BREMISCHE BÜRGERSCHAFT **Drucksache 20/1742**
Landtag **(zu Drs. 20/1536)**
20. Wahlperiode **24. Januar 2023**

Mitteilung des Senats

„Quellen-Telekommunikationsüberwachung und Online-Durchsuchung – Mogelpackung auf Kosten der IT-Sicherheit?“

Mitteilung des Senats an die Bremische Bürgerschaft (Landtag) vom 24. Januar 2023

Die Fraktion Bündnis 90 / Die Grünen hat folgenden Große Anfrage an den Senat gerichtet:

Computer und Smartphones enthalten heutzutage oft eine unermessliche Fülle an Informationen: alltägliche bis intimste E-Mails, SMS und Messenger-Nachrichten, Terminkalender, Kontakte, Gesundheitsdaten von angeschlossenen Fitness-Trackern, Kontoumsätze, Geodaten, Tagebücher und Social-Media-Accounts. Mit Speicherkapazitäten im Giga- bis Terabyte-Bereich enthalten sie ein weitgehendes digitales Abbild unseres Lebens. Das Bremische Polizeigesetz und die Strafprozessordnung enthalten Rechtsgrundlagen, um Computer und Smartphones bei den Betroffenen zu beschlagnahmen, wenn dies zur Gefahrenabwehr oder zur Strafverfolgung erforderlich ist. Diese Rechtsgrundlagen können auch heute bereits dazu genutzt werden, um Daten sicherzustellen, die auf einem Online-Speicher (Cloud) abgelegt sind. Dazu zählen nicht nur E-Mails, Dokumente und Fotos, sondern auch Nachrichten von cloud-basierten Messengern wie Telegram oder Facebook bis hin zu kompletten Geräte-Backups, mit denen die Sicherheitsbehörden auch auf die sonst nur lokal auf dem Gerät gespeicherten Inhalte Zugriff erhalten können. Insgesamt ergeben sich auf diese Weise für die Sicherheitsbehörden Zugriffsmöglichkeiten auf Informationen in einem Umfang, der in früheren Jahrzehnten undenkbar erschien. Die Herausforderung für Ermittler*innen besteht heute oft weniger darin, zusätzliche Informationen zu erlangen, sondern in der nutzbaren Auswertung der riesigen Datenmengen.

Vor diesem Hintergrund erscheinen Aussagen, die Sicherheitsbehörden könnten aufgrund der zunehmenden Verbreitung verschlüsselter Internetkommunikation kaum noch auf diese Inhalte dieser Kommunikation zugreifen und daher schlimmste Verbrechen nicht mehr verhindern oder aufklären, wenig belastbar. Dennoch gibt es auf Bundesebene und in mehreren Bundesländern mit der Online-Durchsuchung und der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) weitergehende Befugnisse. Diese sollen den Sicherheitsbehörden ermöglichen, auf Computer und Smartphones zuzugreifen, ohne dass die Zielperson dies bemerkt, wie es bei einer Sicherstellung unweigerlich der Fall wäre, und ohne dass der Zugriff über Cloud-Anbieter erfolgen muss, die oft im Ausland sitzen und nicht immer für deutsche Behörden erreichbar sind. Beide Instrumente, Quellen-TKÜ und Online-Durchsuchung stehen dem Bundeskriminalamt bereits seit 2008 und den bremischen Strafverfolgungsbehörden seit einer Änderung der Strafprozessordnung im Jahr 2017 zur Verfügung.

Abgesehen von der Nutzung regulärer Funktionen von Messenger-Apps, wie beispielsweise die Gerätekopplung unter Zuhilfenahme des Smartphones der Zielperson, kann der Zugriff auf die Endgeräte bei Online-Durchsuchung und Quellen-TKÜ in der Regel nur durch Hacking erlangt werden, insbesondere per Trojaner. Dabei werden oft Sicherheitslücken in Soft- und Hardware genutzt, die den Herstellern noch unbekannt sind. Staatstrojaner sind für Sicherheitsbehörden nur dann sinnvoll nutzbar, wenn auf möglichst vielen unterschiedlichen Gerätetypen Sicherheitslücken vorhanden sind, die beim staatlichen Hacking ausgenutzt werden können. Das schafft Anreize für die anwendenden Stellen, ein „Arsenal“ von Sicherheitslücken aufzubauen und diese den Herstellern zu verheimlichen, damit sie nicht geschlossen werden. Jede einzelne Lücke in einer solchen elektronischen Waffenkammer kann allerdings nicht nur von Behörden für Hacks von Handys und Computern ausgenutzt werden, sondern auch von Kriminellen. Das gefährdet die Cybersicherheit in Deutschland und auf der ganzen Welt. Spürbar wurde dies einer breiteren Öffentlichkeit etwa im Jahr 2017, als die Erpresser-Software WannaCry weltweit hohe Schäden verursachte und unter anderem das britische Krankenhaussystem lahmlegte. WannaCry beruhte auf Sicherheitslücken in Microsoft Windows, die der US-Auslandsgeheimdienst NSA mindestens fünf Jahre lang genutzt hatte, ohne Microsoft zu informieren. Auch der Anfang Juli 2021 erfolgte Cyber-Angriff mit Verschlüsselungstrojanern auf zahlreiche IT-Dienstleister, deren Kunden und weitere Unternehmen in Deutschland und weltweit beruhte auf einer Sicherheitslücke in einer verbreiteten Software. Das Bundesverfassungsgericht hat vor diesem Hintergrund jüngst die grundrechtliche Schutzpflicht der Sicherheitsbehörden betont, bei jeder Entscheidung über ein Offenhalten einer unerkannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser Sicherheitslücke zu ermitteln und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ zu bestimmen, beides zueinander ins Verhältnis zu setzen und die Sicherheitslücke an den Hersteller zu melden, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt.

Die Verwendung von Staatstrojanern gefährdet nicht nur die IT-Sicherheit, sondern ist teilweise auch mit menschenrechtsverletzenden Geschäftspraktiken verbunden. Bundesregierung und deutsche Sicherheitsbehörden arbeiten seit Jahren mit Unternehmen der Überwachungsindustrie zusammen, die auf die Strategie setzen, zunächst Sicherheitslücken zu finden oder auf dem Schwarzmarkt von Kriminellen abzukaufen, dann mit Hilfe von Trojaner-Software unbemerkt in die IT-Systeme einzudringen und schließlich Daten an Sicherheitsbehörden aus aller Welt auszuleiten. Dabei ist es teilweise Geschäftspraxis dieser Unternehmen, ihre nicht zuletzt mit deutschen Steuermitteln finanzierten Produkte weltweit auch an Regierungen zu verkaufen, die damit Menschenrechtler*innen, Journalist*innen oder Oppositionelle ausspionieren. Dies zeigt unter anderem der Fall der Spionagesoftware FinSpy des britisch-deutschen Unternehmens FinFisher, das auch das Bundeskriminalamt mit Staatstrojaner-Software beliefert. Im Juli 2019 erstatteten mehrere Nichtregierungsorganisationen Strafanzeige wegen Verstoßes gegen § 18 des Außenwirtschaftsgesetzes gegen den Geschäftsführer von FinFisher. Dabei wurden umfangreiche Anhaltspunkte dafür vorgelegt, dass FinFisher die Spionagesoftware FinSpy ohne Genehmigung der Bundesregierung an die türkische Regierung verkauft und so zur Überwachung von Oppositionellen und Journalist*innen in der Türkei beigetragen haben soll. Nachdem sich der Tatverdacht offensichtlich erhärten ließ, durchsuchte die Staatsanwaltschaft München im Zuge der Ermittlungen gegen FinFisher vom 6. bis 8. Oktober 2020 15 Wohn- und Geschäftsräume im In- und Ausland. Ende 2021 erließ das Amtsgericht München einen Vermögensarrest, um die von der FinFisher-Gruppe mit rechtswidrigen Praktiken erlangten Einnahmen für eine mögliche Einziehung zu

sichern. Daraufhin meldeten drei Unternehmen der FinFisher-Gruppe Insolvenz an und stellten ihren Geschäftsbetrieb ein.

Verschiedene journalistische Recherchen haben zudem derart zahlreiche und schwerwiegende Ausspähungsskandale im Zusammenhang mit dem auch von deutschen Behörden eingesetzten Staatstrojaner Pegasus des israelischen Herstellers NSO Group ans Licht gebracht, dass das Europäische Parlament einen Untersuchungsausschuss „zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware“ eingesetzt hat. Der Europäische Datenschutzbeauftragte hat ein umfassendes Verbot der Entwicklung und des Einsatzes von Ausspähsoftware wie Pegasus in der gesamten Europäischen Union gefordert. Die Technologie stelle nicht nur eine Gefahr für Menschen und ihre Geräte dar, sondern auch für Demokratie und Rechtsstaatlichkeit.

Die rechtsstaatliche Kontrolle des Einsatzes staatlicher Spionagesoftware gestaltet sich in der Praxis tatsächlich schwierig. Bereits 2011 brachte eine Analyse des Chaos Computer Clubs ans Licht, dass ein von deutschen Strafverfolgungsbehörden damals zur Quellen-TKÜ verwendeter Staatstrojaner fast sämtliche verfassungsrechtlichen Vorgaben aufs Gröbste missachtete, ohne dass dies Staatsanwaltschaften oder Gerichten zuvor aufgefallen wäre. Der Einsatz von Staatstrojanern muss daher mit entsprechenden technischen Kompetenzen bei den beteiligten Stellen einhergehen. Zudem darf die parlamentarische Kontrolle nicht derart behindert werden, wie es gegenüber dem Deutschen Bundestag geschieht. Das Bundesinnenministerium begründete im Innenausschuss des Bundestags die weitgehende Verweigerung von Antworten auf diverse Kleine Anfragen so: „Die Unternehmen wollen nicht, dass es offenbar wird, dass sie mit der Bundesregierung oder mit Sicherheitsbehörden des Bundes kooperieren. Wenn dies der Fall ist, dann beenden sie ihre Geschäftsbeziehungen mit uns.“

Ungeachtet dessen wurde der Einsatz von Quellen-TKÜ mittlerweile auch auf Nachrichtendienste ausgeweitet. Seit dem 9. Juli 2021 enthält das Artikel-10-Gesetz die Befugnis zur Quellen-TKÜ. Da das Artikel-10-Gesetz nicht nur für das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst und Militärischen Abschirmdienst gilt, sondern auch für die Verfassungsschutzbehörden der Länder, darf jetzt auch das bremische Landesamt für Verfassungsschutz Staatstrojaner einsetzen. Anders als die bisherigen Regelungen zur Quellen-TKÜ in der Strafprozessordnung und im BKA-Gesetz werden die Internet-Provider im Artikel-10-Gesetz sogar verpflichtet, Internetverkehr an die Nachrichtendienste umzuleiten, um das Einschleusen und Installieren von Staatstrojanern zu erleichtern. Insbesondere gegen diese Neuerung wendet sich eine breite Initiative aus zivilgesellschaftlichen Organisationen und Unternehmen, die vom Chaos Computer Club (CCC) über Google und Facebook bis hin zum Bundesverband IT-Mittelstand (MITMi), dem Verband der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) und dem Verband der Internetwirtschaft (eco) reicht. Die Initiative befürchtet, diese Regelung könnte die Anbieter von Kommunikationsdiensten zwingen, die Sicherheit und Integrität ihrer eigenen Dienste einzuschränken, um Nachrichtendiensten bei der Spionage zu unterstützen.

Wir fragen den Senat:

I. Einsatz für Zwecke der Strafverfolgung

1. Wie oft und aufgrund welcher Anlassstraftaten wurden in Bremen und Bremerhaven seit 2017 Maßnahmen der Quellen-Telekommunikationsüberwachung nach § 100a Absatz 1 Satz 2 und 3 oder der Online-Durchsuchung nach § 100b der Strafprozessordnung

a) von der Staatsanwaltschaft beantragt,
b) richterlich angeordnet,
c) wegen Gefahr in Verzug von der Staatsanwaltschaft angeordnet?
d) tatsächlich durchgeführt?

Bitte Quellen-TKÜ und Online-Durchsuchung getrennt ausweisen und jeweils nach Kalenderjahren aufschlüsseln. Bei politisch motivierter Kriminalität bitte zusätzlich nach Phänomenbereich differenzieren.

2. In wie vielen dieser Fälle kam
a) die BKA-Eigenentwicklung RCIS,
b) FinSpy,
c) Pegasus,
d) eine andere Spionagesoftware
zum Einsatz?

3. Soweit angeordnete Maßnahmen der Quellen-TKÜ oder Online-Durchsuchung nicht erfolgreich durchgeführt wurden, aus welchen Gründen scheiterte dies?

4. Welche wesentlichen Ermittlungserfolge konnten von bremischen Strafverfolgungsbehörden seit 2017 durch Maßnahmen der Quellen-TKÜ oder der Online-Durchsuchung erzielt werden?

5. Auf wie viele unterschiedliche Varianten von Trojaner-Software von wie vielen Herstellern für welche Einsatzgebiete können die bremischen Strafverfolgungsbehörden im Bedarfsfall zurückgreifen?
6. Durch welche Stellen werden den bremischen Sicherheitsbehörden die technischen Mittel zur Durchführung von Quellen-TKÜ und Online-Durchsuchung zur Verfügung gestellt?

7. Inwieweit müssen die bremischen Strafverfolgungsbehörden beim praktischen Einsatz von Staatstrojanern auf die Unterstützung von Bundesbehörden (z. B. BKA, ZITIS) oder anderen Stellen zurückgreifen?

8. Die Anwendung welcher der folgenden bekannten Methoden, um einen Staatstrojaner heimlich auf dem Gerät einer beschuldigten Person zu installieren, dürfen die bremischen Strafverfolgungsbehörden unter welchen Voraussetzungen veranlassen:
a) Aufspielen im Rahmen von Sicherheitskontrollen, etwa an Flughäfen,
b) heimliches Betreten von Wohnungs- oder Geschäftsräumen,
c) heimliches Entwenden und Zurücklegen des Geräts, auch unter Inanspruchnahme von Vertrauenspersonen,
d) Aufspielen als versteckter Bestandteil von Software, zu deren Nutzung die beschuldigte Person durch andere Behörden verpflichtet oder angehalten wird (Corona-Warn-App, CovPass, ELSTER, AusweisApp2, NINA, Katwarn, Mängelmelder etc.),
e) Aufspielen durch eine E-Mail oder Nachricht an eine nur von der beschuldigten Person genutzten Zieladresse,
f) Aufspielen durch eine E-Mail oder Nachricht an eine möglicherweise auch von anderen Personen genutzte Zieladresse?

9. Welche Umstände hindern die bremischen Strafverfolgungsbehörden daran, Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung häufiger als bisher einzusetzen?

10. Wie bewertet der Senat die bisher erreichte Einsatzfähigkeit von Quellen-TKÜ und Online-Durchsuchung und ihren effektiven Nutzen für die Strafverfolgung?

11. Wie bewertet der Senat die Koalitionsvereinbarung von SPD, Grünen und FDP auf Bundesebene, die Eingriffsschwelle für den Einsatz von Überwachungssoftware zur Quellen-TKÜ an die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung anzupassen, also den Einsatz auf besonders schwere Straftaten zu begrenzen?

II. Einhaltung verfassungsrechtlicher Vorgaben

12. Welche Stellen sind dafür verantwortlich zu gewährleisten, dass die den bremischen Strafverfolgungsbehörden zur Verfügung stehenden Staatstrojaner den verfassungsrechtlichen Vorgaben genügen, indem tatsächlich und nicht etwa nur scheinbar technisch sichergestellt ist, dass
a) an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
b) die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden,
c) der eingesetzte Staatstrojaner nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist,
d) im Falle der Quellen-TKÜ ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird?

13. Welche Erkenntnisquellen (Quellcodes, Audits, Zertifikate etc.) stehen den zuständigen Stellen zur Verfügung, um prüfen zu können, ob die verfassungsrechtlichen Vorgaben eingehalten werden?

14. Sind die bremischen Sicherheitsbehörden berechtigt, alle vorliegenden Informationen über die ihnen für den Einsatz zur Verfügung stehenden Staatstrojaner an das Gericht bzw. G 10-Kontrollgremium herauszugeben, das für die Anordnung oder rechtliche Überprüfung der Maßnahme zuständig ist?

15. Sind die bremischen Sicherheitsbehörden berechtigt, alle vorliegenden Informationen über die ihnen für den Einsatz zur Verfügung stehenden Staatstrojaner an andere öffentliche Stellen herauszugeben, die über die erforderlichen Kompetenzen verfügen, um die Einhaltung der verfassungsrechtlichen Vorgaben überprüfen zu können (z. B. an das Bundesamt für Sicherheit in der Informationstechnik)?

16. Geht der von bremischen Strafverfolgungsbehörden veranlasste Einsatz von Staatstrojanern mit Geheimhaltungsverpflichtungen oder -zusagen einher, die geeignet sind, die parlamentarische Kontrolle dieser Einsätze durch die Bürgerschaft einzuschränken? Wenn ja, welche Verpflichtungen oder Zusagen sind dies und wem gegenüber gelten sie?

III. IT-Sicherheit und Schwachstellen

17. Welche potentiellen Schäden für kritische Infrastrukturen, Behörden, Unternehmen, Privathaushalte und Umwelt drohen durch Cyberangriffe mit Schadsoftware, wenn hierbei offene Schwachstellen in weit verbreiteten Betriebssystemen ausgenutzt werden können? Welche durch Ransomware-Attacken bereits entstandenen Schäden für bremische Behörden oder Unternehmen sind dem Senat bekannt?

18. Welche Konsequenzen haben deutsche und internationale Sicherheitsbehörden nach Kenntnis des Senats nach den Attacken mit dem sogenannten WannaCry-Trojaner im Hinblick auf die Geheimhaltung von Sicherheitslücken gezogen?

19. Wie hoch bewertet der Senat die Gefahr, dass Zielpersonen, die einen Staatstrojaner auf ihrem Gerät entdecken, die Funktionsweise des Staatstrojaners analysieren und für kriminelle Zwecke nutzen, und welche Sicherheitsvorkehrungen bestehen, um dies zu verhindern?

20. Nutzen die Staatstrojaner, die den bremischen Sicherheitsbehörden zur Verfügung stehen, nach Kenntnis des Senats IT-Schwachstellen aus, welche die Integrität der von vielen Unternehmen und Menschen im Land Bremen verwendeten IT-Produkte bedrohen können, und was unternimmt der Senat, um auf eine Schließung dieser Sicherheitslücken hinzuwirken?

21. Hält der Senat es für vertretbar, mit Hilfe von Staatstrojanern IT-Sicherheitslücken auszunutzen und diese Schwachstellen gegenüber den betroffenen IT-Herstellern geheim zu halten, obwohl sie mit unabsehbaren Folgen auch von kriminellen Personen ausgenutzt werden könnten?

22. Welche Konsequenzen aus der Entscheidung des Bundesverfassungsgerichts vom 8. Juni 2021 zur staatlichen Nutzung von IT-Sicherheitslücken wurden von den deutschen und den bremischen Sicherheitsbehörden gezogen?
a) Durch welche Stellen ist gegebenenfalls die vom Bundesverfassungsgericht geforderte Abwägung zwischen den Gefahren für die allgemeine IT-Sicherheit, die durch eine von Staatstrojanern ausgenutzte Sicherheitslücke verursacht werden, und dem Nutzen, der durch den Einsatz der Staatstrojaner erzielt werden kann, in Bezug auf die Staatstrojaner, die den bremischen Strafverfolgungsbehörden zur Verfügung stehen, mit welchen Ergebnissen durchgeführt worden?
b) Wurde vor dem Einsatz eines Staatstrojaners durch bremische Sicherheitsbehörden insbesondere eine Datenschutz-Folgenabschätzung gemäß § 67 des Bundesdatenschutzgesetzes durchgeführt bzw. wurde dies nachgeholt, nachdem das Bundesverfassungsgericht in seiner Entscheidung vom 8. Juni 2021 darauf hinwies, dass eine Datenschutz-Folgenabschätzung vor dem Einsatz von Überwachungssoftware im Rahmen einer Quellen-TKÜ zweifellos durchzuführen sei? Wenn ja, welche wesentlichen Ergebnisse sind aus der Datenschutz-Folgenabschätzung und ggf. aus der Anhörung der Landesbeauftragten für Datenschutz und Informationssicherheit hervorgegangen?

23. Welche Maßnahmen werden unternommen, um in deutschen Sicherheitsbehörden und bei den Lieferanten der von ihnen verwendeten Staatstrojaner etwaigen Fehlanreizen entgegenzuwirken, gemeingefährliche Sicherheitslücken nicht den betroffenen Herstellern zu melden, weil sie für den effektiven Einsatz von Staatstrojanern ausgenutzt werden sollen?

24. Wie bewertet der Senat die Bedeutung einer sicheren Verschlüsselung von elektronischer Kommunikation für
a) die Pressefreiheit und den Quellenschutz,
b) oppositionelle Kräfte und diskriminierte Minderheiten in Staaten mit politischer Verfolgung,
c) Wirtschaftsunternehmen in Bremen und Bremerhaven?

25. Sind die Sicherheitslücken im iOS-Betriebssystem, durch die der Pegasus-Trojaner mit dem bloßen Empfang einer iMessage installiert und aktiviert werden konnte (Zero-Click-Attacke), nach Kenntnis des Senats mittlerweile vollständig geschlossen? Welche Auswirkungen auf die dienstliche Verwendung von iPhones und iPads im Verantwortungsbereich des Senats hat dieser Sachverhalt?

IV. Staatstrojaner für den Verfassungsschutz

26. In seinem Urteil vom 15. Dezember 1970 zur Frage, ob der Bundesgesetzgeber zum Erlass des Gesetzes zu Artikel 10 Grundgesetz befugt war, meinte das Bundesverfassungsgericht, die Gesetzgebungskompetenz des Bundes für Regelungen über die Überwachung des Brief-, Post- und Fernmeldeverkehrs durch Landesverfassungsschutzbehörden ergebe sich aus der Zuständigkeit für das gerichtliche Verfahren (Artikel 74 Absatz 1 Nummer 1), da die Maßnahmen wenigstens mittelbar der Verhinderung, Aufklärung und Verfolgung von Straftaten dienten. Hält der Senat diese Annahme angesichts der späteren Rechtsprechung des Bundesverfassungsgerichts zur Abgrenzung der Gesetzgebungskompetenzen für die Verfolgung von Straftaten einerseits und der Abwehr von Gefahren sowie der Verhütung von Straftaten andererseits noch für tragfähig?

27. Inwieweit ermächtigt die ausschließliche Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder auf dem Gebiet des Verfassungsschutzes (Artikel 73 Absatz 1 Nummer 10 Buchstabe b des Grundgesetzes) den Bund zur Regelung von Eingriffsbefugnissen der Landesverfassungsschutzbehörden?

28. Bestehen nach Ansicht des Senats Zweifel an der Vereinbarkeit der Regelung in § 11 Absatz 1a des Artikel-10-Gesetzes mit der grundgesetzlichen Gesetzkompetenzverteilung zwischen Bund und Ländern? Bitte begründen.

29. Inwieweit ist der bremische Landesgesetzgeber berechtigt, die für das Landesamt für Verfassungsschutz nach dem Artikel-10-Gesetz bestehenden Befugnisse zu erweitern, zu konkretisieren, einzuschränken oder aufzuheben, etwa durch eine Änderung von § 8 Absatz 1 Nummer 11 des Bremischen Verfassungsschutzgesetzes?

30. Welche der folgenden bekannten Methoden, um einen Staatstrojaner heimlich auf dem Gerät einer Zielperson zu installieren, darf das Bremer Landesamt für Verfassungsschutz aufgrund der in § 2 Absatz 1a Satz 1 Nummer 4 des Artikel-10-Gesetzes geregelten Pflicht zur Umleitung von Telekommunikation unter welchen Voraussetzungen veranlassen:
a) Manipulation oder Fälschung von Webseiten,
b) Manipulation oder Fälschung von Software-Updates,
c) Manipulation oder Fälschung von SSL/TLS-Zertifikaten,
d) Manipulation oder Fälschung von Software-Signaturen?

31. Wie bewertet der Senat die Bedeutung des Vertrauens der Menschen in die Integrität von Sicherheitsupdates, von SSL/TLS-Zertifikaten und von Software-Signaturen für die allgemeine IT-Sicherheit?

32. Wie bewertet der Senat die Koalitionsvereinbarung von SPD, Grünen und FDP auf Bundesebene, die Eingriffsschwelle für den Einsatz von Überwachungssoftware zur Quellen-TKÜ an die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung anzupassen, den Einsatz also auch für Verfassungsschutzbehörden auf die Abwehr einer mindestens konkretisierten Gefahr im polizeilichen Sinne für ein besonders gewichtiges Rechtsgut zu beschränken?

V. Alternativen zu Staatstrojanern

33. Inwieweit nutzen die bremischen Strafverfolgungsbehörden die Möglichkeit, über die Anbieter von Messenger-Apps an Metadaten der verschlüsselten Kommunikation zu gelangen und welche rechtlichen und tatsächlichen Herausforderungen haben sich dabei gezeigt?

34. Inwieweit nutzt die Polizei die nach dem Bremischen Polizeigesetz bestehende Möglichkeit, Smartphones sicherzustellen, um zum Zwecke der Gefahrenabwehr Zugriff auf die auf dem Gerät enthaltenen Daten zu erlangen?

35. Welche gesetzgeberischen, regulatorischen oder sonstigen Versuche der Einwirkung auf die Hersteller von Betriebssystemen und Messengerdiensten mit dem Ziel, eine Installation von technischen Mitteln zur Ausleitung von Daten auf Geräten einer Zielperson ohne das Ausnutzen von den Herstellern unbekannten Schwachstellen zu ermöglichen, sind dem Senat bekannt?

36. Wie bewertet der Senat – im Vergleich zu Staatstrojanern – die Praktikabilität von schonenderen, weil ohne den Einsatz von Staatstrojanern möglichen Methoden der Quellen-Telekommunikationsüberwachung, wie etwa den Zugriff auf die Telekommunikation der Zielperson über Whatsapp Web/Desktop, Telegram Cloud oder Signal Desktop?

37. Wie bewertet der Senat den Vorschlag, die Hersteller von Messenger-Apps und Betriebssystemen zu verpflichten, im Einzelfall auf richterliche Anordnung bestimmten Zielpersonen eine App-Version mit Backdoor oder deaktivierter Verschlüsselung aufzuspielen, um so Zugriff auf die Kommunikation zu erhalten, ohne die Integrität der Verschlüsselung auf anderen Geräten zu beeinträchtigen oder Sicherheitslücken auszunutzen?

38. Wie bewertet der Senat die am 6. November 2020 erhobene Forderung des EU-Ministerrats, den Anbietern sicherer Kommunikationslösungen die Pflicht aufzuerlegen, Hintertüren für staatliche Stellen einzurichten, insbesondere auch in Bezug auf die Auswirkungen für die allgemeine IT-Sicherheit?

39. Wie bewertet der Senat die in dem Verordnungsentwurf der Europäischen Kommission vom 11. Mai 2022 enthaltene Verpflichtung für Anbieter von Ende-zu-Ende-verschlüsselter Kommunikation (wie Signal, Threema oder WhatsApp), auf Anordnung die unverschlüsselten Kommunikationsinhalte auf dem Gerät auf Abbildungen von Kindesmissbrauch sowie sogenanntes „Grooming“ zu scannen und ggf. an staatliche Behörden auszuleiten?

40. Wie bewertet der Senat die Forderung des Europäischen Datenschutzbeauftragten nach einem in der gesamten Europäischen Union geltenden Verbot der Entwicklung und des Einsatzes von Ausspähsoftware wie Pegasus sowie die darüber hinaus gehende Forderung von zivilgesellschaftlichen Organisationen, den Vertrieb und Einsatz von Staatstrojaner international zu ächten und zu sanktionieren?

Der Senat beantwortet die Große Anfrage wie folgt:

I. Einsatz für Zwecke der Strafverfolgung

1. Wie oft und aufgrund welcher Anlassstraftaten wurden in Bremen und Bremerhaven seit 2017 Maßnahmen der Quellen-Telekommunikationsüberwachung nach § 100a Absatz 1 Satz 2 und 3 oder der Online-Durchsuchung nach § 100b der Strafprozessordnung
a) von der Staatsanwaltschaft beantragt,
b) richterlich angeordnet,
c) wegen Gefahr in Verzug von der Staatsanwaltschaft angeordnet?
d) tatsächlich durchgeführt?
Bitte Quellen-TKÜ und Online-Durchsuchung getrennt ausweisen und jeweils nach Kalenderjahren aufschlüsseln. Bei politisch motivierter Kriminalität bitte zusätzlich nach Phänomenbereich differenzieren.
Im Jahr 2019 wurde in einem Verfahren wegen des Verdachts der Vorbereitung einer schweren staatsgefährdenden Straftat nach § 89a StGB eine sogenannte Quellen-TKÜ gemäß § 100a Abs. 1 Sätze 2 und 3 StPO durch die Staatsanwaltschaft Bremen beantragt und richterlich angeordnet. Tatsächlich durchgeführt werden konnte die Maßnahme nicht, weil der technische Zugriff auf das Gerät nicht möglich war. Die zugrundeliegende Tat war dem Phänomenbereich „Islamismus“ zuzuordnen. Weitere Fälle, in denen eine Quellen-TKÜ beantragt, gerichtlich oder auf Grund von Gefahr im Verzug durch die Staatsanwaltschaft angeordnet und durchgeführt wurden, sind für den Zeitraum ab 2017 nicht bekannt.
Durch die Staatsanwaltschaft Bremen wurde seit 2017 weder eine Online-Durchsuchung nach § 100b StPO beantragt noch eine solche durchgeführt. Die Staatsanwaltschaft ist nicht berechtigt, die Online-Durchsuchung wegen Gefahr im Verzug anzuordnen. Eine solche Maßnahme kann lediglich durch den Vorsitzenden der für den Erlass der Anordnung zuständigen Kammer beim Landgericht getroffen werden (§ 100e Abs. 2 Satz 2 StPO). Eine solche Anordnung des Kammervorsitzenden ist seit 2017 nicht ergangen.

2. In wie vielen dieser Fälle kam
a) die BKA-Eigenentwicklung RCIS,
b) FinSpy,
c) Pegasus,
d) eine andere Spionagesoftware
zum Einsatz?
Seit 2017 wurden weder Maßnahmen der Quellen-TKÜ noch der Online-Durchsuchung durchgeführt. In dem unter Ziffer 1 benannten Verfahren aus dem Jahr 2019 scheiterte die Umsetzung der Maßnahme bereits daran, dass der physische Zugriff auf das Gerät nicht möglich war. Es kam somit weder in diesem noch in anderen Verfahren zum Einsatz der genannten Softwareprodukte.

3. Soweit angeordnete Maßnahmen der Quellen-TKÜ oder Online-Durchsuchung nicht erfolgreich durchgeführt wurden, aus welchen Gründen scheiterte dies?
In dem einzigen Fall einer beabsichtigten Quellen-TKÜ im Jahr 2019 konnte die Maßnahme nicht umgesetzt werden, weil der technische Zugriff auf das Gerät scheiterte.

4. Welche wesentlichen Ermittlungserfolge konnten von bremischen Strafverfolgungsbehörden seit 2017 durch Maßnahmen der Quellen-TKÜ oder der Online-Durchsuchung erzielt werden?
Seit 2017 erfolgten weder eine Quellen-TKÜ noch durch eine Online-Durchsuchung. Es konnten daher hierdurch auch keine Ermittlungserfolge erzielt werden.

5. Auf wie viele unterschiedliche Varianten von Trojaner-Software von wie vielen Herstellern für welche Einsatzgebiete können die bremischen Strafverfolgungsbehörden im Bedarfsfall zurückgreifen?

6. Durch welche Stellen werden den bremischen Sicherheitsbehörden die technischen Mittel zur Durchführung von Quellen-TKÜ und Online-Durchsuchung zur Verfügung gestellt?

7. Inwieweit müssen die bremischen Strafverfolgungsbehörden beim praktischen Einsatz von Staatstrojanern auf die Unterstützung von Bundesbehörden (z. B. BKA, ZITIS) oder anderen Stellen zurückgreifen?
Die Fragen zu Ziffern 5. bis 7. werden zusammenhängend wie folgt beantwortet: Gerade im Bereich der Online-Durchsuchung liegen bislang keine praktischen Erfahrungen vor. Bei Beantragung der Maßnahme ist im Einzelfall zu prüfen, welche technischen Anforderungen für die spätere Umsetzung der Maßnahme zu beachten sind und welche Stellen hierfür die erforderliche Unterstützung leisten können.
Das LfV Bremen hat bisher keine Quellen-TKÜ eingesetzt.
Für den Bereich des Verfassungsschutzes sieht der Koalitionsvertrag auf Bundesebene vor, den Einsatz von Überwachungssoftware im Rahmen einer Überwachungsgesamtrechnung zu überprüfen. Dies begrüßt der Senat.

8. Die Anwendung welcher der folgenden bekannten Methoden, um einen Staatstrojaner heimlich auf dem Gerät einer beschuldigten Person zu installieren, dürfen die bremischen Strafverfolgungsbehörden unter welchen Voraussetzungen veranlassen:
a) Aufspielen im Rahmen von Sicherheitskontrollen, etwa an Flughäfen,
b) heimliches Betreten von Wohnungs- oder Geschäftsräumen,
c) heimliches Entwenden und Zurücklegen des Geräts, auch unter Inanspruchnahme von Vertrauenspersonen,
d) Aufspielen als versteckter Bestandteil von Software, zu deren Nutzung die beschuldigte Person durch andere Behörden verpflichtet oder angehalten wird (Corona-Warn-App, CovPass, ELSTER, AusweisApp2, NINA, Katwarn, Mängelmelder etc.),
e) Aufspielen durch eine E-Mail oder Nachricht an eine nur von der beschuldigten Person genutzten Zieladresse,
f) Aufspielen durch eine E-Mail oder Nachricht an eine möglicherweise auch von anderen Personen genutzte Zieladresse?
Die Strafprozessordnung enthält keine ausdrückliche Regelung, welche Eingriffe zulässig sind, um die Überwachungstechnik im oder am Gerät anzubringen. Der Gesetzgeber ist davon ausgegangen, dass die Installation der Software auch an dem Gerät selbst erfolgen kann (BT-Drucks. 18/12785, S. 57). Er hält die Anwendung kriminalistischer List zur Anbringung der Überwachungstechnik für zulässig. Hingegen nimmt der Gesetzgeber an, dass das heimliche Betreten einer Wohnung mit dem Ziel der Installation der Software zumindest zur Durchführung der Quellen-TKÜ nicht von der Anordnung der Maßnahmen nach § 100a Abs. 1 Sätze 2 und 3 StGB gedeckt wird (vgl. BT-Drucks. 18/12785, S. 52). Welche Möglichkeiten der Installation von Überwachungstechnik die bremische Justiz für zulässig erachtet, kann nicht gesagt

werden. Durch die fehlende Nutzung dieser Maßnahmen fehlt es an entsprechenden (gerichtlichen) Entscheidungen.

9. Welche Umstände hindern die bremischen Strafverfolgungsbehörden daran, Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung häufiger als bisher einzusetzen?
Aus Sicht der Staatsanwaltschaft stehen einem vermehrten Einsatz der Ermittlungsmaßnahmen der Quellen-TKÜ und Online-Durchsuchung die hohen technischen Hürden und die Schwierigkeiten bei der zulässigen Anbringung der Überwachungstechnik entgegen. Aus diesem Grund werden entsprechende Maßnahmen – unabhängig von den Anordnungsvoraussetzungen – von den Ermittlungsbehörden schon aus tatsächlichen Gründen nur in Ausnahmefällen in Erwägung gezogen.

10. Wie bewertet der Senat die bisher erreichte Einsatzfähigkeit von Quellen-TKÜ und Online-Durchsuchung und ihren effektiven Nutzen für die Strafverfolgung?
In Bremen fehlt es bislang an praktischen Beispielen in der Umsetzung von Quellen-TKÜ und Online-Durchsuchung, so dass eine Bewertung der tatsächlich erreichten Einsatzfähigkeit und des tatsächlichen (effektiven) Nutzens für die Strafverfolgung keine Aussage getroffen werden kann. Gleichwohl werden die bestehenden Möglichkeiten und der erwartete Nutzen durch die Staatsanwaltschaft als hoch bewertet. Bei den Ermittlungsmaßnahmen der Quellen-TKÜ und der Online-Durchsuchung handelt es sich trotz der hohen Hürden beim Vollzug der Maßnahmen um effiziente Strafverfolgungsmaßnamen, die zur Aufklärung schwerer Straftaten benötigt werden. Die Online-Dursuchung eröffnet im Gegensatz zu einer durch die/den Betroffene/n wahrnehmbaren Durchsuchung die Möglichkeit, nicht nur neu hinzukommende Kommunikationsinhalte, sondern alle auf einem informationstechnischen System gespeicherten Inhalte sowie das gesamte Nutzungsverhalten einer Person zu überwachen. Die Quellen-TKÜ ermöglicht es, Internetprotokoll-(IP)-basierte und zahlreiche „Voice-over-IP“ (VoIP)- und Messenger-Dienste deren Kommunikationsinhalte mit einer Verschlüsselung versehen sind, unverschlüsselt zu erhalten. Diese Maßnahmen dienen insbesondere der Aufklärung schwerer Straftaten aus dem Bereich der Bandenkriminalität und der organisierten Kriminalität, die sich in einer technisierten Welt zu einem Großteil über elektronische Kommunikation abspielt.

11. Wie bewertet der Senat die Koalitionsvereinbarung von SPD, Grünen und FDP auf Bundesebene, die Eingriffsschwelle für den Einsatz von Überwachungssoftware zur Quellen-TKÜ an die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung anzupassen, also den Einsatz auf besonders schwere Straftaten zu begrenzen?
Ein Großteil der Kommunikation erfolgt heute verschlüsselt über Internetprotokoll-(IP-) und zahlreiche „Voice-over-IP“ (VoIP)- und Messenger-Dienste. Deren Verschlüsselungssysteme können durch die Strafverfolgungsbehörden mittels einer Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO nicht entschlüsselt werden. Die Strafverfolgungsbehörden benötigen daher eine angepasste Ermittlungsmöglichkeit. Diese wurde durch die Quellen-TKÜ geschaffen.
Die Quellen-TKÜ greift vergleichbar der Telekommunikationsüberwachung nach § 100a Abs. 1 StPO nur auf die laufende Kommunikation zu. Hierdurch wird zunächst Art. 10 GG tangiert. Bei der Online-Durchsuchung ist darüber hinaus auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1

Abs. 1 GG betroffen. Letzteres kann auch bei der Quellen-TKÜ in seinem Schutzbereich tangiert sein. Ob eine Anpassung der Eingriffsschwelle wie im Koalitionsvertrag der Bundesregierung vorgesehen zu befürworten ist, ist in rechtlicher Hinsicht noch zu prüfen.

II. Einhaltung verfassungsrechtlicher Vorgaben

12. Welche Stellen sind dafür verantwortlich zu gewährleisten, dass die den bremischen Strafverfolgungsbehörden zur Verfügung stehenden Staatstrojaner den verfassungsrechtlichen Vorgaben genügen, indem tatsächlich und nicht etwa nur scheinbar technisch sichergestellt ist, dass
a) an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,
b) die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden,
c) der eingesetzte Staatstrojaner nach dem Stand der Technik gegen unbefugte Nutzung geschützt ist,
d) im Falle der Quellen-TKÜ ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird?

13. Welche Erkenntnisquellen (Quellcodes, Audits, Zertifikate etc.) stehen den zuständigen Stellen zur Verfügung, um prüfen zu können, ob die verfassungsrechtlichen Vorgaben eingehalten werden?

Die Fragen 12 und 13 werden wie folgt gemeinsam beantwortet:
Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung wurden – wie bereits im Rahmen der Frage 2 dargelegt - bislang nicht umgesetzt. Die Frage der Rechtmäßigkeit der eingesetzten Mittel und der Maßnahme kann nicht abstrakt, sondern anhand der Besonderheiten eines jeden Einzelfalles bewertet werden. Ferner ist zu berücksichtigen, dass es sich bei den entsprechenden Programmen nicht um regelmäßig angebotene Produkte handelt, für die anerkannte Qualitätsstandards vorhanden sind. Die Polizei Bremen ist auf die Unterstützung anderer Länder oder des Bundes angewiesen, welche die Maßnahmen für die Polizei Bremen in Amtshilfe umsetzen. Die datenschutzrechtliche Verantwortlichkeit obliegt gemäß § 76f. Bremisches Polizeigesetz der Polizei.

14. Sind die bremischen Sicherheitsbehörden berechtigt, alle vorliegenden Informationen über die ihnen für den Einsatz zur Verfügung stehenden Staatstrojaner an das Gericht bzw. G 10-Kontrollgremium herauszugeben, das für die Anordnung oder rechtliche Überprüfung der Maßnahme zuständig ist?

Die Durchführung von Maßnahmen des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) unterliegt der Kontrolle der Parlamentarischen Kontrollkommission über die Durchführung des Artikel 10-Gesetzes (G 10-Kommission) der Bremischen Bürgerschaft. Sämtliche für diese Kontrolle erforderlichen Informationen sind ihr daher zur Verfügung zu stellen.
Erfolgt eine gerichtliche Überprüfung der Maßnahme, sind die Ermittlungsbehörden verpflichtet, die notwendigen Informationen bzw. das Ergebnis ihrer Prüfung der zum Einsatz kommenden Überwachungstechnik auf Anforderung des Gerichts diesem zukommen zu lassen. In der Umsetzung bestehen zudem Protokollpflichten (§ 100a Abs. 4 StPO und § 100b Abs. 4 i.V.m. § 100a Abs. 6 StPO), um eine Überprüfung der Einhaltung der gesetzlichen Vorgaben zu ermöglichen.
Entsprechend § 1 des bremischen Gesetzes zur Ausführung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldeverkehrs (G 10- Ausführungsgesetz) ist der Senator für Inneres oberste Landesbehörde im Sinne von § 10 Absatz 1 G-10-Gesetzes.

15. Sind die bremischen Sicherheitsbehörden berechtigt, alle vorliegenden Informationen über die ihnen für den Einsatz zur Verfügung stehenden Staatstrojaner an andere öffentliche Stellen herauszugeben, die über die erforderlichen Kompetenzen verfügen, um die Einhaltung der verfassungsrechtlichen Vorgaben überprüfen zu können (z. B. an das Bundesamt für Sicherheit in der Informationstechnik)?
Die Voraussetzungen zur Erteilung von Auskünften aus Strafverfahren und Akteneinsicht an andere nicht am Strafverfahren beteiligte Stellen ergeben sich aus den §§ 474 ff. StPO. Danach können Auskünfte aus Strafverfahren z.B. dann an andere öffentliche Stellen erteilt werden, wenn diesen Stellen in sonstigen Fällen auf Grund einer besonderen Vorschrift von Amts wegen personenbezogene Daten aus Strafverfahren übermittelt werden dürfen oder soweit nach einer Übermittlung von Amts wegen die Übermittlung weiterer personenbezogener Daten zur Aufgabenerfüllung erforderlich ist (§ 474 Abs. 1 Nr. 2 StPO).

16. Geht der von bremischen Strafverfolgungsbehörden veranlasste Einsatz von Staatstrojanern mit Geheimhaltungsverpflichtungen oder -zusagen einher, die geeignet sind, die parlamentarische Kontrolle dieser Einsätze durch die Bürgerschaft einzuschränken? Wenn ja, welche Verpflichtungen oder Zusagen sind dies und wem gegenüber gelten sie?
Besondere Regelungen über die Geheimhaltung der Durchführung von Ermittlungsmaßnahmen im Allgemeinen kennt das Strafverfahrensrecht nicht. Für die jeweiligen Beamten der Strafverfolgungsbehörden greifen die beamtenrechtlichen Verschwiegenheitsverpflichtungen (§ 67 BBG und § 37 BeamtStG), die das Offenbaren dienstlicher Angelegenheiten grundsätzlich nur gestatten, wenn eine entsprechende Genehmigung des Dienstherrn vorliegt.
Geheimhaltungspflichten Dritter – wie etwa von Providern – oder Geheimhaltungszusagen an Dritte im Zusammenhang mit der Vollziehung von Maßnahmen nach § 100a Abs. 1 Sätze 2 und 3 StPO oder § 100b StPO, die über die allgemeinen datenschutzrechtlichen Bestimmungen hinausgehen, sind nicht bekannt. Eine Einschränkung der parlamentarischen Kontrolle ist daher nicht erkennbar.

III. IT-Sicherheit und Schwachstellen

17. Welche potentiellen Schäden für kritische Infrastrukturen, Behörden, Unternehmen, Privathaushalte und Umwelt drohen durch Cyberangriffe mit Schadsoftware, wenn hierbei offene Schwachstellen in weit verbreiteten Betriebssystemen ausgenutzt werden können? Welche durch Ransomware-Attacken bereits entstandenen Schäden für bremische Behörden oder Unternehmen sind dem Senat bekannt?
Für die IT stellt die Ausnutzung von Schwachstellen ein systemimmanentes Risiko dar, dem regelmäßig durch IT-Service-Management-Prozesse und moderne Angriffserkennungen begegnet wird. Die potentiellen Schäden unbekannter – noch nicht geschlossener oder schließbarer Lücken – bei Verwaltung, Wirtschaft und Gesellschaft sind als kritisch anzusehen. Die Verwaltung Bremens war in den vergangenen Jahren einigen ungerichteten Ransomware-Angriffen ausgesetzt, insbesondere durch Emotet, TeslaCrypt, NotPetya, Log4Shell oder auch WannaCry. Befallene Systeme konnten grundsätzlich zeitnah isoliert und die Ausbreitung der Malware eingedämmt werden. Einen größeren Ausfall mussten die norddeutschen Finanzämter im Jahr 2012 durch die Sality Ransomware Emotet bewältigen. Die hier entstandenen finanziellen Aufwände zur Wiederherstellung des Normalbetriebes wurden nicht erfasst.

Alle genutzten Programme, Betriebssysteme oder Anwendungen verfügen über offene Schwachstellen (Exploits / Zero-Day-Exploits). Bekannte Schwachstellen sollten durch die Anbieter schnellstmöglich beseitigt werden und werden auf entsprechenden Seiten (CVE - Common Vulnerabilities and Exposures) öffentlich mitgeteilt. Bei Schwachstellen in entsprechenden IT-Systemen muss grundsätzlich davon ausgegangen werden, dass Schäden entstehen.
Ransomware-Angriffe auf bremische Unternehmen finden seit Jahren statt und beschäftigen unterschiedliche Dienststellen bei der Polizei Bremen. Eine separate Auflistung der bekannt gewordenen Verfahren findet in dem polizeilichen Vorgangsbearbeitungssystem nicht statt. Erkenntnisse bzgl. Angriffe auf bremische Behörden liegen keine vor.

18. Welche Konsequenzen haben deutsche und internationale Sicherheitsbehörden nach Kenntnis des Senats nach den Attacken mit dem sogenannten WannaCry-Trojaner im Hinblick auf die Geheimhaltung von Sicherheitslücken gezogen?
Die Nutzung der Schwachstelle aus dem Microsoft-Betriebssystem war ein Bestandteil aus dem Baukasten der National Security Agency (NSA) und wurde für nachrichtendienstliche Zwecke verwendet, ohne dass Microsoft informiert wurde. Ob die Kenntnis zu der Schwachstelle aus einem Cyberangriff auf die NSA stammt oder eine andere Person/Institution selbst Kenntnis von der Schwachstelle MS17-010 erlangte, wird in diversen Veröffentlichungen unterschiedlich bewertet.
Der Polizei Bremen sind keine der Geheimhaltung unterliegenden Sicherheitslücken bekannt.

19. Wie hoch bewertet der Senat die Gefahr, dass Zielpersonen, die einen Staatstrojaner auf ihrem Gerät entdecken, die Funktionsweise des Staatstrojaners analysieren und für kriminelle Zwecke nutzen, und welche Sicherheitsvorkehrungen bestehen, um dies zu verhindern?
Der Polizei Bremen liegen keine technischen Informationen zu entsprechenden Programmen oder Anwendungen vor. Entsprechend kann dazu keine Aussage getroffen werden.

20. Nutzen die Staatstrojaner, die den bremischen Sicherheitsbehörden zur Verfügung stehen, nach Kenntnis des Senats IT-Schwachstellen aus, welche die Integrität der von vielen Unternehmen und Menschen im Land Bremen verwendeten IT-Produkte bedrohen können, und was unternimmt der Senat, um auf eine Schließung dieser Sicherheitslücken hinzuwirken?
Der Polizei Bremen liegen keine technischen Informationen zu entsprechenden Programmen oder Anwendungen vor. Entsprechend kann dazu keine Aussage getroffen werden.

21. Hält der Senat es für vertretbar, mit Hilfe von Staatstrojanern IT-Sicherheitslücken auszunutzen und diese Schwachstellen gegenüber den betroffenen IT-Herstellern geheim zu halten, obwohl sie mit unabsehbaren Folgen auch von kriminellen Personen ausgenutzt werden könnten?
Rechtliche Befugnisse zur Quellen-Telekommunikationsüberwachung ohne die Möglichkeit, IT-Sicherheitslücken zu nutzen, würden vielfach ins Leere laufen, da ein Zugriff auf moderne Geräte der Telekommunikation auf anderen Wegen oft nicht gelingt. Da gerade im Bereich der organisierten Kriminalität und des Terrorismus immer häufiger Ende-zu-Ende-Verschlüsselun-

gen genutzt werden, um Tat- und Kommunikationsmittel bewusst einem Zugriff durch Strafverfolgungs- und Sicherheitsbehörden zu entziehen, ist die Quellen-Telekommunikationsüberwachung ein wichtiges Instrument für die Sicherheitsbehörden. Dabei sind die vom Bundesverfassungsgericht in seinem Beschluss vom 08.06.2021 aufgestellten Grundsätze und Anforderungen zu berücksichtigen und einzuhalten. 1 (BvR 2771/18).

22. Welche Konsequenzen aus der Entscheidung des Bundesverfassungsgerichts vom 8. Juni 2021 zur staatlichen Nutzung von IT-Sicherheitslücken wurden von den deutschen und den bremischen Sicherheitsbehörden gezogen?
a) Durch welche Stellen ist gegebenenfalls die vom Bundesverfassungsgericht geforderte Abwägung zwischen den Gefahren für die allgemeine IT-Sicherheit, die durch eine von Staatstrojanern ausgenutzte Sicherheitslücke verursacht werden, und dem Nutzen, der durch den Einsatz der Staatstrojaner erzielt werden kann, in Bezug auf die Staatstrojaner, die den bremischen Strafverfolgungsbehörden zur Verfügung stehen, mit welchen Ergebnissen durchgeführt worden?
b) Wurde vor dem Einsatz eines Staatstrojaners durch bremische Sicherheitsbehörden insbesondere eine Datenschutz-Folgenabschätzung gemäß § 67 des Bundesdatenschutzgesetzes durchgeführt bzw. wurde dies nachgeholt, nachdem das Bundesverfassungsgericht in seiner Entscheidung vom 8. Juni 2021 darauf hinwies, dass eine Datenschutz-Folgenabschätzung vor dem Einsatz von Überwachungssoftware im Rahmen einer Quellen-TKÜ zweifellos durchzuführen sei? Wenn ja, welche wesentlichen Ergebnisse sind aus der Datenschutz-Folgenabschätzung und ggf. aus der Anhörung der Landesbeauftragten für Datenschutz und Informationssicherheit hervorgegangen?
Es liegen der Polizei Bremen keine Informationen bzgl. entsprechender Diskussionen oder daraus resultierende Konsequenzen anderer Sicherheitsbehörden vor.
Da seitens der Polizei Bremen keine Maßnahmen der Quellen-TKÜ durchgeführt bzw. angestrebt wurden, wurde auch keine Abwägung unter a) sowie eine Datenschutz-Folgenabschätzung unter b) vorgenommen/erstellt.

23. Welche Maßnahmen werden unternommen, um in deutschen Sicherheitsbehörden und bei den Lieferanten der von ihnen verwendeten Staatstrojaner etwaigen Fehlanreizen entgegenzuwirken, gemeingefährliche Sicherheitslücken nicht den betroffenen Herstellern zu melden, weil sie für den effektiven Einsatz von Staatstrojanern ausgenutzt werden sollen?
Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung wurden – wie bereits im Rahmen der Frage 2 dargelegt - bislang nicht umgesetzt. Entsprechend kam es auch nicht zu einem Einsatz von Software zur Ausnutzung von Sicherheitslücken. Die Frage der Rechtmäßigkeit und spezifischen Gefahren der eingesetzten Mittel, insbesondere der eingesetzten Software und IT kann nicht abstrakt, sondern nur anhand derr Besonderheiten eines jeden Einzelfalles bewertet werden. Ferner ist zu berücksichtigen, dass es sich bei den entsprechenden Programmen nicht um regelmäßig angebotene Produkte handelt, für die anerkannte Qualitätsstandards vorhanden sind. Die datenschutzrechtliche Verantwortlichkeit obliegt gemäß § 76f. Bremisches Polizeigesetz der Polizei.

24. Wie bewertet der Senat die Bedeutung einer sicheren Verschlüsselung von elektronischer Kommunikation für
a) die Pressefreiheit und den Quellenschutz,

b) oppositionelle Kräfte und diskriminierte Minderheiten in Staaten mit politischer Verfolgung,
c) Wirtschaftsunternehmen in Bremen und Bremerhaven?

a) Der Senat sieht die Verschlüsselung von Kommunikationsverbindungen als ein wesentliches der Mittel zum Schutz der Privatsphäre an. Es gibt bestimmte Gruppen, die in besonderem Maße darauf angewiesen sind, dass ihre Kommunikation vertraulich bleibt. Der Senat ist der Auffassung, dass kritischer Journalismus nur möglich ist, wenn sich Bürger:innen vertrauensvoll und offen an Medien wenden können. Er hält es daneben für ebenso wichtig, dass in vielen Bereichen der journalistischen Arbeit auch anonym gearbeitet werden kann; zum Beispiel, wenn Hinweisgeber:innensich vertraulich an Journalist:innen wenden wollen. Dieser Quellenschutz kann im Konflikt zu anderen schützenswerten Rechtsgütern stehen, die Abwägung erfolgt im Rahmen rechtstaatlicher Verfahren.
b) Oppositionelle Kräfte und diskriminierte Minderheiten in Staaten mit politischer Verfolgung sind in besonderem Maße auf die Verschlüsselung von Kommunikationsverbindungen angewiesen, da dort eine fehlende Rechtsstaatlichkeit die offene Verfolgung ihrer Anliegen unmöglich macht.
c) Eine Verschlüsselung wirkt in beide Richtungen – sie kann legitime als auch illegitime Zielefördern, z.B. indem sie Sicherheitseinrichtungen wie Firewalls zu umgehen hilft. Sie muss daher auch immer im Widerstreit mit anderen Schutzzielen gesehen werden.
Die Verschlüsselung der digitalen Kommunikation wird Wirtschaftsunternehmen in Bremen und Bremerhaven im Rahmen von polizeilichen Präventionsvorträgen regelmäßig empfohlen. Insbesondere der unsichere EMail-Verkehr zwischen Unternehmen beinhaltet erhebliche Gefahren und kann unter Umständen zu finanziellen Schäden führen. Die Abwägung zwischen Sicherheit und einfachem Umgang im täglichen Geschäftsverkehr obliegt aber individuell den Unternehmen.

25. Sind die Sicherheitslücken im iOS-Betriebssystem, durch die der Pegasus-Trojaner mit dem bloßen Empfang einer iMessage installiert und aktiviert werden konnte (Zero-Click-Attacke), nach Kenntnis des Senats mittlerweile vollständig geschlossen? Welche Auswirkungen auf die dienstliche Verwendung von iPhones und iPads im Verantwortungsbereich des Senats hat dieser Sachverhalt?
Mobile Endgeräte des Herstellers Apple werden in Bremen und den weiteren Trägerländern des gemeinsamen IT-Dienstleisters Dataport zentral verwaltet. Ein engmaschiges Monitoring der eingesetzten Systeme erfolgt mit einem Mobile Device Management. Updates und Patches werden zeitnah eingepflegt und bei Nichterreichbarkeit der Geräte werden diese mit kurzen Umsetzungsfristen in Isolation verbracht. Ob und wie eine ausnutzbare Schwachstelle mit dem Pegasus-Trojaner zum Einsatz kam, ist nicht bekannt. Die Entscheidung zur Single-Vendor-Strategie – also der Bezug aller Geräte aus der Hand eines Herstellers - im Bereich Smartphones und Tabletts ist hiervon nicht betroffen. Die Verwendung von Apple Geräten wird gegenüber der von Marktbegleitern weiterhin als vorteilhafter eingeschätzt.

IV. Staatstrojaner für den Verfassungsschutz

26. In seinem Urteil vom 15. Dezember 1970 zur Frage, ob der Bundesgesetzgeber zum Erlass des Gesetzes zu Artikel 10 Grundgesetz befugt war, meinte das Bundesverfassungsgericht, die Gesetzgebungskompetenz des Bundes für Regelungen über die Überwachung des Brief-, Post- und Fernmeldeverkehrs durch

Landesverfassungsschutzbehörden ergebe sich aus der Zuständigkeit für das gerichtliche Verfahren (Artikel 74 Absatz 1 Nummer 1), da die Maßnahmen wenigstens mittelbar der Verhinderung, Aufklärung und Verfolgung von Straftaten dienten. Hält der Senat diese Annahme angesichts der späteren Rechtsprechung des Bundesverfassungsgerichts zur Abgrenzung der Gesetzgebungskompetenzen für die Verfolgung von Straftaten einerseits und der Abwehr von Gefahren sowie der Verhütung von Straftaten andererseits noch für tragfähig?
Die Bundesregierung hat zuletzt im Rahmen des Erlasses des Gesetzes zur Anpassung des Verfassungschutzrechts (Gesetz vom 05.07.2021 – BGBl. I 2021 Nr. 40) ausweislich der amtlichen Begründung (BT-Drucksache 19/24785) ihre Gesetzgebungskompetenz zur Änderung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 Gesetz) auf Art. 73 Nr. 10 b), c) Grundgesetz gestützt.

27. Inwieweit ermächtigt die ausschließliche Gesetzgebungskompetenz für die Zusammenarbeit des Bundes und der Länder auf dem Gebiet des Verfassungsschutzes (Artikel 73 Absatz 1 Nummer 10 Buchstabe b des Grundgesetzes) den Bund zur Regelung von Eingriffsbefugnissen der Landesverfassungsschutzbehörden?
Das Grundgesetz (GG) sieht für den Verfassungsschutz eine Zuständigkeit des Bundes und der Länder vor (Art. 70, Art. 73 Abs. 1 Nr. 10 lit. b GG). Der Bund hat hiernach nur die ausschließliche Gesetzgebungskompetenz über „die Zusammenarbeit des Bundes und der Länder […] zum Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes (Verfassungsschutz)“. Diese Zusammenarbeit umfasst nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 133, 277 ff) die laufende gegenseitige Unterrichtung und Auskunftserteilung, die wechselseitige Beratung sowie gegenseitige Unterstützung und Hilfeleistung in den Grenzen der je eigenen Befugnisse und erlaubt funktionelle und organisatorische Verbindungen, gemeinschaftliche Einrichtungen und gemeinsame Informationssysteme. Um eine sinnvolle Zusammenarbeit der Verfassungsschutzbehörden zu gewährleisten, hat der Bundesgesetzgeber u.a. mit der Einführung des Art. 10 Gesetzes und des Bundesverfassungschutzgesetzes von dieser Kompetenz Gebrauch gemacht und den Verfassungsschutzbehörden die dort genannten Aufgaben und Befugnisse zugewiesen.

28. Bestehen nach Ansicht des Senats Zweifel an der Vereinbarkeit der Regelung in § 11 Absatz 1a des Artikel-10-Gesetzes mit der grundgesetzlichen Gesetzkompetenzverteilung zwischen Bund und Ländern? Bitte begründen.
Wie bereits bei Frage 26 dargelegt, hat die Bundesregierung ihre Gesetzgebungskompetenz zur Einführung des § 11 Absatz 1a Art. 10-Gesetz auf Art. 73 Nr. 10 b), c) Grundgesetz gestützt. Diese Bewertung ist nach Einschätzung des Senats rechtlich vertretbar.

29. Inwieweit ist der bremische Landesgesetzgeber berechtigt, die für das Landesamt für Verfassungsschutz nach dem Artikel-10-Gesetz bestehenden Befugnisse zu erweitern, zu konkretisieren, einzuschränken oder aufzuheben, etwa durch eine Änderung von § 8 Absatz 1 Nummer 11 des Bremischen Verfassungsschutzgesetzes?
Bei dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 Gesetz) handelt es sich um ein Bundesgesetz. Für abweichende Landesvorschriften ist daneben grundsätzlich kein Raum, es sei denn das Gesetz selbst ermächtigt den Landesgesetzgeber zu abweichenden Regelungen. Eine solche Ermächtigung an den Landesgesetzgeber sieht §

16 Art. 10-Gesetz lediglich für die Einrichtung einer parlamentarischen Kontrolle in den Ländern vor. Von den in Art. 10-Gesetz vorgesehenen Befugnissen der Verfassungsschutzbehörden kann daher durch den Landesgesetzgeber nicht abgewichen werden.

30. Welche der folgenden bekannten Methoden, um einen Staatstrojaner heimlich auf dem Gerät einer Zielperson zu installieren, darf das Bremer Landesamt für Verfassungsschutz aufgrund der in § 2 Absatz 1a Satz 1 Nummer 4 des Artikel-10-Gesetzes geregelten Pflicht zur Umleitung von Telekommunikation unter welchen Voraussetzungen veranlassen:
a) Manipulation oder Fälschung von Webseiten,
b) Manipulation oder Fälschung von Software-Updates,
c) Manipulation oder Fälschung von SSL/TLS-Zertifikaten,
d) Manipulation oder Fälschung von Software-Signaturen?
§ 2 Absatz 1a Satz 1 Nummer 4 des Artikel-10-Gesetzes verweist für die Voraussetzungen zur Umleitung der Telekommunikation zum Zwecke der Einbringung eines Staatstrojaners auf § 11 Absatz 1 a des Gesetzes. Gemäß § 11 Absatz 1a des Artikel-10-Gesetzes darf die Überwachung und Aufzeichnung der laufenden Telekommunikation, die nach dem Zeitpunkt der Anordnung übertragen worden ist, auch in der Art und Weise erfolgen, dass in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

31. Wie bewertet der Senat die Bedeutung des Vertrauens der Menschen in die Integrität von Sicherheitsupdates, von SSL/TLS-Zertifikaten und von Software-Signaturen für die allgemeine IT-Sicherheit?
Der Sicherheit der eingesetzten IT kommt erhebliche Bedeutung zu. Daher ist die Gewährleistung größtmöglicher IT-Sicherheit ein vorrangiges Ziel staatlicher Einrichtungen. Das Spannungsverhältnis zwischen den mit den Produkten der technischen Überwachung verfolgten Zielen, die dem Schutz überragend wichtiger anderer Rechtsgüter dienen, und dem Ziel der Gewährleistung einer größtmöglichen IT-Sicherheit innerhalb der Spielräume, die der Gesetzgeber offen gelassen hat unter größtmöglichem Schutz für alle betroffenen Rechtsgüter aufzulösen. Dabei sind die vom Bundesverfassungsgericht in seinem Beschluss vom 08.06.2021 aufgestellten Grundsätze und Anforderungen zu berücksichtigen und einzuhalten.

32. Wie bewertet der Senat die Koalitionsvereinbarung von SPD, Grünen und FDP auf Bundesebene, die Eingriffsschwelle für den Einsatz von Überwachungssoftware zur Quellen-TKÜ an die Vorgaben des Bundesverfassungsgerichts für die Online-Durchsuchung anzupassen, den Einsatz also auch für Verfassungsschutzbehörden auf die Abwehr einer mindestens konkretisierten Gefahr im polizeilichen Sinne für ein besonders gewichtiges Rechtsgut zu beschränken?
Für den Bereich des Verfassungsschutzes sieht der Koalitionsvertrag vor, den Einsatz von Überwachungssoftware laufend zu überprüfen. Dabei soll auch überprüft werden, inwieweit es

daher eines Ausbaus der parlamentarischen Kontrolle dieser Maßnahmen bedarf. Dies unterstützt der Senat.

V. Alternativen zu Staatstrojanern

33. Inwieweit nutzen die bremischen Strafverfolgungsbehörden die Möglichkeit, über die Anbieter von Messenger-Apps an Metadaten der verschlüsselten Kommunikation zu gelangen und welche rechtlichen und tatsächlichen Herausforderungen haben sich dabei gezeigt?

Den Strafverfolgungsbehörden liegen keine Erkenntnisse vor, welchem Anbieter welche Art von ermittlungsrelevanten Metadaten vorliegt. Daneben ist auch unbekannt, ob diese Daten möglicherweise einer separaten oder begleitenden Verschlüsselung unterliegen oder überhaupt im Rahmen von damit einhergehenden Rechtshilfeersuchen bei vorhandenen Zustellungsbefugten abgerufen werden können. Unabhängig davon ist darauf hinzuweisen, dass selbst im Falle der Möglichkeit der Abfrage von Metadaten, diesen ein ungleich geringerer Beweiswert als dem von sogenannten Inhaltsdaten zukommt, die mithilfe der Quellen-TKÜ und der Onlinedurchsuchung gesichert werden können.

34. Inwieweit nutzt die Polizei die nach dem Bremischen Polizeigesetz bestehende Möglichkeit, Smartphones sicherzustellen, um zum Zwecke der Gefahrenabwehr Zugriff auf die auf dem Gerät enthaltenen Daten zu erlangen?
Hauptsächlich erfolgen Sicherstellungen/Beschlagnahmen von Smartphones auf strafprozessualer Grundlage. In der Praxis sind seitens des Landeskriminalamts noch keine Sicherstellungen/Beschlagnahmen von Smartphones zur Gefahrenabwehr durchgeführt worden.
Im Bereich der Direktion Einsatz wird diese Möglichkeit im Einzelfall zur Gefahrenabwehr wahrgenommen, um die unzulässige Verbreitung von Bild- und/oder Tonaufnahmen zu verhindern, welche zuvor zulässig aufgenommen wurden.

35. Welche gesetzgeberischen, regulatorischen oder sonstigen Versuche der Einwirkung auf die Hersteller von Betriebssystemen und Messengerdiensten mit dem Ziel, eine Installation von technischen Mitteln zur Ausleitung von Daten auf Geräten einer Zielperson ohne das Ausnutzen von den Herstellern unbekannten Schwachstellen zu ermöglichen, sind dem Senat bekannt?
Seitens der Polizei Bremen sind keine Vorhaben im Sinne der Frage bekannt.

36. Wie bewertet der Senat – im Vergleich zu Staatstrojanern – die Praktikabilität von schonenderen, weil ohne den Einsatz von Staatstrojanern möglichen Methoden der Quellen-Telekommunikationsüberwachung, wie etwa den Zugriff auf die Telekommunikation der Zielperson über Whatsapp Web/Desktop, Telegram Cloud oder Signal Desktop?
Die vermeintliche Praktikabilität wird dadurch eingeschränkt, dass ein manueller Zugriff auf das Gerät gewährleistet werden muss und eine Entdeckungsrisiko der Maßnahme durch den Nutzer jederzeit vorhanden ist.

Bei den in der Frage dargestellten Diensten handelt es sich um Anwendungen, welche über Browser oder separaten Programmen auf dem PC nutzbar sind. Die Kopplung ist für den versierten Nutzer in den Systemen erkennbar und kann entsprechend durch Löschung der Zugangsrechte jederzeit deaktiviert werden. Weiterhin reicht in den meisten Systemen ein einmaliger Neustart aus, um die Kopplung aufzuheben.

37. Wie bewertet der Senat den Vorschlag, die Hersteller von Messenger-Apps und Betriebssystemen zu verpflichten, im Einzelfall auf richterliche Anordnung bestimmten Zielpersonen eine App-Version mit Backdoor oder deaktivierter Verschlüsselung aufzuspielen, um so Zugriff auf die Kommunikation zu erhalten, ohne die Integrität der Verschlüsselung auf anderen Geräten zu beeinträchtigen oder Sicherheitslücken auszunutzen?

Die beschriebene Methode stellt möglicherweise den geringsten Eingriff in die technische Infrastruktur des Geräts dar. Die Hürden im internationalen Rechtsverkehr oder Erreichbarkeit eines Zustellungsbefugten werden hier aber nicht berücksichtigt. Darüber hinausmüssen andere rechtlichen Hürden (wie EuGH, Schrems-II-Urteil aus Sommer 2020 i.V.m. Section 702“ des Foreign Intelligence Surveillance Acts der USA) berücksichtigt werden.

Mit dem "Schrems II"-Urteil erklärte der EuGH den EU-KOM Beschluss (US-Datenexport auf Standarddatenschutzklauseln; KOM Beschluss 2010/87/EU und den EU-KOM Beschluss zum "EU-US-Privacy Shield" als Nachfolgeregelung zu "Safe Harbor") für ungültig, da das US-Recht im Vergleich zum EU-Recht kein im Wesentlichen gleichwertiges Schutzniveau biete. Den US-Sicherheitsbehörden seien unbeschränkte Überwachungsbefugnisse eingeräumt. Den betroffenen Personen hingegen werden keinerlei Garantien für ihre Rechte gewährt. Zudem haben betroffene Nicht-US-Bürger keinerlei gerichtliche Rechtsschutzmöglichkeiten gegenüber den US-Behörden. Das Gericht bezieht sich dabei u. a. auf die US-nachrichtendienstlichen Erhebungsbefugnisse nach Section 702 FISA und Executive Order 12 333. US-Präsident Joe Biden hat am 7. Oktober 2022 ein Dekret unterzeichnet, durch das der Zugang von US-Geheimdiensten zu EU-Daten eingeschränkt und ein Datenprüfungsgericht eingerichtet wird. Es bedarf allerdings noch eines sog. Angemessenheitsbeschlusses auf Seiten der EU, das die KOM vorbereitet, mit dem sie die Gleichwertigkeit des us-amerikanischen Datenschutzes mit unserem bestätigt

Bei der Nutzung us-amerikanischer Messenger und einer damit gekoppelten technischen Hintertür müssen zunächst Daten auf einer us-amerikanischen IT-Struktur gespeichert werden, bevor diese an die anfordernde Stelle abgegeben werden können. Auch wenn diese nur wenige Sekunden dauert, hätten us-amerikanische Dienste Zugriff auf die Daten.

38. Wie bewertet der Senat die am 6. November 2020 erhobene Forderung des EU-Ministerrats, den Anbietern sicherer Kommunikationslösungen die Pflicht aufzuerlegen, Hintertüren für staatliche Stellen einzurichten, insbesondere auch in Bezug auf die Auswirkungen für die allgemeine IT-Sicherheit?

Dem Senat ist keine am 6. November 2020 erhobene Forderung des Rates der Europäischen Union bekannt, den Anbietern sicherer Kommunikationslösungen die Pflicht aufzuerlegen, Hintertüren für staatliche Stellen einzurichten. Soweit sich Frage auf das Ratsdokument 12143/1/20 mit Datum vom 6. November 2020 bezieht, verweist der Senat darauf, dass es sich hierbei um keine offizielle, von den Minister:innen angenommene Entschließung, sondern um ein internes und vorläufiges Arbeitspapier des Rates handelt, das der Senat nicht kommentieren wird.

Der Senat hält die Ende-zu-Ende-Verschlüsselung für wichtig t und möchte sie dort, wo es möglich ist, durch bundesrechtliche Regelungen zum Standard machen möchte. Um eine IT-Sicherheit in der Wirtschaft und Bevölkerung umsetzen zu können, sollten Sicherheitssysteme seines Erachtens daher keine künstlich geschaffenen Zugangsmöglichkeiten beinhalten.

39. Wie bewertet der Senat die in dem Verordnungsentwurf der Europäischen Kommission vom 11. Mai 2022 enthaltene Verpflichtung für Anbieter von Ende-zu-Ende-verschlüsselter Kommunikation (wie Signal, Threema oder WhatsApp), auf Anordnung die unverschlüsselten Kommunikationsinhalte auf dem Gerät auf Abbildungen von Kindesmissbrauch sowie sogenanntes „Grooming“ zu scannen und ggf. an staatliche Behörden auszuleiten?

Mindestens jedes fünftes Kind wird statistisch in der Kindheit Opfer sexueller Gewalt. In einer weltweiten Studie aus dem Jahr 2021 wurde zudem festgestellt, dass mehr als ein Drittel der Befragten im Laufe ihrer Kindheit im Internet zu sexuellen Handlungen aufgefordert worden sind und mehr als die Hälfte der Befragten eine Form des sexuellen Missbrauchs im Internet erlebt hatten. Diese Studienergebnisse sind aus Sicht des Senats alarmierend; auch in Bremen muss eine starke Zunahme von sexuellem Missbrauch von Kindern und Besitz/Verbreitung kinderpornografischer Schriften festgestellt werden. So wurden/werden hier im Zeitraum vom 1. Januar 2021 bis heute 518 Fälle wegen Verbreitung und Besitz kinderpornografischer Schriften geführt. In 15 Fällen liegt dokumentiert der Tatvorwurf des Cybergrooming, also die Kontaktaufnahme zu Kindern zum Zwecke sexueller Anbahnung und schlimmstenfalls des schweren sexuellen Missbrauchs von Kindern, vor.

Kinderpornografische Schriften sind Darstellungen des realen sexuellen Missbrauchs von Kindern, der entweder beendet ist, andauert oder Personen mit entsprechenden Neigungen zu Missbrauch animieren könnte. Das rechtzeitige Erkennen derartiger Darstellungen soll die Verbreitung dieser visualisierten Gewalt verhindern und andauernde oder zukünftige Missbräuche verhindern. Der Gesetzgeber hat die entsprechenden Strafvorschriften nach den Missbrauchsfällen in Lügde und Bergisch-Gladbach (2019) im Juli 2021 deutlich angehoben und bereits den Tatvorwurf des Besitzes/der Verbreitung von Kinderpornografie als Verbrechenstatbestand eingestuft. Auch wenn die Kontaktaufnahmen zu den Missbrauchsopfern in diesen Fällen nach hiesigem Kenntnisstand nicht oder nicht ausschließlich über Cybergrooming erfolgte, muss dennoch angenommen werden, dass die Täter entsprechende Absprachen und Darstellungen dieser Missbräuche und anderweitige kinderpornografische Abbildungen über Messengerdienste verbreitet haben.

gesellschaftliche Missstand wurde durch die Corona-Pandemie zusätzlich verschärft. Das geltende Unionsrecht sieht jedoch bislang lediglich freiwillige Maßnahmen zur Aufdeckung und Meldung durch die Online-Unternehmen vor, wobei selbst diese nur aufgrund der Interimsverordnung VO (EU) 2021/1232 möglich sind, die im August 2024 ausläuft.

Die Europäische Kommission hat daher im Mai 2022 eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern (COM(2022) 209) vorgeschlagen. Danach sieht in Art. 10 für Anbieter von Hostingdiensten oder interpersonellen Kommunikationsdiensten die Pflicht vor, Technologien zu installieren und zu betreiben, um Darstellungen von sexuellem Kindesmissbrauch oder Grooming in einem bestimmten Dienst zu erkennen, soweit eine entsprechende Aufdeckungsanordnung nach Art. 7 vorliegt. Von einer derartigen Aufdeckungsanordnung wäre für eine limitierte Zeit (max. 24 Monate) der gesamte Dienst und damit unterschiedslos alle Nutzerinnen und Nutzer betroffen. Der Verordnungsvorschlag führt dabei im Einzelnen nicht aus, wie genau Anbieter von Hosting- oder interpersoneller Kommunikationsdienste die Suche durchführen sollen. Bei Anbietern von Ende-zu-Ende verschlüsselten Kommunikationsdiensten besteht allerdings das

große Risiko, dass diese entweder Hintertüren in die Verschlüsselung einbauen oder die jeweiligen Inhalte vor dem verschlüsselten Versand auf dem jeweiligen Gerät untersuchen. Beides kann dazu führen, dass der gesamte, über den von der Aufdeckungsanordnung betroffenen Dienst behandelte Inhalt überprüft wird, selbst wenn dieser dem höchstpersönlichen Lebensbereich und/oder besonders geschützten Personengruppen (Ärzt:innen, Anwält:innen, Journalist:innen etc.) zuzuordnen ist.
Der Senat hat daher den entsprechenden Bundesratsbeschluss 337/22 (B) unterstützt, in dem der Bundesrat schwerwiegende grundrechtliche Bedenken gegen die Durchsuchung der privaten Kommunikation erhebt und die Bundesregierung bittet, sich dafür einzusetzen, zur Bekämpfung von sexuellem Missbrauch effektive und zielgerichtete Maßnahmen zu schaffen und gleichzeitig das Recht auf Vertraulichkeit der privaten Kommunikation im höchsten Maße beizubehalten.

40. Wie bewertet der Senat die Forderung des Europäischen Datenschutzbeauftragten nach einem in der gesamten Europäischen Union geltenden Verbot der Entwicklung und des Einsatzes von Ausspähsoftware wie Pegasus sowie die darüber hinaus gehende Forderung von zivilgesellschaftlichen Organisationen, den Vertrieb und Einsatz von Staatstrojaner international zu ächten und zu sanktionieren?
Der Ansatz des Vorschlags ist lobenswert, erscheint jedoch faktisch nichtdurchzusetzen. Eine Vielzahl von Unternehmen weltweit beschäftigt sich mit dem finanziell sehr lohnenswerten Thema und eine Vielzahl von staatlichen Organisationen setzen diese ein. Die Befugnis zum Einsatz von Produkten der informationstechnischen Überwachung ist eine Reaktion auf „die gewandelten Kommunikationsgewohnheiten unter Nutzung modernerTechnik und soll die bestehende „Aufklärungslücke bei Messengerdiensten, die technisch aus dem Speicherplatz des Endgeräts – unverschlüsselt – ausgelesen werden müssen. Diese Befugnisse sind zur Verfolgung von Straftaten insbesondere der organisierten Kriminalität und des internationalen Terrorismus von großer Bedeutung. Eine internationale Ächtung entsprechender technischer Mittel ist vor diesem Hintergrund nicht zu erwarten.
Vielmehr sollte verstärkt in den Schutz, die Aufklärung und in Abwehrmechanismen für die Bevölkerung, Wirtschaft, Behörden und kritische Infrastrukturen investiert werden

Beschlussempfehlung:

Die Bürgerschaft (Landtag) nimmt Kenntnisnahme.