7. August 2018

Stellungnahme an den niedersächsischen Landtag

zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze,

Gesetzentwurf der Fraktion der SPD und der Fraktion der CDU, LT-Drs. 18/850

Constanze Kurz, Jens Kubieziel,

Markus Drenger

1. Einleitung

Diese Stellungnahme zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung widmet sich insbesondere den darin vorgesehenen verdeckten Überwachungsvorhaben, namentlich der Audio- und Videoüberwachung und den beiden Varianten des Staatstrojaners, sowie der elektronischen Fußfessel. Auch andere der geplanten polizeilichen Befugnisse sind kritisch zu sehen, werden hier jedoch nicht betrachtet.

Zu weiteren grundsätzlichen Dilemmata und Risiken für die innere Sicherheit, die mit dem Einsatz von Staatstrojanern einhergehen, verweisen wir auf vorangegangene Stellungnahmen des CCC.[1]

2. Verdeckte Überwachung im öffentlichen Raum

Der Gesetzesvorschlag definiert in § 32 eine Videoüberwachung im öffentlichen Raum. Demnach soll es der Polizei erlaubt werden, bei öffentlichen Versammlungen oder Ansammlungen unter bestimmten Voraussetzungen Bild- und Tonaufzeichnungen anzufertigen. Insbesondere erlaubt der § 32 Abs. 2 auch eine verdeckte Anfertigung von Aufzeichnungen. Dabei scheint sich der Gesetzgeber bessere Ermittlungserfolge oder

---

[1] Stellungnahme des CCC an den Hessischen Landtag, https://www.ccc.de/system/uploads/252/original/CCC-staatstrojaner-hessen.pdf vom 4. Februar 2018, Stellungnahme des CCC an den Bundestag: Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung, https://www.ccc.de/system/uploads/227/original/Stellungnahme_CCC-Staatstrojaner.pdf vom 31. Mai 2017, Stellungnahme des CCC zur „Quellen-TKÜ“, https://www.ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf vom 9. August 2016.

eine Senkung des Kriminalitätsniveaus zu versprechen. Aktuelle Forschung unterstützt diese Annahme allerdings nicht: Das Kriminologische Forschungsinstitut Niedersachsen kommt im Forschungsbericht 143 zu dem Schluss, dass die Effekte von Videoüberwachung im Sinne einer Reduktion von Straßenkriminalität sehr gering ausfielen.[2] Dies ist vergleichbar mit anderen Auswertungen von Videoüberwachungsmaßnahmen im öffentlichen Raum.

Auch fühlt sich die Bevölkerung nach den Forschungsergebnissen des Kriminologischen Forschungsinstituts Niedersachsen weder durch eine offene noch eine verdeckte Videoüberwachung sicherer. Beim subjektiven Sicherheitsgefühl spreche die Auswertung der „Befunde eher gegen eine Erhöhung des subjektiven Sicherheitsgefühls durch die Einführung von Videoüberwachungsmaßnahmen“.[3] Auch nach einer Studie von Bornewasser und Schulz gab es keinen signifikanten Unterschied des Sicherheitsgefühls an Plätzen mit und ohne Videoüberwachung.[4]

Weitere Studien kamen zu ähnlichen Ergebnissen. Die polizeiliche Videoüberwachung bleibt insgesamt ohne maßgeblichen Nutzen zur Prävention, wie in dem Fazit der Studie des Kriminologischen Forschungsinstituts Niedersachsen festgehalten wird. Dieses Ergebnis der Analyse decke sich mit der bisher in der Literatur berichteten Befundlage zur Wirksamkeit der Videobeobachtung im öffentlichen Raum.

---

[2] Vgl. die Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen gemäß § 15a PolG NRW, https://kfn.de/wp-content/uploads/Forschungsberichte/FB_143.pdf

[3] Ebd., S. 12.

[4] Bornewasser, Schulz: Videoüberwachung öffentlicher Straßen und Plätze. Ergebnisse eines Pilotprojektes im Land Brandenburg; 2008; Verlag für Polizeiwissenschaft; Frankfurt/Main.

Diesen Forschungsergebnissen zur Videoüberwachung steht jedoch ein starker Eingriff in die Grundrechte der Betroffenen gegenüber, der wegen der mangelnden Wirksamkeit des Mittels nicht gerechtfertigt ist. Die geplanten Ton- und Videoaufzeichnungen umfassen öffentliche Versammlungen und Ansammlungen. Aufgrund des Charakters solcher Veranstaltungen sind die geplanten Grenzen der erlaubten Aufnahmen äußerst unbestimmt. Es bleibt völlig unklar, welche Personen aufgrund welcher Kriterien aufgezeichnet werden dürfen. Weiterhin gibt es nach dem vorliegenden Gesetzesentwurf für Betroffene keine Möglichkeit, sich rechtliches Gehör zu verschaffen. Es sind keine Pläne ersichtlich, Betroffene über die vorgenommenen (auch verdeckten) Aufnahmen zu informieren. Ohne diese Informationen können Betroffene keinen rechtlichen Schutz in Anspruch nehmen.

Videoüberwachungsmaßnahmen und insbesondere verdeckte Maßnahmen haben eine sehr hohe Eingriffstiefe in die Grundrechte und -freiheiten der Bürgerinnen und Bürger. Daher muss es hierfür hohe Schranken geben, bevor diese eingesetzt werden können. Angesichts der Entwicklungen bei der automatisierten biometrischen Erkennung von Personen birgt die Audio- und Videoüberwachung zudem das Potential, künftig noch stärker in Grundrechte der Betroffenen einzugreifen, und sollte daher nur mit sehr viel mehr Augenmaß und festen, eng gefassten Regeln eingesetzt werden.

Die Vorschriften zur verdeckten Überwachung im öffentlichen Raum sind in Gänze in der vorliegenden Form abzulehnen. Sie stellen einen tiefgreifenden Eingriff in Betroffenenrechte dar, und es gibt keinerlei Ausgleich bei der Kontrolle oder rechtlichen Einhegung dieser Maßnahmen. Insofern kann nur empfohlen werden, die Änderung aus dem Vorschlag zu streichen.

3. Fußfessel

Die elektronische Aufenthaltsüberwachung (§ 17 c), etwa als Fußfessel, einschließlich Begleitmaßnahmen ist für „Gefährder“ geplant, also Menschen, denen keine Straftat oder Vorbereitung einer Straftat vorgeworfen wird. Der Begriff des Gefährders ist dabei nicht ausreichend definiert. Die Einstufung von Menschen als per se gefährliche Personen ist ohnehin ein fragwürdiges Element des Gesetzesentwurfes und unterminiert die Unschuldsvermutung. Nur die Annahme einer Gefahr oder aber ein auffälliges individuelles Verhalten sollen es für einen Betroffenen rechtfertigen, eine elektronische Fußfessel zu tragen. Damit wird in seine Grundrechte auf Freizügigkeit (Art. 11 GG), die Freiheit der Person (Art. 2 Abs. 2 Satz 2 GG) und zudem wegen der Datenerhebung in die informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) eingegriffen.

Für die Abwehr terroristischer Gefahren ist die Fußfessel eine Scheinlösung, deren Wirksamkeit nicht belegt ist. Belegt ist hingegen, dass Attentate trotz getragener Fußfessel bereits verübt wurden.[5] Zudem hat auch bei verurteilten Straftätern eine elektronische Aufenthaltsüberwachung keine Auswirkungen auf die Rückfallquote.[6]

Der ursprünglich vorgesehene, nun gestrichene Satz (ehemals Absatz 3, Nr. 5), dass die Fußfessel-Daten „gegen unbefugte Kenntnisnahme besonders zu sichern“ seien, ist keineswegs entbehrlich. Natürlich sind (Geo-)Daten bei der Übermittlung und Speicherung vor unbefugter Kenntnisnahme zu schützen. Die Betroffenen tragen

---

[5] So im Juli 2016 in Frankreich: IS-Anhänger gelang Anschlag in Kirche trotz Fußfessel, https://www.welt.de/politik/ausland/article157318999/IS-Anhaenger-gelang-Anschlag-in-Kirche-trotz-Fussfessel.html vom 27. Juli 2016.

[6] Vgl. Max-Planck-Institut für ausländisches und internationales Strafrecht, https://www.mpg.de/11984921/fussfessel-rueckfallquote vom 26. März 2018.

schließlich ein permanent Daten aussendendes Überwachungsgerät am Bein, das ihre Aufenthaltsinformationen erfasst. Sofern die geplante Norm bestehen bleibt, ist die besondere Sicherung dieser sensiblen Daten explizit vorzusehen.

4. Staatstrojaner

4.1 Evaluierung

Die „Quellen-TKÜ“ (§ 33 a Abs. 2) und die „Online-Durchsuchung“ (§ 33 d) sollen nach dem Gesetz „bis zum Ende 2023 unter Mitwirkung einer oder eines Sachverständigen durch die Landesregierung evaluiert werden“. Der niedersächsische Landtag sei über „das Ergebnis der Evaluierung von der Landesregierung zeitnah zu unterrichten“. Diese Regelung soll der Tatsache Rechnung tragen, dass es sich um schwerwiegende Grundrechtseingriffe für die Betroffenen handelt, allerdings die „Wirksamkeit zur Gefahrenabwehr noch nicht ausreichend belegt“ ist.

Jedoch ist die vorgesehene Evaluierungsphase mit fünf Jahren exorbitant lang ausgelegt. Schon aufgrund der kurzen Innovationszyklen bei informationstechnischen Geräten und Infektionswegen in deren Software sollte eine Evaluation der Einsatzwirksamkeit innerhalb eines Jahres durch einen unabhängigen Sachverständigen erfolgen. Die explizite Forderung nach der Unabhängigkeit des Sachverständigen fehlt im vorliegenden Gesetzesvorschlag. Die Evaluierung sollte zudem unter wissenschaftlichen Kriterien stattfinden und nicht nur dem Landtag, sondern der Öffentlichkeit zugänglich sein.

4.2 Qualitätssicherung der Trojaner

Besonderes Augenmerk ist auf die Qualität der Systeme zur „Quellen-TKÜ“ und „Online-Durchsuchung“ zu legen, um die Risiken begrenzen, die mit der Infiltration der Zielsysteme unweigerlich verbunden sind. Sollten diese durch den vorliegenden Entwurf gesetzlich kodifiziert werden und zum Einsatz kommen, stellt dies einen tiefgehenden Grundrechtseingriff dar. Daher muss die Software und auch gegebenenfalls die Hardware höchsten Qualitätsanforderungen an die Software-Entwicklung im Allgemeinen und an die IT-Sicherheit im Speziellen genügen.

Vor der Entwicklung und dem eigentlichen Einsatz sind die Anforderungen an das System zu spezifizieren. Diese Spezifikation soll insbesondere dem niedersächsischen Landesbeauftragten für den Datenschutz zur Prüfung vorgelegt werden. Weiterhin ist es empfehlenswert, Fachpersonal für IT-Sicherheit einzubinden, um vor allem Verschlüsselungsverfahren und Nachladefunktionen sowie die Authentifizierungsverfahren für die Fernsteuerung zu prüfen.

Mindestens eine Typmusterprüfung ist gegenüber der Datenschutzbehörde offenzulegen. Zudem ist auch der Quellcode der Datenschutzaufsichtsbehörde vor dem Einsatz zur Prüfung vorzulegen. Der Quellcode muss weiterhin von mindestens einer unabhängigen fachkundigen Person geprüft werden. Das Ergebnis dieser Prüfung ist schriftlich zu dokumentieren und ebenso bei den Datenschutzaufsichtsbehörden einzureichen.

Eine vollständig offengelegte und nachvollziehbar geprüfte Software ist Voraussetzung für den späteren Beweiswert der ausgeleiteten Daten (Manipulationsschutz). Dazu fehlen im Gesetzesentwurf auch konkrete Vorgaben zu den vorgeschriebenen Protokollierungspflichten beim Staatstrojanereinsatz.

4.3 Zusammenarbeit mit kommerziellen Anbietern

Im Gesetzentwurf fehlen Anforderungen an Hersteller und kommerzielle Anbieter der Software zur „Quellen-TKÜ“ und zur „Online-Durchsuchung“, die eine Zusammenarbeit bei der technischen Überwachung regeln würden. Anforderungen an Staatstrojaner-Partnerfirmen sollen durch eine Rechtsvorschrift definiert werden. Anbieter von Staatstrojaner-Software müssen insbesondere in Hinblick auf ihre Fachkompetenz und ihre Vertrauenswürdigkeit geprüft werden. Eine Sicherheitsüberprüfung der dort Beschäftigten ist bisher nicht vorgesehen, auch keine Prüfung hinsichtlich weiterer Mindeststandards, die an solche kommerziellen Partnerfirmen zu stellen sind. Firmen, bei denen eine Zusammenarbeit mit repressiven Regimen im Ausland bekannt ist oder befürchtet werden muss, sollen als Partner explizit ausgeschlossen werden.

Niedersachsen darf nicht den Weg gehen, der bei den Trojanern des BKA in die fatale Situation geführt hat, dass kommerzielle Partnerunternehmen namentlich nicht bekannt sind, faktisch keinerlei Kontrolle unterliegen und zudem die Behörden quasi erpressen könnten. Der Leiter des Kompetenzzentrums Informationstechnische Überwachung (CC ITÜ) beim BKA, Helmut Ujen, fasste die missliche Situation gegenüber Partnerfirmen so zusammen: „Die verbliebenen [Anbieter] haben uns sehr deutlich gemacht, dass es von deren Seite keinerlei Publikation zur Zusammenarbeit

gibt, und wenn es die von unserer Seite gibt, gibt keinerlei Geschäftsbeziehung zu diesen Firmen.“[7]

Die parlamentarische, aber auch die richterliche Kontrolle laufen auf inakzeptable Weise ins Nichts, wenn der Anbieter des Staatstrojaners nicht einmal mit seinem Firmennamen genannt wird, geschweige denn mit Details dazu, wie er die technischen und rechtlichen Anforderungen des Staatstrojaners tatsächlich umsetzt. Diese Situation muss in Niedersachsen per Gesetz vermieden werden, indem übermäßige Geheimhaltung bei den Anbietern unterbunden und eine Kontrolle damit überhaupt ermöglicht wird. Unterlagen zum technischen Vorgehen und zu den Verträgen zwischen Dienstleistern und Behörden sollen dem Parlament und den prüfenden Richtern zugänglich gemacht werden. Dabei sind neben der erforderlichen Prüfung durch den Landesdatenschutzbeauftragten auch dem Parlament wirtschaftliche Parameter und der grundlegende Funktionsumfang zu nennen.

Wenn die Anbieter unter solchen gesetzlichen Regeln nicht mit den Behörden zusammenarbeiten wollen, dann ist auf einen Vertragsschluss zu verzichten. Die in Deutschland entwickelte Software für Staatstrojaner (Remote Communication Interception Software (RCIS)) hat bisher knapp sechs Millionen Euro gekostet, inklusive der Prüfung durch den TÜV Essen.[8] Angesichts dieser hohen Kosten scheint es ohnehin fragwürdig, warum bei kommerziellen Anbietern zugekauft werden sollte und ob dadurch bessere polizeiliche Einsatzkonzepte überhaupt erreicht werden könnten. Angesichts

---

[7] Vgl. Andre Meister: Geheime Sitzung im Bundestag: Regierung verweigert jede Auskunft über Staatstrojaner-Firmen, https://netzpolitik.org/2018/geheime-sitzung-im-bundestag-regierung-verweigert-jede-auskunft-ueber-staatstrojaner-firmen/ vom 12. Juli 2018.

[8] In Höhe von 186.185,20 Euro.

dieser Summen ist es auch unverständlich, warum nicht zuerst naheliegende anderweitige Möglichkeiten, um an die gewünschten Inhalte zu gelangen, ernsthaft geprüft werden.

4.4 Kernbereichsschutz

Der Kernbereich der privaten Lebensgestaltung beschreibt die höchstpersönliche Sphäre eines Menschen. Der Schutz dieses Bereichs ist Teil des Schutzes der Menschenwürde und darf nicht mit der Ausrede einer technischen Nicht-Machbarkeit oder gar einer besseren Praxistauglichkeit eines Trojaners zur Disposition gestellt werden. Das grundsätzliche Erhebungsverbot aus dem Kernbereich darf nicht wegen technischer Unzulänglichkeiten verwässert werden.

Im Urteil zum BKA-Gesetz wurde das erneut betont: Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung „sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen.“[9] Das Urteil zum BKAG führt außerdem aus, „dass eine Kommunikation über Höchstvertrauliches nicht schon deshalb aus dem strikt zu schützenden Kernbereich herausfällt, weil sich in ihr höchstvertrauliche mit alltäglichen Informationen vermischen“.[10] Dem trägt der vorliegende Gesetzesentwurf nicht ausreichend Rechnung.

---

[9] BVerfG-Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html Rn. 120.

[10] Ebd. Rn. 222.

Für den Schutz des Kernbereichs privater Lebensgestaltung fehlen im Gesetzesentwurf klare Regelungen, die diesem Urteil gerecht werden. Das betrifft insbesondere den § 31 b (2). Darin heißt es: „Wenn sich während einer bereits laufenden Datenerhebung tatsächliche Anhaltspunkte dafür ergeben, dass Daten aus dem Kernbereich privater Lebensgestaltung erhoben werden, ist die Datenerhebung unverzüglich und so lange wie erforderlich zu unterbrechen, soweit dies informationstechnisch möglich ist und dadurch die Datenerhebung dem Betroffenen nicht bekannt wird."

Hier soll offenbar der Tatsache Rechnung getragen werden, dass bei Staatstrojanern – anders als bei der Telekommunikationsüberwachung auf dem Leitungsweg – eine Unterbrechung der Aufzeichnung technisch nicht immer möglich sein wird. Schließlich befindet sich das informationstechnische Gerät in der Hoheit des Besitzers, der zu jeder Zeit absichtlich oder unbemerkt Änderungen an seinem Computer vornehmen kann, die sich auf die darauf heimlich installierte Software und deren Basismodule auswirken. So kann es beispielsweise der Fall sein, dass der Spionagesoftware zum Zeitpunkt der Erfassung kernbereichsrelevanter Daten keine Steuerungsbefehle gesendet und damit die Aufzeichnung nicht unterbrochen werden kann.

Für den Einsatz eines Staatstrojaners als „Online-Durchsuchung", der auch Inhalte des informationstechnischen Geräts jenseits von Kommunikation ausleiten darf, ist die geplante Regelung in § 31 b (2) nicht hinreichend. Werden etwa ganze Ordner einer Festplatte ausgeleitet, ist die Abschätzung, ob kernbereichsrelevante Inhalte darunter sind, nicht mit Sicherheit vorab festzustellen. Auch bei einem Staatstrojaner, der als eine

„Quellen-TKÜ“ fungieren soll, kann das Problem auftreten, dass bereits gespeicherte Kommunikation ausgeleitet wird, deren Inhalt jedoch kernbereichsrelevant ist.

Um im Falle des Vorkommens von Kernbereichseingriffen und auch für die generelle Rechtssicherheit der heimlichen Spionagesoftware eine Nachvollziehbarkeit des Vorgehens zu erreichen, sind Herkunft, Integrität und Authentizität aller damit ausgeleiteten Daten zu protokollieren. Ebenso muss ein lückenloser Nachweis ab der Erhebung von Daten bei der berechtigten Stelle erfolgen und dadurch zweifelsfrei nachvollzogen werden können.

4.5 Schutz vor Gefahren für Leben und Gesundheit von Menschen

Im Gesetzentwurf fehlen Schranken für die „Quellen-TKÜ“ und die „Online-Durchsuchung“, die begrenzen, in welche informationstechnischen Systeme ein Trojaner eingebracht werden darf. Die Infiltrationsmöglichkeiten, die per Gesetz erlaubt werden sollen, sind konkret zu benennen. Das soll vermeiden, dass in informationstechnische Systeme eingegriffen wird, deren Funktionsunterbrechung oder anderweitiges fehlerhaftes Funktionieren das Leben oder die Gesundheit von Menschen bedroht. Zu denken ist hier etwa an Fahrzeuge oder Medizinalgeräte, deren Infektion mit Spionagesoftware eine (auch unbeabsichtigte) Gefahr darstellen.

Die Befugnis im Gesetzesentwurf, Schadsoftware in sämtlichen vorstellbaren informationstechnischen Systemen anzuwenden, ist zu weitgehend. Daher sollte die Regelung auf persönliche Kommunikationsgeräte begrenzt werden. Medizinische Geräte, etwa auch Implantate oder Prothesen, oder informationstechnische Systeme, in

denen Menschen sitzen oder mit denen sie zusammenarbeiten, etwa Roboter oder Fahrzeug, sind auszunehmen. Fehlfunktionen, wie sie bei jeder Software zu erwarten sind, dürfen Leib und Leben der Betroffenen, aber auch von Dritten nicht gefährden.

Die Regelung zur „Online-Durchsuchung“ beinhaltet keinen ausreichenden Schutz für Dritte, die von der Maßnahme mitbetroffen sind. Die Regelung sieht vor, dass auch informationstechnische Systeme von Dritten infiltriert werden dürfen, sofern die Zielperson diese Systeme ebenfalls nutzt. Hierbei kann es neben den Risiken für das informationstechnische System selbst auch zur Offenlegung vieler weiterer schützenswerter Daten und Informationen Dritter kommen, etwa Zugangsdaten, Passwörter, Kommunikation von Berufsgeheimnisträgern sowie Daten aus dem Kernbereich privater Lebensgestaltung. Da eine solche Fähigkeit besondere Begehrlichkeiten weckt, muss es explizite Regelungen zum Schutz vor Missbrauch der Technik geben, sowohl durch Innentäter[11] als auch durch Externe. Die Gefahren für Leben und Gesundheit müssen auch ausgeschlossen werden, wenn sie durch Externe drohen.

4.6 „Quellen-TKÜ“

Die Gleichsetzung der Eingriffsvoraussetzungen einer TKÜ und einer „Quellen-TKÜ“ (in § 33 a) konterkariert den Charakter der Maßnahme, da ein Staatstrojaner eine weit höhere Eingriffsintensität hat. Die Polizei muss für die „Quellen-TKÜ“ einen Trojaner auf dem Endgerät plazieren, um die Kommunikation mitlesen zu können. Während eine

[11] Das Beispiel des Missbrauchs bei der Bundespolizei im Jahr 2012, als ein einzelner Beamter einen Trojaner gegen seine Tochter einsetzte und dies zur Kompromittierung der PATRAS-Dienste führte, zeigt, dass Innentäter nicht zu unterschätzen sind: Vater-Tochter-Streit löst Angriff auf Bundespolizei aus, https://www.golem.de/1201/88870.html vom 8. Januar 2012.

TKÜ unter Einschaltung des Providers in das Fernmeldegeheimnis nach Art. 10 GG eingreift, betrifft die „Quellen-TKÜ“ also das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[12]

Entsprechend muss ein verstärkter, nicht nur floskelhafter Schutz der Betroffenen vorgesehen werden. Das gilt unabhängig davon, ob es sich um zugekaufte Software oder um Eigenentwicklungen handelt. Staatstrojaner sollten überhaupt nur bei besonderer Gefahr für Leib, Leben und Gesundheit eingesetzt werden dürfen, auch in der Variante, die als „Quellen-TKÜ“ firmiert.

Die Beantwortung der Frage, wie eine Spionagesoftware in Form einer „Quellen-TKÜ“, etwa zum Abhören von Internettelefonaten, präzise von einer „Online-Durchsuchung“ abgegrenzt werden könnte, ist nicht trivial. Nach § 33 a (Datenerhebung durch Überwachung der Telekommunikation) können bei der „Quellen-TKÜ“ nach Abs. 4, Nr. 1 auch „die Inhalte der Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte“ erhoben werden.

Im Gesetz sollte klar festgeschrieben werden, dass die zur „Quellen-TKÜ“ erforderliche Software so beschaffen ist, dass tatsächlich nur Daten des laufenden Telekommunikationsvorgangs erfasst werden können und explizit keine Informationen aus zurückliegenden Gesprächen oder Protokolldaten früherer oder noch nicht versendeter Kommunikation. Das wären beispielsweise E-Mails oder Messenger-Nachrichten, die auf dem Rechner des Betroffenen geschrieben, aber (noch) nicht versendet wurden. Sie sind schon deshalb keine „Telekommunikationsinhalte“, da noch gar keine

[12] BVerfG-Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07.

Kommunikation stattgefunden hat, sondern die Daten vor einem etwaigen Vorgang der Versendung nur auf dem informationstechnischen System selbst gespeichert sind. Der Zugriff auf die auf den überwachten Endgeräten gespeicherten Daten soll aber bei einer „Quellen-TKÜ“ nicht geschehen, dies unterscheidet sie ja gerade von einer „Online-Durchsuchung“.

Fiele diese Unterscheidung weg, müsste die „Quellen-TKÜ“ nicht mehr nur am Artikel 10 GG, sondern zusätzlich am Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit des informationstechnischen Systems zu messen sein. Im BVerfG-Urteil wird die Bedingung des „laufenden Telekommunikationsvorgangs“ gestellt:
„Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung‘, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.“[13]

Gespeicherte Kommunikation oder andere Daten aus dem ausspionierten Programm sind jedoch keine laufende Kommunikation. Entfällt die Beschränkung auf „laufende Telekommunikationsvorgänge“, ist die Unterscheidung zwischen „Quellen-TKÜ“ und „Online-Durchsuchung“ hinfällig und beide Maßnahmen am Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen zu orientieren.

---

[13] BVerfG-Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07, Rn. 190.

Gleichzeitig ist eine technische Umsetzung der „Quellen-TKÜ“, bei der ausschließlich laufende Kommunikation überwacht werden soll, nahezu ausgeschlossen. Dies würde aufwendige Analysen und Veränderungen im Programmablauf der überwachten Applikationen wie etwa Messengern bedeuten. Daher handelt es sich bei der Regelung zur „Quellen-TKÜ“ im Grundsatz um eine Ermächtigungsgrundlage auf Vorrat, da eine zeitnahe rechtskonforme Umsetzung technisch derzeit nicht als möglich erscheint.

5. Fazit

Der vorliegende Gesetzesentwurf räumt den Polizeibehörden umfassende Möglichkeiten ein, in die Grundrechte der Bürgerinnen und Bürger einzugreifen. Dabei wird dem Schutz dieser Grundrechte zu wenig Raum gegeben. Die geplanten Normen zur Audio- und Videoüberwachung sowie zur Fußfessel sind besonders kritisch zu sehen, zumal ihre Wirksamkeit nicht belegt ist.

Die Regelungen zum Staatstrojaner sind wegen der absehbaren hohen Risiken technischer Art aus dem Gesetzesentwurf zu streichen. Dies ist auch deshalb anzuraten, da der besonders geschützte Kernbereich der privaten Lebensgestaltung bei Betroffenen, aber auch bei unbeteiligten Dritten nicht ausreichend Berücksichtigung gefunden hat. Dies gilt sowohl für die „Online-Durchsuchung“ als auch für die „Quellen-TKÜ“.