Dateneingriffe zur vorbeugenden Kriminalitätsbekämpfung (Teil 2)

Von Gerrit Domenghino LL.M., Münster

„Verhindere Verbrechen, damit Strafe nicht nötig ist“ soll der chinesische Philosoph Konfuzius einst gesagt haben. Um Verbrechen durch offene Maßnahmen – wie sie im ersten Teil des Beitrags einleitend beschrieben wurden[2] – nicht eventuell nur zu verdrängen, statt sie zu verhindern, können die Sicherheitsbehörden auf eine Vielzahl von verdeckten Maßnahmen zurückgreifen, um eine vorbeugende Kriminalitätsbekämpfung zu gewährleisten. Gerade beim verdeckten Dateneingriff kann nicht immer strikt zwischen Gefahrenabwehr und Strafverfolgung getrennt werden, da es Konstellationen geben kann, in den durch diese sogenannten doppelfunktionalen Maßnahmen sowohl präventive als auch repressive Zwecke verfolgt werden.[3] Dabei hat diese heimliche Datenerhebung aufgrund der zunehmenden Technisierung und Digitalisierung der Gesellschaft eine wesentliche Bedeutung und Beachtung im Polizeirecht erhalten. So ist es eine logische Folge, dass die in den entsprechenden Gesetzen regulierten Maßnahmen nicht nur einer steten Überarbeitung unterliegen, sondern dass neue Normen geschaffen werden, um der Kriminalität Einhalt zu gebieten. Auf den folgenden Seiten wird eine Auswahl von Eingriffsbefugnisse in den Fokus genommen, die – nicht unumstritten – Maßnahmen zum verdeckten Dateneingriff legitimieren, bei denen es sich aufgrund ihrer Heimlichkeit gesetzessystematisch um Ausnahmen von dem in den Polizeigesetzen[4] positiv-rechtlich normierten Grundsatz der offenen Datenerhebung handelt.[5]

6 Online-Durchsuchung

Als Online-Durchsuchung wird eine polizeiliche Maßnahme bezeichnet, die einen verdeckten Eingriff in informationstechnische Systeme legitimiert.[6] Diese Eingriffsbefugnis findet in der präventiven Kriminalitätsbekämpfung beispielsweise gem. § 49 Abs. 1 BKAG, Art. 45 Abs.1 BayPAG ihre Anwendung, kann aber auch als repressive Maßnahme auf Grundlage des § 100b Abs. 1 StPO eingesetzt werden. Die Online-Durchsuchung dient primär dem Ziel der Bekämpfung des internationalen Terrorismus, der sich vermehrt moderner Technologie bedient und ein Großteil der Kommunikation mit Hilfe von technischen Kommunikationsmitteln erfolgt, aber auch die Internet-Pornographie und die frühzeitige Entdeckung und Verhinderung von damit verbundenen Straftaten sind mehr und mehr in den Fokus geraten. Durch die Maßnahme wird der Polizei der Zugriff auf Daten gestattet, die entweder noch nicht oder nicht mehr Teil einer laufenden Telekommunikation sind. Hierfür wird ein Spähprogramm – landläufig auch als (Bundes-)Trojaner bezeichnet – auf das Zielsystem aufgespielt, um dessen Nutzung zu überwachen, den Speicher zu durchsuchen und dort befindliche Daten bei dringender Gefahr zu löschen oder zu ändern,[7] wenn diese Gefahr nicht anders abgewendet werden kann. Aber auch das Kopieren sowie das Speichern von Daten und die Nutzung sogenannter Key-Logger, durch die bereits die Tastaturanschläge registriert werden und somit auch ohne eine spätere Speicherung der Eingabe die selbige nachvollzogen werden kann und folglich Daten erfasst werden, die überhaupt nicht im Sinne eines Kommunikationsvorgangs versendet wurden, sind von der Befugnis umfasst.[8] Der Zugriff auf etwaige Kameras oder Mikrofone der Endgeräte ist hingegen auf Grundlage dieser Ermächtigungsgrundlage nicht zulässig. Somit ist die Online-Durchsuchung artverwandt mit der Telekommunikationsüberwachung (TKÜ) und der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), auf die später im Beitrag eingegangen wird.

Vor allem die Entscheidung des BVerfG aus dem Jahr 2016,[9] die dem BKA-Gesetz in der damaligen Fassung eine teilweise

Verfassungswidrigkeit bescheinigte, ließ die Online-Durchsuchung wieder einmal in den der Blickwinkel der Öffentlichkeit geraten. Das BVerfG sah sich in der Folgezeit mit zahlreichen Verfassungsbeschwerden – unter anderem von Rechtsanwälten, Journalisten und Mitgliedern des Bundestages – konfrontiert, die die Frage beantwortet haben wollten, ob das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens aus dem Jahr 2017 und die darin vorgesehene Änderung der Strafprozessordnung in Hinblick auf die Anordnung der Online-Durchsuchung verfassungsgemäß sei.[10] Der Erste Senat des BVerfG hat in seiner Entscheidung zum BKA-Gesetz u.a. klargestellt,[11] dass bei präventiven Maßnahmen das Gewicht der jeweils zu schützenden Rechtsgüter einen wesentlichen Einfluss auf die Zulässigkeit des Eingriffs hat. So ist bei der Online-Durchsuchung grundsätzlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu berücksichtigen, welches als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts aus dem Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet wird. Die Entwicklung und Nutzung der Informationstechnik hatten dazu geführt, dass sich nicht nur neue Möglichkeiten für den einzelnen Nutzer, sondern auch neuartige Gefährdungen der Persönlichkeit begründet hatten. Das Bundesverfassungsgericht hatte mit seiner Entscheidung dementsprechend auf die steigende Bedeutung informationstechnischer Systeme im Rahmen der Lebensgestaltung eines jeden Einzelnen reagiert.[12]

Aufgrund des unter Umständen empfindlichen Eingriffs in das Privatleben des Betroffenen bedarf es einer Gefahr für Leib, Leben und Freiheit einer Person oder einer Bedrohung der Sicherheit des Bundes oder eines Landes, um die Online-Durchsuchung anzuordnen.[13] Aber auch bei einer Gefahr für Güter der Allgemeinheit, die die Existenz von Menschen berühren, kann die Maßnahme verfassungsmäßig sein.[14] Ist die Online-Durchsuchung unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes für die polizeiliche Aufgabenerfüllung notwendig, da die Zweckerreichung ansonsten aussichtslos oder wesentlich erschwert wäre, muss die Maßnahme durch die Behördenleitung beantragt und von einem Richter angeordnet werden. Dabei ist im Rahmen der Gefahrenprognose zu beachten, dass tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für die in der Norm benannten Rechtsgüter vorliegen.[15] Um beispielsweise Rückkehrer aus Terrorcamps überwachen zu können, genügt auch das Verhalten einer Person für die Anordnung einer Online-Durchsuchung, wenn es eine konkrete Wahrscheinlichkeit begründet, dass in einem übersehbaren Zeitraum durch diese Person zumindest auf ihrer Art nach konkretisierte Weise Straftaten von erheblicher Bedeutung begangen werden. Diese Anhaltspunkte müssen sich dabei auf bestimmte Tatsachen stützen und dürfen nicht nur aus bloßen Vermutungen folgen. Liegen die Anordnungsvoraussetzungen vor, kann die Online-Durchsuchung zunächst für höchstens drei Monate angeordnet werden und jeweils um bis zu drei Monate verlängert werden.[16] Im Falle einer Verlängerung ist im Sinne des Verhältnismäßigkeitsgrundsatzes jedoch zu beachten, dass mit zunehmender Dauer die Eingriffsintensität der Maßnahme steigt.[17] Angesichts der hohen Eingriffsqualität der Maßnahme sollte auch bereits bei der Beschaffung und Konfiguration der Überwachungssoftware die gesteigerte Sorgfaltspflicht der Polizei beachtet werden und die Behörde die Funktionalität genau kennen, um eine missbräuchliche Verwendung zuverlässig ausschließen zu können.[18]

Betrachtet man die oben genannten Möglichkeiten und nur teilweise angesprochenen gesetzlichen Vorschriften, kann man einerseits die Online-Durchsuchung als ein mächtiges – wenn auch selten genutztes – Schwert im Kampf gegen internationalen Terrorismus und die Organisierte Kriminalität betrachten, andererseits darf die Eingriffsintensität nicht unberücksichtigt bleiben und aufgrund der strengen Vorgaben einen häufigen Einsatz der Maßnahme in Frage stellen.

Die Heimlichkeit der Maßnahme ist im Verhältnis zu einer möglichen Verdachtslosigkeit einerseits und der möglichen Streubreite andererseits zu betrachten, um die darin innewohnende Gefahr einer grenzenlosen Überwachung durch die Polizei zu entkräften. Hier ist jedoch festzuhalten, dass die Online-Durchsuchung gerade nicht als *„Verdachtsgewinnungseingriff“* zu verstehen ist, sondern die Maßnahme nur angeordnet werden darf, wenn die entsprechenden strengen Vorschriften erfüllt sind. Dass von der Eingriffsbefugnis in Deutschland nur selten Gebrauch gemacht wird, lässt sich allein aus der Tatsache folgern, dass die Online-Durchsuchung derzeit lediglich im BKA-Gesetz sowie im BayPAG, dem HSOG und POG Rheinland-Pfalz normiert ist.

Und auch dort, wo sie zulässig ist, wird die Online-Durchsuchung relativ selten angeordnet. So geht aus dem Bericht der Landesregierung von Rheinland-Pfalz aus dem Jahr 2017 hervor, dass in dem betrachteten Zeitraum von der Maßnahme kein einziges Mal Gebrauch gemacht wurde.[19] Auch bei den Online-Durchsuchungen, die auf Grundlage der Strafprozessordnung angeordnet wurden, sind die die Zahlen überschaubar. So weist das Bundesamt für Justiz in der Übersicht zur Telekommunikationsüberwachung für das Berichtsjahr 2019 zwar 21 durch richterlichen Beschluss angeordnete Online-Durchsuchungen gem. § 100b Abs.1 StPO aus, von denen 11 Verlängerungsanordnungen waren und insgesamt lediglich 12 Eingriffe in ein vom Betroffenen genutztes informationstechnisches System tatsächlich durchgeführt wurden.[20] Zwar wird in Niedersachsen auf politischer Ebene über eine Einführung der Online-Durchsuchung nachgedacht,[21] dass dieses aber dann zu einem massenhaften Einsatz führen wird, dürfte nicht zu befürchten sein. Somit kann die Online-Durchsuchung als ein wichtiger Ton auf der Klaviatur der Eingriffsbefugnisse der Sicherheitsbehörden betrachtet werden, der aber selten genutzt wird.

7 Dateneingriff in die laufende Telekommunikation

Im Zuge der immer schneller fortschreitenden und inzwischen weit verbreiteten Digitalisierung ist es zu einer verstärke Nutzung von informationstechnischen Systemen und speziell der mobilen Telekommunikation im Bereich der kriminellen Machenschaften gekommen. Um diesem zu begegnen, wurden in Bund und Ländern in den vergangenen Jahren neue Eingriffsnormen in Bezug auf die Überwachung, gegebenenfalls die Unterbrechung oder Verhinderung der Kommunikation über informationstechnische Systeme geschaffen. Dabei ist die Notwendigkeit der Maßnahmen oftmals auf Grundlage des internationalen Terrorismus begründet worden; der letztlich geschaffene Anwendungsbereich ist jedoch häufig weiter gefasst und ermöglicht den Einsatz der Maßnahmen gegen ein breites Feld abzuwehrender Gefahren. Bei einem Eingriff in die laufende Telekommunikation ist aufgrund des Fernmeldegeheimnisses, welches verfassungsrechtlich gem. Art. 10 Abs. 1 GG geschützt und einfachgesetzliche in § 88 Abs. 1 Telekommunikationsgesetz (TKG) genauer beschrieben ist, stets zu beachten, dass dieser nur aufgrund einer entsprechenden Ermächtigungsnorm zulässig ist. Dabei wird durch diese grundrechtliche Gewährleistung nicht nur der Kommunikationsinhalt geschützt, sondern auch die näheren Umstände und hier insbesondere *„ob und wann zwischen welchen Personen und Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist.“*[22] Zur Legitimation einer entsprechenden Maßnahme sind in zahlreichen Landesgesetzen Normen vorhanden, die den Dateneingriff zur präventiven Kriminalitätsbekämpfung durch polizeiliche Maßnahmen regeln.[23] Dabei kann man aus rechtlicher und technischer Sicht zwischen der Telekommunikationsüberwachung und der Quellen-Telekommunikationsüberwachung unterscheiden, die in den Polizeigesetzen häufig in einer Norm zusammengefasst werden.

7.1 Telekommunikationsüberwachung

Bei der *„klassischen“* Telekommunikationsüberwachung erfolgt ein Dateneingriff in ein Telefongespräch, die Internetkommunikation oder den E-Mail-Verkehr, indem die laufende Kommunikation durch die Polizei unmittelbar mitverfolgt und unter Umständen aufgezeichnet wird, oder von den Betreiberfirmen Auskünfte zu Teilnehmern, allgemeinen Verkehrsdaten, Inhalten und bisweilen Aufzeichnungen angefordert werden.[24] Dabei kann es sich um Nachrichten in Form von Zeichen, Bildern oder Sprache handeln, die via Telefon oder Telefax übertragen werden; aber auch der Datentransfer in Chats, per Voice-over-IP[25] oder Messenger-Diensten – mobil oder über eine Standleitung – ist inbegriffen.[26] Die Notwendigkeit der TKÜ für die präventive Kriminalitätsbekämpfung wurde zuletzt auch von der Landesregierung in Berlin erkannt, so dass am 11. März 2021 im Abgeordnetenhaus die Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes beschlossen und dadurch die TKÜ im § 25a ASOG normiert wurde. Begründet wurde dieser *„Sinneswandel“* u.a. mit dem Anschlag auf den Weihnachtsmarkt am Breitscheidplatz im Jahre 2016 und der allgemeinen Abwehr schwerster Rechtsgutgefährdungen. Berlin folgt mit dieser Entscheidung den anderen Ländern, die die TKÜ schon erfolgreich eingeführt und erprobt haben, hält sich jedoch vor *„die Wirkungsweise und Anwendung dieser Befugnisse nach einem angemessenen Erprobungszeitraum unabhängig wissenschaftlich zu evaluieren“*.[27]

Um den Anforderungen an die formelle Rechtmäßigkeit zu genügen, müssen – neben den jeweiligen landesspezifischen Vorschriften zu den Grundsätzen der Datenerhebung – der Richtervorbehalt, die Befristung der Maßnahme und eventuell die nachträgliche Unterrichtungspflicht der von der Maßnahme betroffenen Personen beachtet werden. Aus materieller Sicht bedarf es für den im Rahmen der TKÜ vorgesehenen Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG besondere Gründe. So darf eine Beschränkung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 2 S. 1 GG durch Gesetz oder aufgrund eines Gesetzes erfolgen, das dem rechtstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht. Entsprechende Vorschriften finden sich in den Polizeigesetzen der Länder, nach denen die präventivpolizeiliche TKÜ vor allem zur Abwehr einer konkreten Gefahr angeordnet werden kann. Ein wesentlicher Punkt bei der gefahrenabwehrenden Maßnahme gegenüber der Strafverfolgung ist der der Beweislage. Während bei einer Anordnung nach § 100a StPO in der Regel bereits ein konkreter Tatverdacht vorliegt und die Maßnahme der Strafverfolgung dient, findet der Grundrechtseingriff in der präventiven TKÜ zu einem vorgelagerten Zeitpunkt statt, in dem zwar Tatsachen für konkrete Gefahren und die mögliche Begehung einer Straftat sprechen, es jedoch noch offen ist, ob es überhaupt zu der befürchteten Rechtsgutverletzung kommen wird. Aus diesem Grunde müssen hier die für die mögliche Anordnung der TKÜ anlassgebende Straftat sowie die Anforderungen an die Tatsachen, die auf die voraussichtliche Begehung der Straftat hinweisen, so bestimmt umschrieben sein, dass das Risiko einer Fehlprognose verfassungsrechtlich noch vertretbar ist.[28]

7.2 Quellen-Telekommunikationsüberwachung

Seit einigen Jahren hat vor allem die Nutzung von verschlüsselten Kommunikationswegen die Sicherheitsbehörden vor die Herausforderung gestellt, möglichst frühzeitig auf die informationstechnischen Systeme zugreifen zu können, bevor die zu übertragenden Daten kodiert werden. Auch um diesen Anforderungen gerecht zu werden, wurde eine Erweiterung der Befugnis zum Dateneingriff in die laufende Kommunikation zwischen elektronischen Systemen vorgenommen. Die *„neue“* Quellen-TKÜ weist dabei aufgrund der Infiltration eines informationstechnischen Systems mithilfe einer Spähsoftware deutliche Parallelen zur

Online-Durchsuchung auf, bei der ein Zugriff auf die abgeschlossene und auf einem informationstechnischen System gespeicherte Kommunikation sowie sonstige gespeicherte Daten ermöglicht wird. Die Zielrichtung der Quellen-TKÜ ist aufgrund des Zugriffs auf die laufende Kommunikation jedoch eine andere. Nachdem zunächst Telefongespräche via Voice-over-IP im Fokus der Maßnahme standen, auf die bedingt durch die zunehmende Verschlüsselung der Daten nicht mehr auf Grundlage der Regelungen zur TKÜ zugegriffen werden konnte, ist in den letzten Jahren die Überwachung und Aufzeichnung der Kommunikation mittels Messenger-Dienste unter Nutzung von mobilen Endgeräten in den Vordergrund gerückt, da diese in der Regel über eine *„end-to-end“* Verschlüsselung verfügen, die ein Abgreifen und Auslesen der Kommunikation erschwert. Inzwischen kommen die Sicherheitsbehörden bei der Überwachung von informationstechnischen Systemen um Messenger-Dienste wie WhatsApp oder Telegram nicht mehr herum. Vor allem der letztgenannte Dienst wird von Kriminellen für ihre Machenschaften oftmals genutzt, da Telegram im Gegensatz zu anderen Messenger-Diensten kaum Inhalte zensiert, die Nutzer ihre Telefonnummer ausblenden und stattdessen beliebige Namen nutzen dürfen, die Versendung wesentlich größerer Datenmengen möglich ist und Gruppen mehrere hunderttausend Mitglieder haben können. Zusätzlich ist es ein Cloud-basierter Messenger und neue Mitglieder in Gruppen können bei Eintritt auf den Chat-Verlauf und frühere Nachrichten und Daten zugreifen.[29] Zwar gibt es bereits seit 2018 eine Kooperation zwischen Telegram und Europol,[30] um die Nutzung des Dienstes durch terroristische Gruppierungen zu unterbinden, dennoch wächst die Anzahl der Nutzer kontinuierlich und hat zu Beginn dieses Jahres die Marke von 500 Millionen überschritten. Dass unter diesen durchaus eine Großzahl von Verschwörungstheoretikern bis hin zum Terroristen sein könnte, kann man aus der Tatsache schlussfolgern, dass nach dem Sturm auf das Kapitol in Washington/USA und der Sperrung von anderen Messenger-Diensten Telegram binnen 72 Stunden mehr als 25 Millionen neue Nutzer verzeichnen konnte.[31] Als dies und primär die Tatsache der Möglichkeit einer *„end-to-end“* Verschlüsselung zeigt die Notwendigkeit einer präventivpolizeilichen Befugnisnorm, um die Kommunikation überwachen zu können. Dabei ist durch technische Maßnahmen zu gewährleisten, dass – wie wörtlich vom BVerfG in seiner Entscheidung zum BKA-Gesetz vorgegeben und in vielen Gesetzen übernommen – *„ausschließlich laufende Telekommunikation überwacht und aufgezeichnet“* wird.[32] Durch diese gerichtliche Maßgabe ergeben sich für die Praxis neue Herausforderungen, da sich die Frage stellt, in welcher Phase einer Datenübertragung von einer laufenden Kommunikation gesprochen werden kann.

8 Laufende oder ruhende Kommunikation

Nicht einfach zu beantworten ist bei einigen Kommunikationsformen die Frage, ob es sich um eine laufende oder eine *„ruhende“* Kommunikation handelt. Bei einem Telefongespräch kann man unzweifelhaft davon ausgehen, dass das gesprochene Wort unmittelbar übertragen und von dem Gesprächspartner empfangen wird, so dass eine laufende Kommunikation stattfindet. In dem Fall liegt bei einem abhören oder aufzeichnen der Kommunikation ein Eingriff in das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG vor, der jedoch aufgrund der entsprechenden Eingriffsbefugnisse zur TKÜ rechtmäßig sein kann. Schwieriger ist diese Zuordnung bei der Kommunikation via E-Mail oder Messenger-Dienst, da jeweils der technische Ablauf und seine Interpretation ausschlaggebend dafür ist, ob sie als laufende oder *„ruhende“* Kommunikation zu identifizieren ist.

Das BVerfG hat mit einer Entscheidung zur Telekommunikationsüberwachung im Jahr 2016 festgestellt, dass *„nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten [...] nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) und gegebenenfalls durch Art. 13 Abs. 1 GG geschützt“* werden.[33] Danach ist in dieser letzten Phase der E-Mail-Kommunikation ein Eingriff zu repressiven Zwecken auf Grundlage der §§ 94 ff. und 102 ff. StPO oder im Rahmen der Gefahrenabwehr beispielsweise gem.
§ 43 PolG NRW zulässig, wobei das PolG NRW im Gegensatz zur StPO und einigen anderen Landespolizeigesetzen[34] nicht zwischen einer Sicherstellung und einer Beschlagnahme unterscheidet.

Dieser letzten Phase sind nach dem sog. *„Phasenmodell“*[35] drei weiteren vorgelagert. In Phase 1 wird die E-Mail nach dem Verfassen durch den Absender von dessen Endgerät über den Internet-Provider auf den Mail-Server und in das persönliche elektronische Postfach des Empfängers übertragen. Bei diesem Prozess handelt es sich um eine laufende Kommunikation, in die zur Strafverfolgung nach § 100a StPO und zu präventiven Zwecken z.B. auf Grundlage des § 20c PolG NRW eingegriffen werden kann. Vergleichbar ist die Situation in der Phase 3, in der die E-Mail vom Empfänger abgerufen wird, und somit in die laufende Kommunikation nach eben genannten Paragraphen erfolgen kann. Strittig ist hingegen die Frage nach der Ermächtigungsgrundlage in der Phase 2, in der die Nachricht bereits versendet wurde und auf dem Server zwischengespeichert wurde. Das BVerfG hat für die dort gespeicherte – ungelesene als auch gelesene – Nachricht zwar einen Grundrechtsschutz gem. Art. 10 Abs. 1 GG anerkannt, eine Sicherstellung und Beschlagnahme nach § 94 StPO jedoch zugelassen.[36] Dieser Eingriff müsste jedoch dem Betroffenen unverzüglich mitgeteilt werden, eine vorübergehende Verheimlichung aus ermittlungstaktischen Gründen ist nicht zulässig. Aus polizeilicher Sicht ist abschließend etwas versöhnlich, dass bei einer zulässigen Beschlagnahme der Gesetzesverstoß der versäumten Mitteilung an den Betroffenen nicht so schwerwiegend

gewertet wird und es nicht ein Beweisverwertungsverbot begründet,[37] so dass die rechtmäßig erlangten Informationen für ein späteres Verfahren verwendet werden dürfen. Kritik wird an diesem Phasenmodell insofern geübt, dass der Nutzer das Versenden und Empfangen einer E-Mail meist als einen zusammengehörigen Prozess wahrnimmt und nicht eine Unterscheidung in verschiedene Phasen vornimmt.[38]

9 Fazit

Die kontinuierliche Novellierung der Polizeigesetze ist elementare Voraussetzung für eine präventive Gefahrenabwehr. Dies gilt in besonderem Maße bei Eingriffsbefugnissen, die technischen Elemente beinhalten, sei es als Ziel oder Mittel der Maßnahme. Vor allem die informationstechnischen Systeme haben in den vergangenen Jahren eine rasante Entwicklung vorzuweisen, sowohl aus technischer Sicht als auch in Bezug auf deren Verbreitungs- und Nutzungsgrad. Zu Beginn dieses Jahrs hatte allein WhatsApp rund zwei Milliarden aktive Nutzer weltweit und in Deutschland belief sich die Anzahl der Smartphone-Nutzer auf über 60 Millionen.[39] Dies hatte – nicht zuletzt bedingt durch den aufkeimenden internationalen Terrorismus – einen großen Anpassungsdruck im Bereich der Überwachung der informationstechnischen Systeme zur Folge und hat sich in verschiedenen Polizeigesetzen und der Strafprozessordnung *„entladen“*. Mit der Aufnahme der Quellen-TKÜ in der Strafprozessordnung und den entsprechenden Gesetzen zur Regelung der Aufgabenbereiche und Eingriffsbefugnisse der Polizeien von Bayern bis jüngst auch in Berlin wurde den Behörden beispielsweise ein wichtiger Pfeil in den Köcher gelegt. Jetzt liegt es an ihnen, damit verantwortungsvoll umzugehen, um das Vertrauen der Gesellschaft zu wahren. Der Blick in die Vergangenheit lässt jedoch darauf schließen, dass diese neuen Befugnisse nicht inflationär genutzt werden, sowie darauf hoffen, dass durch sie die kriminellen Machenschaften zumindest im Keim erstickt werden können und so durch sie ein Beitrag zur präventiven Kriminalitätsbekämpfung erzielt wird.

Anmerkungen

1. Gerrit Domenghino LL.M. ist Wissenschaftlicher Mitarbeiter im Fachgebiet III.[4] (Öffentliches Recht mit Schwerpunkt Polizeirecht) an der Deutschen Hochschule der Polizei in Münster.
2. Domenghino, Die Kriminalpolizei 1/2021, S. 14-17.
3. Keller, Christoph/Braun, Frank, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, 3. Auflage, Richard Bloorberg Verlag, Stuttgart, 2019, S. 101.
4. Vgl. etwa § 9 Abs. 5 PolG NRW, § 31 Abs. 3 BayPAG.
5. Graulich, Kurt in: Lisken, Hans/Denninger, Erhard, Handbuch des Polizeirechts, 6. Aufl., C.H.Beck, München, 2018, S. 548.
6. Vgl. BR-Drs. 404/08, S. 35.
7. BeckOK PolR Bayern/Petri, Art. 45, Rn. 18.
8. Graulich, Kurt in: Lisken, Hans/Denninger, Erhard, Handbuch des Polizeirechts, 6. Aufl., C.H.Beck, München, 2018, S. 583.
9. BVerfG, Urteil des Ersten Senats vom 20.4.2016, - 1 BvR 966/09 -, NJW 2016, 1781.
10. Vgl. BVerfG, Verfahren, Übersicht für das Jahr 2019, 2. Senat, Nr. 26, online verfügbar unter: www.bundesverfassungsgericht.de/DE/Verfahren/Jahresvorausschau/vs_2019/vorausschau_2019_node.html.
11. Vgl. BVerfG, Urteil des Ersten Senats vom 20.4.2016, - 1 BvR 966/09 -, NJW 2016, 1781, Rn.108.
12. Vgl. dazu grundlegend BVerfGE 120, 274, NJW 2008, S. 822 ff.
13. Ebd. mit Verweis auf BVerfGE 120, 274, Rn. 328, NJW 2008, S. 822 ff.; BVerfGE 125, 260, Rn. 330, NJW 2010, S. 822.
14. Vgl. BVerfGE 120, 274, Rn. 328, NJW 2008, S. 822 ff.
15. BVerfGE 141, 220, Rn. 212, online verfügbar unter: www.servat.unibe.ch/dfr/bv141220.html.
16. Vgl. etwa § 49 Abs. 5 BKAG, Art. 45 Abs. 3 BayPAG.
17. BeckOK PolR Bayern/Petri, Art. 45, Rn. 33.

18. Vgl. BeckOK PolR Bayern/Petri, Art. 45, Rn. 24.
19. Landtag Rheinland-Pfalz, Lt-Drs. 17/2752, Bericht der Landesregierung nach § 100 POG – Evaluation verdeckter polizeilicher Befugnisse, S. 20.
20. Zahlen veröffentlich beim BfJ, online verfügbar unter: www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html.
21. Vgl. Gesellschaft für Freiheitsrechte, Übersicht über die Änderungen der Polizeigesetze in den einzelnen Bundesländern.
22. BVerfG, 1. Senat, Entsch. V. 20.6.1984, 1 BvR 1494/78, Rn. 46.
23. Vgl. etwa Art. 42 BayPAG, § 23a BWPolG, § 33d SOG M-V.
24. Kingreen, Thorsten/Poscher, Ralf, Polizei- und Ordnungsrecht mit Versammlungsrecht, 10. Aufl. C.H.Beck, München, 2018, S. 244.
25. Voice-over-IP (VoIP) ist eine Technologie zur Übertragung von Sprachsignalen über eine Internetleitung.
26. Schmidt, Rolf, Polizei- und Ordnungsrecht, 19. Aufl., Dr. Rolf Schmidt GmbH, 2017, Rn. 293.
27. Abgeordnetenhaus Berlin, Drs. 18/2787, Dreiundzwanzigstes Gesetz zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes und anderer Gesetze, S. 21, online verfügbar unter: pardok.parlament-berlin.de/starweb/adis/citat/VT/18/DruckSachen/d[18]-2787.pdf
28. Vgl. BVerfG, Urteil vom 27.7.2005 - 1 BvR 668/04, NJW 2005, 2603, S. 2608.
29. Zum vorstehenden vgl. t-online, online verfügbar unter: www.t-online.de/digital/internet/id_87872760/telegram-was-steckt-hinter-dem-messenger-telegram-.html.
30. Vgl. Europol, Newsroom, 25.11.2019, online verfügbar unter: www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online.
31. Vgl. NDR, 20.1.2021, online verfügbar unter: www.ndr.de/fernsehen/sendungen/zapp/Joe-Biden-und-sein-schweres-Erbe,biden152.html.
32. BVerfG, 1. Senat, Entsch. v. 20.6.1984, 1 BvR 1494/78, Rn. 228.
33. BVerfG, 2. Senat, Entsch. v. 2.3.2006, 2 BvR 2099/04, 1. Leitsatz.
34. So wird z.B. im PolG von Baden-Württemberg in § 37 die Sicherstellung und in § 38 die Beschlagnahme geregelt.
35. Ausführlich dazu: Keller, Christoph/Braun, Frank, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, 3. Auflage, Richard Bloorberg Verlag, Stuttgart, 2019, S. 39 ff.
36. Vgl. BVerfG, 2. Senat, Entsch. v. 16.6.2009, 2 BvR 902/06, 1. Leitsatz.
37. Mosbacher, Andreas, Aktuelles Strafprozessrecht, JuS 2016, S. 132.
38. Zum vorstehenden vgl.: Keller, Christoph/Braun, Frank, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen, 3. Auflage, Richard Bloorberg Verlag, Stuttgart, 2019, S. 39 ff.
39. Statista, Technik & Telekommunikation, online verfügbar unter: de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/.