

HERAUSGEBER

Prof. Dr. Dr. h.c. Heiner Alwart
Richter am BGH a.D. Dr. Axel
Boetticher
Prof. Dr. Dr. h.c. Otar Gamkrelidze
Präsidentin des Obersten
Gerichtshofs Georgiens a.D.,
Prof. Dr. Nino Gvenetadze
Prof. Dr. Martin Heger
Prof. Dr. Bernd Heinrich
Vizepräsident des BGH a.D. Prof.
Dr. Burkhard Jähnke
Prof. Dr. Edward Schramm
Richter am Obersten Gerichtshof
Georgiens a.D. Prof. Dr. Davit
Sulakvelidze
Vizepräsident des
Verfassungsgerichts Georgiens,
Prof. Dr. Merab Turava

SCHRIFTLEITUNG

Assistant Anri Okhanashvili
(TSU), LL.M. (Jena)

Inhaltsverzeichnis

AUFSÄTZE

- Zur Reform des Art. 136 der georgischen
Strafprozessordnung – rechtsvergleichende und
europarechtliche Überlegungen (2. Teil)**
Von Richter am Bundesgerichtshof Dr. *Wolfgang Bär*, Lehrbeauftragter an
der Friedrich-Schiller-Universität (Jena)/Prof. Dr. *Edward Schramm*,
Friedrich-Schiller-Universität (Jena) 24
- Zentrale Aspekte der Telefonüberwachung nach
der georgischen StPO**
Von Assistent-Prof. Dr. *Maka Khodeli*, LL. M. (Freiburg i.Br.),
Iwane-Dschawachischwili-Staatliche-Universität Tbilissi 31
- Einführung in das deutsche Strafvollzugsrecht –
am Beispiel Nordrhein-Westfalens**
Von wissenschaftlicher Mitarbeiterin *Edith Arians*, Institut für Strafrecht
und Strafprozessrecht Universität zu Köln 36

VERSCHIEDENES

- Bericht zum Arbeitsbesuch einer hochrangigen
georgischen Delegation vom 08.-12. April 2019 in Berlin:
„Rechtsgrundlagen, praktische Anwendung und Kontrolle
von Telekommunikationsüberwachungsmaßnahmen in
Deutschland“**
Von *Khatuna Diasamidze*, Projektmanagerin Südosteuropa II und
Südkaucasus bei der Deutschen Stiftung für Internationale Rechtliche
Zusammenarbeit (IRZ) 40

REDAKTION

Prof. Dr. Dr. h.c. Heiner Alwart
Vorsitzender Richter am LG Bremen a.D., Dr. Bernd
Asbrock
Vizepräsidentin am AG Bremen Ellen Best
Richter am BGH a.D., Dr. Axel Boetticher
Rechtsanwalt David Conrad
Associate Prof. Dr. Irakli Dvalidze
Präsidentin des Obersten Gerichtshofs Georgiens a.D.,
Prof. Dr. Nino Gvenetadze
Prof. Dr. Martin Heger
Prof. Dr. Bernd Heinrich
Vizepräsident des BGH a.D., Prof. Dr. Burkhard Jähne
Associate Prof. Dr. Bachana Jishkariani LL.M. (LMU
Muenchen)
Assistant Prof. Dr. Levan Kharanauli
Assistant Maka Khodeli LL.M. (Freiburg i.Br.)
Richterin am Obersten Gerichtshof Georgiens a.D., Prof.
Dr. Tamar Laliashvili
Assistant Prof. Dr. Lavrenti Maglakelidze
Prof. Dr. Ketewan Mtschedlischwili-Hädrich LL.M.
(Freiburg i.Br.)
Assistant Anri Okhanashvili LL.M. (FSU Jena)
Dr. Anneke Petzsche
Dr. Martin Piazena
Dr. Erol Pohlreich
Wiss. Referentin am MPI für ausländisches und
internationales Strafrecht Dr. Johanna Rinceanu, LL.M.
Associate Prof. Dr. Moris Shalikashvili LL.M. (UH)
Prof. Dr. Edward Schramm
Richter am Obersten Gerichtshof Georgiens a.D., Prof.
Dr. Davit Sulakvelidze
Teresa Thalhammer
Assistant Prof. Dr. Temur Tskitishvili
Associate Prof. Dr. Giorgi Tumanishvili LL.M.
(FU Berlin)
Vizepräsident des Verfassungsgerichts Georgiens, Prof.
Dr. Merab Turava
Prof. Dr. Martin Paul Waßmer

LEKTORAT DER 2. AUSGABE 2019

Übersetzung:

Assistent-Prof. Dr. Maka Khodeli, LL. M. (Freiburg i.Br.),
TSU
Lado Sirdadze (Lektoratsmitglied der DGStZ)
Marika Turava (Lektoratsmitglied der DGStZ)
Khatuna Bagrationi

Redaktionelle Bearbeitung der georgischen Texte und die Korrektur der Übersetzung:

Lado Sirdadze (Lektoratsmitglied der DGStZ)

Redaktionelle Bearbeitung der deutschen Texte und die Korrektur der Übersetzung:

Dr. Martin Piazena

Verantwortlich für die 2. Ausgabe 2019 der DGStZ und redaktionelle Endbearbeitung:

Schriftleiter der DGStZ, Assistant Anri Okhanashvili
LL.M. (Jena), TSU

Technische Unterstützung: Gvantsa Makhatadze

Zur Reform des Art. 136 der georgischen Strafprozessordnung – rechtsvergleichende und europarechtliche Überlegungen (2. Teil*)

Von Richter am Bundesgerichtshof Dr. *Wolfgang Bär*, Lehrbeauftragter an der Friedrich-Schiller-Universität (Jena)/Prof. Dr. *Edward Schramm*, Friedrich-Schiller-Universität (Jena)

IV. Zur europarechtlichen Bewertung des Zugriffs auf Daten aus Infrastruktursubjekten

1. Die Fragestellung

Es soll geklärt werden, ob ein direktes Verbot, der Verteidigung die Videoaufnahmen oder anderen Computerdaten aus dem kritischen Infrastruktursubjekt zur Verfügung zu stellen, europarechtlich vertretbar ist. Eine Alternative könnte in einem derartigen Fall darin bestehen, eine Regelung zu schaffen, die der Verteidigung ein Recht auf Anforderung dieser Daten einräumt, über dessen Ausübung aber ein Gericht auf Antrag der Verteidigung zuständig wäre. Das Gericht könnte dann in jedem konkreten Fall entscheiden, ob die Weitergabe von Videoaufnahmen oder anderen Computerdaten aus diesen kritischen Infrastruktursubjekten an die Verteidigung angemessen ist.

Die „kritischen Infrastruktursubjekte“ i. S. des georgischen Gesetzesentwurfs setzen sich aus zwei Gruppen von Objekten zusammen. Die erste Gruppe umfasst Überwachungsgebäude, d. h. vor allem Dienstgebäude, die für die Strafverfolgung oder sonstige besonderen Zwecke eingerichtet wurden, einschließlich getarnter Objekte (wie z. B. ein getarntes Wohndienstgebäude) sowie solcher Gebäude, die der Aufbewahrung von operativ-technischen Einrichtungen und Ausrüstungen dieser Organe dienen. Diese Objekte unterliegen dem Staatsgeheimnis, weshalb Informationen über sie von erheblicher Bedeutung für die öffentliche Ordnung sind.

Die zweite Gruppe erstreckt sich auf Flughäfen sowie jedes der Objekte, die mit dem Erwerb von Öl- und Gasprodukten, der Elektroenergie oder chemischen, biologischen, radioaktiven und nuklearen Produkten verbunden ist. Deren uneingeschränktes Funktionieren

muss erhebliche Bedeutung für die öffentliche Ordnung des Staates oder der Gesellschaft oder für das uneingeschränkte Funktionieren der Regierung oder Gesellschaft haben.

Die Gesetzinitiative räumt der Verteidigung kein Recht auf Anforderung der Informationen über die auf diesen Objekten eingerichteten Überwachungskameras ein, wobei es keinen Unterschied macht, ob diese Kameras innen oder außen angebracht sind. Ebenso soll die Verteidigung kein Recht auf Anforderung der durch elektronische Mittel gesicherten Kommunikationsangaben über das kritische Infrastruktursubjekt haben. Das Gleiche soll für das Sammeln und Bearbeitung der Informationen über die persönlichen Akten der Ministeriumsmitarbeiter gelten, die mit ihrer Diensttätigkeit oder/und mit der im Ministerium laufende elektronischen Überwachung und Kontrolle verbunden sind.

Nachstehend wird davon ausgegangen, dass der Staatsanwaltschaft oder sonstigen Strafverfolgungsbehörden offenbar der Zugriff auf die eben genannten Daten ermöglicht werden soll. Die Frage, ob ihnen nach dem Willen des Gesetzgebers Beschränkungen durch eine (vorherige oder nachträgliche) Gerichtskontrolle auferlegt werden sollen, kann angesichts des eingeschränkten Umfangs der vorgelegten Informationen an dieser Stelle nicht beantwortet werden.

2. Anwendungsbereich

Die vorgesehene Neuregelung zu den kritischen Infrastruktursubjekten hat einen relativ weiten Anwendungsbereich hinsichtlich des Ausschlusses der Verteidigung. Er erstreckt sich zum einen auf Videoaufnahmen, die außerhalb oder innerhalb des Infrastruktursubjekts vorgenommen wurden. Er umschließt zum anderen Informationen über die Mitarbeiter, die in deren persönlichen Akten enthalten sind und die mit ihrer Diensttätigkeit oder mit der im Ministerium laufenden

* Fortsetzung des Beitrags aus DGSStZ 1/2019.

elektronischen Überwachung und Kontrolle verbunden sind. Außerdem sollen gespeicherte Kommunikationsangaben, die das Infrastruktursubjekt betreffen, nicht der Verteidigung zugänglich gemacht werden.

2.1. Flughafen

Nicht plausibel erscheint hierbei der völlige Ausschluss von Videoaufnahmen, die von einer Überwachungskamera in einem Flughafengebäude erstellt wird. Denn weite Teile von Flughäfen sind – ebenso wie beispielsweise Bahnhöfe oder Schiffshäfen – allgemein zugänglich. Große Bereiche eines Flugzeuggebäudes und Flughafengeländes stellen keinen gesteigerten sicherheitsrelevanten Geheimnisbereich dar und sind für jedermann öffentlich zugänglich, d. h. sie unterliegen keinem beschränkten Zutritt von Personen (z. B. die Schalterhallen und die dortigen Geschäfte, Cafés usw.). Da der Begriff „Flughafen“ in dem Gesetzesentwurf offensichtlich ohne Beschränkung auf persönlichkeitsensible Bereiche (z. B. Umkleidekabinen, Toiletten usw.) erfolgt, sondern auch öffentlich zugängliche Teile eines Flughafens erfasst, erscheint ein so weit gefasster Ausschluss nicht angebracht. Es mutet seltsam an, dass zwar Aufnahmen von einer Überwachungskamera am Flughafen nicht der Verteidigung zur Verfügung gestellt werden dürfen. Aber Filme, die von Flugpassagieren oder Gästen mit dem Smartphone oder einer Digitalkamera im Flughafen angefertigt wurden und womöglich genau dasselbe abbilden wie Überwachungskameras, werden keinen Beschränkungen unterliegen und wohl wie ein normales, der Verteidigung zugängliches Beweismittel angesehen. Diesen Widerspruch sollte der Gesetzgeber auflösen.

2.2. Staatliche Überwachungsgebäude, staatliche Mitarbeiter

Staatliche Überwachungsgebäuden und –techniken lassen sich, wie in dem Gesetzesentwurf, durchaus in den Begriff des „kritischen Infrastruktursubjekts“ einbeziehen.

Soweit die Weitergabe von Informationen über die Identität der beteiligten Mitarbeiter in den Sicherheitssubjekten nicht erfolgt, begegnet dies keinen Bedenken.

Welcher Mitarbeiter mit welcher Technik eine Überwachung vornimmt, ist eine Frage, die nicht per se Relevanz für die Strafverteidigung besitzen wird. Zudem ist es angesichts der Bedrohung staatlicher Strafverfolgung durch Organisierte Kriminalität oder Terrorismus von großer Bedeutung, dass sicherheitsrelevante Geheimnisse gewahrt bleiben, namentlich die Überwachungssubjekte nicht Gegenstand von Sabotagehandlungen oder gar terroristischen Anschlägen werden. Außerdem dürfen die in den Überwachungsinstitutionen tätigen Personen keinen Gefahren durch Dritte ausgesetzt werden. Insoweit sind auch im Strafverfahren die Geheimhaltungsinteressen des Staates und der Allgemeinheit sowie die Schutzinteressen des Personals zu berücksichtigen.

3. Europäische Vorgaben

3.1. Europäisches Sicherheitsrecht

Eine europarechtliche Definition der „kritischen Infrastruktur“, vor allem zum Schutz vor terroristischen Angriffen, findet sich in Art. 2 a) der EU-Richtlinie 2008/114/EG vom 8. 12. 2008¹: Danach ist eine kritische Infrastruktur

- eine in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon,
- die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind²
- und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten.

Auf europäischer Ebene zählen zu der „Europäischen Kritischen Infrastruktur“ die beiden Sektoren Energie (Strom, Öl, Gas) und Verkehr (Straßenverkehr, Schienenverkehr, Luftverkehr, Binnenschifffahrt, Hochsee- und Küstenschifffahrt und Häfen). In dieser Richt-

¹ Richtlinie über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (Amtsblatt der EU v. 23. 12. 2008, L 345/75).

² Dazu gehören nach der Richtlinie 2013/40/EU vom 12. August 2013 (4. Erwägungsgrund) namentlich Kraftwerke, Verkehrsnetze oder staatliche Netze.

linie werden dagegen staatliche Überwachungsgebäude, anders als im georgischen Gesetzesentwurf, an keiner Stelle zu den kritischen Infrastruktursubjekten gezählt. Solche Überwachungsgebäude werden in der Richtlinie nicht erwähnt.

Im deutschen Sicherheitsrecht wird dagegen der Kreis der Sektoren weiter gezogen. Zu ihnen gehören auch Staat und Verwaltung unter Einschluss der Justizbehörden.³

Eine europarechtliche Vorgabe, Informationen zu einem kritischen Infrastruktursubjekt oder aus einem kritischen Infrastruktursubjekt insbesondere in einem Strafprozess einem besonderen Geheimnisschutz zu unterwerfen, existiert – soweit ersichtlich – nicht. Die eben erwähnte Richtlinie schweigt sich darüber aus. Allerdings betont die Richtlinie an mehreren Stellen allgemein, dass den nationalen Geheimhaltungsinteressen des Staates Rechnung getragen werden müsse, d. h. gerade bei kritischen Infrastruktursubjekten die Bestimmungen zur Geheimhaltung eingehalten werden müssen.⁴

3.2. Europäisches Datenschutzrecht

Vielfach wird es sich bei den Daten aus dem Infrastruktursubjekt um sog. personenbezogene Daten handeln. Personenbezogene Daten sind solche Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person erstrecken.⁵ Dies ist etwa der Fall, wenn die Personen, die beispielsweise auf der Kamera-Aufzeichnung zu sehen sind, bereits namentlich bekannt oder zumindest identifizierbar sind. Damit ist zugleich der Anwendungsbereich des Datenschutzrechts eröffnet. Die im Mai 2018 in Kraft getretene EU-Datenschutz-Grundverordnung (DGSVO)⁶ enthält bewusst keine Regelungen für den Bereich des Sicherheits- und des Strafrechts: In Art. 2 Abs. 2 lit. d) der DGSVO ist geregelt, dass diese Verordnung keine Anwendung findet

auf die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

An die Stelle der DGSVO tritt für das Strafverfahren die Datenschutz-Richtlinie Polizei und Justiz 2016/680,⁷ also eine erst noch im jeweiligen nationalen Recht umzusetzende rechtliche Vorgabe. Die Richtlinie (EU) 2016/680 gilt – anders als noch der vorherige Rahmenbeschluss zum Datenschutz RB 2008/977/JI – nicht nur für grenzüberschreitende, sondern auch für rein innerstaatliche Sachverhalte. Die Umsetzung in Deutschland erfolgte inzwischen durch vielfältige Gesetzesänderungen, u. a. der Strafprozessordnung^{8,9} Die Richtlinie erlaubt für repressive und präventive Zwecke die Datenverarbeitung durch die zuständigen Behörden (Art. 1 RL), sofern sie verhältnismäßig ist und anderen datenschutzrechtlichen Vorgaben genügt, wie sie in Art. 4 der RL aufgestellt sind. Dabei ist es auch zulässig, dass die Behörden personenbezogene Daten an Außenstehende oder andere Dritte übermitteln, sofern die Voraussetzungen des Art. 4 RL gewahrt sind. Es ist also datenschutzrechtlich zulässig, personenbezogene Daten an die Verteidigung herauszugeben. Auch im 72. Erwägungsgrund der Richtlinie wird explizit die Übermittlung von personenbezogenen Daten für zulässig erachtet. Es wird darin aber eine strikte Anbindung an den Grundsatz der Erforderlichkeit vorgeschrieben. Wenn es für die Ausübung der Verteidigungsrechte erforderlich ist, diese Informationen an den Verteidiger des Tatverdächtigen zu übermitteln, so ist dies datenschutzrechtlich erlaubt. Die Richtlinie enthält auch Vorgaben für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen (Art. 35 ff. RL)

³ So das deutsche Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; abrufbar unter www.bbk.bund.de.

⁴ 7. und 18. Erwägungsgrund der Richtlinie 2013/40/EU.

⁵ Vgl. die Definition in Art. 4 Nr. 1 der DSGVO.

⁶ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

⁷ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

⁸ Im Folgenden als StPO abgekürzt.

⁹ Gesetz zur Anpassung des Datenschutzrechts an die VO (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DsAnpUG-EU) v. 30.07.2017, BGBl I 2017, 2097 ff.

3.3. Europäische Menschenrechtskonvention

Falls der Strafverteidigung kein Zugriff auf die genannten Informationen aus den kritischen Infrastruktursubjekten erhalten sollte, würde dies in den Anwendungsbereich des Art. 6 Abs. 1 S. 1 EMRK, das Recht des Beschuldigten auf ein faires Verfahren, fallen.

a) Waffen- und Chancengleichheit

Der prinzipiell ungehinderte Zugang zu Beweismitteln ist eine selbstverständliche Maxime eines rechtsstaatlichen Strafprozesses.¹⁰ Grundsätzlich besteht ein Recht des Beschuldigten bzw. seines Verteidigers auf Zugang zu allen Beweisen, über die die Anklage verfügt.¹¹ Dahinter steht der Gedanke der Waffen- und Chancengleichheit von Beteiligten in einem Strafverfahren.¹² Es kann aber geboten sein, bestimmte Beweise dem Beschuldigten und seinem Verteidiger vorzuenthalten, wenn dies im öffentlichen Interesse ist. Wenn somit bestimmte Informationen über kritische Infrastruktursubjekte einschließlich staatlicher Überwachungsstrukturen der Strafverteidigung nicht offengelegt werden, kann dies aus den genannten Geheimnis- und Sicherheitsgründen (z. B. wegen Terror- oder Sabotagerisiken) geboten sein.

Wenn die Staatsanwaltschaft oder das Gericht in der späteren Hauptverhandlung diese Beweise dennoch verwertet, bestünde in einem solchen Fall eine Verpflichtung der Verfahrensbeteiligten zur Kompensation: Die Nachteile, die der Verteidigung durch die Vorenthaltung eines Beweismittels entstehen, können und müssen durch andere Maßnahmen ausgeglichen werden. Dies kann vor allem durch die Hinzuziehung weiterer Beweismittel sowie die besonders sorgfältige Würdigung der für die Verteidigung nicht zugänglichen Beweismittel geschehen.¹³ Denn entscheidend ist

nach der ständigen Rechtsprechung des EGMR, dass in einer Gesamtbetrachtung das Verfahren *insgesamt* fair ist.¹⁴

Auf keinen Fall darf nach der Rechtsprechung des EGMR ein Beweismittel, das nur der Anklagebehörde im Ermittlungsverfahren oder dem Gericht, nicht aber der Verteidigung zur Verfügung stand, in einem voll kontradiktorischen Strafverfahren (wie z. B. in Georgien) als ausschließliches oder entscheidendes Beweismittel in der Hauptverhandlung verwendet werden.¹⁵ Diese Grundsätze fairer Beweisaufnahme, die vom EGMR für die Vernehmung eines anonymen Zeugen oder bei fehlender Frage- und Konfrontationsmöglichkeit durch die Verteidigung entwickelt wurden,¹⁶ können ohne weiteres auf die hier zu erörternden Fallkonstellationen übertragen werden.

b) Einziges entlastendes Beweismittel

Besonders problematisch ist Ausschluss des Angeklagten, wenn die Videoaufzeichnung das einzige und entscheidende Beweismittel ist, mit dem er seine Unschuld beweisen kann. Denn es bedeutet einen Verstoß gegen das Prinzip „in dubio pro reo“ und damit den „fair trial“-Grundsatz, wenn dem Angeklagten eine extrem hohe Entlastungs-Beweislast auferlegt wird, die jeden Beweis zugunsten des Angeklagten ausschließt.¹⁷ Man halte sich das Beispiel vor Augen, dass einem Angeklagten zu Unrecht vorgeworfen wird, er habe am Flughafen einen Polizisten verprügelt. Wenn die Polizisten falsch vor Gericht aussagen, wird dies der Angeklagte – sofern ihm nicht noch andere Beweismittel zur Verfügung stehen – nur dadurch entkräften können, dass eine entsprechende Aufnahme einer Videoüberwachungskamera zur Verfügung gestellt wird. Dann kann sich nur aus dieser Videoaufzeichnung ergeben, dass vielmehr er selbst verprügelt wurde. Ihm wäre der Zugriff auf diese Aufnahme

¹⁰ Jähnke/Schramm, Europäisches Strafrecht (EuStR), 2017, Kap. 9 Rn. 55.

¹¹ Meyer-Ladewig/Harrendorf/König, in: Mayer-Ladewig/Nettesheim/von Raumer, EMRK, 4. Aufl. 2017, Art. 6 Rn. 140.

¹² EGMR 22. 2. 1996 – 17358/90, Bulut v. Austria, Rn. 47: „each party must be afforded a reasonable opportunity to present his case under conditions that do not place him at a disadvantage vis-à-vis his opponent (...)“

¹³ Vgl. auch BGHSt 55, 70 Rn. 29 mit Bspr. Schramm HRRS 2011, 156.

¹⁴ EGMR NStZ 2007, 103 (Haas v. Deutschland); BVerfG NJW 2010, 925; Meyer-Gößner/Schmitt, Art. 6 EMRK Rn. 22a; Schramm, Internationales Strafrecht, 2. Aufl. 2018, Kap. 3 Rn. 49.

¹⁵ EGMR NJOZ 2010, 1903 Rn. 207. Vgl. auch Jähnke/Schramm, EuStR, Kap. 9 Rn. 26: „Was dem Gericht vorliegt, muss auch der Verteidiger kennen.“

¹⁶ Meyer-Gößner/Schmitt, 61. Aufl. 2018, Art. 6 EMRK Rn. 22a m. w. N.

¹⁷ Meyer-Ladewig/Harrendorf/König, in: Mayer-Ladewig/Nettesheim/von Raumer, EMRK, Art. 6 EMRK Rn. 140.

me verweigert, sofern nicht doch die Staatsanwaltschaft selbst dieses Beweismittel einführt.

c) **Qualifizierter Richtervorbehalt**

Nach alledem wäre es unter dem Gesichtspunkt des fairen Verfahrens wünschenswert, wenn die Verteidigung vom Zugriff auf die Videoaufnahmen oder anderen Computerdaten aus dem kritischen Infrastruktursubjekt nicht ausgeschlossen wäre. Dafür dürfte freilich ein bloßer Antrag an eine Strafverfolgungsbehörde nicht ausreichen. Es müsste wegen der möglicherweise hohen Sicherheitsrelevanz des kritischen Infrastruktursubjekts einem Richtervorbehalt (auch Richterprivileg genannt) unterstellt werden. Dabei könnte man nicht nur einem einfachen, sondern einem qualifizierten Richtervorbehalt einführen: Denkbar wäre es etwa, dass über den Antrag ein speziell für den Staatsschutz zuständiges Strafgericht entscheidet (vergleichbar einer deutschen Staatsschutzkammer beim Landgericht gem. § 74 a GVG). Außerdem könnte man die Entscheidung nicht nur in die Hand eines einzigen Richters legen, sondern stattdessen mehrere Richter (etwa 3 Richter) über die Weitergabe der Informationen an den Angeklagten entscheiden lassen.¹⁸ Diese gerichtliche Entscheidung sollte wiederum selbst durch ein anderes Gericht (etwa in Form einer Beschwerte) überprüft werden können.

4. **Regelungen in der deutschen Strafprozessordnung**

Der Begriff des „kritischen Infrastruktursubjekts“ taucht in der deutschen StPO nicht auf. Es finden sich auch im sonstigen Strafverfahrensrecht Deutschlands keine Regelungen zur kritischen Infrastruktur. Nur im materiellen Strafrecht wird in der Sache diese Infrastruktur erwähnt und mit einem verstärkten strafrechtlichen Schutz versehen, namentlich im Straftatbestand der Computersabotage (§ 303b Abs. 4 Nr. 3 StGB)¹⁹

¹⁸ So verfährt man etwa in Deutschland bei der Anordnung der akustischen Raumüberwachung (sog. großer Lauschangriff-§ 100c StPO) oder der Online-Durchsuchung (§ 100b StPO) nach der Verfahrensregelung des nach § 100e Abs. 2 StPO i. V. m. § 74 a Abs. 5, 76 Abs. 2 GVG; vgl. SK-StPO-Frister, § 74a GVG Rn. 32.

¹⁹ Vgl. Schramm, Strafrecht Besonderer Teil 1, 2017, § 6 Rn. 59.

oder bei der Störung öffentlicher Betriebe (§ 316b Abs. 1 StGB).

a) **Schutz der Geheimhaltungsinteressen über Sperrerkklärungen**

Verfahrensrechtlich schützt die deutsche StPO die Geheimhaltungsinteressen des Staates und die Vertraulichkeit der Behörden mit den allgemeinen Rechtsinstituten der Aussagegenehmigung und der Sperrerkklärung.

So ist die Vernehmung von Polizisten, Staatsanwälten, Richtern, Verwaltungsbeamten oder anderen Angehörigen des öffentlichen Dienstes aufgrund ihrer dienstlichen Verschwiegenheitspflicht ausnahmsweise nur dann möglich, wenn zuvor eine Aussagegenehmigung der zuständigen höherrangigen Behörde eingeholt wurde (§ 54 StPO). Liegt diese Genehmigung nicht vor, sind die Beamten zur Zeugnisverweigerung verpflichtet.²⁰ Ähnlich verhält es sich, wenn Behörden in sonstiger Weise um Auskunft gebeten werden oder von einer staatlichen Stelle die Herausgabe von Akten oder anderen in amtlicher Verwahrung befindlichen Sachen verlangt wird (z. B. Computerdateien, Videoaufnahmen²¹): Auch dies kann die oberste Dienstbehörde verweigern (§ 96 StPO). Diese Weigerung (sog. Sperrerkklärung) ist aber nur dann begründet, wenn das Bekanntwerden der Akten usw. dem Wohl der Bundesrepublik oder eines Bundeslandes Nachteile bereiten würde. Eine solche Preisgabe von Informationen bzw. solch Vernehmungen von Zeugen (Mitarbeitern) aus dem Bereich der kritischen Infrastruktursubjekte nur nach Genehmigung der obersten Dienstbehörde wäre womöglich auch für den georgischen Strafprozess eine legislative Mechanismus zum Schutz staatlicher Geheimhaltungsinteressen.

b) **Richterliche Überprüfung von Überwachungsmaßnahmen; G 10 – Gesetz**

Betont werden muss zudem, dass gleichermaßen eine richterliche Anordnung für die Preisgabe von Informationen im Zusammenhang eines kritischen Infrastruktursubjekts rechtsstaatlich auch in Georgien in den Fällen vorzugswürdig wäre, in denen die Staatsanwaltschaft und Polizei diese Informationen nutzen möchte.

²⁰ Eschelbach, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 54 Rn. 2; Percic, Münchener Kommentar zur StPO, 2014, § 54 Rn. 1.

²¹ Eschelbach, in: Satzger/Schluckebier/Widmaier, § 96 Rn. 2.

In Deutschland ist der Zugriff der Polizei und der Staatsanwaltschaft auf den Inhalt einer Telekommunikation (§ 100a StPO), einer Online-Durchsuchung (§ 100b StPO), auf die Verkehrsdaten eines Telekommunikationsvorgangs (§ 100j StPO) oder etwa auf Videofilme, die auf einem Computer oder Smartphone gespeichert sind (Beschlagnahme nach §§ 94, 98 StPO), nur auf der Grundlage einer richterlichen Anordnung möglich (§ 98 Abs. 1, § 100e Abs. 1 S. 1 StPO). Andernfalls würde die Gefahr drohen, dass zur Aufklärung der Straftaten ohne richterliche Genehmigung heimliche Abhörmaßnahmen durchgeführt werden. Es könnte dann vielleicht auch keiner feststellen, ob eine solche Überwachung überhaupt stattgefunden hat. Zwar besteht die Möglichkeit für die Strafverfolgungsbehörden, in Eilfällen auch ohne richterliche Anordnung abzuhören bzw. eine Beschlagnahme durchzuführen. Aber diese Maßnahme muss dann innerhalb von drei Tagen gerichtlich bestätigt werden (§ 98 Abs. 2 S. 1, § 100e Abs. 1 S. 2, 3 StPO).

Hierzu sei auch auf die eingangs (unter II.) erläuterte Entscheidung des Verfassungsgerichts Georgiens vom 14. 4. 2016 hingewiesen, in dem eine „überzeugende Prozesstransparenz und Kontrollmechanismen auf der legislativen Ebene“ gefordert wurden, um einen direkten Zugriff auf Kommunikationskanäle durch nationale Sicherheitsbehörden zu verhindern.²²

Damit wird zugleich eine weitere europarechtliche Dimension berührt: Eine gerichtliche Kontrolle der Anordnung sowie gegebenenfalls auch der Durchführung der Überwachungsmaßnahme würde das Recht des Angeklagten auf Schutz seiner privaten Daten – die vom Europäischen Gerichtshof für Menschenrechte als Teil des Privatlebens im Sinne von Art. 8 EMRK angesehen werden²³ – institutionell besonders absichern. Bei der staatlichen Kommunikationsüberwachung ist das Miss-

brauchsrisiko sehr hoch und muss das innerstaatliche Recht nach den Vorgaben der EGMR-Rechtsprechung willkürliche Eingriffe durch Behörden verhindern: Diejenige Person oder Einrichtung, die für die Genehmigung der Abhörmaßnahme zuständig ist, muss unabhängig sein und einer gerichtlichen oder sonst unabhängigen Kontrolle unterliegen. Die Abhörmaßnahmen müssen zeitlich beschränkt sein, wie auch Regelungen getroffen werden müssen, die eine unveränderte Übermittlung von Abhörprotokollen an den Verteidiger ermöglichen.²⁴

Anders verhält es sich aber etwa in Deutschland dann, wenn deutsche Sicherheitsbehörden nicht repressiv tätig sind, d. h. keine Straftaten verfolgen, sondern vielmehr vorbeugend präventiv-polizeilich oder weit im Vorfeld einer konkreten Rechtsgutsgefährdung²⁵ tätig sind: Die deutschen Verfassungsschutzbehörden und der deutsche Bundesnachrichtendienst können auch ohne richterliche Anordnung die Telekommunikation dann überwachen und aufzeichnen, wenn es zur Abwehr einer Gefahr für die freiheitlich-demokratische Grundordnung erforderlich ist (§ 1 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, sog. G-10-Gesetz).²⁶ Allerdings unterliegt die Tätigkeit einer Kontrolle durch ein parlamentarisches Kontrollorgan nach § 16 G 10-Gesetz sowie eine G 10-Kommission²⁷ bzw. nach § 16 des Gesetzes über den Bundesnachrichtendienst durch ein unabhängiges Gremium, das aus drei Bundesrichtern zusammengesetzt ist und dem Parlamentarische Kontrollgremium berichtet.

5. Würdigung

Videoaufnahmen oder anderen Computerdateien aus einem kritischen Infrastruktursubjekt tangieren im Regelfall staatliche Geheimhaltungsinteressen. Mit Blick

²² Vgl. გეგეშიძე, ელექტრონული კომუნიკაციების საშუალებებიდან მოპოვებული ინფორმაციის სისხლის სამართლის პროცესში გამოყენება – ქართული სამართალი და საერთაშორისო სტანდარტები, გერმანულ-ქართული სისხლის სამართლის ჟურნალი, მეორე გამოცემა – აგვისტო, 2017 წელი 44 (= Gegeshidze, Die Verwendung von erlangten Daten aus der elektronischen Kommunikation im Strafprozess – das georgische Recht und internationale Standards, Deutsch-georgische Strafrechtszeitung 2017, S. 44).

²³ EGMR NJW 2007, 1433 Rn. 76 ff (Weber/Saravia v. Deutschland.); Meyer-Ladewig/Nettesheim, in: Mayer-Ladewig/Nettesheim/von Raumer, EMRK, Art. 8 EMRK Rn. 32.

²⁴ Meyer-Ladewig/Nettesheim, in: Mayer-Ladewig/Nettesheim/von Raumer, EMRK, Art. 8 EMRK Rn. 39 unter Verweis auf EGMR NJW 2007, 1433 (Weber/Saravia v. Deutschland).

²⁵ Roggan, in: G-10-Gesetz, Kommentar, 2012, G 10 § 1 Rn. 3 – 5.

²⁶ Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) v. 26. Juni 2001 (BGBl. I S. 1254), zuletzt geändert durch Gesetz vom 7. Dezember 2011 (BGBl. I S. 2576, 2580).

²⁷ Zur Konformität dieses Gesetzes mit Art. 8 EMRK vgl. EGMR 2007, 1433 (Weber/Saravia v. Deutschland).

auf etwaige Gefährdungen dieser Infrastrukturen und ihres Personals durch Sabotage, Akte des Terrorismus, Einschüchterungen oder Drohungen ist es legitim, diese Dateien nicht ohne weiteres der Verteidigung zur Verfügung zu stellen. Da solche Dateien aber durchaus für die Verteidigung und den Angeklagten von entscheidender Bedeutung sein können, namentlich wenn sie den Angeklagten entscheidend entlasten, ist ein ausnahmsloser Ausschluss des Zugangs zu solchen Beweismitteln unter dem Gesichtspunkt des fairen Verfahrens (Art. 6 EMRK) europarechtlich nicht vertretbar. Es sollte aber dann ein richterlicher Genehmigungsvorbehalt eingeführt werden, d. h. ein Gericht sollte darüber befinden, ob dem Verteidigungsinteresse des Angeklagten ein größeres Gewicht beizumessen ist als dem Geheimhaltungs- und Schutzinteressen des Staates und der Allgemeinheit. Hier könnte man das Gesetz auch so gestalten, dass man prinzipiell die Herausgabe erlaubt und im Rahmen einer Ausnahme-Klausel diese Herausgabe nur im Ausnahmefall einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung verbietet. Im Sinne der Waffengleichheit in einem kontradiktorischen Strafverfahren wäre es dann auch konsequent, auch die überwachende Tätigkeit der staatlichen Sicherheits- und Strafverfolgungsbehörden – in Anlehnung an das deutsche Modell (§§ 98, 100e StPO) – insoweit einem Richterprivileg zu unterwerfen: Sie sollten in einem Strafverfahren dann solche Daten auch erst nach der Genehmigung durch ein Gericht erheben oder erhalten können.

Zentrale Aspekte der Telefonüberwachung nach der georgischen StPO*

Von Assistent-Prof. Dr. *Maka Khodeli*, LL. M. (Freiburg i.Br.), Iwane-Dschawachischwili-Staatliche-Universität Tbilissi

I. Einleitung

Das Thema der Telefonüberwachung erregt bis heute eine leidenschaftliche Diskussion. Die Durchführung der Telefonüberwachung gehörte bis zum 1. August 2014 zum sog. postsowjetischen Modell der Regulierung von operativ-ermittelnder Tätigkeit.¹ Im Wesentlichen das bedeutet dies, dass nur weniger strenge Vorschriften die Durchführung der operativen Maßnahmen regeln. So bestimmt der Gesetzgeber beispielsweise keinen Katalog von Anlassstraftaten als wichtige materielle Voraussetzung für die Durchführung der operativen Maßnahmen.² Aufgrund des Gesetzes vom 1. August 2014³ wurde die Überwachung und Aufzeichnung von Telefongesprächen⁴ als eine verdeckte Ermittlungsmaßnahme in der georgischen Strafprozessordnung⁵ reguliert.⁶

Die Effizienz und Notwendigkeit der Telefonüberwachung zum Zweck der Strafverfolgung stehen nicht in Frage. Wegen ihrer besonders sensiblen Rechtsnatur wurde es als zweckmäßig angesehen, diese Maßnahme vollständig im strafprozessgesetzlichen Rahmen einzuschränken.⁷ Interessant ist die Auseinandersetzung mit

der Frage, inwieweit die in der georgischen StPO angelegten Vorschriften rechtsstaatlichen Anforderungen und verfassungsrechtlich bestimmten Standarten entsprechen. Um diese Frage zu klären, werden im vorliegenden Aufsatz sowohl die wichtigen verfassungsrechtlichen (II. Teil) als auch strafprozessrechtlichen (III. Teil) normativen Grundlagen dargestellt. Im IV. Teil werden in einem Fazit die Schlussfolgerungen gezogen.

II. Verfassungsrechtliche Grundlagen der Telefonüberwachung

Die Unantastbarkeit der Privatsphäre, die Unverletzlichkeit der persönlichen Kommunikation und das Fernmeldegeheimnis sind in der Verfassung von Georgien verankerte, aber keine absoluten Grundrechte.⁸ Bei Vorliegen der entsprechenden Voraussetzungen sind Einschränkungen dieser Grundrechte, u.a. zur Durchführung einer Telefonüberwachung, gesetzlich zugelassen.

In Bezug auf die gesetzlich bestätigten Einschränkungen der Unantastbarkeit der Privatsphäre und der Unverletzlichkeit der persönlichen Kommunikation sollte betont werden, dass es einen absoluten unantastbaren geschützten Kernbereich der privaten Lebensgestaltung gibt.⁹ Nach dem georgischen Verfassungsgericht gehören zum Kernbereich der privaten

* Deutsche Übersetzung des Aufsatzes von Assistent-Prof. Dr. *Maka Khodeli*.

¹ *Usenashvili, Jaba*, Journal of Law, 2 (2012), 82, 87.

² *Usenashvili, Jaba*, Journal of Law, 2 (2012), 82, 95.

³ Gesetz vom 1. August 2014, №2634, (abrufbar unter: <http://info.parliament.ge/file/1/BillReviewContent/33336> zuletzt abgerufen am 22.07.2019).

⁴ Es sei darauf hingewiesen, dass infolge der Gesetzesänderung vom 22. März 2017 in der georgischen Strafprozessordnung der –Begriff der „Überwachung des Telefongesprächs“ in „Überwachung der telefonischen Kommunikation“ geändert wurde. Letzterer ist ein weiter Begriff und beinhaltet auch Telefongespräche. Siehe *Khodeli, Maka*, Die Überwachung und Aufzeichnung von Telefongesprächen im Strafprozess (nach georgischem und deutschem Recht), 2019, S. 213 ff.

⁵ Im Folgenden als StPO abgekürzt.

⁶ Art. 143¹-143¹⁰ StPO.

⁷ *Khodeli, Maka*, Die Überwachung und Aufzeichnung von Telefongesprächen im Strafprozess (nach georgischem und deutschem Recht), 2019, S. 254ff.

⁸ Art. 12 und Art. 15 georgische Verfassung.

⁹ Bemerkenswert ist die Ansicht des georgischen Verfassungsgericht, dass „Kernbereich der privaten Lebensgestaltung [...] soll vor der Überwachung vom Staat und jene dritten Person besonders geschützt sein“ (Entscheidung des georgischen Verfassungsgerichts – „Ombudsman und andere gegen georgisches Parlament“ vom 14. April 2016, №1/1/625, 640, (abrufbar unter: <https://www.constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-dameveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lasha-tugushi-zviad-qoridze-aaip-fondi-giasazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page>, zuletzt abgerufen am 22.07.2019).

Lebensgestaltung „intime, sexuelle Beziehungen, das Familienleben, menschliche Gewohnheiten, im Rahmen einer Beichte vor einem Geistlichen offenbarte Informationen, Ergebnisse ärztlicher Untersuchungen, in der Privatsphäre geäußerte menschliche Emotionen und Gefühle“.¹⁰ Die Gewährleistung eines absoluten Schutzes des Kernbereichs der privaten Lebensgestaltung ist jedoch mit praktischen Schwierigkeiten verbunden. Auch das deutsche Bundesverfassungsgericht hat angemerkt, dass sich eine Erhebung von Kommunikationsinhalten mit Kernbereichsbezug im Voraus häufig kaum vermeiden lässt.¹¹ Mit der Einfügung der Vorschriften über den unantastbaren und absolut geschützten Kernbereich der privaten Lebensgestaltung in der StPO sollte eine besondere Garantie für den Schutz der Menschenrechte verankert werden. Was deren Kriterien betrifft, kommt es vor allem auf eine richtige Bestimmung des Adressaten (Objekt¹²) der Überwachungsmaßnahmen an. Es sollen nur solche Personen überwacht werden, die eine direkte Verbindung mit der Zielperson der Überwachung haben; ansonsten muss die Durchführung der Überwachungsmaßnahme sofort unterbrochen werden.

Um die besondere Bedeutung des Kernbereichs der privaten Lebensgestaltung zur Geltung zu bringen, sollte dieser von der georgischen StPO auch unter besonderem Schutz gestellt werden; wie es z.B. in der deutschen StPO der Fall ist. Wünschenswert ist es daher, auch in der georgischen StPO Vorschriften einzuführen, die sowohl die Erhebung als auch die Verwertung aus dem Kernbereich privater Lebensgestaltung gewonnener Er-

kenntnisse regeln.¹³ Erforderlich ist dafür eine gesetzliche Regelung nach der es möglich ist, die Überwachung und Aufzeichnung von Telefongesprächen jederzeit – zu Gunsten des Schutzes des Kernbereichs der privaten Lebensgestaltung – zu unterbrechen.

III. Strafprozessuale Grundlagen der Telefonüberwachung

Eine wichtige materielle Voraussetzung für die Durchführung der Telefonüberwachung ist die Bestimmung eines Straftatenkatalogs, d.h. eine vom Gesetzgeber vorgenommene Beschränkung der Eingriffe in das Fernmeldegeheimnis auf bestimmte abschließend aufgeführte Straftaten. In der georgischen StPO wurden zur Bestimmung dieses Katalogs sowohl die Kategorien von Straftaten als auch eine Reihe von konkreten Tatbeständen verwendet (Art. 143³ Abs. 2 StPO).

Wie schon erwähnt wurde, ein bedeutender Punkt ist richtige Bestimmung des Adressaten der Telefonüberwachung. In der Terminologie der georgischen StPO wird diese Person als „Objekt“ der verdeckten Ermittlungsmaßnahmen (Art. 3 Abs. 31 StPO) bezeichnet. Der georgische Gesetzgeber hat drei Personengruppen definiert, gegen welche im Falle des Vorliegens eines hinreichenden Tatverdachts verdeckte Ermittlungsmaßnahmen durchgeführt werden dürfen:

1. Personen, die verdächtig sind, eine von den in Art. 143³ Abs. 2 Satz „a“ gelisteten Straftaten begangen zu haben („mit der Straftat in direktem Kontakt stehende Person“);
2. Personen, die von der mit der Straftat in direktem Kontakt stehenden Person bestimmte von ihr herührende Mitteilungen entgegengenommen oder an sie weitergegeben haben;
3. Personen, deren Kommunikationsmittel von der mit der Straftat in direktem Kontakt stehenden Person benutzt werden.

Umstritten ist dabei die in Art. 143³ Abs. 2 –verwendete Formulierung „mit der Straftat in direktem Kontakt stehende Person“. Dieser Begriff kann durchaus zu einer sehr weiten Auslegung des Objekts der Telefonüberwachung führen. Besonders wenn man berücksichtigt, dass

¹⁰ Entscheidung des georgischen Verfassungsgerichts – „Ombudsman und andere gegen georgisches Parlament“ vom 14. April 2016, №1/1/625, 640, (abrufbar unter: <https://www.constcourt.ge/ge/legal-acts/judgments/saqartvelos-saxalxo-damcveli-saqartvelos-moqalaqeebi-giorgi-burdjanadze-lika-sadjaia-giorgi-gociridze-tatia-qinqladze-giorgi-chitidze-lashatugushi-zviad-qoridze-aaip-fondi-gia-sazogadoeba-saqartvelo-aaip-saertashoriso-gamchvirvaloba-saqartvelo-aaip-saqar.page>, zuletzt abgerufen am 22.07.2019).

¹¹ Bundesverfassungsgericht 2 BvR 236/08, Beschl. v. 12.10.2011, Anmerkungen B. Gercke, StV 2012, 257, 259.

¹² Begriff – Objekt (Adressat) verdeckter Ermittlungsmaßnahmen wurde aufgrund des am 22. März 2017 verabschiedeten Gesetzes über die Änderung der georgischen StPO bestimmt, (№476-IIS), (abrufbar unter: <https://matsne.gov.ge/ka/document/view/3597520#DOCUMENT:1> zuletzt abgerufen am 22.07.2019), siehe, Art. 3 Abs. 31.

¹³ Vgl. §100d deutsche StPO.

bei einer telefonischen Kommunikation die Zahl der Betroffenen ohnehin häufig sehr hoch ist.¹⁴ So definiert die deutsche StPO – anders als die georgische – als Objekt der Überwachung den Beschuldigten und die mit ihm verbundenen Personen.¹⁵

Wie bereits erwähnt, sind verdeckte Ermittlungsmaßnahmen nur gegen bestimmte Personen, d.h. konkret bestimmte Adressaten zulässig. Mit der Bestimmung des Beschuldigten als Betroffenen der Überwachungsmaßnahme betont die deutsche StPO, dass nicht schon abstrakte Vermutungen einen hinreichenden Anlass geben können, sondern vielmehr bestimmte Tatsachen den Verdacht der Begehung einer schweren Straftat begründen müssen. Insofern besteht in Georgien das Problem einer nicht eindeutigen Rechtslage, da die Bestimmung des Objekts der Überwachung zu der Auslegung unterliegt und somit von Fall zu Fall individuell interpretiert werden kann. Wäre aber in der georgischen StPO als Objekt der Überwachungsmaßnahme der Beschuldigte bestimmt worden, dann wäre diese nicht mehr erfolgversprechend, da nach der georgischen StPO ein Beschuldigter sofort über seine Rechte zu belehren ist. Dazu muss man bemerken, dass die Telefonüberwachung nicht nur bei der Anklageerhebung, sondern schon dann verwendet wird, wobei es noch kein Beschuldigte gibt.

Zur Gewährleistung der Beachtung der Grundrechte und des Bestehens eines verfahrensrechtlichen Standards bedarf es normativer Voraussetzungen für die Durchführung der Telefonüberwachung. Derselbe Standard ist auch für die Erhebung der Anklage gesetzlich vorgesehen, namentlich ein hinreichender Tatverdacht (Gesamtheit von Tatsachen und Informationen, die zu-

sammen mit aktuellem Ermittlungsstand aus objektiver Sicht genügen, um die mögliche Begehung einer Straftat anzunehmen, Art. 3 Abs. 11 georgische StPO).

Die Besonderheit der Verfahrenssituation der Telefonüberwachung bedingt auch deren besondere Regulierung, d.h. die betreffenden gesetzlichen Vorschriften in der StPO. Diesbezüglich ist insbesondere auf das Institut des Richtervorbehalts hinzuweisen. Jedoch existieren in diesem Zusammenhang mehrere Problempunkte.¹⁶ Besonders kritisch diskutiert wird die Frage des Prüfungsumfanges des anordnenden Richters, da dieser keine umfassende Kontrollmöglichkeit hat. In diesem Kontext ist anzumerken, dass im georgischen Parteiprozess die Verstärkung der Kontrollfunktion von Richtern im Ermittlungsverfahren nur schwer vorstellbar ist. Abgesehen von den bestehenden Kritikpunkten (Schwäche der Kontrollmechanismen, Zeitdruck) spielt der Richtervorbehalt unbestritten eine verhindernde Rolle im Hinblick auf mögliche Rechtsmissbräuche durch die Exekutive. Der Richter als neutraler Dritter stellt einen wichtigen Garanten des Rechtsschutzes dar. Darüber hinaus ist nicht ersichtlich, welches Rechtsinstitut effektiver und geeigneter sein könnte als der Richtervorbehalt.

Es sei darauf hingewiesen, dass der Richtervorbehalt nicht mit der Ermittlungsphase endet. Nach Art. 219 georgische StPO, prüft der Richter die Verwertbarkeit der erlangten Beweismittel (einschließlich des durch eine Telefonüberwachung gewonnenen Beweismaterials). Der Richtervorbehalt spielt also auch im prozessualen Verfahren eine Rolle, da es dem Richter obliegt, die Rechtmäßigkeit der im Ermittlungsverfahren erlangten Ergebnisse zu bewerten. Insgesamt führt diese Form der Kontrolle zur Disziplinierung und Gesetzestreue der Ermittlungsbehörden und hat damit eine positive Wirkung auf deren Tätigkeit.

Es soll auch darauf hingewiesen werden, dass nach der georgischen StPO das zur Durchführung befugte Organ nach Beendigung der Überwachungsmaßnahme verpflichtet ist, ein Protokoll zu erstellen und an das Gerichtsregister zu senden (Art. 143⁷ Abs. 14 StPO). Dieses Erfordernis bestätigt wiederum die weitreichende Wirkung des Richtervorbehalts im Kontrollsystem der verdeckten Ermittlungsmaßnahmen auch nach der Be-

¹⁴ Es ist darauf hinzuweisen, dass der Europäische Gerichtshof eine ähnliche Formulierung (im Gesetzestext von Moldawien) als sehr breit und dementsprechend, streitig bewertet hat. siehe, *Korff, Douwe/Cannataci, Joseph A./Sutton, Graham*, Opinion of the Directorate General Human Rights and Rule of Law Data Protection Unit on the Draft laws of Georgia relating to Surveillance Activities of Law Enforcement Authorities and National Security Agencies, Council of Europe, DGI (2014) 8, Strasbourg, 14 February 2014, 18-19, (abrufbar unter: <https://rm.coe.int/16806af19b>, zuletzt abgerufen am 22.07.2019).

¹⁵ § 100a Abs. 3 deutschen StPO: Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

¹⁶ *Khodeli, Maka*, Die Überwachung und Aufzeichnung von Telefongesprächen im Strafprozess (nach georgischem und deutschem Recht), 2019, Kapitel I, 6.2.2.; Kapitel II, 5.2.2.

endigung dieser Maßnahmen. Als weitere Ausdrucksform der justiziellen Kontrolle ist auf Art. 143⁶ Abs. 15 hinzuweisen, wonach die zuständige Behörde bereits während der Durchführung der verdeckten Ermittlungsmaßnahmen auf Anfrage des Staatsanwalts/Richters ein Zwischenprotokoll erstellen muss.

Es ist begrüßenswert, dass aus Gründen der Transparenz nach der Beendigung der Telefonüberwachung deren Eintragung in das Gerichtsregister der verdeckten Ermittlungsmaßnahmen gesetzlich vorgesehen ist (Art. 143¹⁰ StPO). Dies dient vor allem dem Gewinn des öffentlichen Vertrauens sowie dem Zwecke der tatsächlichen Bewertung verdeckter Ermittlungsmaßnahmen.¹⁷

Die kriminalistische Eignung der Telefonüberwachung als Ermittlungsmaßnahme beruht auf ihrer Heimlichkeit. Freilich liegt in der Heimlichkeit auch die besondere prozessuale Problematik dieser Maßnahme. Da der Betroffene nicht weiß, dass er Objekt einer verdeckten Ermittlungsmaßnahme ist, kann er seine Rechte nicht geltend machen. Eine bedeutende Rolle spielt daher die gesetzlich vorgesehene Pflicht, die Adressaten der Telefonüberwachung zu benachrichtigen. Hinzuweisen ist allerdings auch darauf, dass diese Benachrichtigungspflicht zu einer Überlastung der Ermittlungsbehörden führen kann, weil die Zahl der zu benachrichtigenden Personen häufig sehr hoch ist.

Die georgische StPO sieht keine Ausnahmen von der Benachrichtigungspflicht vor. Es soll unterstrichen werden, dass bei einem Unterbleiben der Benachrichtigung ein – wie auch immer gestaltetes – nachträgliches Kontrollsystem nicht greifen und somit die Gewährleistung der Rechte der Betroffenen nicht garantiert werden kann. Die Umsetzung der Benachrichtigungspflicht dient also dazu, das während einer Telefonüberwachung objektiv bestehende Defizit des Schutzes der Grundrechte zu überwinden.¹⁸ Dementsprechend ist der Staat, der das Telefongespräch eines Bürgers über-

wacht, verpflichtet, nach der Beendigung der Maßnahme alle Überwachungsadressaten ausnahmslos zu benachrichtigen.

Besonders kritisch diskutiert werden die Fragen der technischen Durchführung der Telefonüberwachung und die Ausübung der Kontrolle^{19,20}. Dies bestätigt das gegenwärtig vor dem georgischen Verfassungsgericht laufende Verfahren, das die Tätigkeit der operativ-technischen Agentur, die u.a. für die Durchführung von Telefonüberwachungen zuständig ist, und die Verfassungsmäßigkeit der entsprechenden gesetzlichen Regulierung betrifft.²¹

IV. Fazit

Aufgrund der vorangehenden Ausführungen ist zusammenzufassen, dass die gesetzliche Regulierung der Telefonüberwachung nach georgischem Recht dem europäischen Standard grundsätzlich entspricht. Das verdient eine positive Bewertung.

Zugunsten von Sicherheitsgründen und des Strafverfolgungsinteresses erlaubt der Gesetzgeber die Einschränkung der Privatsphäre und des Fernmeldegeheimnisses. Dies ist unumstritten und in einem modernen Staat unvermeidlich. Die Überwachungsmaßnahmen als ein wirksames und effektives Mittel der Verbrechensbekämpfung sind für die Strafverfolgungsbehörden unverzichtbar. Die Ermittlungsbehörden sollen befugt sein, durch Telefonüberwachung Informationen legal zu gewinnen. Allerdings verlangt die rechtliche Regulierung dieses Bereiches besonderes Fingerspitzengefühl des Staates. Von hoher Bedeutung für die Gewährleistung der Rechtsstaatlichkeit ist es, die normativen Voraussetzungen klar und für den Einzelnen erkennbar gesetzlich festzulegen. Ein sehr kritischer Punkt besteht in der Umsetzung verdeckter Überwachungsmaßnahmen in der Praxis. Nach den sta-

¹⁷ Siehe die statistischen Angaben zur Telefonüberwachung, (abrufbar unter: <http://www.supremecourt.ge/farulebi> zuletzt abgerufen am 22.07.2019), *Khodeli, Maka*, Die Überwachung und Aufzeichnung von Telefongesprächen im Strafprozess (nach georgischem und deutschem Recht), 2019, Kapitel II, 5.5.

¹⁸ Siehe *Kleih, Björn-Christian*, Die strafprozessuale Überwachung der Telekommunikation, Unter besonderer Berücksichtigung drahtloser lokaler Netzwerke, 2010, S. 268; Vgl.: Bundesverfassungsgericht 109, 279.

¹⁹ Bemerkenswert sind die Kontrollmechanismen des Parlaments, Gerichts, Staatsinspektors und Staatsrechnungshofs, siehe *Khodeli, Maka*, Die Überwachung und Aufzeichnung von Telefongesprächen im Strafprozess (nach georgischem und deutschem Recht), 2019, Kapitel II, 5.3.2.

²⁰ *Khodeli, Maka*, Die Überwachung und Aufzeichnung von Telefongesprächen im Strafprozess (nach georgischem und deutschem Recht), 2019, Kapitel II, 5.3.

²¹ Abrufbar unter: <https://matsne.gov.ge/ka/document/view/3982960> (zuletzt abgerufen am 22.07.2019).

tistischen Angaben zur Telefonüberwachung²² besteht ein Risiko darin, dass diese effektive Maßnahme zu einem Massengeschäft in der Hand der Ermittlungsbehörden werden könnte. In der Praxis muss gewährleistet sein, dass die gesetzlich vorgesehenen Vorschriften über die Telefonüberwachung sorgfältig und präzise ausgeführt werden. Das Gesetz wiederum lässt die Anwendung verdeckter Überwachungsmaßnahmen nur als letztes Mittel (Ultima Ratio) zu.

²² Siehe die statistischen Angaben zur Telefonüberwachung, (abrufbar unter: <http://www.supremecourt.ge/farulebi> zuletzt abgerufen am 22.07.2019).

Einführung in das deutsche Strafvollzugsrecht – am Beispiel Nordrhein-Westfalens

Von wissenschaftlicher Mitarbeiterin *Edith Arians*, Institut für Strafrecht und Strafprozessrecht
Universität zu Köln

Der Strafvollzug wird meist erst bei negativen Begebenheiten oder Vorkommnissen beachtet – ganz nach dem Motto: „Only bad news are good news.“ An solche schließt sich zumeist eine gesellschaftliche und kriminalpolitische Debatte an, die nicht selten das gesamte System in Frage stellt. Im Folgenden sollen die Grundlagen des deutschen Strafvollzugsrechts skizziert werden: Auf welche normative Grundlage wird dieses Rechtsgebiet gestützt? Wozu dient der Strafvollzug? Was soll und was kann dieser leisten?

I. Einleitung und Begrifflichkeiten

Das Strafvollzugsrecht stellt die rechtliche Grundlage für den Vollzug der Freiheitsstrafe dar. Normiert wird das „Wie“ des Strafvollzuges. Das „Ob“ der Freiheitsstrafe wird in dem vorgeschalteten Strafverfahren (insbesondere nach den Vorschriften des Strafgesetzbuches¹ und der Strafprozessordnung²) mit der Verurteilung verbindlich geklärt. Der Strafvollzug umfasst alle stationären freiheitsentziehenden Kriminalstrafen. Beginnend mit der Aufnahme des Verurteilten in die Justizvollzugsanstalt bis zu dessen Entlassung aus der selbigen. Konkret werden folgende freiheitsentziehende Kriminalstrafen erfasst: Die Freiheitsstrafe (§§ 38 f. StGB); die Jugendstrafe (§§ 17 f. Jugendgerichtsgesetz³); die Unterbringung in einem psychiatrischen Krankenhaus (§ 63 StGB); in einer Entziehungsanstalt (§ 64 StGB); in der Sicherungsverwahrung (§§ 66 StGB).⁴

¹ Im Folgenden als StGB abgekürzt.

² Im Folgenden als StPO abgekürzt.

³ Im Folgenden als JGG abgekürzt.

⁴ Die Untersuchungshaft (§§ 112 StGB) sowie die Abschiebungshaft gem. § 62 Aufenthaltsgesetz (AufenthG) sind als freiheitsentziehende stationäre Maßnahme zu qualifizieren. Die Untersuchungshaft dient jedoch der Sicherung zur Durchführung des staatlichen Strafverfahrens und der nachfolgenden Strafvollstreckung einer freiheitsentziehenden Strafe oder Maßregel (Entscheidungen des Bundesverfassungsgerichts

II. Gesetzliche Grundlagen

Die heutige Rechtslage betreffend den Strafvollzug basiert auf dem Gesetz über den Vollzug der Freiheitsstrafe und der freiheitsentziehenden Maßregeln der Besserung und Sicherung⁵, das zum 01.01.1977 in Kraft trat. Dies galt nur für den Erwachsenenstrafvollzug. Die Regelungen für den Jugendstrafvollzug (d.h. für Jugendliche im Alter zwischen 14 und 18 Jahren bzw. ggf. für Heranwachsende im Alter zwischen 18 und 21 Jahren) waren auf einige wenige Normen im Jugendgerichtsgesetz beschränkt (§§ 91, 92, 115 JGG). Diese verwiesen auf die Anwendung des BundesStVollzG, sodass über Umwege im Wesentlichen das Erwachsenenstrafvollzugsgesetz galt. Diese fehlende gesetzliche Grundlage wurde vom Bundesverfassungsgericht moniert und für verfassungswidrig erklärt.⁶ Das Bundesverfassungsgericht verlangte die Schaffung eines „eigenen“ Jugendstrafvollzugsgesetzes. Bevor der Gesetzgeber diesbezüglich tätig werden konnte, wurde im Wege der Föderalismusreform den einzelnen Bundesländern die Gesetzgebungskompetenz hinsichtlich der Regelung des Vollzuges der Freiheitsstrafe übertragen. Folglich musste jedes Bundesland die gesetzliche Normierung des Erwachsenen- und Jugendstrafvollzuges eigenverantwortlich übernehmen. Somit wurde die gesetzliche Grundlage für den (Jugend- und Erwachsenen-) Straf-

(BVerfGE) 32, 87, 93; *Böhm, Klaus Michael/Werner, Eric*, in Münchener Kommentar, Strafprozessordnung, 1. Aufl. 2014, § 112 Rn. 2). Sie stellt somit gerade keine Vollziehung einer bereits rechtskräftigen Kriminalstrafe dar, sondern ist dieser vorgelagert. Ähnlich verhält es sich mit der Abschiebungshaft gem. § 62 Aufenthaltsgesetz (AufenthG). Diese dient als Sondermaßnahme des Ausländerrechts zum einen der Vorbereitung der Auslieferung (Vorbereitungshaft) und der Sicherung der Abschiebung (Sicherungshaft) (Vgl. *Senge, Lothar*, in Erbs/Kohlhaas, Aufenthaltsgesetz (AufenthG), 224. Ergänzungslieferung März 2019, § 62 Rn. 1-1a).

⁵ Im Folgenden als BundesStVollzG abgekürzt.

⁶ Vgl. Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 116, 69, 69 ff.

vollzug vollkommen erneuert. In Deutschland existieren daher 16 Strafvollzugsgesetze der Länder zuzüglich ihrer jeweiligen Jugendstrafvollzugsgesetze. Die Gesetzgebungsbefugnis wurde den Ländern jedoch nur für den Regelungsbereich „Strafvollzug“ übertragen, nicht für weitere Gebiete wie zum Beispiel für das gerichtliche Verfahren. Diese unterliegen weiterhin der Gesetzgebungskompetenz des Bundes, sodass die entsprechenden Regelungen im Strafvollzugsgesetz (§§ 109-121 BundesStVollzG) weiterhin gelten. Daher kommt diesem doch noch eigenständige Bedeutung zu. In Deutschland ist die Gesetzeslage somit gespalten. Einerseits gilt in den einzelnen Bundesländern das jeweilige Landesrecht zum Strafvollzug. Andererseits – nämlich in den Bereichen, in denen der Landesgesetzgeber keine Gesetzgebungskompetenz hat (z.B. im gerichtlichen Verfahren) – gilt weiterhin das Bundesstrafvollzugsgesetz. In Deutschland besteht folglich eine breite Landschaft an strafvollzugsrechtlichen Vorschriften: 16 (Erwachsenen-)Strafvollzugsgesetze zuzüglich ihre jeweiligen Jugendstrafvollzugsgesetze sowie das „ursprüngliche“ Bundesstrafvollzugsgesetz von 1977, das jedoch nur einen beschränkten Anwendungsbereich hat. Die nachfolgenden rechtlichen Ausführungen gründen daher exemplarisch auf dem Strafvollzugsgesetz des Landes Nordrhein-Westfalen (StVollzG NRW).

III. Ziel des Strafvollzugs

Das Ziel des Strafvollzugs ist zuvorderst in § 1 StVollzG NRW normiert. Dieses lautet wie folgt: „*Der Vollzug der Freiheitsstrafe dient dem Ziel, Gefangene zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen.*“ Alleiniges Ziel des Strafvollzuges ist damit die sogenannte „Resozialisierung“ des Strafgefangenen. Diese ist im Sinne der positiven Spezialprävention zu verstehen.⁷ Sogleich mag die Frage aufkommen, ob Ziel des Strafvollzuges nicht zumindest auch der Opferschutz und die Sicherheit der Allgemeinheit ist. Dies ist schlichtweg zu verneinen. Bei diesen handelt es sich lediglich um nachrangigere Auf-

gaben. Ihnen kommt allenfalls reflexartige Bedeutung zu. Sie stellen jedoch kein eigenständiges Vollzugsziel dar. Ein solches lässt sich weder mit dem Wortlaut (siehe oben) noch mit der Systematik vereinbaren. Die Sicherheit der Allgemeinheit wird erst in einer differenzierten Regelung in § 6 StVollzG NRW getrennt und nachgeordnet behandelt. Es heißt in § 6 Abs. 1 StVollzG NRW: „*Der Vollzug der Freiheitsstrafe dient auch dem Schutz der Allgemeinheit vor weiteren Straftaten.*“ Es geht deutlich aus dem Wortlaut hervor, dass dies lediglich eine nachrangige Bedeutung hat (vergleiche Wortlaut „auch“). Hierfür spricht zudem die separate Normierung in § 6 StVollzG NRW statt einer Ansiedelung in § 1 StVollzG NRW.⁸

Doch was bedeutet Resozialisierung?⁹ Namentlich verwendet der Gesetzgeber den Begriff der „Resozialisierung“ nicht. Dies mag der Tatsache geschuldet sein, dass dieser Begriff nicht einheitlich verwendet wird.¹⁰ Ursprünglich stammt dieser aus der Soziologie und wurde erst im Nachhinein von anderen Wissenschaften wie zum Beispiel der Psychologie, Kriminologie und der Strafvollzugskunde übernommen.¹¹ Aufgrund dieser verschiedenen Ansätze der unterschiedlichen Bezugswissenschaften konnte keine Einigung über Inhalt und Tragweite erzielt werden.¹² Einigkeit besteht jedoch darüber, dass sich das Recht des Strafgefangenen auf Resozialisierung und der Resozialisierungsauftrag des Staates unmittelbar aus den zentralen Verfassungsgrundsätzen der Menschenwürde und dem Sozialstaatsprinzip ergibt: Zum einen folgt das Grundrecht des Strafgefangenen auf Resozialisierung aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz¹³. Dieses wurde von der Rechtsprechung sogar als Anspruch auf Resozialisierung eingeordnet.¹⁴ Zum anderen ergibt sich die Verpflichtung des Staates zur Bereitstellung der erforderlichen Ressourcen für die Resozialisierung aus

⁷ Vgl. Arloth, Frank, in Arloth/Krä, Strafvollzugsgesetz (StVollzG), 4. Aufl. 2017, § 2 Rn. 2; Neubacher, Frank, in Laubenthal/Nestler/Neubacher/Verrel, Strafvollzugsgesetz (StVollzG), 12. Aufl. 2015, Teil B – Rn. 41.

⁸ Vgl. Arloth, Frank, in Arloth/Krä, Strafvollzugsgesetz (StVollzG), 4. Aufl. 2017, § 1 Rn. 1.

⁹ Ausführlich Cornel, Heinz, in Cornel/Kawamura-Reindl/Sonnen, Resozialisierung, 2018, S. 31 ff; 310 ff.

¹⁰ Vgl. Laubenthal, Klaus, Strafvollzug, 6. Aufl. 2015, Rn. 140.

¹¹ Vgl. Kaiser, Günther/Schöch, Heinz, Strafvollzug, 5. Aufl. 2002, § 5 Rn. 8.

¹² Vgl. Laubenthal, Klaus, Strafvollzug, 6. Aufl. 2015, Rn. 140.

¹³ Im Folgenden als GG abgekürzt.

¹⁴ Vgl. Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 45, 187, 239.

Art. 20 Abs. 1 GG und Art. 28 Abs. 1 GG.¹⁵ Damit hat die Resozialisierung Verfassungsrang, was die außerordentliche Bedeutsamkeit manifestiert.¹⁶ Vielfach befasste sich das Bundesverfassungsgericht mit der Materie der Resozialisierung von Strafgefangenen. Es versteht darunter „die Wiedereingliederung des Straftäters in die Gesellschaft“. Diese gilt für alle Strafgefangenen unabhängig von deren Staatsangehörigkeit oder der Länge der Freiheitsstrafe, sodass auch bei zu lebenslanger Freiheitsstrafe Verurteilten das Vollzugsziel der Resozialisierung Anwendung findet.¹⁷ Eine Wiedereingliederung ist letztendlich zwingend notwendig, da der Freiheitsentzug eine Ausgliederung auf Zeit darstellt.¹⁸

IV. Grundsätze der Vollzugsgestaltung

Zur Verbüßung der Freiheitsstrafe begeben sich die Gefangenen in eine „andere“, von Gefängnismauern umgebene Welt. Das Leben in dieser ist mit zahlreichen Entbehren verbunden. Zuvorderst sind dies natürlich der Entzug der Freiheit und das Herauslösen aus dem sozialen Umfeld. Weiterhin kommt es zu einem Verlust der Autonomie.¹⁹ Im Strafvollzug sind alle Lebensbereiche streng reglementiert, sodass die Selbstfürsorge und Selbstverantwortung in der sogenannten „erlernten Hilfslosigkeit“ münden.²⁰ Hierbei wird der Gefangene in seinem Selbstbild als eigenverantwortliches Individuum erschüttert. Um diese Verluste zu kompensieren, passen

sich die Gefangenen an die sogenannte Insassensubkultur an.²¹ Zu verstehen ist diese als eine Gegenordnung mit eigenen „Gesetzen“, Sitten, Normen sowie einer Hierarchie unter den Gefangenen.²² Hierbei spielen auch Gewalt und sexueller Missbrauch von Mitgefangenen eine Rolle.²³ Daraus resultieren Angst und ein hohes Viktimisierungsrisiko für neue Häftlinge.²⁴ Allein diese wenigen, nur oberflächlich angedeuteten Aspekte verdeutlichen, dass die Umstände im Strafvollzug keineswegs ideal sind, um die Resozialisierung des Einzelnen zu erreichen. Um dieses „Knast-Dilemma“ jedenfalls abzumildern, sind sogenannte Gestaltungsgrundsätze gesetzlich geregelt. Diese sind sogleich in § 2 StVollzG NRW benannt. Dabei handelt es sich um den Angleichungs-, den Gegensteuerungs- und den Integrationsgrundsatz.²⁵ Aus ihnen können jedoch keine Rechte oder gar Ansprüche abgeleitet werden.²⁶ Sie sind allerdings als verbindliche Anweisungen an die Vollzugsbehörde einzuordnen.²⁷ Der Angleichungsgrundsatz²⁸ gemäß § 2 Abs. 1 S. 1 StVollzG NRW (§ 3 Abs. 1 S. 1 JStVollzG NRW²⁹) besagt, dass das Leben im Vollzug den allgemeinen Lebensverhältnissen soweit wie möglich anzu-

¹⁵ Vgl. Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 35, 202, 235 f. Näher dazu *Leyendecker, Natalie Andrea*, (Re-) Sozialisierung und Verfassungsrecht, 2002, S. 95 ff.

¹⁶ Eingehend siehe auch *Bachmann, Mario*, Bundesverfassungsgericht und Strafvollzug, 2015.

¹⁷ Vgl. Entscheidungen des Bundesverfassungsgerichts (BVerfGE) 45, 187, 239; 98, 169, 200; Bundesverfassungsgericht (BVerfG), Nichtannahmebeschluss vom 10.10.2012 – 2 BvR 2025/12 –, juris; *Arloth, Frank*, in *Arloth/Krä*, Strafvollzugsgesetz (StVollzG), 4. Aufl. 2017, § 2 Rn. 6 mit weiteren Nachweisen.

¹⁸ Vgl. *Jehle, Jörg-Martin*, in *Schwind/Böhm/Jehle/Laubenthal*, Strafvollzugsgesetz (StVollzG), 6. Aufl. 2013, § 3 Rn. 13.

¹⁹ Vgl. *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 201.

²⁰ Vgl. *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 201.

²¹ Vgl. *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 211 f.

²² Vgl. *Kaiser, Günthrt/Schöch, Heinz*, Strafvollzug, 5. Aufl. 2002, § 13 Rn. 15; *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 213, 217.

²³ Vgl. *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 214, 216.

²⁴ Vgl. *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 214.

²⁵ Einige Landesstrafvollzugsgesetze haben noch weitere Vollzugsgrundsätze geregelt. In Nordrhein-Westfalen ist zudem in einem eigenständigen Paragraphen die opferbezogene Vollzugsgestaltung normiert. Bei der Vollzugsgestaltung sollen auch die Belange der Opfer berücksichtigt werden z.B. im Rahmen vollzugsöffnender Maßnahmen oder bei der Erteilung von Weisungen (§ 7 Abs. 1 S. 1 StVollzG NRW). Der vermehrt opferorientierte Strafvollzug stellt im Vergleich zum Bundesstrafvollzugsgesetz eine besondere Errungenschaft dar.

²⁶ Vgl. *Neubacher, Frank*, in *Laubenthal/Nestler/Neubacher/Verrel*, Strafvollzugsgesetz (StVollzG), 12. Aufl. 2015, Teil B – Rn. 49.

²⁷ Vgl. *Arloth, Frank*, in *Arloth/Krä*, Strafvollzugsgesetz (StVollzG), 4. Aufl. 2017, § 3 Rn. 1.

²⁸ Ausführlich dazu *Matthey, Isabell*, Der Angleichungsgrundsatz, 2011.

²⁹ Gesetz zur Regelung des Jugendstrafvollzuges in Nordrhein-Westfalen.

gleichen ist. Damit werden die Vollzugsbehörden verpflichtet, den „Besonderheiten des Anstaltslebens, die den Gefangenen lebensuntüchtig machen können, möglichst zurückzudrängen, so dass der Unterschied zwischen dem Leben in der Anstalt und dem Leben draußen nicht stärker als unvermeidbar ist“³⁰ (z.B. Gestaltung des Hafttraums mit einer Tagesdecke,³¹ Aushändigung von Freizeitkleidung und das Tragen eigener Kleidung bei Gerichtsterminen,³² Ausgabe der Mahlzeiten zu den entsprechenden Tageszeiten,³³ Zugänglichmachung von Tageszeitungen am Tag ihres Erscheinens³⁴). Dabei ist offenkundig, dass Angleichung nicht Gleichstellung bedeuten kann.³⁵ Dieser Grundsatz ist freilich nur begrenzt zu realisieren. Diese Grenze ergibt sich bereits aus dem Wortlaut „soweit wie möglich“. Daher normiert der sogenannte Gegensteuerungsgrundsatz gemäß § 2 Abs. 1 S. 4 StVollzG (§ 3 Abs. 2 S. 3 JStVollzG), dass den schädlichen Folgen des Freiheitsentzuges entgegengewirkt werden soll. Dies beruht darauf, dass der Aufenthalt im Strafvollzug mit zahlreichen negativen Folgen, Schädigungen, Haftdeprivationen und der Bildung von Subkulturen verbunden ist.³⁶ Diese sollen durch gezielte Gegenwirkungen minimiert werden (z.B. Schutz vor Gewalt durch Mitgefangene, Verhütung von Selbsttötungen). Somit hat der Gesetzgeber diese Problembereiche des Strafvollzugs erkannt und sie eingeräumt. Der Integrationsgrundsatz ist wohl am engsten mit dem Vollzugsziel der Resozialisierung verbunden.³⁷ § 2 Abs. 1 S. 2 StVollzG NRW (§ 3 Abs. 2 S. 4 JStVollzG) normiert, dass der Vollzug von Beginn an darauf auszurichten ist, die Gefangenen zu befähigen, sich nach

der Entlassung in das Leben in Freiheit einzugliedern. Dies gründet vor allem darauf, dass der Freiheitsentzug möglichst problemlos wieder in die Freiheit transferiert werden muss (z.B. durch soziale Trainingsprogramme, Kontaktförderungen, insbesondere Verlegung in Wohnortnähe,³⁸ Therapieangebote für Suchtkranke).

V. Zusammenfassung

Zusammenfassend ist festzuhalten, dass das deutsche Strafvollzugsrecht „gespalten“ ist und eine Vielzahl von Gesetzen und Vorschriften existieren. Das Vollzugsziel, die Resozialisierung, gilt jedoch für alle gleichermaßen. Dieses ist nämlich in der Verfassung verankert und ergibt sich aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 und Art. 20 Abs. 1 GG. Inhaltlich ist die Resozialisierung jedoch nur schwer zu definieren. Die Gestaltungsgrundsätze – der Angleichungs- Gegensteuerungs- und Integrationsgrundsatz – konkretisieren das Vollzugsziel im Rahmen des Möglichen. Die Schwierigkeit und das Dilemma des Strafvollzugs besteht nämlich darin, dass die Strafgefangenen befähigt werden sollen, zukünftig in Freiheit straffrei zu leben. Der Prozess zur Erreichung des Vollzugsziels erfolgt jedoch gerade in einer Umgebung von ihrerseits resozialisierungsbedürftigen Mitgefangenen.

³⁰ Bundestags-Drucksache 7/918 S. 46.

³¹ Vgl. Oberlandesgericht Koblenz (OLG), Zeitschrift für Strafvollzug und Straffälligenhilfe (ZfStrVo), Sonderheft 1979, 85.

³² Vgl. Bundesverfassungsgericht (BVerfG), Neue Zeitschrift für Strafrecht (NStZ)2000, 166.

³³ Vgl. *Neubacher, Frank*, in Laubenthal/Nestler/Neubacher/Verrel, StVollzG, 12. Aufl. 2015, Teil B – Rn. 54.

³⁴ Vgl. Oberlandesgericht (OLG) Nürnberg, Zeitschrift für Strafvollzug und Straffälligenhilfe (ZfStrVo) 1993, 116.

³⁵ Vgl. *Kaiser, Günther/Schöch, Heinz*, Strafvollzugsgesetz (StVollzG), 5. Aufl. 2002, § 6 Rn. 61.

³⁶ Näher: *Laubenthal, Klaus*, Strafvollzug, 6. Aufl. 2015, Rn. 200 ff.

³⁷ Vgl. *Neubacher, Frank*, in Laubenthal/Nestler/Neubacher/Verrel, Strafvollzugsgesetz (StVollzG), 12. Aufl. 2015, Teil B – Rn. 57.

³⁸ Vgl. Oberlandesgericht (OLG) Hamm, Zeitschrift für Strafvollzug und Straffälligenhilfe (ZfStrVo) 1985, 373 f.

Bericht zum Arbeitsbesuch einer hochrangigen georgischen Delegation vom 08.-12. April 2019 in Berlin: „Rechtsgrundlagen, praktische Anwendung und Kontrolle von Telekommunikationsüberwachungsmaßnahmen in Deutschland“

Von *Khatuna Diasamidze*, Projektmanagerin Südosteuropa II und Südkaukasus bei der Deutschen Stiftung für Internationale Rechtliche Zusammenarbeit (IRZ)

Die IRZ ist seit 2006 in Georgien beratend tätig. Der Schwerpunkt der Beratungen liegt im Bereich des Strafrechts. Im Rahmen dieser bilateralen Zusammenarbeit organisierte die IRZ in der Zeit vom 8. bis zum 12. April 2019 den Arbeitsbesuch einer hochrangigen georgischen Delegation in Berlin. Die Delegation bestand aus drei Ausschussvorsitzenden des Parlaments, dem Präsidenten und zwei Vizepräsidenten des Verfassungsgerichts sowie der georgischen Datenschutzbeauftragten. Es wurden Gespräche im Bundesministerium der Justiz und für Verbraucherschutz (BMJV), im Bundesministerium des Innern, für Bau und Heimat (BMI), mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), mit Vertretern des Bundeskriminalamts (BKA) und des Verfassungsschutzes des Landes Berlin, in der Generalstaatsanwaltschaft des Landes Berlin, im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages, im Gremium nach Art. 13 Abs. 6 GG des Deutschen Bundestages und zuletzt in der G 10-Kommission und im parlamentarischen Kontrollgremium (PKGr) geführt. Der Austausch mit den deutschen Kolleginnen und Kollegen galt den Themen Zulassung, Zugriff, Nutzung und Speicherung der Verkehrsdaten einer Telekommunikationsüberwachung (TKÜ) und deren Vereinbarkeit mit den verfassungsmäßig garantierten Grundrechten.

Der vorliegende Bericht fasst die während des Arbeitsbesuchs gewonnenen Erkenntnisse zusammen und versucht einen kurzen Gesamtüberblick über die TKÜ in Deutschland zu geben.

Die TKÜ zählt zu den Ermittlungsmaßnahmen, denen sowohl bei der Bekämpfung der Organisierten Kriminalität, der Terrorismusbekämpfung sowie des Schutzes nationaler Sicherheit hohe Aufmerksamkeit

geschenkt und hohes Potenzial zugeordnet wird.¹ In Zeiten der Globalisierung und einer voranschreitenden Digitalisierung nimmt ihre praktische Bedeutung kontinuierlich zu.² Zugleich stellt die TKÜ den Rechtsstaat vor neue Herausforderungen. Größte Schwierigkeiten bereitet dabei eine sachgerechte Abwägung zwischen dem sich aus der TKÜ ergebenden Nutzen einerseits und den mit der Überwachung zwangsläufig verbundenen Eingriffen in die grundrechtlich geschützten Positionen der betroffenen Personen andererseits.

In der Bundesrepublik Deutschland ist eine TKÜ – je nach Anlass und Ziel der Überwachungsmaßnahme – entweder auf der Grundlage der Polizeigesetze in Bund und Ländern, des § 100a ff. der Strafprozessordnung³, des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz) durch die Nachrichtendienste des Bundes oder die Landesbehörden für Verfassungsschutz oder des § 23a des Zollfahndungsdienstgesetzes (ZFDG) möglich. Die TKÜ nach § 100a StPO ist in der Praxis mit Abstand häufigster Fall. Aufgrund ihrer Häufigkeit standen zwar die TKÜ-Maßnahmen im Rahmen eines strafrechtlichen Ermittlungsverfahrens im Vordergrund der Gespräche, die TKÜ nach dem Artikel 10-Gesetz wurde aber nicht zuletzt wegen ihrer übergeordneten Bedeutung ebenfalls sehr ausführlich erläutert.

Weil die TKÜ einen schwerwiegenden Eingriff in das von Art. 10 GG garantierte Brief-, Post- und Fernmeldegeheimnis sowie in das Allgemeine Persönlich-

¹ abrufbar unter: https://rsw.beck.de/docs/librariesprovider5/rsw-dokumente/Abschlussbericht_1_1 (zuletzt abgerufen am 1.8.2019).

² Vgl. https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html (zuletzt abgerufen am 1.8.2019).

³ Im Folgenden als StPO abgekürzt.

keitsrecht und das Recht auf informationelle Selbstbestimmung nach Art. 2 I i.V.m. Art. 1 GG darstellt, hat das BVerfG hohe verfassungsrechtliche Anforderungen an derartige Eingriffe in die Grundrechte aufgestellt⁴ und den Gesetzgeber mit der Schaffung einer entsprechenden Rechtsgrundlage beauftragt.

Im Rahmen der Strafverfolgung ist die TKÜ durch die Strafprozessordnung geregelt. Hierin bestimmen die §§ 100a und 100e StPO die Voraussetzungen und das Verfahren unter denen eine Überwachung zulässig ist. Darüber hinaus regeln die §§ 100g und 100i StPO die Erhebung von Verkehrsdaten und die Standortbestimmung von Mobilfunkendgeräten. Im Einzelnen regelt das Telekommunikationsgesetz⁵ die Pflichten der Telekommunikationsanbieter zur Bereithaltung von Daten und Mitwirkung im Ermittlungsverfahren.

§100a StPO gestattet nicht nur die Überwachung der Telekommunikation, sondern darüber hinaus auch die Aufzeichnung der Gespräche durch die Ermittlungsbehörde. Dabei ist der Anwendungsbereich des § 100a StPO nicht nur auf die herkömmlichen Formen der Telekommunikation⁶ beschränkt, sondern umfasst jegliche Art der unverschlüsselten Nachrichtenübertragung, z.B. auch in Form von SMS oder E-Mails, Messenger-Dienste und sämtlichen Arten der Internet-Telefonie. Bei verschlüsselten Kommunikationen dagegen wird auf Grundlage des seit der StPO-Reform von 2017 neu eingefügten § 100a I S. 2 und 3 StPO die „Quellen – Telekommunikationsüberwachung“ (Quellen-TKÜ) durchgeführt. Die Quellen-TKÜ erlaubt den Ermittlungsbehörden das Abfangen von unverschlüsselten Daten entweder bevor die Daten verschlüsselt werden oder nachdem die Daten wieder durch den Internetdienst entschlüsselt wurden. Das Abfangen erfolgt, indem heimlich eine Spionage-Software auf das Zielgerät installiert wird. Die Zugriffsrechte der Behörde sind dabei auf die laufende Kommunikation beschränkt.

⁴ BVerfG 1 BvR 370/07, 1 BvR 595/07 (Erster Senat) – Urteil vom 27. Februar 2008; BVerfG 120, 274; BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09.

⁵ Telekommunikationsgesetz (TKG) vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 5 Absatz 22 des Gesetzes vom 21. Juni 2019 (BGBl. I S. 846) geändert worden ist; abrufbar in deutscher Sprache unter https://www.gesetze-im-internet.de/tkg_2004/TKG.pdf (zuletzt abgerufen am 1.8.2019).

⁶ Zum Begriff der Telekommunikation vgl. § 3 Nr. 22 TKG.

Die Voraussetzungen der TKÜ sind in den §§ 100a und 100e StPO festgelegt und erfordern den durch Tatsachen begründeten Verdacht, dass die betroffene Person entweder Täter oder Teilnehmer einer in § 100a II StPO genannten Straftat ist, die auch im Einzelfall schwer wiegt (§100a I Nr. 2 StPO). Gem. § 100a I Nr. 3 StPO ist die Überwachungsmaßnahme nur dann zulässig, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes andernfalls aussichtslos oder wesentlich erschwert ist.

Die TKÜ-Maßnahmen dürfen gem. § 100e I StPO nur auf Antrag der Staatsanwaltschaft⁷ durch das Gericht angeordnet werden. Bei Gefahr im Verzug darf die StA eine kurzfristige Anordnung treffen, die innerhalb von drei Werktagen gerichtlich bestätigt werden muss (§ 100e I 3 StPO). Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht (§ 100e I 5 StPO). Die Anordnung richtet sich in erster Linie gegen den Tatverdächtigen. Darüber hinaus kann die TKÜ auch unmittelbar gegen Dritte angeordnet werden (vgl. § 100a III StPO). Die Betroffenen sind von der Überwachung nachträglich zu benachrichtigen (§ 101 IV 1 Nr. 3 StPO). Der Kernbereich privater Lebensgestaltung erhält durch § 100d I StPO einen besonderen Schutz.

Die Quellen-TKÜ hat größtenteils die gleichen Voraussetzungen wie die herkömmliche TKÜ und ist gegenüber dieser subsidiär. Zu beachten sind allerdings die in § 100a V StPO enthaltenen zusätzlichen Voraussetzungen für das technische Verfahren. Grundsätzlich können gem. § 100a V 1 Nr. 1 StPO mittels einer Quellen-TKÜ nur die laufende Telekommunikation oder Inhalte und Umstände der Kommunikation, welche ab dem Anordnungszeitraum auch mit einer „normalen“ TKÜ erfasst werden dürfen, überwacht und aufgezeichnet werden. Darüber hinaus fordert § 100a V 1 Nr. 2 StPO, dass das betroffene informationstechnische System nur insoweit verändert wird, wie es für die Datenerhebung unerlässlich ist. Sofern Veränderungen am System erfolgt sind, müssen diese nach Beendigung der Maßnahme automatisch rückgängig gemacht werden (§ 100a V 1 Nr. 3 StPO). Des Weiteren muss nach § 100a V 2 StPO sicher-

⁷ Im Folgenden als StA abgekürzt.

gestellt werden, dass kein unbefugter Zugriff auf die Spionage-Software erfolgt. Schließlich sind die durch die Quellen-TKÜ erlangten Daten auch gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen (§ 100a V 3 StPO). Darüber hinaus gelten bei der Quellen-TKÜ besondere Protokollierungspflichten (§ 100a VI StPO).

Bei der Durchführung der TKÜ im Rahmen eines strafrechtlichen Ermittlungsverfahrens trägt die StA die Letztverantwortung für die Rechtmäßigkeit des Ermittlungsverfahrens. Gem. § 152 Abs. 1 Gerichtsverfassungsgesetz (GVG) ist die StA gegenüber den sog. Ermittlungspersonen der StA – in erster Linie den Polizeibeamten – weisungsbefugt. Die StA hat im Zusammenhang mit einer TKÜ die Erforderlichkeit einer solchen Maßnahme und das Vorliegen der gesetzlichen Voraussetzungen zu überprüfen. Sie ist zuständig für die Beantragung einer richterlichen Anordnung beim Ermittlungsrichter (vgl. § 162 StPO). Wie bereits oben erwähnt, kann die TKÜ bei besonderer Eilbedürftigkeit (Gefahr im Verzug) gem. § 100e I S. 2 und 3 StPO auch von der StA selbst angeordnet werden (vgl. oben). Gem. § 161 I StPO kann die StA die Ermittlungen selbst vornehmen oder diese durch die Polizei vornehmen lassen. In der Praxis werden die Ermittlungen regelmäßig von der Polizei durchgeführt.

Bestimmte grundrechtsintensive Ermittlungsmaßnahmen unterliegen einem Richtervorbehalt. Bei den zuständigen Amtsgerichten sind bestimmte Richter mit der Wahrnehmung von Entscheidungen im Ermittlungsverfahren betraut. Diese Ermittlungsrichter entscheiden über die Anträge der StA durch Beschluss.

Da die sachbearbeitende Polizeidienststelle in der Regel nicht über die nötige Ausstattung verfügt, um eine TKÜ oder eine Quellen-TKÜ vornehmen zu können, wird von der StA das BKA bzw. LKA mit der Durchführung beauftragt.

Die praktische Umsetzung der TKÜ ist in der Telekommunikationsüberwachungsverordnung⁸ geregelt.

⁸ Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV) in der Fassung der Bekanntmachung vom 11. Juli 2017 (BGBl. I S. 2316), die zuletzt durch Artikel 16 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202) geändert worden ist, abrufbar unter https://www.gesetze-im-internet.de/tk_v_2005/tkuv.pdf (zuletzt abgerufen am 1.8.2019).

Bei der Umsetzung unterscheidet sich die Quellen-TKÜ wesentlich von der konventionellen TKÜ. Sie ist auch wegen ihrer hohen Eingriffsintensität, die vor allem in ihrer technischen Umsetzung begründet ist, sehr umstritten.⁹

Bei der konventionellen TKÜ wird der Telekommunikationsanbieter aufgrund einer richterlichen Anordnung aufgefordert, die im Rahmen eines laufenden Telekommunikationsvorgangs anfallenden Daten direkt an die Strafverfolgungsbehörden weiterzugeben. Wird die Kommunikation verschlüsselt übertragen, ist diese Vorgehensweise in der Regel technisch nicht zielführend. In solchen Fällen darf der Einsatz der Quellen-TKÜ angeordnet werden. Nach der Anordnung der Maßnahmen beauftragt das BKA bzw. LKA ein externes Unternehmen mit der Erstellung einer maßgefertigten Software, die für die Infiltration auf dem Zielgerät installiert wird. Ob die Funktionalität der angebrachten Software von der jeweiligen richterlichen Anordnung abgedeckt ist, konnte bis zum gegenwärtigen Zeitpunkt nicht abschließend beantwortet werden.¹⁰

Was die Kontrollmechanismen anbetrifft, steht die TKÜ nach § 100a StPO einerseits unter der gerichtlichen und andererseits datenschutzrechtlichen Kontrolle durch den BfDI.

Die Telekommunikation darf im Einzelfall auch vom Bundesnachrichtendienst (BND), den Verfassungsschutzbehörden des Bundes (BfV) und der Länder und dem Militärischen Abschirmdienst (MAD) nach dem Artikel 10-Gesetz überwacht und aufgezeichnet werden. Voraussetzung für eine G 10-Maßnahme ist, dass tatsächliche Anhaltspunkte für die Planung oder Begehung bestimmter Katalogstraftaten, zu denen neben Friedens-

⁹ abrufbar unter: https://www.strafverteidigervereinigungen.org/Material/Themen/Technik%20&%20Ueberwachung/37_buermeyer.html (zuletzt abgerufen am 1.8.2019); <https://www.morgenpost.de/politik/article215139967/Der-Staat-als-Spion-wie-weit-darf-Ueberwachung-gehen.html> (zuletzt abgerufen am 1.8.2019); <https://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html> (zuletzt abgerufen am 1.8.2019); https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html (zuletzt abgerufen am 1.8.2019).

¹⁰ abrufbar unter: <https://investigativ.welt.de/2017/07/26/der-bundestrojaner-das-kann-er-und-das-nicht/> (zuletzt abgerufen am 1.8.2019).

und Hochverrat (§§ 80a bis 83 des Strafgesetzbuches¹¹), inzwischen auch Landfriedensbruch oder Volksverhetzung (§§ 129a bis 130 des StGB) und Straftaten nach § 95 I Nr. 8 des Aufenthaltsgesetzes (Einschleusen von Ausländern) gehören, gegeben sind. Der Straftatenkatalog deckt sich im Wesentlichen mit dem des § 100a StPO. Zudem darf der BND die internationalen Telekommunikationsbeziehungen suchwortgesteuert und in begrenztem Umfang – z.B. zur rechtzeitigen Erkennung terroristischer Anschläge – überwachen und aufzeichnen (§ 5 G 10-Gesetz).

Zur Anordnung von G 10-Maßnahmen der Nachrichtendienste des Bundes sind das BMI und für die Landesbehörden für Verfassungsschutz die jeweiligen obersten Landesbehörden zuständig. Über die Notwendigkeit und Zulässigkeit sämtlicher durch die Nachrichtendienste des Bundes (BfV, BND, MAD) beantragten und vom BMI angeordneten G 10-Maßnahmen entscheidet die G 10-Kommission des Deutschen Bundestages, auf der Landesebene die entsprechenden Kommissionen der jeweiligen Landtage. Darüber hinaus übt die G 10-Kommission Kontrollbefugnisse aus. Neben der G 10-Kommission gibt es weitere Kontrollorgane im Bereich der Nachrichtendienste. Dies sind das PKGr einerseits und der BfDI andererseits. Die Aufzählung aller Kontrollorgane zeigt, dass die Vielzahl bzw. die Zersplitterung eine intensive Zusammenarbeit dieser Stellen erfordert, um Kontrolllücken auszuschließen und einen effektiven Grundrechtsschutz der Betroffenen zu gewährleisten. Das BVerfG hat seine Entscheidung zur Anti-Terror-Datei¹² mit dem Urteil zum Bundeskriminalamtgesetz (BKAG) vom 20. April 2016 bekräftigt und ausgeführt, dass „der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung“ zukommt, weil „eine Transparenz der Datenerhebung und -verarbeitung sowie die Ermöglichung individuellen Rechtsschutzes für heimliche Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können“.¹³

Abschließend darf bei einer Gesamtbetrachtung der TKÜ das zentrale Thema der Vorratsdatenspeicherung nicht außer Acht gelassen werden.

In Deutschland ist die Rechtslage mit Blick auf die sogenannte Vorratsdatenspeicherung derzeit unklar. Nach dem das Oberverwaltungsgericht des Landes Nordrhein-Westfalen am 22. Juni 2017 das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten für unvereinbar mit europäischen Vorgaben erklärte, setzte die Bundesnetzagentur die Regelungen der Vorratsdatenspeicherung aus.¹⁴

Vertreter der Sicherheitsbehörden und Politiker kritisieren die aktuelle Rechtslage und warnen vor Schwierigkeiten beim Kampf gegen schwere Formen der Kriminalität und Terrorismus. Kritiker der umstrittenen Vorratsdatenspeicherung bestreiten dies und sehen darüber hinaus gravierende verfassungsrechtliche Probleme. Anfang Juni 2019 haben die Justizminister der EU erneut über eine europäische Regelung der Verkehrsdatenspeicherung beraten. Von konkreten Vorschlägen, wie die Maßgaben der Urteile des Europäischen Gerichtshofs (EuGH)¹⁵ gegen eine anlasslose Bevorratung von Verkehrsdaten umgesetzt werden könnten, sind die Mitgliedstaaten allerdings noch weit entfernt.¹⁶ Die weitere Entwicklung bleibt abzuwarten.

¹⁴ abrufbar unter: http://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/01_archiv/2017/36_170622/index.php (zuletzt abgerufen am 1.8.2019).

¹⁵ EuGH, – Urteil vom 21.12.2016 – C-203/15, C-698/15, abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=DE> (zuletzt abgerufen am 1.8.2019).

¹⁶ abrufbar unter: <https://www.heise.de/newsticker/meldung/Neue-Beratungen-in-der-EU-Und-ewig-gruesst-die-Vorratsdatenspeicherung-4434861.html> (zuletzt abgerufen am 1.8.2019).

¹¹ Im Folgenden als StGB abgekürzt.

¹² BVerfG, Urteil vom 24.4.2013, 1 BvR 1215/97.

¹³ BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rz 140.