Schleswig-Holsteinischer Landtag
Umdruck 20/6252

Toppoint e.V
vorstand@toppoint.de

Jan Kürschner

Vorsitzender des Innen-
und Rechtsausschusses
des Schleswig-Holsteinischen Landtags

Stellungnahme zum Entwurf der Landesregierung eines Gesetzes zur Stärkung des Verfassungsschutzes im Lande Schleswig-Holstein, Landtags-Drucksache 20/3754

Zusammenfassung

Wir haben nicht den gesamten Regierungsentwurf einer Revision unterzogen, sondern unsere Stellungnahme auf einige informationstechnische Fragestellungen beschränkt, zu denen wir über Expertise verfügen. Dabei gehen wir davon aus, dass Schleswig-Holstein einen arbeits- und leistungsfähigen Verfassungsschutz benötigt. Mit den nicht spezifisch IT-bezogenen Regelungen haben wir uns überwiegend nicht befasst, da die ebenfalls für eine Stellungnahme angefragten juristischen Fachkräfte und Bürgerrechtsorganisationen hierfür kompetent sind und diese Aspekte in ihren Stellungnahmen hoffentlich berücksichtigen werden.

1. In § 30 (4) des Regierungsentwurfs wurde ein Verweis auf § 53 Absatz 1 Satz 1 Strafprozessordnung vergessen.
2. In § 34 sollte klargestellt werden, dass diese Regelung nicht der Umgehung von an anderer Stelle des Gesetzes vorgenommenen Befugnisbeschränkungen dienen darf.
3. Im Regierungsentwurf fehlt eine Regelung für den Umgang mit Schwachstellen, die für die Quellen-TKÜ eingesetzt werden sollen. Diese Regelung setzt das Bundesverfassungsgericht für einen verfassungskonformen Einsatz der Quellen-TKÜ voraus. Wir schlagen in § 45a eine Regelung vor.
4. Die Vorschriften des Entwurfs zur Sicherheit der eingesetzten Datenverarbeitungssysteme müssen allgemein für die gesamte Datenverarbeitung des Verfassungsschutzes gelten, nicht nur für die IT-gestützte Informationsanalyse. Wir schlagen dazu § 67a vor.
5. Der § 69 des Regierungsentwurfs ist ungeordnet, unübersichtlich und teilweise in sich widersprüchlich. Gesetzestexte sollten allgemein-verständlich geschrieben werden, zumindest aber so, dass sie für juristisch und fachlich gebildete Personen verständlich und eindeutig sind.[1] Sie sollen übersichtlich strukturiert, sachlich gegliedert und vernünftig zitierbar sein.[2] Der Regierungsentwurf hat dieses verfassungsrechtliche Gebot zutreffend erkannt (Seite 2-6), aber leider bei § 69 nicht hinreichend umgesetzt.

   Wir haben mit den § 69 ff. in unserer Stellungnahme eine Alternative formuliert, die sich an den sehr lesenswerten Vorgaben des Handbuchs der Rechtsförmlichkeit[3] orientiert. Diese ist so gehalten, dass sie die wesentlichen Punkte des Regierungsentwurfs übernimmt, informationstechnische Fehler des Regierungsentwurfs korrigiert und die einschlägige Rechtsprechung des BVerfG berücksichtigt. Die hochgestellt formatierten Verweise in unserem Entwurfstext lassen erkennen, welche Teile des Regierungsentwurfs an welcher Stelle eingearbeitet wurden.

   Fußnoten in unseren Begründungen beziehen sich hingegen auf andere, jeweils genannte Quellen. Der Regierungsentwurf und seine Begründung wurden nach der Drucksache 20-03754 zitiert.
5. In §§ 70, 74, 91 des Entwurfes schlagen wir einige Ergänzungen vor.
6. Die erweiterten Befugnisse der Novelle fordern zwangsweise eine intensivere Kontrolle. Wir schlagen vor, dem Parlamentarischen Kontrollgremium erweiterte Einsichtsrechte und permanenten IT-Sachverstand zu Verfügung zu stellen (§§ 98, 99).
7. Dass sich Verfassungsschutzmitarbeiter nur illegal an Presse oder Abgeordnete wenden können, falls sie Sorge wegen interner Rechtsverstöße haben, ist unwürdig und befördert Leaks und Indiskretionen, wir schlagen mit § 99a einen legalen Weg vor, der dadurch auch dem Geheimschutz

[1] Handbuch der Rechtsförmlichkeit, Abschnitt III, RZ 242
[2] Handbuch der Rechtsförmlichkeit, Abschnitt III, RZ 249 ff.
[3] https://hdr4.bmj.de/

Rechnung trägt. Außerdem würden wir dem Verfassungsschutz, wenn gewünscht, eine häufigere Berichterstattung ermöglichen (§ 100).

8. Landesamt für Informationssicherheit

   Unabhängig von diesem Gesetzentwurf halten wir es für notwendig, dass Schleswig-Holstein nach dem Vorbild anderer Bundesländer (Bayern, Baden-Würtemberg) ein unabhängiges Landesamt für Informationssicherheit erhält. Die gesamte Landes-IT einschließlich der Kommunen und der kritischen Infrastruktur ist, da sie überwiegend mit dem Internet verbunden ist, laufend durch Sabotage und Angriffe bedroht. Dabei muss nicht nur mit gewöhnlichen Kriminellen, sondern auch mit Angriffen staatlicher Akteure gerechnet werden. Deren Ursachen müssen untersucht und für die Zukunft abgestellt werden.

   Die Unabhängigkeit einer solchen Dienststelle von der Landesregierung ist besonders wichtig, um sicherzustellen, dass eine wirksame Kontrolle der gesamten Landes-IT einschließlich der Kommunen und der kritischen Infrastruktur ohne Rücksicht auf Behördenhierarchieen erfolgt. Gleichzeitig sollen Meldungen über Sicherheitslücken - auch anonym und auch aus der Landesverwaltung - an diese Behörde erfolgen können, ohne Repressalien von Vorgesetzten, Kollegen oder Strafverfolgern befürchten zu müssen. Eine allgemeine Aufmerksamkeit für Sicherheitsmängel und eine positive „Meldekultur“ sind im Interesse der IT-Sicherheit unbedingt notwendig. Leider ist die Rechtslage, Rechtsprechung und allgemeine Stimmung in Deutschland hierfür sehr ungünstig, dem sollte so weit wie möglich entgegengewirkt werden.

   Der Verfassungsschutz muss u.a. wegen der Quellen-TKÜ Sicherheitslücken managen. Das ist ein Zielkonflikt zur IT-Sicherheit. Offensive- und defensive Fähigkeiten beim Verfassungsschutz zu bündeln, zwingt den Verfassungsschutz dazu, eines zugunsten des anderen zu vernachlässigen. Zusätzlich ist aus historischen Gründen und aufgrund der §§ 202a ff. StGB das Verhältnis zwischen Exekutive und IT-Sicherheitsexperten belastet. Schon deshalb muss diese Stelle unabhängig sein.

   Um Verwaltungsoverhead einzusparen und Synergien zu nutzen, halten wir es für sinnvoll, diese Zuständigkeit beim Unabhängigen Landeszentrum für Datenschutz anzusiedeln und diese Behörde entsprechend mit Personal auszustatten. Die Datenschutzbeauftragten genießen hohes Vertrauen und Ansehen bei IT-Sicherheitsexperten.

§ 34 Informationserhebung aus elektronischen Quellen

(1) Zulässig ist sowohl die offene als auch verdeckte Informationserhebung aus elektronischen Quellen, soweit dadurch nicht Telekommunikation nach § 1 Absatz 1 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298; ber. 2007 S. 154), zuletzt geändert durch Artikel 4 des Gesetzes vom 22. Dezember 2023 (BGBl 2023 I Nr. 413), überwacht oder aufgezeichnet wird. Hierzu darf die Verfassungsschutzbehörde die nach pflichtgemäßem Ermessen erforderlichen Maßnahmen treffen. Dies beinhaltet insbesondere die Sichtung, Nutzung und Auswertung der Inhalte und Angebote elektronischer Quellen sowie die Teilnahme an Kommunikationseinrichtungen des Internets und die Suche nach ihnen. Informationen zu unbeteiligten Dritten, die in diesem Zusammenhang erhoben werden, sind zu löschen.

(2) Sofern die aus elektronischen Quellen zu erlangenden Daten ihrer Art nach ansonsten Mittel mit besonderer Eingriffsintensität erfordern würden, sind die §§ 35 bis 46 entsprechend anzuwenden.

(3) Sofern die aus elektronischen Quellen zu erlangenden Daten ihrer Art nach ansonsten die in Abschnitt 2 geregelten besonderen Auskunftsverlangen erfordern würden, sind die §§ 48 bis 62 entsprechend anzuwenden.

(4) Die Befugnis nach Absatz 1 gilt nicht für Daten, deren Erhebung und Verarbeitung nach Abschnitt 2 dieses Gesetzes unzulässig wäre.

Begründung

Die in den §§ 35 bis 62 geregelten Beschränkungen dürfen nicht umgangen werden, indem sich die Behörde Daten, deren Erhebung unzulässig oder nur eingeschränkt oder nur nach einem besonderen Verfahren erlaubt wäre, aus anderen Quellen besorgt, etwa durch Ankauf. Dies ist insbesondere dann zu verhindern, wenn sonst auf diesem Wege Massenüberwachungsdaten in die IT-gestützte Informationsanalyse nach § 69 ff. gelangen könnten.

§ 45a Schutz von Mitteln zur Quellentelekommunikationsüberwachung

(1) Die Verfassungsschutzbehörde führt für jedes Mittel zur Quellentelekommunikationsüberwachung, das ihr zur Verfügung steht, eine Risikoabschätzung für das Vorhalten und vor jedem Einsatz im Einzelfall durch.

(2) In der Risikoabschätzung ist die Gefahr, dass Unbefugte über das Mittel zur Quellentelekommunikationsüberwachung, Bestandteile oder die zugrundeliegenden Sicherheitslücken Verfügung erlangen könnten, und der drohende Schaden zu berücksichtigen.

(3) Im Falle der Verfügungserlangung durch Unbefugte ist das Parlamentarische Kontrollgremium unverzüglich zu informieren. Die vorbereiteten Maßnahmen nach Absatz 4 sind unverzüglich umzusetzen.

(4) Die Verfassungsschutzbehörde hat geeignete Maßnahmen zur Schadensminimierung im Rahmen der Risikoabschätzung vorzubereiten.

(5) Die Risikoabschätzungen und vorbereiteten Maßnahmen zur Schadensminimierung sind dem Parlamentarischen Kontrollgremium bekannt zu geben.

(6) Die Maßnahmen und Risikoabschätzungen sind fortlaufend aktuell zu halten.

(7) Sobald das Interesse an der Integrität informationstechnischer Sicherheit das Aufklärungsinteresse überwiegt, sind die vorbereiteten Maßnahmen zur Schadensminimierung unverzüglich einzuleiten.

Begründung

Für die Quellentelekommunikationsüberwachung nach §45 benötigt die Verfassungsschutzbehörde Überwachungssoftware. Diese basieren auf Sicherheitslücken (z.B. Zero-Day-Exploits), die nicht nur in den Geräten von nach diesem Gesetz überwachten Personen existieren, sondern in denen aller Nutzer. Das Bundesverfassungsgericht hat in seinem Beschluss vom 8.6.2021[4] dargelegt, dass den Staat eine Pflicht trifft, „dazu beizutragen, dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt werden“ (RZ 33-39). Diese grundrechtliche Schutzpflicht verlangt „eine 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-Telekommunikationsüberwachungen andererseits aufzulösen hat. … Es ist 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 In-

[4] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/06/rs20210608_1bvr277118.html

teresse an der Offenhaltung der Lücke überwiegt.“ (RZ 44). § 9 ff. des Artikel 10-Gesetzes enthalten keine Regelung, die diesen Anforderungen gerecht wird, deshalb ist hier eine Regelung erforderlich.

Diese Exploits unterliegen einem ständigen Proliferationsrisiko, sowohl durch Aufklärung während oder nach dem Einsatz, als auch durch unabhängige Entdeckung der ihnen zugrundeliegenden Sicherheitslücken. Im Mai 2017 konnte die Schadsoftware WannaCry unter Verwendung eines der NSA gestohlenen Cyberwaffe hunderttausende Rechner weltweit lahmlegen. Betroffen waren u.a. die Deutsche Bahn und der englische National Health Service, bei dem auch die Patientenversorgung betroffen war. In einem anderen Fall konnte eine Entwicklerin Spuren und Teile der genutzten Zero-Day-Exploits, die Strafverfolgungsbehörden gegen ihre Geräte genutzt hatten, sichern. Sie hat diese veröffentlicht.

§ 64 Weiterverarbeitung personenbezogener Informationen

(1) Die Verfassungsschutzbehörde darf zur Erfüllung ihrer Aufgaben personenbezogene Informationen weiterverarbeiten, wenn

1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass die Person an Bestrebungen oder Tätigkeiten nach §§ 8 bis 14 teilnimmt und dies für die Beobachtung der Bestrebung oder Tätigkeit erforderlich ist,
2. dies für die Erforschung und Bewertung von Tätigkeiten nach § 14 oder gewaltorientierten Bestrebungen nach §§ 8 bis 13 erforderlich ist oder
3. dies zur Schaffung oder Erhaltung nachrichtendienstlicher Zugänge über Bestrebungen oder Tätigkeiten nach §§ 8 bis 14 erforderlich ist.

Erkenntnisse, die nach Satz 1 gespeicherte Angaben belegen, dürfen auch gespeichert werden, wenn sie weitere personenbezogene Informationen Dritter enthalten; *diese sind, soweit möglich, zu anonymisieren*

(2) Die nach Absatz 1 gespeicherten Informationen dürfen für die dort genannten Zwecke genutzt werden. Soweit dieses Gesetz nichts anderes bestimmt, kann die Verfassungsschutzbehörde Informationen auch zweckändernd weiternutzen, wenn sich aus ihnen im Einzelfall tatsächliche Anhaltspunkte für den Verdacht von Bestrebungen oder Tätigkeiten nach den §§ 8 bis 14 ergeben.

(3) In Dateien gespeicherte personenbezogene Informationen müssen durch Aktenrückhalt belegbar sein.

(4) In Dateien ist die Speicherung von personenbezogenen Informationen nur zulässig, soweit diese für die Beurteilung der Person von Bedeutung sind.

(5) Personenbezogene Informationen, die mit nachrichtendienstlichen Mitteln erhoben wurden, sind zu kennzeichnen.

(6) Die Weiterverarbeitung der Informationen darf zum Zwecke der Datenschutzkontrolle protokolliert werden. Die Protokolldaten dürfen auch zur Aufklärung eines Verdachts auf Datenmissbrauch verwendet werden.

(7) Soweit die Weiterverarbeitung automatisierte Verfahren umfasst, finden die §§ 69 ff. entsprechende Anwendung.

Begründung zu Absatz (1) Satz 2:

Durch die Anonymisierung personenbezogener Daten Dritter wird der Eingriff in deren Rechte reduziert, ohne die Dokumentations- und Beweisfunktion der gespeicherten Erkenntnisse zu beeinträchtigen. Sie stellt damit ein verhältnismäßiges Mittel zum Ausgleich zwischen Aufgabenerfüllung der Behörde und Datenschutzinteressen Dritter dar.

§ 67 Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Informationen

(1) Personenbezogene Informationen in Dateien sind

1. zu berichtigen, wenn sie unrichtig sind; sie sind zu ergänzen, wenn sie unvollständig sind und dadurch schutzwürdige Interessen der Person, deren personenbezogene Informationen verarbeitet wurden, beeinträchtigt sein können;
2. zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist und schutzwürdige Interessen der Person, deren personenbezogene Informationen verarbeitet wurden, nicht beeinträchtigt werden;
3. in ihrer Verarbeitung einzuschränken, wenn die Löschung unterbleibt, weil Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen der Person, deren personenbezogene Informationen verarbeitet wurden, beeinträchtigt würden; gesperrte Informationen dürfen nur mit Einwilligung dieser Person verwendet werden;
4. *in ihrer Verarbeitung einzuschränken, wenn die Löschung aus zwingenden technischen Gründen unterbleibt; gesperrte Informationen dürfen nur mit Einwilligung dieser Person verwendet werden.*

(2) ~~In Dateien gelöschte personenbezogene Informationen sind in ihrer Verarbeitung eingeschränkt.~~ Unterlagen sind zu vernichten, wenn sie zur Erfüllung der Aufgaben nach § 5 nicht oder nicht mehr erforderlich sind, es sei denn, dass ihre Aufbewahrung zur Wahrung schutzwürdiger Interessen der Person, deren personenbezogene Informationen verarbeitet wurden, oder zu wissenschaftlichen Zwecken notwendig ist. Die Vernichtung unterbleibt, wenn die Unterlagen von anderen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand getrennt werden können.

Begründung zum Änderungsvorschlag zu § 67 Abs. 1 Nr. 4, Abs. 2 S. 1:

Die Regelung des Entwurfs („In Dateien gelöschte personenbezogene Informationen sind in ihrer Verarbeitung eingeschränkt.“) widerspricht direkt Abs. 1 Nr. 2.

Abs. 1 Nr. 4 behandelt Fälle vor dem Hintergrund, dass in gängigen Datenbanksystemen eine Löschung im Sinne einer vollständigen Entfernung nicht erfolgt, sondern Datensätze tatsächlich nur als gelöscht markiert werden, die Information aber noch vorhanden ist.

Hinsichtlich der Aufbewahrung zu wissenschaftlichen Zwecken stellt sich uns die Frage, welche das sind, wie die Daten in der Vergangenheit genutzt wurden und wer über die wissenschaftliche Bedeutung nach welchen Grundsätzen entscheidet.

§ 67a Sicherheit der eingesetzten Datenverarbeitungssysteme

(1) Eingesetzte Datenverarbeitungssysteme, bestehend aus Hard- und Software, sind regelmäßig zu überprüfen und auf dem Stand der Technik zu halten. [§ 69 (6) Satz: 1] und zwar nach den Regeln für die höchste Risikostufe. Bei der Überprüfung ist auch der Stand der Wissenschaft im Hinblick auf mögliche Angriffe, unerwünschte Veränderungen, Fehler oder Unzulänglichkeiten zu beachten. [§ 69 (6) Satz: 2]

(2) Auch Systeme, die nicht ans Internet angeschlossen sind, sind hinsichtlich ihrer Sicherheit so zu behandeln, als wären sie es.

(3) Bei der Beschaffung der Datenverarbeitungssysteme ist darauf zu achten, dass der Verfassungsschutz die eingesetzten Systeme auch tatsächlich kontrolliert und dass Hersteller und Lieferanten und deren Mitarbeitende keine Eingriffs- oder Zugriffsmöglichkeiten haben. Dabei ist auch auf mögliche Manipulationen zu achten.

(4) Der Zugang und die Nutzung von automatisierten technischen Systemen zur Informationsverarbeitung ist mit einem Rechte- und Rollenkonzept zu regeln. In diesem ist die Zahl der Nutzerinnen und Nutzer angemessen zu begrenzen. Der Zugang zu der Anwendung ist auf bestimmte diesbezüglich qualifizierte Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde beschränkt und unterliegt einer Zugriffskontrolle. Bei jeder Nutzung sind Zeitpunkt, Angaben, die die Feststellung der verarbeiteten Daten ermöglichen sowie Angaben zur Feststellung der Nutzerin oder des Nutzers zu protokollieren. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen. § 69 (8) Satz: 1

Begründung

Absatz (1) stammt aus dem Regierungsentwurf von § 69. Es sollte jedoch selbstverständlich sein, dass diese Sicherheitsvorschriften nicht nur für die IT-gestützte Datenanalyse, sondern für alle IT-System des Verfasungsschutzes gelten müssen.

Die Verfassungsschutzbehörde ist als Spionageabwehrbehörde Ziel von gegnerischen Geheim- und Nachrichtendiensten. Dieses Bedrohungsmodell bedeutet, das die VS-Behörde, möchte sie geheim gegenüber diesen Angreifern handeln können, Maßnahmen ergreifen muss, die über die Maßnahmen der normalen Verwaltung und Wirtschaft hinausgehen. Die Regelung, auch nicht ans Netz angeschlossene Systeme als internetverbunden behandeln zu müssen, ergibt sich aus der Schwierigkeit indirekte Verbindungen zum Internet auszuschließen. Die Atomzentrifugen des Irans waren „air-gapped“, also nicht direkt mit dem Internet verbunden. Trotzdem sind diese Systeme schon vor ~15 Jahren durch Schadsoftware (Stuxnet) infiziert worden.

Im Bereich der Sicherheitsorgane ist digitale Souveränität unumgänglich notwendig. Dieser Aspekt wurde in der Vergangenheit sträflich vernachlässigt. Auch Hersteller von Hard- und Software und deren Datenverarbeitungssysteme können zu Angreifern werden, entweder absichtlich oder - bereits häufig vorgekommen - versehentlich.

Fachlich erfoderlich ist eine personelle Besetzung des Verfassungsschutzes mit Personen, die über Fachkunde in der Abwehr von IT-gestützter Sabotage und Angriffen haben und über Kenntnisse im Pentesting verfügen. Inwieweit das der Fall ist oder sein wird, wissen wir nicht.

Unterabschnitt 2

IT-gestützte Informationsanalyse

§ 69 Grundsätze

(1) Die Verfassungsschutzbehörde darf zur Aufklärung von Bestrebungen oder Tätigkeiten nach §§ 8 bis 14 bereits erhobene Informationen, insbesondere im elektronischen Aktensystem oder im nachrichtendienstlichen Informationssystem gespeicherte personenbezogene Informationen, auch unter Verwendung automatisierter technischer Systeme zur Informationsverarbeitung zusammenführen und anschließend zur Gewinnung neuer Erkenntnisse weiterverarbeiten (IT-gestützte Informationsanalyse).§ 69 (1) Satz: 1

(2) Die Implementierung des gesamten Analysesystems muss deterministisch und reproduzierbar arbeiten und die Analyse selbst muss regelbasiert, deterministisch und ohne Zufallselemente erfolgen und einem klar definierten, unveränderlichen logischen Ablauf folgen.

(3) Eine IT-gestützte Informationsanalyse darf nur erfolgen, wenn zu erwarten ist, dass die aus ihr

gewonnenen Erkenntnisse für die Aufklärung von Bestrebungen oder Tätigkeiten nach §§ 8 bis 14 im Einzelfall geeignet, erforderlich und verhältnismäßig sind.

(4) IT-gestützte Informationsanalysen dürfen zum ursprünglichen Zweck der Informationserhebung nicht außer Verhältnis stehen.[§ 69 (1) Satz: 2]

(5) Bei der IT-gestützten Informationensanalyse ist jede Unterscheidung nach den in Artikel 3 Absatz 3 des Grundgesetzes geschützten Kategorien, direkt oder indirekt, verboten, sofern dies nicht ausnahmsweise für die Aufklärung zwingend erforderlich ist.[§ 69 (3) Satz: 6]

(6) Eine Verknüpfung der Analysesysteme mit dem Internet erfolgt nicht.[§ 69 (3) Satz: 4]

Begründung

Der Text entspricht überwiegend sinngemäß dem Regierungsentwurf, wurde aber kleinteiliger gegliedert. Wenig sinnvolle Bezüge auf die technische Umsetzung wurden entfernt. Es ist beispielsweise nicht erkennbar, warum die Beschränkungen aus Artikel 3 GG nur für „Algorithmen“, nicht aber für Suchanfragen gelten sollen. Dafür wurden wichtige Grundsätze aus der Begründung des Regierungsentwurfs in den Gesetzestext übernommen.

In Absatz 1 wurde klargestellt, dass die Regelungen der §§ 69 ff. auch dann anwendbar sind, wenn die IT-gestützte Informationsanalyse nur auf eine einzelne Informationsquelle angewendet wird, also keine Zusammenführung von Daten vorliegt.

Absatz 2 entstammt der Begründung des Regierungsentwurfes (S. 142); diese Implementierungsgrundsätze gehören in den Gesetzestext. Hinzugefügt wurden die Aspekte „deterministisch“ und „ohne Zufallselemente“. Zufällig hergestellte Verknüpfungen können in einem Rechtsstaat keine rechtliche Grundlage für Grundrechtseingriffe darstellen, das sollte offensichtlich sein. Die Reproduzierbarkeit der Ergebnisse ist Voraussetzung für eine rechtsstaatliche Überprüfung.

In Absatz 3 wurden die Punkte „unbedeutende Informationen und Erkenntnisse ausgeschlossen“ und „Suchkriterien gewichtet“ gestrichen. Was bedeutend oder unbedeutend oder wie zu gewichten ist, erfordert eine Prognoseentscheidung, das kann ein IT-System nicht zuverlässig leisten. Zur weiteren Begründung siehe unten zu § 69b.

§ 69a Informationsquellen für die Informationsanalyse

(1) In eine IT-gestützte Informationsanalyse dürfen nur Informationen einbezogen werden, die durch offene Erkenntnisse oder durch nachrichtendienstliche Mittel ohne besondere Eingriffsintensität (§ 32) gewonnen wurden.[§ 69 (4) Satz: 1]

(2) Informationen, die mit besonders eingriffsintensiven nachrichtendienstlichen Mitteln erhoben wurden, dürfen nur dann mit in die Analyse aufgenommen werden, wenn sie der Aufklärung besonders beobachtungsbedürftiger Bestrebungen gemäß § 35 Absatz 2 dienen.[§ 69 (4) Satz: 2]

(3) Informationen, die aus Wohnraumüberwachungen gewonnen wurden oder die einer besonderen Zweckbindung unterliegen, dürfen nur dann einbezogen werden, wenn auch für ihre Weiterverarbeitung die Voraussetzungen für diese Maßnahmen vorliegen.[§ 69 (4) Satz: 3]

(4) Informationen, die aus Maßnahmen nach dem Artikel 10-Gesetz gewonnen wurden, dürfen nur dann miteinbezogen werden, wenn auch für ihre Weiterverarbeitung die Voraussetzungen für diese Maßnahmen vorliegen und sie der Aufklärung besonders beobachtungsbedürftiger Bestrebungen gemäß § 35 Absatz 2 dienen. Die G 10-Kommission ist über diese Verarbeitung zu unterrichten.[§ 69 (4) Satz: 3]. Die Ergebnisse unterliegen insgesamt den Verarbeitungsregelungen des Artikel 10-Gesetzes[Analog: § 69 (4) Satz: 4].

(5) Werden Informationen im Sinne von Absatz 3 und 4 in die Informationsverarbeitung einbezogen,

ist ihre Kennzeichnung nach § 64 Absatz 5 sicherzustellen und aufrechtzuerhalten.[§ 69 (4) Satz: 5]

(6) Das Einbeziehen polizeilicher Datenbanken ist unzulässig.[§ 69 (4) Satz: 6]

(7) Es dürfen nur personenbezogene Daten des in § 7 benannten Personenkreises einbezogen werden.[§ 69 (5) Satz: 1], gegen die konkrete Tatsachen vorliegen, die einen Verdacht begründen.

(8) Datensätze aus Internetquellen dürfen einbezogen werden, wenn dies im Einzelfall erforderlich ist. Ein unmittelbarer automatisierter Abgleich von personenbezogenen Informationen aus Internetdiensten ist unzulässig.[§ 69 (4) Satz: 7]

Begründung

Der Text entspricht sinngemäß dem Regierungsentwurf. Neu ist Absatz (7), dessen Notwendigkeit aus BVerfG BvR 1547/19, näheres siehe unten, folgt.

§ 69b Zulässige Verarbeitungsverfahren

(1) Das Analyseverfahren besteht aus der Auswahl relevanter Akten und Dateien durch eine datei- und informationssystemübergreifende Suchfunktion mittels logisch verknüpfter Suchbegriffe. Die Auswertung erfolgt mittels simultan ausgelöster, regelbasierter und logisch verknüpfter Anweisungen, die auf Wenn-Dann-Operationen basieren und den vorher ausgewählten zusammengeführten Informationsbestand durchsuchen.

(2) Hierzu können insbesondere datei- und informationssystemübergreifend

1. Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt,
2. ~~unbedeutende Informationen und Erkenntnisse ausgeschlossen,~~
3. ~~Suchkriterien gewichtet,~~
4. ~~die eingehenden Erkenntnisse bekannten Sachverhalten zugeordnet~~
5. sowie gespeicherte Informationen statistisch ausgewertet werden.[§ 69 (1) Satz: 2]

(3) ~~Die Verfassungsschutzbehörde darf im Rahmen der Informationsverarbeitung nach Absatz 1 Systeme mit mathematisch-statistischen Verfahren, maschinellem Lernen und künstlicher Intelligenz nutzen. In diesem Fall darf die Nutzung von Informationen aus dieser Auswertung durch nicht adaptive Verfahren des maschinellen Lernens und künstlicher Intelligenz nur erfolgen, wenn die Rückschlüsse und die auf ihnen beruhenden Ergebnisse der automatisierten Analyse durch Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde nachvollzogen und abschließend bewertet werden können.~~[§ 69 (3) Satz: 3] Systeme, die Entscheidungsbäume, Zufallsbäume, Stützvektormethoden oder neuronale Netze nutzen, dürfen nur dann verwendet werden, wenn keine personenbezogenen Daten in die Analyse einfließen. Darüber hinaus finden Systeme, die maschinelles Lernen nutzen, keine Anwendung.

(4) Der Einsatz selbst weiterlernender Systeme ist unzulässig.[§ 69 (3) Satz: 3]

(5) Große Sprachmodelle dürfen für die Transkription von Audioaufzeichnungen und für die Übersetzung von fremdsprachigen Texten benutzt werden. Das benutzte Sprachmodell darf nicht außerhalb der Verfassungsschutzbehörde betrieben werden. Vor der Einleitung grundrechtseinschränkender Maßnahmen ist das Ergebnis der Sprachmodellnutzung durch die Behörde, gegebenenfalls unter Nutzung externen Sachverstands, fachkundig zu überprüfen.

Begründung zu Absatz (1)

Absatz 1 entstammt der Begründung des Regierungsentwurfes (S. 142), die Implementierungsgrundsätze gehören aber in den Gesetzestext.

Begründung zu Absatz (2)

Die Erwartungen des Regierungsentwurfs an das Analysesystem sind sehr hoch und im wesentlichen begründet durch überschätzte Fähigkeiten der sogenannten „künstlichen Intelligenz“. Sie würden in der Umsetzung zu Grundrechtsverletzungen (siehe dazu zu Absatz 3), aber auch schlicht zu Mehrarbeit durch Falschzuschreibungen führen.

Zu **Punkt 1**: Die Analyse von solchen Beziehungen und Zusammenhängen ist ein wichtiger Teil der Arbeit des Verfassungsschutzes. Grundlage dieser Arbeit müssen aber tatsächlich im Datenbestand bestehende, in der Vergangenheit festgestellte konkrete Beziehungen und Zusammenhänge sein und nicht statistisch generierte Vermutungen (dazu unten mehr zu Absatz 3). Ein herkömmliches Datenanalysesystem, das ohne maschinelles Lernen und ohne große Sprachmodelle arbeitet, sondern einfach nur den Datenbestand in einem fest vorgegebenen Verfahren auswertet, erfüllt diese Aufgabe zuverlässig.

Die **Punkte 2 und 3** erfordern die Bewertung der Bedeutung und sinnvollen Gewichtung einzelner Kriterien. Diese kann in bestimmten Zusammenhängen möglicherweise fest vorgegeben werden. In den meisten Fällen wird aber mit der Bewertung eine Prognose verbunden sein, von der der Regierungsentwurf hofft, dass sie mit maschinellem Lernen erreicht werden kann. Aber selbst scheinbar gleichgelagerte Fälle unterscheiden sich, nach Wahrscheinlichkeiten berechnete Prognosen können im Einzelfall zutreffend sein oder eben auch nicht. Das Ergebnis wären im letzteren Fall dann fehlgeleitete oder fälschlicherweise unterlassene Aufklärungsversuche.

Zu **Punkt 4** ist völlig unklar, wie ein System dies zuverlässig bewältigen soll. Namensgleichheiten, Übertragungsfehler, Rechtschreibfehler werden zu zahlreichen Fehlzuordnungen führen, deren händische Korrektur sehr aufwendig wäre. Zudem sollte die Halluzinationsgefahr bedacht werden (dazu unten). Im Laufe der Zeit werden Fehlzuordnungen zunehmend den Datenbestand vergiften. Dem Verfassungsschutz ist damit nicht gedient, das Ergebnis wäre ein Datenbestand, dessen Korrektheit niemand mehr nachvollziehen kann und der dann schon allein deshalb nicht mehr als Begründung für grundrechtseinschränkende Aufklärungsmaßnahmen herangezogen werden kann.

Statistische Auswertungen gemäß **Punkt 5**, etwa für die Berichte des Verfassungsschutzes, können natürlich durch IT-Systeme erstellt werden, mit lange bewährten, anerkannten Verfahren ganz ohne sogenannte „Künstliche Intelligenz“. Aussagen über Einzelfälle können sie nicht treffen.

Begründung zu Abs. (3): Mathematisch-statistische Verfahren

Statistische Verfahren können zwar eine Basis für bestimmte, etwa gesetzgeberische, Entscheidungen bilden, aber nur, soweit es um größere Gruppen geht. Je kleiner die betrachtete Gruppe ist, desto weniger verlässlich sind statistische Aussagen. Über den Einzelfall kann ein statistisches System überhaupt keine zuverlässigen Aussagen treffen.

Dennoch können statistische Auswertungen hilfreich sein, solange es nicht um prediktive Analyse geht, etwa für die Berichtserstellung, siehe Absatz (2), letzter Punkt.

Bei Maßnahmen des Verfassungsschutzes, inbesondere bei solchen, die Grundrechte einschränken, geht es aber immer um die Beurteilung von Einzelfällen und einzelnen Personen oder Gruppen einzelner Personen. Über die Verfassungstreue der einzelnen Person sagt eine errechnete Wahrschein-

lichkeit überhaupt nichts aus. Jede Maßnahme, die sich auf Wahrscheinlichkeitsberechnungen stützt, kann völlig unbeteiligte Personen treffen.

Begründung zu Abs. (3): Wahrscheinlichkeitsmodelle und Maschinelles Lernen

Nach der Begründung des Entwurfs (S. 143) besteht das Ziel „typischerweise darin, Muster in Daten zu erkennen, Zusammenhänge zu modellieren oder Prognosen unter Unsicherheiten zu ermöglichen, stets mit expliziter Kontrolle über die Annahmen und mit nachvollziehbarer, analytischer Ableitung der Ergebnisse." Das ist ein Widerspruch in sich: Eine „Prognose unter Unsicherheiten" bleibt im Ergebnis eine unsichere Prognose, egal, welche Adjektive man mit dem Wort „Kontrolle" verbindet. Maschinelles Lernen besteht laut der Begründung des Regierungsentwurfs in der „Fähigkeit eines Modells, Vorhersagen zu treffen oder Klassifikationen vorzunehmen, basierend auf Mustern in Trainingsdaten." Beides bedeutet, der Verfassungsschutz soll Aufklärungsmaßnahmen ergreifen dürfen aufgrund einer auf Wahrscheinlichkeiten und Mustern basierenden Prognose. Prediktiv begründete Überwachungsmassnahmen sind eine die Menschenwürde verletzende Praxis, denn sie negieren die Entscheidungsmacht des einzelnen Gruppenangehörigen zu rechtstreuem Verhalten und reduzieren ihn auf die Eigenschaft „gruppenangehörig".

„Personen in der Union (sollen) stets nach ihrem tatsächlichen Verhalten beurteilt werden" und nicht nach den Vorhersagen einer KI.[5] Systeme "zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen", sind nach Artikel 5 (1) d der EU KI-VO verbunden mit „inacceptable risk" und verboten. Die Ausnahme für „KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen" erfordert eine Bindung der Analyse an objektive und beweisbare Fakten. Dem trägt der Regierungsentwurf nicht Rechnung.

Auch wenn die Ausnahme nach Art. 2 (3) EU KI-VO für „KI-Systeme … ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit …" wahrscheinlich zur Nicht-Anwendbarkeit für den Verfassungsschutz führt, behalten die Wertungen der Art. 5 (1), Erwägungsgrund 42 der EU KI-VO dennoch sachlich ihre Berechtigung.

Das BVerfG kommt für die polizeiliche Gefahrenabwehr zu genau dem gleichen Ergebnis wie die KI-VO: „Eine Datenanalyse … darf nur durchgeführt werden, wenn bestimmte, genügend konkretisierte Tatsachen den Verdacht begründen, dass eine besonders schwere Straftat … begangen wurde und aufgrund der konkreten Umstände eines solchen im Einzelfall bestehenden Verdachts für die Zukunft mit weiteren, gleichgelagerten Straftaten zu rechnen ist".[6] Wendet man das Urteil auf den Verfassungsschutz an, müssen also konkrete Tatsachen im Einzelfall den Verdacht für das Vorliegen einer bereits begangenen verfassungsfeindlichen Handlung begründen und konkrete Umstände auf deren Wiederholung schließen lassen.

Der Regierungsentwurf beruft sich in seiner Begründung darauf, dass gemäß dem BverfG „die konkretisierte Gefahr … eine für die Polizei maßgebliche Einsatzschwelle (sei), die für nachrichtendienstliche Gefahrerforschung nicht unter den gleichen Voraussetzungen gilt, auch nicht zum Ein-

[5] Erwägungsgrund 42 der EU KI-VO

[6] 1 BvR 1547/19 und 1 BvR 2634/20 vom 16. Februar 2023, Tenor https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

satz besonders eingreifender heimlicher Überwachungsmaßnahmen“.[7] Dabei wird übersehen, dass sich das Urteil auf die Regelung nachrichtendienstlicher Überwachungsmaßnahmen bezog und nicht auf automatisierte Analysesysteme. Zudem geht es in Rz. 161 ausdrücklich um Auslandsaufklärung. Weiter spricht das BVerfG in Rz. 162 von einem „grundsätzlich geringeren Eingriffsgewicht“ der Befugnisse einer Verfassungsschutzbehörde. Die grundrechtsrelevanten Gefahren, die mit automatischen Analysesystemen prediktiver Natur verbunden sind, sind aber nicht geringer sondern ganz anders gelagert, denn sie beruhen auf der realen Gefahr, dass völlig Unbeteiligte ins Visier der Behörde geraten. Am ehesten könnte Rz. 163 für die Auffassung des Regierungsentwurfs herangezogen werden, aber auch dort geht es lediglich um eine herabgesetzte Eingriffsschwelle, nicht aber um Eingriffe völlig ohne Anknüpfungstatsachen für einen Verdacht. Das BVerfG spricht von „organisierter Verfasstheit“ und (etwa in sozialen Medien geäußerten) „verfassungsfeindlichen Ideen“. Dies sind Verdachtstatsachen, deren Vorliegen eine Überwachung und auch eine Einbeziehung in eine Analyse rechtfertigen können. Der Regierungsentwurf hat eine solche Beschränkung aber nicht vorgenommen.

§ 69 des Regierungsentwurfs würde es ermöglichen, solche Verdachtstatsachen durch die Analyse erst ermitteln zu wollen. Das ist nach beiden Urteilen verfassungswidrig.

Für diese Einordnung gibt es auch ganz praktisch gute Gründe: Insbesondere Large Language Models neigen zur Halluzination, das heißt zum Erfinden von Informationen, die im Datenbestand nicht vorhanden sind, aber plausibel klingen. Die Halluzinationsquote marktüblicher Large Language Model liegt etwa zwischen 15% und 50%.[8] Die Gründe für Halluzinationen sind immer noch unerforscht. Ob sich an der Halluzinationsquote überhaupt etwas ändern läßt und wenn ja, wie, ist umstritten und Gegenstand der Forschung. Wir wissen, dass bekannte Hersteller behaupten, sie hätten Lösungen gegen Halluzinationen gefunden, aber dabei handelt es sich um bloße Werbeversprechen. Die Forschung kommt zu anderen Ergebnissen. Dem Verfassungsschutz ist mit erfundenen Analyseergebnissen aber mehr geschadet als geholfen.

Zusätzlich stellen große Sprachmodelle eine Unterwanderungsgefahr dar. Sie sind prinzipbedingt anfällig für sogenannte Prompt-Injections, d.h. eine zu untersuchende Information, etwa ein Text, kann das Sprachmodell dazu veranlassen, gezielt falsche Antworten zu erzeugen, das System zu manipulieren oder, wenn Kommunikation irgendwie möglich ist, sogar Informationen auszuleiten.

Begründung zu Abs. (3): „Künstliche Intelligenz“

Die sogenannte „künstliche Intelligenz“ ist ein mathematisch-statistisches Verfahren und kein darüber hinausgehendes Zauberwirken. Die Begründung des Entwurfs (S. 144 unter 3.) spricht von einer Fähigkeit, die „über den rein datenanalytischen Fokus hinausgeht und auch kognitive, logische und funktionale Aspekte automatisierter Intelligenz adressiert.“ Das ist Marketing. „Kognitiv“ und „intelligent“ sind nur die Entwickler dieser Verfahren, aber nicht die Verfahren selbst. Die sogenannte „künstliche Intelligenz“ ist ein mithilfe maschinellen Lernens erstelltes mathematisch-statistisches Verfahren, mehr nicht.

Der Propaganda-Begriff „künstliche Intelligenz“ hat sich zwar leider im allgemeinen Sprachgebrauch etabliert und schürt, wie in der Entwurfsbegründung deutlich wird, falsche Erwartungen, die über bloße Statistik hinausgehen. Es handelt sich um die Berechnung von Wahrscheinlichkeiten; mit der kognitiven Problemlösefähigkeit von Lebewesen hat das alles nichts zu tun. Dabei darf nicht vergessen werden, dass der Begriff erfunden wurde von den einschlägigen amerikanischen Unternehmen,

[7] 1 BvR 1619/17 vom 26. April 2022, Rn. 161 f, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2022/04/rs20220426_1bvr161917.html

[8] Comparing LLM Hallucination Rates for Place-Based Legal Queries, https://arxiv.org/abs/2511.06700

die damit konkrete wirtschaftliche, aber auch politische und pseudo-religiöse Ziele verfolgen.[9] Ein solcher politischer Kampfbegriff hat in einem Gesetzestext keine Berechtigung. Stattdessen sollten die zulässigen Verfahren, wenn man sie denn zulassen will, fachlich korrekt beschrieben werden.

Begründung zu Abs. (3): Nachvollziehbarkeit

Damit die Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde „die Rückschlüsse und die auf ihnen beruhenden Ergebnisse der automatisierten Analyse“ in den vom Regierungsentwurf vorgesehenen Verfahren nachvollziehen können, benötigen sie als erstes ein abgeschlossenes IT-Studium mit entsprechender Fachqualifikation. Ohne dies können sie weder die Arbeitsweise des Systems noch die eingesetzten Algorithmen verstehen. Die Funktionsweise etwa neuronaler Netze ist Gegenstand der Forschung und von der Wissenschaft noch nicht vollständig verstanden.

Für den praktischen Einsatz in grundrechtsrelevanten Bereichen eignen sich unzureichend erforschte Systeme offensichtlich nicht. Ganz praktisch wird der Einsatz bekannt unzuverlässiger Analysesysteme beim Verfassungsschutz dessen Arbeit nicht erleichtern, sondern erschweren, weil Halluzinationen erkannt und aussortiert werden müssen. Das Ergebnis der vom Regierungsentwurf beabsichtigten Analyseverfahren ist eine Wahrscheinlichkeitsangabe, die auch vollständig erfunden sein kann - nach welchem Maßstab sollen die Mitarbeiterinnen und Mitarbeiter unter diesen Umständen eine Bewertung für den Einzelfall vornehmen?

Deshalb halten wir die Verwendung von „Künstlicher Intelligenz“ und maschinellem Lernen im Verfassungsschutz für rechtsstaatswidrig und tatsächlich auch im Hinblick auf das mögliche Ergebnis in der täglichen Arbeit für wenig hilfreich. Wir empfehlen herkömmliche Methoden der Datenauswertung.

Begründung zu Abs. (4)

Das Verbot selbstlernender Systeme ist aus dem Regierungsentwurf übernommen.

Begründung zu Abs. (5)

Die Benutzung wahrscheinlichkeitsbasierter großer Sprachmodelle (LLM) für die Auswertung und Übersetzung von Texten ohne personenbezogene Daten, etwa für Übersetzungen fremdsprachiger Texte oder bei der Nutzung juristischer Fachdatenbanken, lässt keine rechtsstaatlichen Risiken erkennen, sofern das Ergebnis vor der Einleitung konkreter Maßnahmen von einer fachkundigen Person unter Einsatz menschlicher Intelligenz überprüft wird. Allerdings besteht auch hierbei das Problem möglicher Prompt-Injection-Angriffe.

§ 69c Prüfung der Auswertung

(1) Die Ergebnisse von IT-gestützten Informationsanalysen müssen jederzeit durch die Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde nachvollzogen, geprüft und abschließend bewertet werden können.[§ 69 (3) Satz: 2] Wenn eine Beschwer des Betroffenen durch die Analyse absehbar ist, muss eine menschliche Kontrolle des Auswertungsergebnisses erfolgen.

(2) Alle verwendeten Techniken und Methoden, sowie die Analysen insgesamt, müssen jederzeit nachvollziehbar sein, mit Aufschluss darüber, welche der verwendeten Eingangsdaten zum Ergebnis geführt haben und wie die Eingangsdaten für ein anderes oder gegenteiliges Ergebnis hätten abweichen müssen.

---

[9] Adam Becker, More Everything Forever: AI Overlords, Space Empires, and Silicon Valley's Crusade to Control the Fate of Humanity, sehr gut zusammengefasst in https://www.lawfaremedia.org/article/the-same-old-fantasies-behind-ai-and-new-technology

(3) Auswertungsergebnisse, deren Prüfung nach Absatz (1) nicht erfolgreich ist, sind zu löschen und dürfen nicht genutzt werden.

(4) In der IT-gestützte Informationsanalyse erstellte Informationen zu nicht in § 7 genannten Personen dürfen nicht weiterverarbeitet werden und sind zu löschen.[§ 69 (5) Satz: 1]

Begründung

Jede Maßnahme des Verfassungsschutzes muss rechtsstaatlich korrekt begründet werden. Sofern IT-gestützten Informationsanalysen zur Anordnung der Maßnahme geführt haben, müssen diese auch gerichtlich überprüfbar sein.

§ 69d Entwicklung von Analysewerkzeugen

(1) Zur Entwicklung, Überprüfung, *oder* Änderung ~~oder zum Trainieren~~ von IT-Produkten darf die Verfassungsschutzbehörde allgemein zugängliche und bei ihr vorhandene personenbezogene Informationen weiterverarbeiten, soweit dies erforderlich ist, weil

1. unveränderte Daten benötigt werden oder
2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. [§ 69 (6) Satz: 3]

Soweit möglich, sollen dabei Informationen aus allgemein zugänglichen Quellen genutzt werden.[§ 69 (6) Satz: 4]

(2) Informationen aus Wohnraumüberwachungen nach § 46 dürfen nicht nach Absatz (1) verarbeitet werden. [§ 69 (6) Satz: 5]

(3) Die Informationen sind so auszuwählen, dass statistische Verzerrungen und diskriminierende Verarbeitungsprozesse möglichst vermieden werden. [§ 69 (6) Satz: 6]

(4) Nach (1) erforderliche Information, sind getrennt von den Akten und Dateien nach § 64 vorzuhalten. [§ 69 (6) Satz: 6]

(5) Eine Verwendung dieser getrennt vorgehaltenen Informationen zu anderen Zwecken ist unzulässig. Sie sind zum frühestmöglichen Zeitpunkt zu anonymisieren und zu löschen, sobald die Verfahren nicht mehr genutzt werden, zu deren Entwicklung, Überprüfung, Änderung oder Training sie verwendet wurden. [§ 69 (6) Satz: 7]

§ 69e Kontrolle

(1) Alle IT-gestützten Analysen sind mit:

1. Zweck,
2. vollständiger Eingabe,
3. Ausgabe und allen weiteren Parametern, die zur deterministischen Wiederholung notwendig sind,
4. kryptographisch sicher identifizierter Durchführungsperson, und, falls vorhanden, Auftraggeberperson,

zu protokollieren.

(2) Analyseergebnisse stellen automatische Dateien im Sinne von § 63 (3) dieses Gesetzes dar.

(3) Die Protokolle sind revisionssicher zu speichern. Zum Zwecke des Geheimschutzes kann aus den Protokollen in externe Dateien oder Akten verwiesen werden, sofern diese ebenfalls revisionssicher sind. Die Vollständigkeit und Integrität der Protokolle und ihrer Verweisstrukturen ist mindestens jährlich zu überprüfen und durch geeignete Verfahren sicherzustellen.

(4) Die Verarbeitung von Informationen mit Hilfe automatisierter technischer Systeme unterliegt der Kontrolle durch die nach § 11 Absatz 1 des Artikel 10-Gesetzes für die G 10-Aufsicht zuständigen Person. Die Kontrolle erfolgt in Stichproben.[§ 69 (9) Satz: 1]

§ 69f Ermächtigung

(1) Die Entscheidung über den Einsatz von automatisierten technischen Systemen zur Informationsverarbeitung nach Absatz 1, bei denen auch mit nachrichtendienstlichen Mitteln erhobene Informationen verarbeitet werden, trifft die Leitung der Verfassungsschutzabteilung oder ihre Vertretung im Amt. Die Entscheidung ist zu dokumentieren. In ihr sind das Ziel der Informationsauswertung sowie die einzubeziehenden Daten darzustellen.[§ 69 (8) Satz: 1] Vor der Entscheidung ist das Parlamentarische Kontrollgremium anzuhören.

(2) Das Nähere zur Nutzung der automatisierten Verfahren nach Absatz 1 sowie zur Entwicklung, Überprüfung, Änderung oder dem Training entsprechender IT-Produkte im Sinne des Absatzes 6 ist in einer Dienstanweisung zu regeln. Die Dienstanweisung ergeht nach Anhörung des Parlamentarischen Kontrollgremiums; gleiches gilt für jede Änderung der Dienstanweisung.[§ 69 (10) Satz: 1]

§ 70 Übermittlungsauftrag, Verfahren und Dokumentation

(1) (unverändert)

(2) (unverändert)

(3) (unverändert)

(4) *Die für die übermittelten personenbezogenen Informationen geltende Speicherdauer und bestehende Verarbeitungseinschränkungen bleiben durch die Übermittlung sowohl bei der übermittelnden als auch bei der empfangenden Stelle unberührt; eine kürzere Speicherung und weitergehende Verarbeitungseinschränkungen sind zulässig.*

Begründung zu Absatz (4):

Die Anpassung stellt sicher, dass durch die Übermittlung personenbezogener Daten die bestehenden Beschränkungen nicht aufgeweicht werden, strengere Beschränkungen jedoch weiterhin zulässig bleiben.

§ 74 Zweckbindung

(1) Die empfangende Stelle darf personenbezogene Informationen nur zu dem Zweck verwenden, zu dem sie ihr übermittelt wurden. Die empfangende Stelle ist auf den Zweck der Übermittlung sowie die Verwendungsbeschränkung hinzuweisen. Dies gilt nicht für Übermittlungen im Rahmen legendierter Einsätze.

(2) *Sobald die Gefahr der Enttarnung entfällt, ist eine Zweckbindung für die erhobenen Daten einzuführen.*

Begründung (2)

In der Begründung zum Entwurf steht „Die Einschränkung in Satz 3 dient dazu, dass verdeckte Mitarbeiterinnen und Mitarbeiter ihre Legende erhalten können, auch wenn sie im Rahmen verdeckter Tätigkeiten Informationen übermitteln, und sich nicht durch einen Hinweis auf die Zweckbindung „enttarnen“.“ Der neu eingeführte Abs. 2 sorgt dafür, dass erhobene Daten nachträglich eine Zweckbindung erhalten, wenn dem nichts mehr im Wege steht.

§ 78 Mit nachrichtendienstlichen Mitteln erhobene personenbezogene Informationen

(1) Die Verfassungsschutzbehörde darf personenbezogene Informationen, die mit nachrichtendienstlichen Mitteln erhoben worden sind, an andere Stellen als das Bundesamt für Verfassungsschutz, die Verfassungsschutzbehörden der Länder, das Bundesamt für den Militärischen Abschirmdienst sowie den Bundesnachrichtendienst nur übermitteln, wenn sie dem Schutz besonders gewichtiger Rechtsgüter dienen*, die empfangende Behörde die Informationen zu dem jeweiligen Übermittlungszweck mit vergleichbar schwerwiegenden Mitteln hätte erheben dürfen* und die besonderen Übermittlungsvoraussetzungen nach §§ 81 bis 87 für die unterschiedlichen Stellen, die die Informationen empfangen, gegeben sind.

Begründung zu Absatz (1)

Die Begründung des Entwurfs (S. 84, 154 ff.) bezieht sich ausdrücklich auf das Kriterium der hypothetischen Neuerhebung, unterlässt aber eine allgemeine entsprechende Regelung. Die Einzelregelungen in den §§ 81-87 stellen lediglich auf die Schwere der Rechtsgutverletzung[10] ab und berücksichtigen nicht das zweite Kriterium, ob nämlich die empfangende Stelle die Daten selbst mit vergleichbaren Mitteln hätte erheben dürfen.[11]

§ 91 Datenschutzrechtliche Auskunftserteilung

(1)-(7) (unverändert)

(8) Hat sich ein Verdacht, der zur Speicherung oder Verarbeitung personenbezogener Informationen geführt hat, nicht erhärtet, ist die betroffene Person nach Ablauf einer angemessenen Frist von Amts wegen hierüber zu unterrichten, soweit dadurch nicht schutzwürdige Interessen Dritter oder überwiegende öffentliche Belange beeinträchtigt werden.

Begründung

Die Vorschrift dient der Transparenz und dem Rehabilitationsinteresse der betroffenen Person. Wird ein Verdacht nicht bestätigt, soll sie hiervon Kenntnis erhalten, um mögliche fortwirkende Beeinträchtigungen auszuräumen und ihre informationelle Selbstbestimmung wirksam wahrnehmen zu können

§ 98 Befugnisse

(1) Soweit sein Recht auf Kontrolle reicht, kann das Parlamentarische Kontrollgremium von der Landesregierung die erforderlichen Auskünfte sowie Einsicht in Akten, Schriftstücke, Dateien *und IT-Systeme* der Verfassungsschutzbehörde verlangen. Ihm ist zu diesen Zwecken nach vorheriger Ankündigung Zutritt zu den Diensträumen der Verfassungsschutzbehörde zu gewähren.

(2) Diesen Verlangen des Parlamentarischen Kontrollgremiums hat Landesregierung unverzüglich zu entsprechen. § 97 Absatz 3 gilt entsprechend.

[10] BVerfG 1 BvR 1619/17 vom 26.04.2022. Leitsätze c-e

[11] BVerfG 1 BvR 1619/17 vom 26.04.2022. Leitsatz 3 und Rz. 231

Begründung

Eine wirksame Kontrolle durch das Parlamentarische Kontrollgremium erfordert, falls nötig, auch Einsicht in die Datenverarbeitungssysteme, das ansonsten die Analyseabläufe nicht kontrolliert werden können.

§ 99 Geschäftsstelle, Unterstützung des Parlamentarischen Kontrollgremiums

(1)-(4) (unverändert)

(5) *Der Geschäftstelle gehört mindestens eine Person mit abgeschlossenem Studium der Informatik zur Unterstützung des Parlamentarischen Kontrollgremiums in technischen Fragen an.*

Begründung

Die Kontrolle durch das Parlamentarischen Kontrollgremium ist nicht auf rechtliche Fragen beschränkt. Die gesteigerten Grundrechtseingriffe durch die neuen Datenverarbeitungsbefugnisse gebieten eine angemessene Kontrolle. Es kann von den Mitglieder:innen des Parlamentarischen Kontrollgremiums nicht erwartet werden, dass diese die notwendige Fachkenntnis mitbringen oder sich erarbeiten. Dementsprechend ist unterstützendes Personal notwendig. Insbesondere die Kontrolle der Cybereigensicherung der Verfassungsschutzbehörde und die Bewertung der nach § 99a getroffenen Maßnahmen erfordern besondere Kenntnisse für ihre Wirksamkeit.

§ 99a Geheimschutz bei Gesetzesverstößen

Mitarbeitende der Verfassungsschutzbehörde dürfen sich an Mitglieder des Parlamentarischen Kontrollgremiums oder die Mitarbeitenden der Geschäftsstelle des Parlamentarischen Kontrollgremiums wenden, wenn sie Besorgnis haben, an der Einhaltung der Gesetze durch die Verfassungsschutzbehörde zu zweifeln. Sie dürfen deshalb keine disziplinarischen, strafrechtlichen oder sonstigen Nachteile erleiden.

Begründung

Der derzeitige Zustand, das Mitarbeitenden der Verfassungsschutzbehörde bei internen Rechtsverstößen nur der Weg über die Presse oder Abgeordnete im Schutze der Auskunftsverweigerungsrechte bleibt, ist unwürdig. Dieser Zustand befördert Leaks und Indiskretionen. Deshalb braucht es einen rechtssicheren Weg für die Mitarbeitenden der Verfassungsschutzbehörde. Das Parlamentarische Kontrollgremium als Aufsichtsorgan ist hierfür besonders geeignet, da es ohnehin Kontrollfunktionen wahrnimmt und so Kenntnisse über Probleme und Verstöße innerhalb des Verfassungsschutzes bekommen kann, ohne das die Öffentlichkeit beteiligt werden muss.

§ 100 Berichterstattung an den Landtag

(1) Das Parlamentarische Kontrollgremium erstattet dem Landtag *mindestens* einmal im Jahr einen zusammenfassenden Bericht über seine Kontrolltätigkeit. Dieser wird zuvor vom Parlamentarischen Kontrollgremium beraten und der Landesregierung ist Gelegenheit zur Stellungnahme zu geben.

(2) Die Grundsätze des § 96 Absatz 3 sind zu beachten.

Begründung

Das Parlamentarische Kontrollgremium sollte selbst entscheiden können, in welchem Turnus Berichte erstellt werden, falls das nötig sein sollte.