Viel Freiheitsverlust für wenig Sicherheit?

Quellen-Telekommunikationsüberwachung und Onlinedurchsuchung auf dem Prüfstand. *Von Stefan Brink und Lena Mitsdörffer*

zuRechtgerückt
Communicatio Socialis

Am 15. November 2017 hat der Landtag von Baden-Württemberg ein neues Polizeigesetz (PolG BW) beschlossen. Mit diesem wird in Baden-Württemberg erstmals auf Landesebene die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) eingeführt (vgl. § 23b Abs. 2 PolG BW). Damit schließt sich das Land einer schon auf Bundesebene angelegten Tendenz zur Ausweitung der Überwachungsbefugnisse der Sicherheitsbehörden an, die mit einem gravierenden Eingriff in informationstechnische Systeme einhergeht: Für den präventiven Bereich finden sich seit dem Jahr 2008 Befugnisse zur Quellen-TKÜ und Onlinedurchsuchung in §§ 20 l Abs. 2 und § 20 k Abs. 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG). Beide Vorschriften sind nach dem Urteil des Bundesverfassungsgerichts zum BKAG (vgl. BVerfG, Urteil vom 20.4.2016) zwar nicht mit dem Grundgesetz vereinbar, gelten jedoch bis zu einer Neuregelung, längstens bis zum 30. Juni 2018, fort. Für den repressiven Bereich sehen §§ 100a Abs. 1 S. 2 und 100b Abs. 1 der Strafprozessordnung (StPO) nun seit August 2017 ähnliche Befugnisse vor.

Das PolG BW orientiert sich dabei in wesentlichen Bereichen am BKAG im Lichte der hierzu ergangenen Entscheidung des BVerfG. Dies ist insofern problematisch, als auch die Entscheidung des BVerfGs im Hinblick auf die Vorgaben zum Kernbereichsschutz und die technische Umsetzung und Abgrenzung

Dr. Stefan Brink ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württembergs (LfDI BW).

Lena Mitsdörffer ist die persönliche Referentin des Landesbeauftragten.

Communicatio Socialis (1/2018) 51: 60-67. DOI: 10.5771/0010-3497-2018-1-60

der einzelnen Maßnahmen durchaus kritisch zu bewerten ist. Gerade am Beispiel der Quellen-TKÜ und der Onlineüberwachung wird deutlich, dass ein potentielles „Mehr" an Sicherheit gravierende Folgen für die Freiheit aller haben kann.

Um dies aufzuzeigen, werden die Maßnahmen der Quellen-TKÜ und der Onlinedurchsuchung, die wesentlichen verfassungsgerichtlichen Maßstäbe vorgestellt, sowie die hier maßgeblichen Urteile des BVerfGs und die gesetzlichen Ermächtigungen, insbesondere das neue PolG BW, kritisch gewürdigt.

Quellen-TKÜ und Onlinedurchsuchung[1]

Sowohl die Quellen-TKÜ als auch die Onlinedurchsuchung setzen auf der Ebene der Endgeräte an. Grund ist die inzwischen durch viele Anwendungen wie WhatsApp oder Skype umgesetzte Ende-zu-Ende-Verschlüsselung der Kommunikation, die einem Abfangen der Inhalte auf dem Weg zwischen den Kommunikatoren entgegensteht. Finden Sicherheitsbehörden keinen Weg, die Verschlüsselung selbst zu dekodieren – was angesichts der heutigen Verschlüsselungsstandards regelmäßig zu erwarten steht – bleibt ihnen nur der Weg, an die Quelle bzw. den Empfangsort der Nachrichten zu gehen und letztere im unverschlüsselten Stadium abzufangen. Dies kann etwa über ein Belauschen über das interne Mikrofon des Geräts (etwa bei einer Skype-Unterhaltung) oder auch mittels des Erstellens von Screenshots (z. B. zur Anzeige von WhatsApp-Chats) erfolgen. Die Quellen-TKÜ ist dabei in den rechtlichen Ermächtigungsgrundlagen begrenzt auf die Überwachung der laufenden Kommunikation[2], während der Begriff der Onlinedurchsuchung weiter gefasst ist. Er beschreibt die Suche nach und den Zugriff auf beliebige Daten auf dem Endgerät, seien es Dokumente, Videos, E-Mails oder eben auch die laufende Kommunikation, also den Zugriff auf das Gerät selbst (vgl. § 20k Abs. 1 BKAG, § 100b Abs. 1 StPO). Die Notwendigkeit des Eingriffes zur Überwachung und Aufzeich-

1 *Für hilfreiche Erläuterungen zu den technischen Grundlagen danken wir Alvar Freude, Referent für technisch-organisatorischen Datenschutz und Datensicherheit beim LfDI BW.*

2 *§ 23b Abs. 2 Nr. 1 PolG BW, § 20l Abs. 2 Nr. 1 BKAG, nur bedingt bei § 100a Abs. 1 S. 2 StPO – hier darf auch auf gespeicherte Inhalte zugegriffen werden, wenn dies auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz zulässig gewesen wäre, vgl. § 100a Abs. 1 S. 3 StPO. Dies ist technisch sicher zu stellen, § 100a Abs. 5 Nr. 1 StPO.*

nung der Telekommunikation gerade auch in unverschlüsselter Form wird dabei zur Bedingung für den Eingriff gemacht.[3]

Verfassungsgerichtliche Maßstäbe

Wird im Wege der Quellen-TKÜ auf die laufende Kommunikation zugegriffen, so stellt dies einen Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 Grundgesetz (GG) dar. Das Fernmeldegeheimnis schützt die Vertraulichkeit individueller, unkörperlicher Kommunikation auf Distanz, und zwar sowohl ihren Inhalt selbst, als auch ihre äußeren Umstände, also die Verbindungsdaten (vgl. Durner in: Maunz/Dürig 2016, Art. 10 Rn. 81 ff., 57. EGL 2010).

Die Onlinedurchsuchung greift dagegen in das vom BVerfG aus dem allgemeinen Persönlichkeitsrecht (vgl. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein (vgl. BVerG, Urteil vom 27.2.2008). Dieses geht über den Schutz, den das Recht auf informationelle Selbstbestimmung für persönliche Daten bietet, hinaus, indem es nicht nur die einzelne Datenerhebung, sondern auch das zu ihrer Verarbeitung genutzte System als Ganzes vor Zugriff und Veränderung schützt.

Aufgrund ihrer Heimlichkeit, der Möglichkeit, Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten, und der Streubreite der Eingriffe, handelt es sich bei den infrage stehenden Maßnahmen um sehr intensive Eingriffe in die beschriebenen Grundrechte, denen durch geeignete Verfahrensvorkehrungen Rechnung getragen werden muss.[4]

Rechtliche Würdigung

Aus grund- und datenschutzrechtlicher Sicht stellen sich die gesetzlichen Ermächtigungen auf Bundes- und Landesebene zur Online-Durchsuchung bzw. Quellen-TKÜ als problematisch dar. Zwar hat sich insbesondere der Landesgesetzgeber Baden-Württemberg bei der Normgebung stark an der Rechtsprechung des BVerfG zu orientieren versucht, trifft aber bereits nicht

3 *vgl. § 23b Abs. 2 Nr. 2 PolG BW, § 20l Abs. 2 Nr. 2 BKAG, § 100a Abs. 1 S. 2 StPO*

4 *BVerfG – Onlinedurchsuchung, Rn. 203, 231 f., 257, 297; BVerfG – BKAG, Leitsatz 1b, Rn. 92, 105, 117, 119, 134 ff., 217 f., 237 f.*

den Ausnahmecharakter der infrage stehenden Maßnahmen (1.). Zudem kann auch die verfassungsgerichtliche Rechtsprechung, insbesondere die Entscheidung des BVerfG zum BKAG, nicht vollständig überzeugen, da sie zu wenig die technischen Gegebenheiten in den Blick nimmt und einen echten Kernbereichsschutz der Sicherheitsdoktrin opfert (2.). Dies wird durch die einfachgesetzliche Ausgestaltung perpetuiert, sodass es zu hohen Kollateralschäden bei gleichzeitig zweifelhaftem Nutzen kommen kann und wird.

(1.) Mithilfe der Quellen-TKÜ und umso mehr der Onlinedurchsuchung wird tief in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen. Das PolG BW enthält zwar, wie das BKAG und die StPO auch, eine Vielzahl der vom BVerfG formulierten verfahrensrechtlichen Sicherungen. So erlaubt es nur solche technischen Veränderungen am informationstechnischen System, die für die Datenerhebung unerlässlich sind[5], enthält Vorschriften zum Schutz der kopierten Daten gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme[6] und zum Schutz des Kernbereichs privater Lebensgestaltung[7]. Auch sind grundsätzlich eine Unterrichtung der betroffenen Personen[8] und die Anordnung der Maßnahme durch ein Gericht vorgesehen[9]. Schließlich ist die Datenerhebung zu protokollieren und sind die Protokolldaten für datenschutzrechtliche Kontrollen[10] aufzubewahren. Das PolG BW sieht diesbezüglich auch die Kontrollpflicht des LfDI vor (§ 23b Abs. 13 PolG BW). Mit diesen Verfahrensbestimmungen hat sich der Landesgesetzgeber – schon ausweislich der Gesetzesbegründung (vgl. LT-Drs. 16/2741 vom

Das PolG BW erlaubt nur technische Veränderungen am informationstechnischen System, die für die Datenerhebung unerlässlich sind.

5 *vgl. § 23b Abs. 3 S. 1 Nr. 1 PolG, § 20k Abs. 2 S. 1 Nr. 1 BKAG, § 20l Abs. 2 S.2 BKAG, § 100a Abs. 5 Nr. 2 und 3 StPO, 100b Abs. 4 StPO.*

6 *vgl. § 23b Abs. 3 S. 2 PolG, 20k Abs. 2 S. 2 BKAG, § 20l Abs. 2 S. 2 BKAG, § 100a Abs. 5 S. 2 und 3 StPO, § 100b Abs. 4 StPO.*

7 *vgl. § 23b Abs. 9 PolG BW, § 20k Abs. 7 BKAG, § 20l Abs. 6 BKAG, 100d StPO.*

8 *vgl. § 23b Abs. 10 PolG BW, § 20w Abs. 1 Nr. 6 und 7 BKAG, § 101 Abs. 4 StPO.*

9 *vgl. § 23b Abs. 4 und 7 PolG BW, § 20k Abs. 5 BKAG, § 20l Abs. 3 BKAG, § 100e StPO.*

10 *vgl. § 23b Abs. 11 und Abs. 9 S. 11 ff. PolG BW, § 20k Abs. 3 PolG BW, 20l Abs. 2 S. 2 BKAG, § 100a Abs. 6 StPO.*

26.9.2017, S. 21 und 30 f.) – maßgeblich an der Entscheidung des BVerfGs zum BKAG orientiert, ohne jedoch selbst einen angemessenen Ausgleich der betroffenen Rechtsgüter herzustellen. Erst nach z. T. harscher Kritik in der Anhörung zum Gesetzgebungsverfahren u. a. durch den LfDI BW wurden noch rasche Anpassungen vorgenommen:

So eröffnet der Tatbestand des § 23b Abs. 1 Nr. 1 PolG BW die Quellen-TKÜ nicht mehr nur zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, sondern macht auch die Erheblichkeit der Gefahr zur Voraussetzung. Außerdem wird nicht mehr nur auf eine Gefahr für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, abgestellt, sondern auf wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Das PolG BW begrenzt die neue Befugnis zur Quellen-TKÜ jedoch nicht auf die Abwehr terroristischer und extremistischer Anschläge, wie der deutlich in diese Richtung „eingefärbte" allgemeine Teil der Gesetzesbegründung (vgl. ebd., S. 20) suggeriert. Insofern geht das Gesetz weit über die präventiven Befugnisse des maßstäblichen BKAG hinaus, da diese ausschließlich im Zusammenhang mit der Abwehr von Gefahren des internationalen Terrorismus bestehen. Damit wird die Quellen-TKÜ gleichsam in den Kanon der Standardmaßnahmen der Polizeiarbeit aufgenommen und dadurch das Verhältnis von Eingriffsintensität und Schutzgut grundlegend infrage gestellt. Lediglich bei den Schutzgütern von § 23 Abs. 1 Nr. 2 und 3 PolG BW werden ähnlich existenzielle Gefahren zur Voraussetzung gemacht (insofern ungenau vgl. ebd., S. 57).

Kernpunkt der Kritik: technische Probleme der Kommunikationsüberwachung, die juristische Abstufungen unterlaufen.

(2.) Die Rechtsprechung des BVerfG, insbesondere die Entscheidung zum BKAG, erscheint getragen von dem Gedanken, den Sicherheitsbehörden die von diesen mutmaßlich benötigten Instrumente nicht zu nehmen und verschiebt so Rechtsprobleme auf die praktische Ebene, wo sie jedoch verfassungskonform nicht mehr gelöst werden können: Kernpunkt der Kritik sind letztlich technische Grundprobleme der Kommunikationsüberwachung, die allzu feine juristische Abstufungen unterlaufen. So ist der genaue Funktionsumfang einer Software technisch kaum eingrenzbar. Um die gewünschten Inhalte abhören zu können, müssen Funktionen wie etwa das Mikrofon des Endgeräts übernommen, d. h. Veränderungen an dem System selbst vorgenommen werden. Gleichzeitig die Manipulation anderer

Inhalte beweisbar auszuschließen, ist kaum möglich. Zudem stellen sich gerade bei der Quellen-TKÜ noch andere, kaum lösbare Abgrenzungsaufgaben für die Software: So müsste sie erkennen können, welche Kommunikation zur laufenden zählt und müsste gezielt nur solche Kommunikation erfassen können, auf die sich das Anliegen der Sicherheitsbehörden bezieht. Der Nutzer kann aber z. B. gleichzeitig eine Vielzahl von Browserfenstern geöffnet haben: Über das eine chattet er laufend mit einem anderen Verdächtigen, über das andere mit seiner Ehefrau, beim dritten schreibt er gerade nur einen E-Mail-Entwurf, den er vielleicht nie abschickt, der also bloße Gedanken und Interna enthält, beim vierten führt er sein Tagebuch. Diese Informationen fein säuberlich voneinander zu trennen, gerade bei der Überwachung der Kommunikation mittels Screenshots, ist technisch nicht nur aufwändig, sondern kaum realisierbar. Dieses Dilemma erkennt das Gericht, löst es aber nicht:

> *„Ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, betrifft die Anwendung der Norm, nicht aber ihre Gültigkeit. […] Das Gesetz lässt jedenfalls keinen Zweifel, dass eine Quellen-Telekommunikationsüberwachung nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt ist. […] Sollten zum gegenwärtigen Zeitpunkt diese Anforderungen nicht erfüllbar sein, liefe die Vorschrift folglich bis auf weiteres leer" (BVerfG- BKAG, Rn. 234).*

Das ist eine bemerkenswerte Feststellung – und ein starker Rückzug auf formale Positionen, mithin ein Rückzug aus der Realität. Im Hinblick auf den Kernbereichsschutz errichtet das Gericht einerseits strenge Hürden, gerade im Hinblick auf die Wohnraumüberwachung (vgl. BVerfG, Urteil vom 3.3.2004, Rn. 134 ff.). Bei Eingriffen in informationstechnische Systeme senkt es den Kernbereichsschutz jedoch ab, bzw. „verschiebt" den Schutz „ein Stück weit von der Erhebungsebene auf die nachgelagerte Aus- und Verwertungsebene" (ebd., Rn. 278 ff.; BVerfG – BKAG, Rn. 218). Dies bedeutet nichts anderes, als dass die Erhebung der Daten durch den Staat nicht gesetzlich reguliert wird, selbst in Bereichen wie dem heimlichen Zugriff auf informationstechnische Systeme, die nach Auffassung auch des Gerichts typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten in sich tragen und damit eine besondere Kernbereichsnähe aufweisen (vgl. BVerfG – BKAG, Rn. 218). Das

BVerfG verknüpft hier das Schutzniveau des Kernbereichs und damit die Verfassungsmäßigkeit der Maßnahmen auch damit, inwieweit sich der Schutz bei der jeweiligen Maßnahme herstellen lässt, ein kaum überzeugendes Ergebnis.

Hinzu kommt, dass die jeweilige Späh-Software erst einmal auf das jeweilige Endgerät gelangen muss. Hierfür gibt es zwei Wege: Die Software kann direkt auf das Endgerät aufgespielt werden – dies setzt aber den Einbruch in die jeweilige Wohnung oder zumindest eine längere Zugriffsmöglichkeit auf das (unverschlüsselte) Gerät voraus. Oder, und dies ist wohl der auch von den Sicherheitsbehörden präferierte Weg, die Software wird über die Internetverbindung aufgespielt. In beiden Fällen müssen die Ermittler also jene Wege nehmen, die sonst nur Kriminelle beschreiten, und bestehende Sicherheitslücken ausnutzen, die sie im gleichen Zug an anderer Stelle, z. B. beim Diebstahlschutz oder bei der Cyberabwehr, zu schließen versuchen. Erinnert sei an dieser Stelle nur an den 2017 kursierenden Erpressungstrojaner „Wannacry", der erhebliche Schäden angerichtet hat.

Das Offenhalten von Sicherheitslücken stellt ein ernst zu nehmendes Risiko für die Sicherheit aller Bürger dar.

Das Offenhalten von Sicherheitslücken, wie im Dezember 2017 zuletzt wieder von der Innenministerkonferenz gefordert, stellt aber ein ernst zu nehmendes Risiko für die Sicherheit aller anderen Bürger dar, ein Umstand, den das BVerfG ersichtlich nicht berücksichtigt, wenn es von Eingriffen ohne große Streubreite ausgeht (vgl. ebd., Rn. 101). Gleichzeitig stellt es fest, dass „über die Art der praktischen Durchführung der bisherigen ‚Online-Durchsuchungen' und deren Erfolge wenig bekannt" sei (BVerfG, Urteil vom 27.2.2008, Rn. 7).

Fazit

Der verfassungsgerichtliche Umgang mit den Instrumenten der Onlinedurchsuchung und der Quellen-TKÜ zeugt vor allem von einem rechtspolitischen Dilemma im Bereich der Gefahrenabwehr: Rechtlich und technisch lassen sich die infrage stehenden Maßnahmen kaum so präzise abgrenzen und regeln, dass sie den strengen Blick des Verfassungs- und Datenschutzrechts bestehen. Ohne diese Maßnahmen scheint aber eine Terrorabwehr kaum effektiv möglich, trotz bisher ausstehender gründlicher Evaluation der Wirksamkeit der infrage stehenden Maßnahmen. Dieses „ganz oder gar nicht", welches auch das BVerfG thematisiert (vgl. BVerfG – BKAG, Rn. 217 f.), wird durch die

Entscheidung mit einem „ganz, aber…“ gelöst, das dogmatisch nicht zu überzeugen vermag – und den Praxistest kaum bestehen kann. Einstweilen ergeben sich hier gerade zum gleichzeitig erklärten Ziel der Datensicherheit und der Cyberabwehr erhebliche Brüche und Widersprüche, die nicht unaufgelöst bleiben können.

Literatur

Bundesverfassungsgericht (2016): Urteil vom 20.4.2016, Az.1 BvR 966/09, 1 BvR 1140/09 – BKAG http://www.bverfg.de/e/rs20160420_1bvr096609.html.

Bundesverfassungsgericht (2008): Urteil vom 27.2.2008, Az. 1 BvR 370/07 – Onlinedurchsuchung http://www.bverfg.de/e/rs20080227_1bvr037007.html.

Bundesverfassungsgericht (2004): Urteil vom 3.3.2004, Az.1 BvR 2378/98 – Großer Lauschangriff. http://www.bverfg.de/e/rs20040303_1bvr237898.html.

Gesetz zur Änderung des Polizeigesetzes Baden-Württemberg (2017): Landtagsdrucksache 16/3001. https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/3000/16_3011_D.pdf.

Gesetz zur Änderung des Polizeigesetzes und des Gesetzes über die Ladenöffnung in Baden-Württemberg (2017): Landtagsdrucksache Baden-Württemberg 16/2741. http://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/2000/16_2741_D.pdf.

Maunz, Theodor/Dürig, Günter (2016): Grundgesetz Kommentar, Bd. II (Art- 6-15), München.

Alle Internetquellen zuletzt aufgerufen am 17.12.2017.