Der Einsatz des „Staatstrojaners“

– Zusammenspiel von effektiver Gesetzgebung, Rechtswirklichkeit und Exekutivkontrolle

Dr. Anika D. Luch, Kiel *

Neue Medien erfordern neue Maßnahmen. Die Parallelität von analoger und Online-Welt gilt auch im Bereich der Gefahrenabwehr und Strafverfolgung. Klassische Telefonüberwachung und die Möglichkeit zur Kenntnisnahme von Gesprächen per Internettelefonie sind für die Ermittlungsbehörden ebenso wichtig wie die physische Durchsuchung einer Wohnung sowie eines PCs oder die virtuelle Ausforschung der Festplatte und Internetnutzung. Strafverfolgungsbehörden versuchen sich in der Suche nach geeigneten Ermittlungsmethoden, ohne dass ein grundrechtskonformes Regelungswerk bereits zu den konkreten und in der Auswirkung intensiven Grundrechtseingriffen ermächtigen würde.

I. Rechtswirklichkeit: Was kann die eingesetzte Spionagesoftware?

Im letzten Jahr veröffentlichte der Chaos Computer Club (CCC) seine Erkenntnisse über eine eingesetzte staatliche Überwachungssoftware (sog. Staatstrojaner). Diese sollte in erster Linie das Aufzeichnen von Internettelefonaten (Voice over IP – VoIP) und das Anfertigen von Bildschirmfotos (Screenshots) in bestimmten Intervallen ermöglichen. Darüber hinaus war das Programm so ausgestaltet, dass weitere Funktionen wie die Überwachung eines Raumes mittels Webcam und Mikrofon oder das Auslesen und Manipulieren von Dateien auf der Festplatte hätten aktiviert werden können. Möglich waren insofern neben der eigentlich beabsichtigten Quellentelekommunikationsüberwachung (Quellen-TKÜ) Maßnahmen der Online-Durchsuchung und des „Großen Lauschangriffs“.

Die Quellen-TKÜ soll in tatsächlicher Hinsicht nur das Äquivalent zur bislang herkömmlichen analogen Telekommunikationsüberwachung bilden, um der vermehrten Internettelefonienutzung Rechnung zu tragen. Es geht bei beiden Vorgängen um die Überwachung der Kommunikationsinhalte. Technisch bestehen jedoch erhebliche Unterschiede, die wiederum mit rechtlichen Unterschieden einhergehen. Während die Überwachung von gewöhnlichen Telefongesprächen über den Telefondiensteanbieter durchgeführt werden kann, wird bei der VoIP-Technologie das Endgerät des überwachten Kommunikationsteilnehmers mit einer speziellen Überwachungssoftware infiltriert, die die Kommunikationsinhalte jeweils vor der Verschlüsselung bzw. nach der Entschlüsselung unbemerkt weiterleitet. Bei der eingesetzten Spionagesoftware war sowohl die Ferninstallation über das Internet in automatisierter oder manueller Weise als auch die unmittelbare manuelle Installation möglich.[1]

Weitere Problemstellungen ergeben sich aus dem Umstand, dass die Daten vom überwachten Rechner nicht direkt an die ermittelnden Behörden, sondern zunächst auf einen privat betriebenen Server in den USA (Ohio) übermittelt wurden, um im Anschluss an die staatlichen Stellen gesandt zu werden.

Auch die Spionagesoftware selbst war von einer privaten Firma entwickelt worden, ohne dass die dieses Programm einsetzenden staatlichen Stellen zumindest ab der Einsatzphase Zugriff auf den Quellcode gehabt hätten, um zu überblicken, welche Funktionalitäten damit verknüpft werden könnten und wie sicher das System gegenüber unberechtigten Zugriffen Dritter sein würde. Problematisch ist nach Angaben des CCC, dass die von der Software ausgehenden Daten zwar verschlüsselt wurden, der verwendete Code jedoch in allen Versionen des Programms gleich war und die Kommandos an die Software weder verschlüsselt erfolgten noch überprüft wurden, ob sie vom legitimierten Server oder von einem unberechtigten Dritten stammten.[2]

II. Verfassungsrechtlicher Rahmen

Die Ermittlungsbehörden als ausführender Arm des Staates sind insbesondere bei ihren unmittelbar in Grundrechte eingreifenden Maßnahmen nicht nur durch die nachfolgend dargestellten individuellen Freiheitspositionen beschränkt, sondern selbstverständlich auch an Recht und Gesetz gebunden (Art. 20 Abs. 3 GG). Dabei haben sie insbesondere bei der Eröffnung eines Anwendungsbereichs für abwägende Entscheidungen auch die jeweils geschützten, gegenüber stehenden Positionen wie die staatlichen Schutzpflichten in Form von Gefahrenabwehr im präventiven Bereich oder auch der Spezial- und Generalprävention als Zwecke der Strafverfolgung und -ahndung angemessen zu berücksichtigen.

1. Betroffene Schutzbereiche

Der Einsatz der Spionagesoftware mit den beschriebenen Einsatz- und Weiterungsmöglichkeiten sowie Sicherheits-

* Referentin im Wissenschaftlichen Dienst des Schleswig-Holsteinischen Landtags und freie Mitarbeiterin am Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel. Der Beitrag gibt ausschließlich die persönliche Rechtsauffassung der Verfasserin wieder.

1 Skisitims/Roßnagel, ZD 2012, 3 (4) unter Verweis auf Fox, DuD 2007, 827 (829).

2 Zum Ganzen „Analyse einer Regierungs-Malware“ v. 8.10.2011 durch den CCC, S. 3 f., 11 f., abrufbar unter: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (Stand: 26.2.2012); vgl. auch Braun/Roggenkamp, K&R 2011, 681 (682).

risiken tangiert Schutzbereiche unterschiedlicher Grundrechtspositionen.

a) Art. 10 Abs. 1 GG – Fernmeldegeheimnis

Im Kern geht es bei der Quellen-TKÜ wie bei der „herkömmlichen“ TKÜ um das Abhören von auf Distanz geführten Gesprächen und damit um einen unmittelbaren Eingriff in die über Art. 10 Abs. 1 GG gewährleistete Telekommunikationsfreiheit.

b) Art. 2 Abs. 1 GG – Recht auf informationelle Selbstbestimmung

Das Abhören des Gesprächs beinhaltet zugleich eine Erhebung von Daten rund um den Kommunikationsvorgang hinsichtlich Inhalt, Teilnehmer, Rahmendaten wie Uhrzeit und Dauer etc. Hierbei handelt es sich jeweils um einen Eingriff in das aus dem Allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung. Jede weitere Ermittlungsmaßnahme, wie Screenshots oder das Ausforschen von anderen auf der Festplatte des jeweils infiltrierten PC enthaltenen Daten, stellt ebenfalls einen Eingriff in den Schutzbereich dieses „Datenschutzgrundrechts“ dar. Soweit gleichzeitig Art. 10 Abs. 1 GG einschlägig ist, kann zwar von einer Spezialität dieses Freiheitsrechts gesprochen werden, das Recht auf informationelle Selbstbestimmung, das als spezielle Einzelausprägung an der Auffangfunktion des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG teilhat,[3] greift dennoch subsidiär ein.

Darüber hinaus stellen nicht nur das Erheben der einzelnen Daten, sondern auch deren Weitergabe an Dritte (über die USA) oder Verwendung (inhaltliche Auswertung zwecks Ermittlung) weitere Eingriffe in das Recht auf informationelle Selbstbestimmung der einzelnen Betroffenen dar.

c) Art. 2 Abs. 1 GG – Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Im Zuge der Entscheidung des Bundesverfassungsgerichts zur Verfassungswidrigkeit des in NRW in § 5 Abs. 2 Nr. 11, 2. Alt. VSG[4] unternommenen Versuchs der Schaffung einer Rechtsgrundlage für eine zu präventiven Zwecken einsetzbare Online-Durchsuchung gelangten die Verfassungsrichter zu der Erkenntnis, dass eine weitere Ausprägung des Allgemeinen Persönlichkeitsrechts das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (kurz: „IT-Grundrecht“) bildet. Getreu der lückenschließenden Funktion des Allgemeinen Persönlichkeitsrechts fülle dieses IT-Grundrecht die Lücke, die weder durch das Recht auf informationelle Selbstbestimmung noch das Fernmeldegeheimnis gemäß Art. 10 GG oder den Schutz der Wohnung aus Art. 13 GG abgedeckt werden könne. Die Nutzung komplexer informationstechnischer Systeme sei vermehrt aus dem festen Alltag der Mehrheit der Bevölkerung nicht wegzudenken, ohne dass der Einzelne die Komplexität der darüber generierten Daten übersehen oder die Systeme selbst effektiv gegen jedwede denkbaren Zugriffe schützen könne. Der Einzelne sei daher auf die Gewährleistung der Vertraulichkeit und Integrität angewiesen. Als Anknüpfungspunkt wird insofern das Infiltrieren eines gesamten Systems und nicht der Zugriff auf einzelne Daten oder Kommunikationsvorgänge gewählt. Die Phase vor einem konkret erfolgenden Eingriff in das Recht auf informationelle Selbstbestimmung – mithin die Persönlichkeitsgefährdung – wird über die Vertraulichkeitserwartung Bestandteil des Schutzbereichs des IT-Grundrechts. War es schon bei der Entwicklung des Rechts auf informationelle Selbstbestimmung um die Verlagerung des effektiven Grundrechtsschutzes bereits in den Bereich der Persönlichkeitsgefährdung gegangen, weil die Bündelung selbst für sich genommen belangloser Daten schlussendlich zur Erstellung von umfänglichen Persönlichkeitsprofilen genutzt werden könnte, so findet dieser Ansatz im neuen „Computer-Grundrecht“ seine Weiterentwicklung und Zuspitzung.[5] Das BVerfG weist darauf hin, dass Art. 10 Abs. 1 GG alleiniger Prüfungsmaßstab sei, wenn ausschließlich laufende Telekommunikationsdaten erfasst werden.[6] Dieses setze allerdings voraus, dass die Software technisch nicht in der Lage sei, auch Informationen zu erfassen, die keinen Bezug zur Telekommunikation haben.[7] Deutlich wird hierüber, dass es auf die mögliche Streubreite und Intensität des jeweiligen Grundrechtseingriffs ankommt. Durch die Infiltration eines informationstechnischen Systems, die das Aufspielen unterschiedlichster Funktionen wie das Erstellen von Screenshots, Raumüberwachung mittels Webcam, Datenausspähung der Festplatte, Keylogging etc. ermöglicht, vergrößert sich die potentielle Erhebung von Daten auf gegebenenfalls sämtliche Aktivitäten, die mit dem Computer und vor dem Gerät geschehen, während die ausschließliche Telekommunikationsüberwachung auf Informationsaustausch mit anderen Kommunikationspartnern beschränkt ist. Solche Eingriffe weisen daher eine andere Qualität als bestimmte Datenerhebungen auf.

2. Schranken – Voraussetzungen eines verfassungsgemäßen Eingriffs

Die genannten verfassungsrechtlichen Schutzpositionen sind allerdings nicht schrankenlos gewährleistet. Eine an der jeweils formulierten Schrankenbestimmung und dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz ausgerichtete Beschränkung der Freiheit des Einzelnen wäre außerhalb des jeweils absolut geschützten Kernbereichs gerechtfertigt.

Das Freiheitsrecht der Telekommunikationsfreiheit steht über Art. 10 Abs. 2 GG unter einem Gesetzesvorbehalt. Eine grundsätzlich für eine TKÜ verfassungsgemäße Ausgestaltung dieses Vorbehalts findet sich im Bereich der Strafverfolgung insbesondere in den §§ 100a ff. StPO, die die Voraussetzungen solcher Eingriffe in die Telekommunikationsfreiheit normieren.

---

3 Siehe dazu ausf. *Luch*, Das Medienpersönlichkeitsrecht, 2008, S. 203 ff.

4 BVerfGE 120, 274.

5 *Luch*, in: Schliesky (Hrsg.), Technikgestütztes Identitätsmanagement, 2010, S. 142.

6 BVerfGE 120, 274 (309).

7 *Hoffmann-Riem*, JZ 2008, 1009 (1021).

Für das Recht auf informationelle Selbstbestimmung hat das BVerfG in seiner Entscheidung zum Volkszählungsgesetz deutlich zum Ausdruck gebracht, dass für (nicht anonymisierte) Eingriffe eine bereichsspezifische Ermächtigungsgrundlage einzufordern ist,[8] die die Voraussetzungen und den Umfang der Datenerhebung, -speicherung und/oder -verwendung ausgestaltet. Hintergrund war und ist die Annahme, dass es keine belanglosen Daten gebe, weil die Sammlung einer Vielzahl solcher für sich genommen belangloser Daten ebenfalls zur Erstellung eines Persönlichkeitsprofils genutzt werden könnte. Auch die Bestimmungen der StPO enthalten insofern für den Bereich der Strafverfolgung bereichsspezifische datenschutzrechtliche Ermächtigungen; soweit Lücken bestehen finden daneben auch die allgemeinen Datenschutzregelungen Anwendung.
Für den Gewährleistungsgehalt des IT-Grundrechts hat das BVerfG in der Entscheidung zur Online-Durchsuchung ebenfalls festgestellt, dass dieser auch nicht schrankenlos eingeräumt werde. Eingriffe könnten sowohl zu präventiven Zwecken als auch zur Strafverfolgung gerechtfertigt sein.[9] Nähere Vorgaben finden sich in den Ausführungen des Gerichts dem Streitgegenstand entsprechend nur für den Bereich des Verfassungsschutzes (im Sinne einer Gefahrenabwehr bzw. Gefahrenvorsorge). Gefordert wird zur Gewährleistung der Verhältnismäßigkeit des Grundrechtseingriffs im engeren Sinne – angesichts der Intensität der freiheitsbeeinträchtigenden Wirkung eines heimlichen Zugriffs auf ein informationstechnisches System – eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut.[10] Zudem müsse das Gesetz den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen wie den Vorbehalt richterlicher Anordnung (Ausnahme nur für Eilfälle)[11] sichern und gesetzliche Vorkehrungen treffen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden.[12]
In Folge dessen, dass es sich beim Gewährleistungsgehalt des IT-Grundrechts um eine Zuspitzung oder Ausbreitung des Schutzbereichs in den vorgelagerten Bereich des Rechts auf informationelle Selbstbestimmung handelt, können die Schlussfolgerungen des Gerichts für die Voraussetzungen einer verfassungsgemäßen Eingriffsermächtigung ebenfalls als Erfordernis einer bereichsspezifischen Ermächtigungsgrundlage verstanden werden.[13] Dieses ergibt sich einerseits daraus, dass im Falle einer Infiltration informationstechnischer Systeme die Eingriffsbreite ausgeprägt ist, weil Daten jeglicher Qualität (Öffentlichkeits-, Privat- und Intimsphäre) und in einer – selbst für den Betroffenen – unübersehbaren Fülle betroffen sein können und zum anderen weil die technischen Möglichkeiten hier so ausdifferenziert sind, dass genaue Vorgaben erforderlich werden. Diese sind umso wichtiger als der Einzelne aufgrund der Heimlichkeit und Ferne des Eingriffs nicht schutzlos stehen darf und die Zugriffsmöglichkeiten so verschieden ausgestaltet sein können.

III. Ausreichende einfachgesetzliche Ermächtigungsgrundlagen?

Vor dem verfassungsrechtlichen Hintergrund lassen sich ausreichende einfachgesetzliche Ermächtigungsgrundlagen allenfalls für den Bereich der Gefahrenabwehr, keinesfalls jedoch für einen Einsatz der Online-Durchsuchung oder der Quellen-TKÜ zu Zwecken der Strafverfolgung ausfindig machen.

1. Online-Durchsuchung

a) § 20k BKAG

§ 20k BKAG[14] bietet für den Bereich der Gefahrenabwehr eine spezifische Ermächtigungsgrundlage für verdeckte Eingriffe in informationstechnische Systeme.[15] Der Abgleich mit den durch das Bundesverfassungsgericht aufgestellten Anforderungen an eine verfassungsrechtlich tragfähige Ermächtigungsgrundlage für Eingriffe in das IT-Grundrecht macht deutlich, dass die Norm diesen Vorgaben Rechnung trägt (ähnliche Ermächtigungen finden sich auch im Polizeirecht einiger Länder[16]). Es sind zunächst die Rechtsgüter von überragender Bedeutung genannt, für deren Gefährdung ein bestimmtes Maß an Wahrscheinlichkeit vorliegen muss. Zudem muss sich die Maßnahme als ultima ratio für einen Ermittlungserfolg darstellen. Veränderungen am informationstechnischen System des Betroffenen müssen auf das erforderliche Maß reduziert bleiben. Das eingesetzte Mittel muss nach dem Stand der Technik gegen unbefugte Nutzung Dritter geschützt werden. Der Einsatz ist detailliert zu protokollieren. Andere Personen als die „Verdächtigen“ dürfen nur betroffen werden, soweit dies unvermeidbar ist. Die Maßnahmen sind nur auf Antrag des Präsidenten des BKA vom Gericht anzuordnen, wobei die Anordnung detaillierte Vorgaben zu Art, Umfang, Dauer etc. enthalten muss und zu befristen ist. Ferner werden gesetzliche Vorkehrungen fixiert, die den Kernbereich privater Lebensgestaltung schützen sollen.

b) §§ 102 ff. StPO

Abgesehen von der seitens des Bundesverfassungsgerichts nicht abschließend erörterten Frage, welchen Anforderungen eine Ermächtigungsgrundlage für eine Online-Ausforschung informationstechnischer Systeme im repressiven Bereich gerecht werden müsste – hier könnten höhere Hürden aufzustellen sein, weil gerade keine akuten Gefahren

[8] BVerfGE 65, 1 (46).
[9] BVerfGE 120, 274 (315).
[10] BVerfGE 120, 274 (326). „Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“, ebenda, S. 328.
[11] BVerfGE 120, 274 (331 f.).
[12] BVerfGE 120, 274 (335).
[13] So auch *Becker/Meinicke*, StV 2011, 50; *Buermeyer/Bäcker*, HRRS 2009, 433 ff. m.w.N.; *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 14 f. m.w.N.; *Hoffmann-Riem*, JZ 2008, 1009 (1022); *Hornung*, VR 2008, 299 (300 f.); *Böckenförde*, JZ 2008, 925 (934); *Braun/Roggenkamp*, K&R 2011, 681 (682 f.). Siehe BVerfGE 120, 274 (316): „Der Gesetzgeber hat Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen.“
[14] Siehe auch Art. 6e Abs. 1 Satz 1 BayVSG.
[15] Krit. hierzu *Roggan*, NJW 2009, 257 (261 f.).
[16] Siehe Art. 34d PAG Bayern; § 31c POG Rheinland-Pfalz.

für Rechtsgüter gebannt werden können, sondern nur noch repressiv dem Sühnegedanken und der Spezial- und Generalpräventionsfunktion von Strafe entsprechend reagiert wird –, ist festzustellen, dass im Bereich der Strafverfolgung keine den § 20 k BKAG entsprechende Ermächtigung in der StPO zu finden ist. Zurückgegriffen wird zur Rechtfertigung von Online-Durchsuchungsmaßnahmen durch die strafprozessualen Ermittlungsbehörden auf §§ 102 ff. StPO, die lediglich herkömmliche „analoge“ Durchsuchungsmaßnahmen von Räumlichkeiten erlauben.[17] Von solchen Maßnahmen unterscheidet sich die heimliche Aufspielung einer Ausforschungssoftware auf dem privaten Rechner eines Betroffenen aber in erheblichem Maße. Strafverfahrensrechtlich zulässig sind de lege lata daher lediglich die offene Sicherstellung bzw. Beschlagnahme eines Datenträgers sowie der darauf gepeicherten Daten gem. §§ 94 ff. StPO und die Durchsicht elektronischer Speichermedien bei einem von einer offenen Durchsuchung nach §§ 102 ff. StPO Betroffenen (zu räumlich entfernten Speichermedien vgl. § 110 Abs. 3 StPO).[18]

2. Quellen-TKÜ

a) § 20 l BKAG

Auch für die Quellen-TKÜ findet sich im Verfassungsschutzrecht des Bundes eine an den Vorgaben des Bundesverfassungsgerichts ausgerichtete Norm, die auf die technischen Vorkehrungen und Rahmenbedingungen in § 20 k Abs. 2 und 3 BKAG Bezug nimmt; zudem muss im Fall der beabsichtigten Überwachung des Kommunikationsverhaltens technisch sichergestellt sein, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.

b) §§ 100a ff. StPO

Weniger eindeutig verhält sich das Schrifttum zur Zulässigkeit der Quellen-TKÜ im strafprozessualen Bereich.[19] Zwar erlaubt § 100a StPO unter bestimmten Voraussetzungen eine heimliche Überwachung und Aufzeichnung von „Telekommunikation“[20]; es wird insbesondere eine im Einzelfall schwer wiegende Katalogstraftat vorausgesetzt und die Bedingung als ultima ratio-Ermittlungsmethode aufgestellt. Bei der Quellen-TKÜ ist aber problematisch, dass zur Ermöglichung der eigentlichen Kommunikationsüberwachung das vom Betroffenen genutzte informationstechnische System „angezapft“ werden muss. § 100a StPO bedeutet jedoch nur die Ermächtigung zum Abhören und zur Aufzeichnung der geführten Gespräche (Primärmaßnahme) nicht auch der möglicherweise darüber hinaus erforderlichen Vorbereitungsmaßnahmen (Sekundärmaßnahme[21]), soweit diese einen qualitativ eigenständigen Grundrechtseingriff mit sich bringen. Gleiches gilt für § 23a Zollfahndungsdienstgesetz. Zum Teil wird versucht, die Eingriffsermächtigung im Wege einer „Annexkompetenz“ zu kreieren.[22] Dies überzeugt jedoch nur dort, wo es sich entweder um unerhebliche Eingriffe in die Allgemeine Handlungsfreiheit oder um Eingriffe in den gleichen Gewährleistungsgehalt durch Primär- wie Sekundärmaßnahme geht. So kann beispielsweise von genehmigten, erforderlichen Vorbereitungsmaßnahmen gesprochen werden, wenn im Zuge einer (rechtmäßigen) Überwachung ein GPS-Sender am Kraftfahrzeug des Betroffenen installiert [23] oder zum Zwecke eines genehmigten Großen Lauschangriffs eine Abhörvorrichtung in der Wohnung platziert wird. Insbesondere im letztgenannten Fall ermächtigt bereits die Genehmigung der Primärmaßnahme zu einem Eingriff in Art. 13 GG und die Ermächtigungsgrundlage enthält spezifische beschränkende Vorgaben.[24]

Die §§ 100a, 100b StPO sind auf die herkömmliche Telekommunikationsüberwachung zugeschnitten. Sie berücksichtigen die nur einer Quellen-TKÜ immanente Gefährdung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht in ausreichendem Maße. Der Komplexität der notwendigen Begleitmaßnahmen (von der Installation des Trojaners bis hin zur Datenübermittlung) wird nicht in dem vom verfassungsrechtlichen Bestimmtheitsgebot gefordertem Umfang Rechnung getragen.[25] Wenn das Bundesverfassungsgericht mehrfach darauf hinweist, dass nur hinreichend bestimmte Normen einen konkreten Eingriff in Grundrechte legitimieren können, bedarf zwangsläufig jeder technisch konkretisierbare Eingriff einer spezifischen Ermächtigungsgrundlage durch die Gesetzgeber.[26]

Zwar ist es vom Sinn und Zweck der Strafverfolgungsvor-

---

[17] Von der strafprozessualen Unzulässigkeit der Online-Durchsuchung geht wohl die h.M. aus, vgl. BGH, MMR 2007, 237 m. Anm. *Bär; Brodowski*, JR 2011, 533 (538) m.w.N.; *Schmitt*, in: Meyer-Goßner, StPO, § 100a Rn. 7b m.w.N.; *Popp*, ZD 2012, 51; *Braun/Roggenkamp*, K&R 2011, 681 (682); *Stadler*, MMR 2012, 18 (20); anders noch BGH, wistra 2007, 28; *Hofmann*, NStZ 2005, 121 (123 ff.).

[18] So auch *Popp*, ZD 2012, 51 (52).

[19] Für die Unzulänglichkeit der §§ 100a ff. StPO bspw. *Hoffmann-Riem*, JZ 2008, 1009 (1022); *Hornung*, CR 2008, 299 (300); *Buermayr/Bäcker*, HRRS 2009, 433 ff.; *Braun*, K&R 2011, 681 (682 f.); *Becker/Meinicke*, StV 2011, 50; *Vogel/Brodowski*, StV 2009, 632 (634); *Sankol*, CR 2008, 13 (14 ff.); *Skisitims/Roßnagel*, ZD 2012, 3 (6); *Popp*, ZD 2012, 51 (53 f.); a.A. AG Bayreuth, MMR 2010, 266 m. Anm. *Bär*; LG Landshut, MMR 2011, 690 m. Anm. *Bär*; LG Hamburg, 31.8.2010, Az.: 608 Qs 17/10; *Bär*, TK-Überwachung, 2010,
§ 100a Rn. 32 ff.; BeckOK-StPO/Graf, § 100a Rn. 114 ff.; *Schmitt*, in: *Meyer-Goßner*, StPO, § 100a Rn. 7a. Die Grenze des Zulässigen ist aber auch für die Rspr. erreicht, sobald es zu „Screenshots“ kommt, LG Landshut, MMR 2011, 690.

[20] *Popp*, ZD 2012, 51 (54), weist auf den bedenkenswerten Punkt hin, dass die Quellen-TKÜ den eigentlichen Kommunikationsvorgang umgeht, indem das Endgerät infiltriert und die Kommunikationsinhalte vor dem Verschlüsseln und Aussenden bzw. nach dem Entschlüsseln abgehört werden. Die Legaldefinition des Begriffs der Telekommunikation in § 3 Nr. 22 TKG scheint von einem engeren Begriffsverständnis auszugehen. Siehe dazu BGH, NJW 2003, 2034 (2035).

[21] *Sankol*, CR 2008, 13 (17); *Bär*, TK-Überwachung, 2010, § 100a Rn. 32.

[22] Siehe LG Landshut, MMR 2011, 690 m. Anm. *Bär* m.w.N.; *Schmitt*, in: Meyer-Goßner, StPO,54. Aufl. 2011, § 100a Rn. 7a.

[23] Beispiel wie bei *Popp*, ZD 2012, 51 (54).

[24] H.M., u.a. BeckOK-StPO/*Hegmann*, § 100c Rn. 3; *Stern*, Handbuch des Staatsrechts, Bd. 4/1, 2006, S. 283 f.; *Papier*, in: *Maunz/Dürig*, GG, Art. 13 Rn. 47, 79, 89; *Meyer/Hetzer*, NJW 1998, 1017 (1026).

[25] *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 14 f. m.w.N.; *Braun/Roggenkamp*, K&R 2011, 681 (683, 684).

[26] *Hermonies*, Recht und Politik 2011, 193 (194).

schrift her gedacht, folgerichtig, dass es zunächst keinen Unterschied macht, ob ein Internettelefonat oder ein auf hergebrachte Weise geführtes Telefonat abgehört werden soll. Soweit die in den Vorschriften genannten Voraussetzungen vorliegen, ist die inhaltliche Kenntnisnahme im Ergebnis gerechtfertigt. Jedoch darf dabei nicht vergessen werden, dass sich der Zugang zu den Informationen in beiden Konstellationen gänzlich unterschiedlich gestaltet und mit völlig unterschiedlich intensiven Grundrechtseingriffen verbunden ist. Bei der herkömmlichen TKÜ wird ausschließlich der Zugriff auf den Telefonkanal über den Diensteanbieter eröffnet. Bei der Internettelefonüberwachung wird die Quelle, also das Endgerät des Betroffenen infiltriert. Da es sich hierbei in jedem Fall zunächst auch um einen Eingriff in das IT-Grundrecht handelt, muss die Maßnahme den vom Bundesverfassungsgericht erläuterten Eingriffsvoraussetzungen genügen. Insbesondere muss gesetzlich sichergestellt werden, dass ausschließlich eine TKÜ und nicht auch weitere Funktionen über die aufgespielte Überwachungssoftware – weder von den ermittelnden Behörden selbst noch durch Dritte – aktiviert werden können. „Die Quellen-TKÜ ist (…) in technischer Hinsicht eine Online-Durchsuchung, die vom Gesetzgeber im Käfig der Telefonüberwachung gehalten werden muss“.[27] Wäre dies anders, könnte man in der Konsequenz auch davon ausgehen, dass im Falle einer genehmigten TKÜ es keinen Unterschied machte, ob das Abhören des Gesprächs über das Einklinken in die Telekommunikationsverbindung oder das physische Eindringen in die Wohnung des Betroffenen geschieht.

Bei der Infiltration des informationstechnischen Systems für eine VoIP-Überwachung handelt es sich somit um einen eigenständig bedeutsamen Grundrechtseingriff in das IT-Grundrecht, der eine eigene bereichsspezifische Ermächtigungsgrundlage erfordert. Die Regelung des § 20 l BKAG macht dabei deutlich, dass hiervon grundsätzlich auch der Gesetzgeber ausgeht, der im Verfassungsschutzrecht eine spezielle Ermächtigungsnorm mit spezifischen Anordnungen und verfahrensrechtlichen Vorkehrungen geschaffen hat.[28] Eine TKÜ erfordert zum einen keinesfalls zwingend die Installation einer Spionagesoftware, zum anderen ist mit der Installation eine maßgebliche Hürde genommen, die besondere Vorkehrungen erfordert, die einer missbräuchlichen Verwendung für andere Zwecke oder auch durch Dritte vorbeugt. Die §§ 100a ff. StPO enthalten an keiner Stelle die nach Ansicht des Bundesverfassungsgerichts unabdingbare rechtliche Begrenzung der eingesetzten Maßnahme auf einen Eingriff in das Telekommunikationsgeheimnis; die Gefährdungslage für das IT-Grundrecht kann nicht allein durch die Hoffnung auf eine konkretisierende richterliche Anordnung der Maßnahme ausgeschlossen werden.[29]

Im Rahmen der Verhältnismäßigkeit der Quellen-TKÜ ist zudem zu berücksichtigen, dass stets darauf zu achten ist, dass keine milderen gleich geeigneten Mittel zur Verfügung stehen, die die Erforderlichkeit der Maßnahme auszuschließen vermögen. Zum Teil wird nämlich der Vorwurf erhoben, eine Quellen-TKÜ sei gerade bei der überwiegend verbreiteten Nutzung des Internetdienstes Skype nicht erforderlich. Die TKÜ der Internetgespräche könne über sog. Backdoors, die bereits im Skype-System eingebaut seien und von anderen Ländern zur TKÜ genutzt würden, erfolgen.[30] Insofern genüge ähnlich wie der Telefonüberwachung durch Einschaltung der Telefondiensteanbieter auch im Bereich der Internettelefonie die Überwachung mit Hilfe des Telekommunikationsdienstleisters anstelle des unmittelbaren Zugriffs auf das Endgerät.

3. Datenverarbeitung – allgemeines Datenschutzrecht

Das allgemeine Datenschutzregime spielt auch im Falle des strafprozessualen Einsatzes von Ermittlungsmethoden eine Rolle, soweit das Strafprozessrecht keine speziellen vorrangigen Datenschutzregelungen aufweist.[31] Dies ist im Fall des Einsatzes des „Staatstrojaners“ insofern besonders relevant, als die Daten nicht unmittelbar bei den Ermittlungsbehörden gesammelt, sondern zunächst an einen privat betriebenen Server in den Vereinigten Staaten übermittelt werden. Diese Datenverarbeitung im Sinne des § 3 Abs. 4 BDSG zieht die Rechtspflicht gemäß § 9 Satz 1 BDSG i.V.m. Satz 2 Nr. 3 der Anlage nach sich. Es sind Schutzvorkehrungen zu treffen, die sicherstellen, „dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“. Die USA als Zielort der „Datenumleitung“ gelten als Drittland ohne angemessenes Schutzniveau im Datenschutzbereich i.S.d. Art. 25 Abs. 4 der Datenschutzrichtlinie, so dass das erforderliche Schutzniveau im Einzelfall sicherzustellen ist, vgl. § 4 b Abs. 3 BDSG.[32] Auch der Umstand, dass die kryptografische Absicherung der Spionagesoftware nach Aussagen des CCC mangelhaft ist und nicht gegen Zugriffe unbefugter Dritter Schutz zu gewähren vermag,[33] widerspricht der datenschutzrechtlichen Schutzverpflichtung.

4. Ermächtigungsgrundlage auf Vorrat?

Im Zuge der Debatte, ob eine Quellen-TKÜ de lege ferenda auf rechtssicheres Fundament gestellt werden könnte, findet sich zum Teil der Hinweis, dass die effektive Beschränkung einer Überwachungssoftware auf die ausschließliche Nutzung zur TKÜ technisch nicht realisierbar sei. Die Schaffung einer Eingriffsbefugnis stehe unter dem

---

27 *Stadler*, MMR 2012, 18 (20).

28 So auch *Popp*, ZD 2012, 51 (54).

29 Ähnlich *Popp*, ZD 2012, 51 (53); *Braun*, K&R 2011, 681 (683); *Brodowski*, JR 2011, 533 (536); *Vogel/Brodowski*, StV 2009, 632 (634); *Braun/Roggenkamp*, K&R 2011, 681 (683); *Buermeyer/Bäcker*, HRRS 2009, 433 (438); a.A. *Schmitt*, in: *Meyer-Goßner*, StPO,54. Aufl. 2011, § 100a Rn. 7a.

30 Siehe nur *Braun/Roggenkamp*, K&R 2011, 681 (685); *Stadler*, MMR 2012, 18 (19).

31 Siehe auch SK-StPO/*Weßlau*, Vor § 474 Rn. 30.

32 Vgl. *Popp*, ZD 2012, 51 (55); *Braun/Roggenkamp*, K&R 2011, 681 (684).

33 „Analyse einer Regierungs-Malware“ v. 8.10.2011 durch den CCC, S. 6, abrufbar unter: http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (Stand: 26.2.2012).

Vorbehalt des technisch Möglichen.[34] Soweit dies zuträfe, wären auch beim Einsatz einer Quellen-TKÜ stets die Voraussetzungen für einen rechtfertigungsfähigen Einsatz einer in der Intensität und Streubreite des Grundrechtseingriffs weitergehenden Online-Durchsuchung, wie sie vom Bundesverfassungsgericht formuliert wurden, zu beachten und anzuwenden.

Aus der mangelnden technischen Realisierbarkeit wird zum Teil gefolgert, dass es dem Gesetzgeber verwehrt sei, eine Ermächtigungsgrundlage auf Vorrat zu schaffen, die eine Quellen-TKÜ ausschließlich orientiert am Maßstab des Art. 10 GG erlaubt.[35] Hier werden Rechtswirklichkeit und Rechtsetzung untrennbar miteinander verbunden und die Schaffung einer Rechtsgrundlage unter den Vorbehalt des „tatsächlich Möglichen“ gestellt. Begründet wird dieser Konnex mit der Gefahr des Missbrauchs oder sorglosen Gebrauchs der Rechtsgrundlage durch die Behörden. Diese Sichtweise ist mit dem überwölbenden Prinzip der Rechtsstaatlichkeit nicht zu vereinbaren. Der Gesetzgeber ist gehalten, insbesondere im grundrechtssensiblen Bereich, inhaltlich bestimmte und in der Sache abgewogene verfassungskonforme Regelungen zu schaffen. Diese können nur abstrakt-generell formuliert werden. Aufgabe der ausführenden staatlichen Stellen ist die Beachtung sämtlicher gesetzlicher Vorgaben beim Vollzug, also auch die Suche nach einer den gesetzlichen Maßstäben genügenden Software.

Es liegt eine klare Aufgabenteilung vor; der Gesetzgeber kann nur die rechtlichen Vorkehrungen treffen, um die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang zu beschränken; die ebenfalls vom Bundesverfassungsgericht[36] geforderten technischen Voraussetzungen sind von der Exekutive bei der konkreten Anwendung sicherzustellen. Mangelt es an einem geeigneten Programm zur auf Telekommunikationsvorgänge beschränkten Überwachung, so haben die Behörden auf entsprechende Maßnahmen zu verzichten oder eine Online-Durchsuchung zu beantragen, die auch zur Quellen-TKÜ ermächtigt. Entsprechende Vorgehensweisen sind durch eine effektive Kontrolle der Exekutivmaßnahmen[37] sicherzustellen wie sie im verfassungsrechtlichen System der „checks and balances“ angelegt ist.

Es gilt, dass der rechtswidrige Vollzug einer Maßnahme nicht die Rechtswidrigkeit der zugrundeliegenden Ermächtigungsgrundlage begründet. Soweit der Gesetzgeber die Voraussetzungen für den verfassungsgemäßen Einsatz einer Quellen-TKÜ-Software abstrakt-generell verfassungskonform formuliert und damit auch konkretisiert, ist für die Entwicklung einer sachgemäßen Software erst ein rechtssicherer Rahmen vorgegeben, der Planungssicherheit zu gewährleisten vermag. Das Recht hat sich insofern nicht an den technischen Gegebenheiten auszurichten. Von daher wäre es auch irreführend zu behaupten, dass das IT-Grundrecht aufgrund des technischen Fortschritts entwickelt worden wäre; vielmehr ist es so, dass der Grundrechtskatalog die Schutzposition von Anfang an mit umfasste, sie aber erst im Zuge des Fortschreitens der Technik aktiviert wurde und zum Zuge kam.

IV. Fazit

Die Komplexität der modernen Lebensumstände darf weder zu einem Strafermittlungsdefizit noch zu einem Vollzusgkontrolldefizit führen. Eine Problemstellung, die von struktureller Natur ist.

Der Gesetzgeber (auch die Exekutive) ist vermehrt auf die Beratung durch externen Sachverstand angewiesen, um technische oder andere hoch komplexe Sachverhalte angemessen einordnen zu können. Dies darf jedoch weder die Handlungsfähigkeit der Staatsgewalt noch demokratietheoretische Bedenken begründen, weil die Entscheider mehr und mehr nicht in der Lage wären, aus eigenem Sachverstand und optimaler vollumfänglicher Informationsbasis heraus Regelungen zu schaffen und Kontrolle auszuüben. Es bleibt primäre Aufgabe, dass jeder einzelne befasste Abgeordnete nach bestem Wissen und Gewissen überprüft, ob mit Hilfe von Sachverständigenanhörungen und den spezialisierten Regierungsmitarbeitern erarbeitete Lösungswege überzeugend und rechtsstaatlich ausgestaltet erscheinen. Ausschlaggebend ist nicht das technische Verständnis im Detail, sondern die bestimmten und in sich konsequenten, am Maßstab der Verfassung ausgerichteten abstrakten Vorgaben, deren rechtsstaatliche Nutzung effektiv überprüft werden muss. Demokratie bedeutet insofern nicht die Notwendigkeit des Allwissens des Gesetzgebers oder bringt in der heutigen komplex-modernen Zeit zwingend das Legitimationsdilemma der Allmacht der Sachverständigen und Lobbyisten mit sich. Überdies kann der im Bundesstaat angelegte Ordnungswettbewerb konstruktiv dazu führen, dass die (Landes-)Gesetzgeber um die „grundrechtskonformsten“ und dem Bestimmtheitsprinzip genügenden Regelungen ringen[38] – dies kann allerdings aufgrund der grundgesetzlichen Kompetenzverteilung nur im Bereich der Gefahrenabwehr Geltung beanspruchen.

Die ausgeprägte Debatte im Bereich der Online-Gefahrenabwehr- oder Ermittlungsmaßnahmen ist geprägt von dem Wunsch, missbräuchliche Verwendung durch überehrgeizige staatliche Stellen auszuschließen. Unter der Prämisse des Rechtsstaats ist es jedoch befremdlich und nur mit der Verunsicherung im komplexen hochtechnisierten Bereich zu erklären, wenn neben den positiven Voraussetzungen für den rechtmäßigen Einsatz von Ermittlungsmethoden die Selbstverständlichkeit normiert werden soll, dass ein missbräuchlicher Einsatz ausgeschlossen werden muss.

Aufgrund der stark datenschutzrechtlich geprägten Problematik wäre die effektive Vollzugskontrolle des Einsatzes einer Quellen-TKÜ möglicherweise am sachgerechtesten bei den Datenschutzbeauftragten des Bundes und der Län-

---

[34] *Braun/Roggenkamp*, K&R 2011, 681 (685, 686).

[35] *Braun/Roggenkamp*, K&R 2011, 681 (686).

[36] BVerfGE 120, 274 (309).

[37] Ebenso hilfreich und mit präventiver Funktion ausgestattet sind möglichst eindeutige Handlungsanweisungen an die ermittelnden Behörden. *Hermonies*, Recht und Politik 2011, 193 (195).

[38] *Hermonies*, Recht und Politik 2011, 193 (194 f.).

der angesiedelt.[39] Ferner wäre darauf zu achten, dass eine von privater Seite eingekaufte Software vollumfänglich – einschließlich Quellcode[40] – durch die staatlichen Stellen kontrolliert eingesetzt werden kann und – am Stand der Technik ausgerichtet – ein Zugriff von dritter Seite oder vom Hersteller ausgeschlossen wird.

Der Gesetzgeber ist gehalten, eine gemessen an den verfassungsrechtlichen Anforderungen tragfähige Ermächtigungsgrundlage für den Einsatz einer Quellen-TKÜ zum Zwecke der Strafverfolgung zu schaffen, soweit er diese Ermittlungsmethode für erforderlich erachtet, und deren rechtmäßigen Vollzug sorgfältig zu kontrollieren. Eine entsprechende Rechtsgrundlage müsste mindestens die gleichen Standards wie in § 20 l BKAG im Gefahrenabwehrbereich abfordern[41] und bei der Einschätzung der Angemessenheit der Norm dem Gedanken Rechnung tragen, dass im Strafverfolgungsbereich keine konkreten akuten Gefahren für bedeutsame Rechtsgüter ausgeräumt, sondern nur repressiv reagiert werden soll. Im BKAG fehlen darüber hinaus Regelungen zur zulässigen Art und Weise der Infiltration des Zielsystems (heimliches händisches Aufspielen bei Gelegenheiten wie Gepäckkontrollen, das Eindringen in die Wohnung oder via Internet), die wünschenswerte Klarstellung, dass durch die Maßnahme ausschließlich das Zielgerät betroffen werden darf sowie der Hinweis, dass durch die eingesetzte Software das Nachladen von Inhalten nicht gestattet sein darf.[42]

[39] So auch *Braun/Roggenkamp*, K&R 2011, 681 (685).

[40] Nur wer den Quellcode kennt, kann auch die Funktionsweise des Programms kontrollieren und gewährleisten. *Hermonies*, Recht und Politik 2011, 193 (194).

[41] *Braun/Roggenkamp*, K&R 2011, 681 (685): „Den diesbezüglichen Mindeststandard bildet § 20 l Abs. 2 BKAG“.

[42] So (z.T.) zutreffend *Braun/Roggenkamp*, K&R 2011, 681 (685).