010, C-38/06, Rn. 62 (*Kommission/Portugal*).

und die Vorschrift weiter auch eng auszulegen sei,[273] gesteht die Norm den Mitgliedstaaten doch explizit einen Ermessensspielraum zu,[274] den das Gericht eher umsichtig zu behandeln scheint.[275]

3. Ergebnis

Im Ergebnis kommt eine Regulierung des Schwachstellen- und Spywaremanagements durch die EU daher nur begrenzt in Betracht. Die EU könnte wohl, gestützt auf Art. 114 Abs. 1 Satz 2 AEUV, anbieterseitige Anforderungen an den Verkauf von Spyware-Software im EU-Territorium aufstellen. Die Einführung einer Pflicht zum staatlichen Schwachstellenmanagement durch Sicherheitsbehörden scheint hingegen durch die Kompetenzgrenze der „nationale Sicherheit“ gem. Art. 4 Abs. 2 Satz 3 EUV ausgeschlossen.

II. Vorgaben des Unionsrechts

Selbst wenn der Union keine Kompetenz zur gesetzlichen Regelung des staatlichen Umgangs mit IT-Schwachstellen oder Spyware zukommen sollte,[276] kommt doch in Betracht, dass sie gewisse Teilaspekte dieser Handlungsfelder regeln darf bzw. bereits geregelt hat.[277] Auch weil Regelungen auf nationaler Ebene unionale Vorgaben aufgrund des Vorrangs des Unionsrechts nicht verletzen dürfen, muss deshalb im Folgenden der Frage nachgegangen werden, ob bestehende Regeln des Unionsrechts

---

[273] Siehe nur EuGH, Urteil vom 20.03.2018, C-187/16, Rn. 77 (*Kommission/Österreich*).

[274] Calliess/Ruffert/*Wegener* (2022), Art. 346 AEUV Rn. 3.

[275] Calliess/Ruffert/*Wegener* (2022), Art. 346 AEUV Rn. 3.

[276] Siehe oben C.I.

[277] Vgl. auch Geiger/Khan/Kotzur/Kirchmair/*Geiger/Kirchmair* (2023) Art. 5 EUV Rn. 3 („periphere Auswirkungen kompetenzgemäßer Handlungen”); zu eng deshalb Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 281, der meint, Auswirkungen bestehender Unionsrechtsakte auf das Schwachstellenmanagement seien in jedem Fall unionsrechtswidrig.

bestimmte Teilbereiche des Schwachstellenmanagements bzw. des Ankaufes von Spyware bereits heute regulieren.

1. NIS-2-Richtlinie

Die NIS-2-Richtlinie stellt den aktuell zentralen Rechtsakt der unionalen IT-Sicherheits-Gesetzgebung dar. Sie verpflichtet insbesondere Betreiber kritischer Infrastrukturen und anderer sog. „wesentlicher und wichtiger Einrichtungen" zu Maßnahmen des Cyber-Risikomanagements sowie zur Meldung von Sicherheitsvorfällen.[278] Dies umfasst gem. Art. 21 Abs. 2 lit. e) NIS-2-RL auch Maßnahmen zu „Management und Offenlegung von Schwachstellen".

Auch „Einrichtungen der öffentlichen Verwaltung" gelten dabei gem. Art. 3 Abs. 1 lit. d), Art. 2 Abs. 2 lit. f) cif. i) NIS-2-RL als „wesentliche Einrichtungen" und haben demnach die vorgesehenen IT-Sicherheits-Verpflichtungen zu erfüllen. Nach Art. 2 Abs. 6 lässt die Richtlinie „die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis, andere wesentliche staatliche Funktionen zu schützen [aber] unberührt". Gem. Art. 2 Abs. 7 gilt die Richtlinie deswegen explizit nicht für „Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten". Zu diesem Zweck können die Mitgliedstaaten deshalb gem. Art. 2 Abs. 8 NIS-2-RL derartige Behörden und auch Einrichtungen, die ausschließlich für solche Behörden Dienste erbringen, von den materiellen IT-Sicherheitspflichten ausnehmen. Von dieser Befreiungsmöglichkeit hat der deutsche Gesetzgeber durch das NIS2UmsCG in § 37 Abs. 2 und 3 BSIG Gebrauch gemacht.[279]

---

[278] Art. 20 ff. NIS-2-RL.

[279] Zuständig für diese Entscheidung ist danach das Bundesministerium des Innern. Es kann eine Befreiung auf Vorschlag des Bundeskanzleramts und verschiedener Ministerien

Weiter umfasst die Richtlinie gem. Art. 2 Abs. 11 nicht „die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde" und bleibt Art. 346 AEUV gem. Art. 2 Abs. 13 NIS-2-RL unbeschadet.[280]

Schließlich ist zu beachten, dass die NIS-2-RL nur zu Maßnahmen verpflichtet, „um die Risiken für die Sicherheit der Netz- und Informationssysteme, *die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen*, zu beherrschen und die *Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste* zu verhindern oder möglichst gering zu halten". Die Entdeckung einer Sicherheitslücke kann demnach ohnehin schon nur dann zu Maßnahmen (etwa zur Meldung der Sicherheitslücke) verpflichten, wenn die Sicherheitslücke Netz- oder Informationssysteme betrifft, die die Behörde selbst für ihren Betrieb benutzt,[281] oder aber die Entdeckung als „Sicherheitsvorfall" verstanden werden kann, d.h. als „Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt". Beides ist denkbar, scheint für den Regelfall aber eher unwahrscheinlich.[282]

Insbesondere vor dem Hintergrund der Möglichkeit einer Befreiung der maßgeblichen (Sicherheits-)behörden wird die NIS-2-RL deshalb keinen

---

oder auf eigenes Betreiben hin anordnen. Ein Antragsrecht der betreffenden Einrichtungen existiert nicht.

[280] Siehe oben C.I.2.

[281] Das kann freilich schwierige Auslegungsfragen dazu auslösen, was als Betrieb und Dienst einer bestimmten Behörde zu verstehen ist.

[282] Zu pauschal verneinend Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 283.

relevanten Einfluss auf die hier betroffenen Fragen des Schwachstellenmanagements und Spyware-Ankaufs haben.

2. ePrivacy-Richtlinie

Die ePrivacy-Richtlinie dient dem Schutz der Privatsphäre in der elektronischen Kommunikation. Gem. Art. 5 ePrivacy-RL stellen die Mitgliedstaaten zu diesem Zweck „die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher". Sie haben insbesondere „das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer" zu untersagen, Art. 5 Abs. 1 Satz 2 ePrivacy-RL.

Allerdings sind gem. Art. 5 Abs. 1 Satz 2 a.E. i.V.m. Art. 15 nationale Ausnahmeregeln zulässig, sofern diese „für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig" sind.

Auf der Grundlage von Art. 5 ePrivacy-RL erklärte der EuGH 2020 und 2022 die nationalen Regelungen Frankreichs, Großbritanniens und Deutschlands zur Vorratsdatenspeicherung für europarechtswidrig,[283] erklärte dann aber 2024 die neue französische Regelung der Vorratsdatenspeicherung für zulässig.[284]

---

[283] EuGH, Urteil vom 6. Oktober 2020, C-511/18 (*La Quadrature du Net ua*); EuGH, Urteil vom 6. Oktober 2020, C-623/17 (*Privacy International*); EuGH, Urteil vom 20. September 2022, C-793/19 und C-794/19 (*SpaceNet*).

[284] Urteil des EuGH vom 30. April 2024, C-470/21 (*La Quadrature du Net*).

Ob die ePrivacy-RL Einfluss auf nationale Vorgaben zum Schwachstellenmanagement oder Spyware-Ankauf hat, richtet sich danach, ob derartige Praktiken „die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten" betreffen bzw. beeinträchtigen. Unzweifelhaft ist zunächst, dass staatlich genutzte Schwachstellen die Vertraulichkeit von Nachrichten, die mit von der ePrivacy-RL erfassten Kommunikationsdiensten (bspw. Messenger-Diensten) übertragen werden, faktisch beeinträchtigen können. Gegen eine Erfassung der hier in Frage stehenden Regelungen unter Art. 5 ePrivacy-RL spricht aber, dass die dort genannten Beispiele („Mithören, Abhören, Speichern, Abfangen oder Überwachen von Nachrichten") eher das tatsächliche Abfangen von Nachrichten als das Verfügen über Infrastruktur, die potenziell zum Abfangen genutzt werden kann (bspw. IT-Schwachstellen, Spyware), ins Auge nimmt. Dem entspricht, dass die Regelungen die Vertraulichkeit der *Nachrichten*, nicht aber der *Kommunikationsdienste* schützen will.

Gleichwohl ist aber nicht undenkbar, dass im Wege einer extensiven Auslegung auch Schwachstellen-Wissen oder angekaufte Spyware als von Art. 5 ePrivacy-RL erfasste Beeinträchtigung der Vertraulichkeit von übertragenen Nachrichten verstanden werden kann, die folglich national nur unter Einhaltung der in Art. 5 Abs. 1 Satz 2 a.E. i.V.m. Art. 15 ePrivacy-RL vorgesehenen Grundrechtsgarantien eingeführt werden dürften.[285] Spezifische Vorgaben zur Ausgestaltung des Schwachstellenmanagements ergeben sich aus der Vorschrift jedoch nicht.

---

[285] So wohl auch European Parliament, *Recommendation*, S. 9-10; zu pauschal verneinend deswegen Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 284; das hätte insbesondere Folgen für das anzuwendende Grundrechtsregime, siehe oben B.I.1.

3. DSGVO

Die DSGVO stellt das zentrale sektorübergreifende Datenschutzgesetz der EU dar, das Anforderungen an den Datenschutz für private wie öffentliche Stellen aufstellt.

Anwendung findet sie aber nur, wo es um die Verarbeitung „personenbezogener Daten" geht. Dies ist bei der der Entscheidung über die Offenhaltung oder Meldung einer Schwachstelle selbst nicht der Fall,[286] sodass sich Vorschriften zum Schwachstellenmanagement dem Regelungsbereich der DSGVO entziehen.[287]

Anderes könnte aber für die Nutzung von kommerziellen Spyware-Dienstleistungen gelten. Jedenfalls wenn die Dienstleistung so ausgestaltet ist, dass tatsächlich personenbezogene Daten an eine andere Stelle – konkret: Spyware-Anbieter – übermittelt werden, kommt es zu einer (der eigentlichen Datenausspähung vorgelagerten) datenschutzrechtlich relevanten Datenverarbeitung. Es ist denkbar, dass diese Datenverarbeitung auf die Auswahl konkreter Anbieter bzw. die Entscheidung über den Ankauf eine bestimmten Produkts vorwirkt. Die DSGVO enthält nämlich verschiedene Regelungen, die schon auf die Gestaltung datenverarbeitender Systeme Auswirkungen zeitigen können: dazu zählen Art. 25 DSGVO („data protection by design"), nach dem Verantwortliche schon „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung [...] geeignete technische und organisatorische Maßnahmen" treffen müssen, um die Datenschutzgrundsätze zu realisieren; Art. 28 DSGVO, nach dem Verantwortliche nur mit Auftragsverarbeitern zusammenarbeiten dürfen, die „hinreichend Garantien dafür bieten", dass die Datenverarbeitung in Einklang mit den Vorschriften der Verordnung erfolgt; Art. 32 DSGVO, nach dem

---

[286] Freilich kann eine Schwachstelle später ausgenutzt werden, um über *Exploits* personenbezogene Daten zu erlangen. Dieser Vorgang kann und muss dann aber separat datenschutzrechtlich bewertet werden.

[287] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 285.

„geeignete technische und organisatorische Maßnahmen" zur Gewährleistung der Datensicherheit getroffen werden müssen; und Art. 35 DSGVO, nach dem vor der Durchführung besonders riskanter Datenverarbeitungsformen eine sog. Datenschutz-Folgeabschätzung erfolgen muss.

Diese Vorgaben wären allerdings nur dann zu berücksichtigen, wenn bezüglich der Inanspruchnahme von privaten Spyware-Kapazitäten keine Bereichsausnahme der DSGVO greift.

Gem. Art. 2 Abs. 2 lit. d) DSGVO findet die Verordnung aber für die Datenverarbeitung durch Strafverfolgungs- und Polizeibehörden keine Anwendung. Diese haben sich allenfalls an die Vorschriften der JI-Richtlinie zu halten.[288]

Gem. Art. 2 Abs. 2 lit. a) DSGVO findet die Verordnung weiter auch für Tätigkeiten, die „nicht in den Anwendungsbereich des Unionsrechts" fallen, keine Anwendung. Der EuGH will diese Ausnahmevorschrift zwar explizit eng verstanden wissen.[289] In Übereinstimmung mit der Vorgängerbestimmung Art. 3 Abs. 2 RL 95/46 und ErwG 16[290] geht aber auch der EuGH davon aus, dass eine Datenverarbeitung durch „staatliche[] Stellen im Rahmen einer Tätigkeit, die der Wahrung der nationalen Sicherheit dient, oder einer Tätigkeit, die derselben Kategorie zugeordnet werden kann," nicht von der DSGVO erfasst wird.[291] Als auf die Wahrung der nationalen Sicherheit abzielende Tätigkeiten seien „insbesondere solche [zu verstehen], die den Schutz der grundlegenden Funktionen des Staates und der grundlegenden Interessen der Gesellschaft bezwecken".[292] Im Urteil zur französischen

---

[288] Siehe sogleich C.II.4.

[289] EuGH, Urteil vom 22.06.2021, C-439/19, Rn. 62 (*Latvijas Republikas Saeima*) (m.w.N.).

[290] „[…] Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen, wie etwa die nationale Sicherheit betreffende Tätigkeiten".

[291] EuGH, Urteil vom 22.06.2021, C-439/19, Rn. 62-66 (*Latvijas Republikas Saeima*).

[292] EuGH, Urteil vom 22.06.2021, C-439/19, Rn. 67 (*Latvijas Republikas Saeima*).

Regelung der Vorratsdatenspeicherung hat der EuGH dem Begriff noch weitere Konturen gegeben. Hier hielt er fest, dass die ausschließlich mitgliedstaatliche Verantwortung für die nationale Sicherheit „dem zentralen Anliegen [entspreche], die wesentlichen Funktionen des Staates und die grundlegenden Interessen der Gesellschaft zu schützen" und „die Verhütung und Repression von Tätigkeiten [umfasse], die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen".[293] Das erfasse „insbesondere terroristische Aktivitäten".[294] Davon seien Tätigkeiten zur Repression von allgemeiner, auch schwerer Kriminalität und auch zum allgemeinen Schutz der öffentlichen Sicherheit, inklusive dem Schutz vor Gefahren „selbst schwerer Spannungen oder Störungen im Bereich der öffentlichen Sicherheit", zu unterscheiden.[295]

Ob nach diesen Maßstäben (alle) Aufklärungstätigkeiten beispielsweise des Bundesnachrichtendienstes oder der Verfassungsschutzbehörden als die „nationale Sicherheit" betreffend beurteilt werden können, kann letztlich nur gerichtlich entschieden werden. Die hohen Anforderungen des EuGH sprechen aber dafür, dass dies nicht pauschal und für alle Aktivitätsbereiche bejaht werden kann.

4. JI-Richtlinie

Die JI-Richtlinie regelt den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch öffentliche Behörden, die zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit tätig werden.

---

[293] EuGH, Urteil vom 06.10.2020, C-511/18, Rn. 135 (*La Quadrature du Net ua*).

[294] EuGH, Urteil vom 06.10.2020, C-511/18, Rn. 135 (*La Quadrature du Net ua*).

[295] EuGH, Urteil vom 06.10.2020, C-511/18, Rn. 136 (*La Quadrature du Net ua*).

Auch unter der JI-RL stellt die Entscheidung über den Umgang mit einer Sicherheitslücke allerdings keine Verarbeitung von personenbezogenen Daten dar,[296] sodass wiederum nur die Inanspruchnahme externer Spyware-Kapazitäten potenziell eine Einhegung erfährt. Auch die JI-Richtlinie enthält insofern Regeln, die schon auf den Einkauf eines bestimmten Produkts vorwirken könnten, insbesondere Art. 20 JI-RL („data protection by design"), Art. 22 JI-RL („Auftragsverarbeiter") und Art. 27 („Datenschutzfolgenabschätzung").

Auch die JI-Richtlinie gilt allerdings wiederum nur für Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, Art. 2 Abs. 3 lit. b) JI-RL. Auch hier sind also Tätigkeiten, die dem Schutz der „nationalen Sicherheit" dienen, ausgenommen.[297]

Die gewöhnlichen Tätigkeiten der Strafverfolgungs- und Polizeibehörden, die durch die JI-Richtlinie ja gerade reguliert werden sollen, können, auch wenn sie schwere Kriminalitätsformen betreffen, aber nicht als die „nationale Sicherheit" betreffend verstanden werden.[298]

5. Cyber Resilience Act

Mit dem Cyber Resilience Act hat die Europäische Union einheitliche IT-Sicherheitsanforderungen für „Produkte mit digitalen Elementen" eingeführt (bspw. Software oder IoT-Geräte). Auch wenn die Verordnung dementsprechend vor allem Hersteller und Händler derartiger Produkte anspricht, sieht sie doch auch gewisse Rechte und Pflichten für die Mitgliedstaaten vor.

Konkret dürfen die Mitgliedstaaten gem. Art. 4 Abs. 1 „die Bereitstellung auf dem Markt von Produkten mit digitalen Elementen, die dieser Verordnung entsprechen, [nicht behindern]". Wie auch ErwG 13 der Verordnung

---

[296] Siehe bereits oben C.II.3.

[297] Vgl. auch ErwG 14 JI-RL.

[298] Siehe bereits oben C.I.2.

klarmacht, ist der Zweck dieser Vorschrift aber, den Erlass zusätzlicher, über die Verordnung hinausgehender Cybersicherheitsanforderungen zu verhindern. Dass sie auch Maßnahmen, die die Cybersicherheit von Produkten negativ beeinträchtigen können, verhindern will, scheint nicht angezeigt.

Einer Erfassung von Spyware-"Produkten" scheint entgegenzustehen, dass die Verordnung gem. Art. 2 Abs. 7 nicht für Produkte gelten soll, „die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind" und gem. Art. 2 Abs. 8 die in der „Verordnung festgelegten Verpflichtungen [...] nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde[, umfassen]".

Das IT-Schwachstellenmanagement wie auch der Ankauf von Spyware ist durch den Cyber Resilience Act deswegen nicht betroffen.[299]

6. Cybersecurity Act

Mit dem Cybersecurity Act stärkte die EU 2019 das Mandat der europäischen Cybersecurity-Behörde ENISA und legte Regeln zu deren Kompetenzen, der Zusammenarbeit mit nationalen Behörden und einem einheitlichen europäischen Zertifizierungsrahmen fest. Vorgaben für ein IT-Schwachstellen-Management oder den Ankauf von Spyware lassen sich der Verordnung aber nicht entnehmen.[300]

---

[299] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 286-288.

[300] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 286.

7. Ergebnis

Angesichts der Unklarheiten, wie weit die im Primär- und Sekundärrecht für die Sicherheitsbehörden geschaffenen Bereichsausnahmen reichen, kann nicht mit Sicherheit ausgeschlossen werden, dass einzelne Vorschriften der NIS-2-Richtlinie, der ePrivacy-Richtlinie, der DSGVO und der JI-Richtlinie punktuell Einfluss auf den staatlichen Umgang mit IT-Schwachstellen und kommerzieller Spyware haben.

Eine umfassende Regelung der hier betroffenen Fragen findet sich im Unionsrecht derzeit aber nicht. Das bedeutet auch, dass das Unionsrecht insoweit derzeit keine Sperrwirkung für nationale Regelungen des Schwachstellenmanagements oder des Spyware-Ankaufs entfaltet.

III. Kompetenzverteilung im Bundesstaat

Innerhalb Deutschlands richtet sich die Gesetzgebungskompetenz nach den Art. 70 ff. GG. Nach der Grundregel des Art. 70 Abs. 1 GG haben grundsätzlich die Länder das Recht der Gesetzgebung, soweit das Grundgesetz nicht explizit dem Bund Gesetzgebungskompetenzen einräumt. Dies tut das Grundgesetz vor allem in den Artikeln 73 und 74 GG, in denen dem Bund ausschließliche (Art. 73 GG) und konkurrierende Legislativkompetenzen (Art. 74 GG) eingeräumt werden.

Eine Bundeskompetenz zur Regelung des Schwachstellenmanagements und Spyware-Ankaufs durch die Sicherheitsbehörden des Bundes folgt dabei schon aus der Kompetenz des Bundes, die Ausnutzung von Schwachstellen durch diese Behörden zu regeln.[301] Konkret betrifft dies BND (Art. 73 Abs. 1 Nr. 1 GG), MAD (Art. 73 Abs. 1 Nr. 1 Var. 2 GG), BKA (Art. 73 Abs. 1 Nr. 9a, Nr.

[301] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 214 f.

10 GG) und Bundespolizei (Art. 87 Abs. 1 Satz 2 i.V.m. Art. 73 Abs. 1 Nr. 5 GG).[302]

Für die Regelung des Umgangs mit Schwachstellen durch andere Bundesbehörden besteht eine ungeschriebene Gesetzgebungskompetenz aus der Natur der Sache[303] bzw. aus Sachzusammenhang.[304] Für das Schwachstellenmanagement und den Spyware-Ankauf durch die Strafverfolgungsbehörden aus der Zuständigkeit für das gerichtliche Verfahren, Art. 74 Abs. 1 Nr. 1 GG.[305]

Fraglich ist dann, ob der Bund darüber hinaus auch für Landesbehörden Regeln zum Umgang mit Schwachstellen bzw. kommerziellen Spyware-Kapazitäten treffen darf.

Einen einheitlichen Kompetenztitel für die Regelung der Informationssicherheit kennt das Grundgesetz nicht.[306] Der Bundesgesetzgeber geht allerdings davon aus, dass jedenfalls die derzeitigen bundesweiten IT-Sicherheitsvorgaben des BSI-Gesetzes für kritische Anlagen und sog. wichtige und besonders wichtige Einrichtungen neben sektoralen Regelungskompetenzen (bspw. für die Telekommunikation gem. Art. 73 Abs. 1 Nr. 7 GG) auch auf die Kompetenz zur Regelung des Rechts der Wirtschaft gem. Art. 74 Abs. 1 Nr. 11 GG gestützt werden können.[307] Auch die Erforderlichkeit einer bundesgesetzlichen Regelung zur Wahrung der Wirtschaftseinheit im gesamtstaatlichen Interesse gem. Art. 72 Abs. 2 GG sei

---

[302] Näher Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (50 ff.).

[303] Vgl. auch die Gesetzesbegründung zum NIS-2-UmsuCG, Deutscher Bundestag, *Drucksache 21/1501*, S. 98.

[304] Dazu näher Wischmeyer, in: Dreier, Grundgesetz, 4. Aufl., Art. 70 Rn. 58 f. Vgl. auch für eine ähnliche Konstellation BVerfGE 125, 260 (314 ff.); 130, 151 (185 f.); 170, 79 (131 Rn. 149).

[305] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 214 f.

[306] Siehe auch Wischmeyer, *Informationssicherheit*, 2023, S. 164.

[307] Deutscher Bundestag, *Drucksache 21/1501*, S. 97 f.

angesichts der gestiegenen Bedrohungslage wegen ansonsten drohender „erheblicher Wettbewerbsverzerrungen" gegeben.[308]

Eine Regelung des Schwachstellenmanagements bzw. des Spyware-Ankaufs kann aber wohl nicht auf die Kompetenz zur Regelung des Wirtschaftsrechts gestützt werden. Denn auch wenn IT-Sicherheitslücken offensichtlich (große) wirtschaftliche Auswirkungen haben,[309] handelt es sich doch in erster Linie um Materien, die dem Bereich „Gefahrenabwehr" zuzurechnen sind.[310]

In Betracht kommen aber eine Reihe weiterer Kompetenztitel, insbesondere Art. 73 Abs. 1 Nr. 10 Var. 1 GG i.V.m. Art. 87 Abs. 1 Satz 2 GG: Gem. Art. 73 Abs. 1 Nr. 10 Var. 1 GG darf der Bund Regeln für „die Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei [und] zum Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Verfassungsschutz)" treffen. Institutionell kann die Zusammenarbeit auch über sog. Zentralstellen organisiert werden, zu deren Einrichtung auf gewissen Gebieten Art. 87 Abs. 1 Satz 2 GG ermächtigt.[311]

Nach verfassungsgerichtlicher Definition ist unter „Zusammenarbeit" dabei „die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse [sowie] funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und

---

[308] Deutscher Bundestag, *Drucksache 21/1501*, S. 97 f.

[309] Siehe auch B.I.6.

[310] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 215 (m.w.N.); siehe auch Kipker, *IT-SiG 2.0: Kompetenzgerangel zwischen Bund und Ländern* (09.02.2021), Beck Blog.

[311] Art. 87 Abs. 1 Satz 2 GG „Durch Bundesgesetz können Bundesgrenzschutzbehörden, Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen, für die Kriminalpolizei und zur Sammlung von Unterlagen für Zwecke des Verfassungsschutzes [...] eingerichtet werden."; zum Verhältnis zwischen Art. 73 Abs. 1 Nr. 10 Var. 1 GG i.V.m. Art. 87 Abs. 1 Satz 2 GG, Dürig/Herzog/Scholz/*Ibler* (August 2025) Art. 87 GG Rn. 117-120.

gemeinsame Informationssysteme".[312] Wie diese Definition schon nahelegt, liegt der Kern der Zusammenarbeit in der Schaffung gemeinsamer (Kommunikations-)Infrastrukturen, Einrichtungen und Ressourcen.

Diskutiert wird allerdings auch, ob die Kompetenz dem Bund (in Ausnahmefällen) auch gestattet, den Ländern materielle Eingriffsbefugnisse zu erteilen,[313] die Länder dazu zu verpflichten, ihre Behörden mit bestimmten Befugnissen auszustatten,[314] die Länder dazu zu verpflichten, die für eine Zusammenarbeit erforderlichen Rahmenbedingungen zu schaffen,[315] dem Bund für Konfliktfälle Weisungsbefugnisse gegenüber Landesbehörden einzuräumen,[316] oder sogar anstelle der Länder tätig zu werden.[317]

---

[312] BVerfG, Beschluss vom 10. November 2020, Rn. 76 (*Antiterrordateigesetz II*); BVerfG, Urteil vom 24. April 2013, Rn. 97 (*Antiterrordateigesetz I*).

[313] Ablehnend Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (58 ff.); Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 GG Rn. 235.

[314] Ablehnend Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (58 ff.); Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 GG Rn. 235; BeckOK GG/*Seiler* (November 2025), Art. 73 GG Rn. 46.3.

[315] Bejahend Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 GG Rn. 233

[316] Restriktiv Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (65 ff.). Bejahend, aber begrenzt auf Zwecke der Koordinierung, Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 GG Rn. 234 („sofern dies im Hinblick auf den intendierten Zweck der Koordinierung geeignet und erforderlich und mit dem Gebot eines rücksichtsvollen Umgangs mit den Landesbehörden vereinbar ist"); nach derzeitigem Recht sind derartige Weisungsbefugnisse sowohl Bundes-Zentralstellen, konkret: dem BKA (§ 4 BKAG), als auch der Bundesregierung, konkret: in § 7 BVerfSchG, eingeräumt.

[317] Bejahend, aber unter dem Vorbehalt einer ausdrücklichen verfassungsrechtlichen Ermächtigung, Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 GG Rn. 231. Ablehnend zu einer sektoralen Zentralisierung de constitutione lata auch Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, S. 35 (71 ff.).

Der Zweck der Kompetenznorm legt eine Anwendung auf das Schwachstellenmanagement, dessen besonderes Koordinationsbedürfnis insbesondere dadurch ausgelöst wird, dass eine einmal offengelegte Schwachstelle für alle potenziellen behördlichen Nutzer verbrannt wird,[318] eigentlich nahe.[319]

Im Ergebnis würde es aber eine von Art. 73 Abs. 1 Nr. 10 GG nicht mehr gedeckte Aushöhlung bzw. Übertragung von Landeskompetenzen bedeuten, wenn der Bund die Länder zur Durchführung von Schwachstellenmanagement oder zur obligatorischen Inanspruchnahme eines bundesweit zentralisierten Verfahrens hierfür verpflichten würde.[320]

Möglich ist aber, für die Zwecke der Zusammenarbeit den Ländern die optionale Inanspruchnahme eines beim Bund eingerichteten Schwachstellenmanagement-Prozesses zu erlauben, und zudem durch bundesrechtliche Anordnung – hier liegt der Kern der Zentralstellenfunktion – wechselseitige Beteiligungs- und Informationspflichten vorzusehen.[321] Dies würde bedeuten, dass der Bund Landesbehörden nicht dazu verpflichten kann, Schwachstellen-Management nach gewissen Vorgaben durchzuführen, die Länder (und auch der Bund) aber dazu verpflichtet werden können, im Falle der Einrichtung eines Schwachstellen-Management-Prozesses die jeweils andere Verbandsebene in das Entscheidungsverfahren einzubinden. Dies könnte beispielsweise durch eine Stellungnahmemöglichkeit im Entscheidungsverfahren oder ein Recht, über entdeckte und geheim gehaltene Schwachstellen informiert zu werden, sichergestellt werden.

---

[318] Gleichsam wie eine geheim gehaltene Schwachstelle regelmäßig auch Gefahren für Personen und Einrichtungen auslösen wird, deren Schutz Behörden einer anderen Verbandsebene aufgetragen ist.

[319] Vgl. auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 217-218.

[320] So auch Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 219.

[321] Ähnlich Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 216-220; zu weit geht aber wohl bereits die These, der Bund dürfe „einheitliche Kriterien und Mindeststandards für die Entscheidung über den Umgang mit IT-Sicherheitslücken festlegen", Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, S. 220.

Weiter in Betracht kommt Art. 91c Abs. 1 GG, der es Bund und Ländern erlaubt, „bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammen[zu]wirken". Allerdings enthält die Norm keine Gesetzgebungskompetenz des Bundes.[322] Sie schreibt vielmehr nur fest, dass eine föderale Kooperation im Bereich der IT-Systeme, bspw. durch Staatsverträge oder Verwaltungsabkommen, erlaubt ist. Außerdem erfasst die Norm nur Planung, Errichtung und Betrieb von IT-Infrastruktur. Handlungs- oder Kooperationsbefugnisse, die über derartige technische Fragen hinausgehen, sollen durch die Norm nicht zugeteilt werden.[323] Demnach bemächtigt Art. 91c Abs. 1 GG den Bund weder dazu, Landesbehörden zur Durchführung von Schwachstellen-Management zu verpflichten, noch, ihnen Vorgaben für den Einsatz von kommerzieller Spyware zu machen.

Im Ergebnis steht dem Bund also eine Gesetzgebungskompetenz zur Regelung des Umgangs mit IT-Schwachstellen und des Spyware-Ankaufs durch die Bundesbehörden, nicht aber durch Landesbehörden zu. Darüber hinaus könnte der Bund die Länder zu gewissen Kooperationsmaßnahmen in diesen Gebieten verpflichten.

---

[322] Anders Art. 91c Abs. 4 und 5 GG, die für die hier interessierenden Fragen aber keine Rolle spielen.

[323] Siehe auch Dreier Band III/*Heun/Thiele* (2018) Art. 91c Rn. 8 ff.

Regelungsvorschlag

Wie in der obenstehenden Analyse zum Ausdruck gebracht wurde, gebietet das Grundgesetz eine formellgesetzliche Regelung des Schwachstellen- und Spywaremanagements, die gewisse Mindestaspekte umfasst.

Dieses verfassungsrechtlich erforderliche Minimum würde durch den folgenden Regelungsvorschlag erfüllt.

Innerhalb dieses Rahmens bestehen für den Bundesgesetzgeber allerdings gewisse Entscheidungsspielräume, insbesondere was Auswahl und Ausgestaltung des Entscheidungs- und des Kontrollorgans angeht. Im folgenden Regelungsvorschlag wird davon ausgegangen, dass der Gesetzgeber sich insofern zur Schaffung eines neuen Entscheidungskörpers entscheidet („Gremium für Schwachstellenmanagement“), das samt Sekretariat am Bundeskanzleramt angesiedelt wird und der Kontrolle durch den Unabhängigen Kontrollrat untersteht. Dabei handelt es sich aber um Entscheidungen, die nach der vorstehenden Analyse zwar gut begründbar, verfassungsrechtlich aber nicht zwingend sind, sondern vielmehr im gesetzgeberischen Ermessen stehen. Dies wird im Text durch eine [eckige Umklammerung dieser ausfüllungsbedürftigen bzw. optionalen Regelungsaspekte] markiert.

§ 1 Schwachstellenmanagement

(1) [1]Behörden und sonstige öffentliche Stellen des Bundes sind verpflichtet, ihnen bekannt gewordene Schwachstellen gem. § 2 Nr. 38 BSIG, die dem Hersteller des betroffenen Produkts und der Öffentlichkeit unbekannt sind, an den Hersteller des betroffenen Produkts zu melden. [2]Dazu hat die Behörde oder sonstige öffentliche Stelle die Schwachstelle dem Bundesamt für die Sicherheit in der Informationstechnik zum Zwecke der koordinierten Offenlegung nach Artikel 12 Absatz 1 der NIS-2-Richtlinie zu melden. [3]Ist die

Behörde der Ansicht, dass die Schwachstelle aufgrund eines entgegenstehenden überwiegenden öffentlichen Interesses ausnahmsweise geheim gehalten werden soll, hat sie die Schwachstelle unverzüglich dem geregelten Verfahren zur Entscheidung über die Geheimhaltung einer Schwachstelle gem. Absatz 3 zuzuführen. [4]Dies gilt unabhängig von der Herkunft der Kenntnis. [5]Ausgenommen von der Pflicht nach Satz 3 sind Schwachstellen, die der Behörde oder sonstigen öffentlichen Stelle ausschließlich zum Zwecke der koordinierten Offenlegung gemeldet wurden, sowie Fälle dringender Gefahren, die ein sofortiges Handeln erfordern.

(2) [1]Zuständig für die Entscheidung über die Geheimhaltung einer Schwachstelle ist [das Gremium für Schwachstellenmanagement]. [[2]Dem Gremium gehören Vertreter der Bundesministerien des Innern, der Verteidigung, für Wirtschaft und Energie, der Justiz und für Verbraucherschutz und für Digitales und Staatsmodernisierung sowie des Bundeskanzleramtes, des Bundesamtes für Sicherheit in der Informationstechnik, der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, des Bundesamtes für Verfassungsschutz, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes, des Bundeskriminalamtes, der Bundespolizei, der Bundeswehr und des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe an. [3]Es wird in seiner Arbeit durch ein Sekretariat unterstützt, das beim Bundeskanzleramt angesiedelt ist. [4]Das Gremium soll seine Entscheidungen im Einvernehmen treffen.]

(3) [1]Zur Entscheidung über den Umgang mit der Schwachstelle sind die gegenläufigen Belange, insbesondere die Gefahren, die durch eine Geheimhaltung der Schwachstelle drohen, und der Nutzen einer möglichen staatlichen Nutzung der Schwachstelle, gegeneinander abzuwägen. [2]Im Regelfall ist für die Offenlegung der Schwachstelle zu entscheiden; von einer Offenlegung darf nur abgesehen werden, wenn im Einzelfall das Interesse an der Geheimhaltung überwiegt. [3]Das Verfahren ist so auszugestalten, dass eine sachgerechte und zeitnahe Entscheidung gewährleistet ist.

(4) [1]Als Entscheidungsfolgen kommen in Betracht:

1. die Meldung der Schwachstelle an den Hersteller im Wege eines koordinierten Verfahrens gem. Artikel 12 Absatz 1 der NIS-2-Richtlinie;
2. die befristete Geheimhaltung;
3. die Weitergabe risikomindernder Informationen ohne vollständige Offenlegung;
4. die Einschränkung der Nutzung durch staatliche Stellen; sowie
5. die vertrauliche Weitergabe an andere Behörden.

[2]Geheim gehaltene Schwachstellen sind regelmäßig neu zu überprüfen und offenzulegen, sobald die Voraussetzungen für ihre Geheimhaltung entfallen.

(5) Für die Speicherung und Verarbeitung von Informationen über Schwachstellen gelten erhöhte Anforderungen an die Informationssicherheit, die dem jeweiligen Stand der Technik entsprechen müssen.

(6) [1]Entscheidungen über die Geheimhaltung unterliegen einer unabhängigen Kontrolle durch [den Unabhängigen Kontrollrat]. [2]Dem [Unabhängigen Kontrollrat] sind die Entscheidungen samt tragender Erwägungen vorzulegen und alle für die Kontrolle erforderlichen Informationen zu erteilen. [3]Das Parlamentarische Kontrollgremium ist über die Entscheidungen zu unterrichten.

(7) [1]Die Entscheidungen des [Gremiums für Schwachstellenmanagement] sind zu dokumentieren. [2]Über Umfang und Art des Umgangs mit Schwachstellen ist regelmäßig in geeigneter Weise öffentlich Bericht zu erstatten.

(8) Das Nähere, insbesondere zu Verfahren, Abwägungskriterien und Sicherheitsanforderungen, wird durch Rechtsverordnung der Bundesregierung geregelt.

§ 2 Nutzung externer Cyberkapazitäten

(1) Behörden und sonstige öffentliche Stellen des Bundes dürfen externe Cyberkapazitäten, insbesondere von privaten Anbietern oder ausländischen

Sicherheitsbehörden, nur in Anspruch nehmen, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist und die Nutzung nicht durch Gesetz ausgeschlossen ist.

(2) [1]Vor der Beschaffung oder Nutzung externer Cyberkapazitäten ist ein strukturiertes Prüf- und Entscheidungsverfahren durch das [Gremium für Schwachstellenmanagement] durchzuführen. [2]In diesem sind zumindest zu prüfen:

a) die Vereinbarkeit der Nutzung der externen Cyberkapazitäten mit geltendem Recht, insbesondere mit datenschutzrechtlichen Anforderungen;
b) die Gefahren, die von den externen Cyberkapazitäten für die Sicherheit in der Informationstechnik ausgehen, insbesondere durch ausgenutzte oder offengehaltene Schwachstellen;
c) die Vertrauenswürdigkeit des Anbieters, einschließlich dessen Lieferketten und Investoren;
d) die Gefahr der Weiterverbreitung oder missbräuchlichen Nutzung der eingesetzten Technologien;
e) das Risiko nachrichtendienstlicher Einflussnahme oder sonstiger sicherheitsgefährdender Abhängigkeiten;
f) die Einhaltung rechtsstaatlicher Mindeststandards durch den Anbieter, insbesondere hinsichtlich des Ausschlusses von Lieferungen an Staaten oder Akteure, die grundlegende rechtsstaatliche Prinzipien nicht wahren.

(3) [1]Die Bewertung hat auf der Grundlage belastbarer, aktueller und überprüfbarer Informationen zu erfolgen. [2]Sie ist vollständig zu dokumentieren und fortlaufend zu aktualisieren. [3]Die Anbieter sind zur Mitwirkung, insbesondere zur Offenlegung relevanter Informationen, zu verpflichten. [4]Eine Nutzung ist unzulässig, wenn die Risiken nach Absatz 2 nicht hinreichend beherrscht werden können.

(4) Gegenüber privaten Anbietern ist die Einhaltung gesetzlicher Vorgaben durch vertragliche Abreden und angemessene Sanktionsmechanismen abzusichern.

(5) Die Einhaltung der Anforderungen nach den Absätzen 2 bis 4 unterliegt einer unabhängigen Kontrolle durch [den Unabhängigen Kontrollrat].

(6) Das Nähere, insbesondere zu Verfahren und Prüfkriterien, wird durch Rechtsverordnung der Bundesregierung geregelt

Literatur

Bernsen, Winnona DeSombre (2024), Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace, abrufbar unter https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/.

Bundesamt für Sicherheit in der Informationstechnik (2022), Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess (01.12.2022), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf

Bundesministerium des Innern, für Bau und Heimat (2021), Cybersicherheitsstrategie für Deutschland 2021, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2.

Calliess, Christian/Baumgarten, Ansgar (2020), Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective, *German L. J.* 21 (2020), S. 1149.

Calliess, Christian/Ruffert, Matthias (2022), EUV • AEUV (6. Auflage), C.H. Beck München.

Deibert, Ron (2026), The Perils of Privatized Cyberwarfare, *Lawfare* (01.04.2026), abrufbar unter https://www.lawfaremedia.org/article/the-perils-of-privatized-cyberwarfare.

Deutscher Bundestag (2015), Drucksache 21/1501.

Dreier, Horst (Hrsg.) (2018), Grundgesetz-Kommentar. Band III: Artikel 83-146 (3. Auflage), Mohr Siebeck Tübingen.

Dürig, Günter/Herzog, Roman/Scholz, Rupert (Hrsg.) (2025), Grundgesetz (108. Auflage), C.H. Beck München.

Epping, Volker/Hillgruber, Christian (Hrsg.) (2025), BeckOK Grundgesetz (63. Edition), C.H. Beck München.

European Parliament (2023), Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation) (P9_TA(2023)0244).

Executive Office of the President (2023), Executive Order 14093 - Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security (27.03.2023).

FIRST.Org, Inc. (2024), Common Vulnerability Scoring System Version 4.0: Specification Document (Version 1.2), abrufbar unter https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf.

Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus/Kirchmair, Lando (2023), EUV/AEUV (7. Auflage), C.H. Beck München.

Google Threat Analysis Group (2024), Buying Spying, abrufbar unter https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.) (2025), Das Recht der Europäischen Union. Band I EUV/AEUV (85. EL), C.H. Beck München.

Herpig, Sven/Schwartz, Ari (2023), The Future of Vulnerabilities Equities Processes Around the World, *Lawfare* (4. Januar 2023) abrufbar unter https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world.

Herpig, Sven (2018), Schwachstellen-Management für mehr Sicherheit, abrufbar unter https://www.interface-eu.org/storage/archive/files/vorschlag.schwachstellenmanagement.pdf.

Kipker, Dennis-Kenji (2021), IT-SiG 2.0: Kompetenzgerangel zwischen Bund und Ländern, Beck Blog (09.02.2021), abrufbar unter https://intrapol.org/2021/02/09/it-sig-2-0-kompetenzgerangel-zwischen-bund-und-laendern/.

Krempl, Stefan (2023), Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert, Heise Online (31.07.2023), abrufbar unter https://www.heise.de/news/Trotz-Verbot-FBI-hat-ueber-Vertragsfirma-NSO-Spyware-finanziert-9231066.html.

Meister, Andre (2022), Staatstrojaner Pegasus wird alle 40 Minuten eingesetzt, Netzpolitik (22.06.2022), abrufbar unter https://netzpolitik.org/2022/pega-untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/.

Panagiotopoulos, Vas (2026), Policymakers Ignore Spyware Middlemen Driving Global Proliferation, Tech Policy Press (18.03.2026), abrufbar unter https://www.techpolicy.press/policymakers-ignore-spyware-middlemen-driving-global-proliferation/.

Roberts, Jen/Herr, Herr/Bansal, Nitansha/Messieh, Nancy (2024), Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights, abrufbar unter https://www.atlanticcouncil.org/wp-content/uploads/2026/03/Mythical-Beasts-Cyber-Statecraft.pdf.

Sandhu, Aqila (2024), Squaring the Circle: The CJEU between Fundamental Rights Guardian and Architect of a Security Union, *Verfassungsblog* (02.12.2024), abrufbar unter https://verfassungsblog.de/squaring-the-circle-data-retention/.

Smally, Suzanne (2024), Testimony from NSO Group raises questions about its culpability for spyware abuses, The Record (19.11.2024), abrufbar unter https://therecord.media/nso-group-whatsapp-case-documents.

SPD (2021), Koalitionsvertrag 2021-2025, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

Streinz, Rudolf (Hrsg.) (2018), EUV/AEUV (2. Auflage), C.H. Beck München.

The Citizen Lab (2026), Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the United Nations

Working Group on the Use of Mercenaries, abrufbar unter https://citizenlab.ca/wp-content/uploads/2026/04/CitLab-Submission-to-the-UN-WG-on-the-use-of-mercenaries.pdf.

Tzanou, Maria/Vogiatzoglou, Plixavra (2025), National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach, *European Papers eJournal* (18.11.2025).

U.S. Department of Commerce (2021), Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (03.11.2021) abrufbar unter https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

U.S. Government (2017), Vulnerabilities Equities Policy and Process for the United States Government (15.11.2017), abrufbar unter https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

Wischmeyer, Thomas (2020), Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), *Nachrichtendienste in vernetzter Sicherheitsarchitektur*, S. 35 .

Wischmeyer, **Thomas** (2023), Informationssicherheit, Mohr Siebeck, Tübingen.

Wischmeyer Thomas (2024), Staatliche Nutzung von IT-Sicherheitslücken – Grundzüge des staatlichen Schwachstellenmanagements, in: Raue, Benjamin (Hrsg.), *Digitale Resilienz: Effektives Recht auf sichere Software (Band II)*