Prof. Dr. Jan Dirk Roggenkamp
Korrespondenzadresse
c/o Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Tel: 0521-1639 1639
Fax: 0521-6 11 72

An das
Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe

Karlsruhe/Bielefeld, den 30. Oktober 2019

Verfassungsbeschwerde

Der Frau [redacted] - Beschwerdeführerin zu 1 -

der Frau - Beschwerdeführerin zu 2 -

des Herrn - Beschwerdeführer zu 3 -

des Herrn - Beschwerdeführer zu 4 -

der Frau - Beschwerdeführerin zu 5 -

der Frau - Beschwerdeführerin zu 6 -

<u>Prozessbevollmächtigter:</u>

Prof. Dr. jur. Jan Dirk Roggenkamp
c/o Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Namens und im Auftrag der Beschwerdeführerinnen und Beschwerdeführer (im Weiteren als „Beschwerdeführer*innen“ bezeichnet) erhebe ich unter Beifügung entsprechender Vollmachten Verfassungsbeschwerde gegen den § 20c des Polizeigesetzes des Landes Nordrhein-Westfalen (im Weiteren: „PolG NRW“) sowie den dort referenzierten § 8 Abs. 4 PolG NRW.

und beantrage

1. § 20c PolG NRW sowie § 8 Abs. 4 PolG NRW in der Fassung des Gesetzes zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden vom 18. Dezember 2018 (GV. NRW. S. 741, ber. 2019 S. 23), in Kraft getreten am 29. Dezember 2018 bzw. des Gesetzes zur Stärkung der Sicherheit in Nordrhein-Westfalen - Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen vom 13. Dezember 2018 (GV. NRW. S. 684, ber. 2019 S. 23), in Kraft getreten am 20. Dezember 2018 für mit dem Grundgesetz unvereinbar und nichtig zu erklären;

2. den Beschwerdeführer*innen die notwendigen Auslagen zu erstatten.

Die Beschwerdeführer*innen rügen die Verletzung ihrer Grundrechte aus Art. 1 Abs. 1 GG, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie Art. 10 Abs. 1 GG durch die oben genannten Vorschriften und begründen die Verfassungsbeschwerde wie folgt:

Gliederung

A. Sachverhalt

I. Angegriffene Regelungen

Die Beschwerdeführer*innen rügen die Verletzung ihrer Grundrechte aus Art. 1 Abs. 1 GG, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie Art. 10 Abs. 1 GG durch § 20c PolG NRW sowie den dort referenzierten § 8 Abs. 4 PolG NRW.

1. § 20c PolG NRW – Telekommunikations- und Quellen-Telekommunikationsüberwachung

Durch das „Gesetz zur Stärkung der Sicherheit in Nordrhein-Westfalen - Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen vom 13. Dezember 2018“ (GV. NRW. S. 684, ber. 2019 S. 23), in Kraft getreten am 20. Dezember 2018 wurde mit § 20c PolG NRW eine Befugnis zur Telekommunikations- und Quellen-Telekommunikationsüberwachung geschaffen. Bereits wenige Tage später – mit „Gesetz zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden vom 18. Dezember 2018“ (GV. NRW. S. 741, ber. 2019 S. 23), in Kraft getreten am 29. Dezember 2018 – wurden Abs. 8 Sätze 6 und 7 der ursprünglichen Fassung des hier gegenständlichen § 20c PolG NRW geändert, der Abs. 9 aufgehoben, der bisherige Abs. 10 zu Abs. 9 und neu gefasst, sowie Abs. 11 aufgehoben. Die Verfassungsbeschwerde richtet sich gegen den § 20c PolG NRW in der Fassung des letztgenannten Gesetzes, die die derzeit aktuelle Fassung darstellt.

Die Regelung ist wie folgt gefasst:

> **§ 20c PolG NRW - Datenerhebung durch die Überwachung der laufenden Telekommunikation**
>
> (1) Die Polizei kann ohne Wissen der betroffenen Person die laufende Telekommunikation einer Person überwachen und aufzeichnen,
>
> 1. die nach den §§ 4 oder 5 verantwortlich ist, wenn dies zur Abwehr einer gegenwärtigen Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib oder Leben einer Person geboten ist,
>
> 2. deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 8 Absatz 4 begehen wird,

3. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder

4. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird

und die Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(3) Bei Maßnahmen nach Absatz 2 ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist gegen unbefugte Nutzung zu schützen. Kopierte Daten sind gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(4) Maßnahmen nach den Absätzen 1 und 2 dürfen nur auf Antrag der Behördenleitung oder deren Vertretung durch das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat, angeordnet werden. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,

2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,

3. Art, Umfang und Dauer der Maßnahme,

4. im Falle des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll, sowie die Bezeichnung des Herstellers und der Softwareversion des einzusetzenden technischen Mittels,

5. der Sachverhalt und

6. eine Begründung.

(6) Die Anordnung des Gerichts ergeht schriftlich. In ihr sind anzugeben:

1. eine Kennung des Kommunikationsanschlusses oder des Endgeräts, bei dem die Datenerhebung durchgeführt wird,

2. im Falle des Absatzes 2 zusätzlich eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll.

Im Übrigen gilt § 18 Absatz 2 Satz 3 mit Ausnahme der Bezeichnung der betroffenen Wohnung entsprechend. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. § 18 Absatz 2 Satz 5 bis 9 gilt entsprechend.

(7) Aufgrund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), der Polizei die Maßnahmen nach Absatz 1 zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation. Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

(8) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den Absätzen 1 und 2 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit im Rahmen von Maßnahmen nach den Absätzen 1 und 2 neben einer automatischen Aufzeichnung eine unmittelbare Kenntnisnahme erfolgt, ist die Maßnahme unverzüglich zu unterbrechen, soweit sich während der Überwachung tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte, die dem Kernbereich privater

> Lebensgestaltung zuzurechnen sind, erfasst werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den Absätzen 1 und 2 erlangt worden sind, dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle gemäß § 33c verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 33 Absatz 2 Satz 1 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung nach § 33 Absatz 4 Satz 7 zu löschen. Ist die Datenschutzkontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren. Im Übrigen gilt § 18 Absatz 3 Satz 3 und Absatz 4 Satz 2 bis 7 entsprechend.
>
> (9) Bei der Erhebung von Daten nach den Absätzen 1 und 2 sind die in § 33b Absatz 1 und 2 genannten Angaben zu protokollieren. Im Falle des Absatzes 2 sind darüber hinaus folgende Angaben zu protokollieren:
>
> 1. Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen, nicht nur flüchtigen Veränderungen,
>
> 2. Angaben zum Hersteller des zur Datenerhebung eingesetzten Mittels und zur eingesetzten Softwareversion.
>
> (10) *(weggefallen)*
>
> (11) (*weggefallen*)
>
> (12) Die Landesregierung überprüft die Wirksamkeit der Vorschrift bis zum 31. Dezember 2022 und berichtet dem Landtag über das Ergebnis der Evaluierung. § 20c tritt am 31. Dezember 2023 außer Kraft.

2. § 8 Abs. 4 PolG NRW – Terroristische Straftaten im Sinne des PolG NRW

Mit dem „Gesetz zur Stärkung der Sicherheit in Nordrhein-Westfalen - Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen“ vom 13. Dezember 2018 (GV. NRW. S. 684, ber. 2019 S. 23), in Kraft getreten am 20. Dezember 2018 wurde mit § 8 Abs. 4 PolG NRW eine Legaldefinition der sog. terroristischen Straftaten im Sinne des PolG NRW eingefügt. Im Rahmen des „Gesetzes zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden“ vom 18. Dezember 2018 (GV. NRW. S. 741, ber. 2019 S. 23), in Kraft getreten am 29. Dezember 2018 erfolgte keine Änderung des § 8 Abs. 4 PolG NRW. Die Legaldefinition wird im Zusammenhang mit der Formulierung der Voraussetzungen bzw.

Eingriffsschwellen unterschiedlicher Befugnisse, insbesondere aber auch im Zusammenhang mit der hier angegriffenen Regelung des § 20c PolG NRW – namentlich § 20c Abs. 1 Nr. 2 PolG NRW verwendet, weshalb sich diese Verfassungsbeschwerde auf diese Regelung erstreckt.

§ 8 Abs. 4 PolG NRW ist wie folgt gefasst:

> **§ 8 PolG NRW - Allgemeine Befugnisse, Begriffsbestimmung**
> [...]
> (4) Straftaten nach
> 1. § 211, § 212, § 226, § 227, § 239a, § 239b, § 303b, § 305, § 305a, §§ 306 bis 306 c, § 307 Absatz 1 bis 3, § 308 Absatz 1 bis 4, § 309 Absatz 1 bis 5, § 313, § 314, § 315 Absatz 1, 3 oder 4, § 316b Absatz 1 oder 3, § 316c Absatz 1 bis 3, § 317 Absatz 1, § 328 Absatz 1 oder 2, § 330 Absatz 1 oder 2 oder § 330a Absatz 1 bis 3 des Strafgesetzbuchs,
> 2. den §§ 6 bis 12 des Völkerstrafgesetzbuchs vom 26. Juni 2002 (BGBl. I S. 2254), das durch Artikel 1 des Gesetzes vom 22. Dezember 2016 (BGBl. I S. 3150) geändert worden ist,
> 3. § 19 Absatz 1 bis 3, § 20 Absatz 1 oder 2, § 20a Absatz 1 bis 3, § 19 Absatz 2 Nummer 2 oder Absatz 3 Nummer 2, § 20 Absatz 1 oder 2, § 20a Absatz 1 bis 3, jeweils auch in Verbindung mit § 21, oder § 22a Absatz 1 bis 3 des Gesetzes über die Kontrolle von Kriegswaffen in der Fassung der Bekanntmachung vom 22. November 1990 (BGBl. I S. 2506), das zuletzt durch Artikel 6 Absatz 2 des Gesetzes vom 13. April 2017 (BGBl. I S. 872) geändert worden ist, und
> 4. § 51 Absatz 1 bis 3 des Waffengesetzes vom 11. Oktober 2002 (BGBl. I S. 3970, 4592; 2003 I S. 1957), das zuletzt durch Artikel 1 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2133) geändert worden ist,
> sind terroristische Straftaten im Sinne dieses Gesetzes, wenn und soweit sie dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und

sie durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können.

II. Technische Hintergründe

1. Telekommunikationsüberwachung (§ 20c Abs. 1 PolG NRW) in der Praxis

Mit § 20c Abs. 1 PolG NRW wurde eine Ermächtigungsgrundlage zur Durchführung einer präventiv-polizeilichen Telekommunikationsüberwachung in das PolG NRW eingeführt. Durch diesen wird der Polizei gestattet, heimlich „*die laufende Telekommunikation*“ zu überwachen und aufzuzeichnen.

Nach § 20c Abs. 7 Satz 1 PolG NRW gilt

> „*Aufgrund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), der Polizei die Maßnahmen nach Absatz 1 zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation.*“

Referenziert werden u.a. die §§ 3 Abs. 1, 9 der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (TKÜV[1]).

Auf Basis der TKÜV ist es bei Telekommunikationsüberwachungsmaßnahmen gang und gäbe, dass die Diensteanbieter den Ermittlungsbehörden/der Polizei sog.

[1] Telekommunikations-Überwachungsverordnung 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.

Überwachungskopien (§ 2 Nr. 14 TKÜV) des gesamten über einen bestimmten Telekommunikationsanschluss verursachten „Rohdatenstroms" zuleiten.[2]

a. Stets: Überwachung der Mensch-zu-Mensch-Kommunikation

Aus diesem Rohdatenstrom kann zunächst grundsätzlich die gesamte **Individualkommunikation** zwischen zwei (oder mehreren) Menschen (Mensch-zu-Mensch-Kommunikation) entnommen werden, z.B. Telefonie, Fax, E-Mail, SMS und andere Text- und Sprachnachrichten.

b. Standard: Überwachung der Mensch-zu-Maschine-Kommunikation

Der im Rahmen einer Telekommunikationsüberwachung an die Polizei auszuleitende Datenstrom in Form der Überwachungskopie beinhaltet aber nicht nur Daten, die, etwa als Internettelefonie, der Individualkommunikation zwischen zwei Menschen zugeordnet werden können. Er umfasst auch alle sonstigen Daten, die durch den oder die Nutzerinnen und Nutzer des Anschlusses (oder durch die über den Anschluss mit dem Internet verbundenen Geräte – hierzu sogleich) bei der Internetnutzung erzeugt werden.[3]

Im Rahmen einer „herkömmlichen" Telekommunikationsüberwachung besteht die technische Möglichkeit auf das gesamte Internetnutzungsverhalten der Zielperson zuzugreifen. Ausgeleitet werden mit dem Rohdatenstrom sämtliche Eingaben und sonstigen Aktivitäten im Internet (z.B. Up- und Downloads sowie der Aufruf und die Nutzung von Internetseiten – z.B. die Eingabe von Suchbegriffen) kurz: die Kommunikation „Mensch-zu-Maschine".

Die Verwendung von Verschlüsselungsmechanismen bietet dabei kaum Schutz. Verschlüsselt übermittelte Daten können aus dem Rohdatenstrom ausgefiltert und automatisiert mittels entsprechender Software oder manuell durch besonders geschultes

[2] *Albrecht/Braun*, HRRS 2013, 500 (500) m.w.N.
[3] *Albrecht/Braun*, HRRS 2013, 500 (500) m.w.N; *Hiéramente*, HRRS 2016, 448 (450f.)

Personal entschlüsselt werden.[4] Derartiges wird beispielsweise offenbar durch die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS) geleistet[5]:

> „*Innerhalb ZITiS unterstützt der Bereich Kryptoanalyse insbesondere Projekte in der Digitalforensik und Telekommunikationsüberwachung, in denen der Umgang mit Verschlüsselung eine große Rolle spielt. Dafür wird auf das hier vorhandene Spezialwissen und die entwickelten Methoden zurückgegriffen.*“[6]

Eingesetzt werden (sollen) hierzu unter anderem Hochleistungs- und Quantencomputer.[7] Mit letzteren dürften in absehbarer Zeit alle heute üblichen Verschlüsselungsverfahren „geknackt“ werden können.

Zudem ist es offenbar nicht unüblich, dass die notwendigen Informationen zur Entschlüsselung von den Anbietern von Internetkommunikations- und Cloudanwendungen bezogen werden bzw. zumindest bezogen werden können. In einem Bericht von Telepolis aus dem Jahr 2013 über Enthüllungen des Edward Snowden über die Zusammenarbeit der NSA mit Microsoft heißt es:

> „*Microsoft versicherte angesichts der neu veröffentlichten Dokumente erneut gegenüber dem Guardian, dass Kundendaten nur als "Antwort auf legale Prozesse" an Behörden weiter gegeben werden. Man weise Anfragen zurück, wenn sie nicht als berechtigt empfunden würden. Und man erfülle keine allgemeinen Anfragen, sondern nur solche in Bezug auf bestimmte Accounts oder Identitäten.* ***Man müsse aber, wenn Produkte aktualisiert werden, "unter bestimmten Bedingungen rechtliche Verpflichtungen erfüllen, um die Möglichkeit zu gewährleisten,***

[4] *Albrecht/Braun*, HRRS 2013, 500 (500) m.w.N.
[5] Nach Auskunft der *BReg* sollen „*Die zuständigen Behörden der Länder [...] an den Ergebnissen der Tätigkeit der ZITiS mittelbar partizipieren*“ können, Antwort Nr. 2 auf Kleine Anfrage BT-Drs. 19/6246, S. 3.
[6] Selbstdarstellung ZITiS (Stand: Oktober 2019) abrufbar unter https://www.zitis.bund.de/DE/Arbeitsfelder/Kryptoanalyse/kryptoanalyse_node.html - Ausdruck anbei als **Anlage 1**.
[7] Siehe Antwort des Staatssekretärs *Vitt* zu Frage 16 und 17 der „Schriftlichen Fragen mit den in der Woche vom 22.10.2018 eingegangenen Antworten der Bundesregierung“, BT-Drs. 19/5282, S. 10.

> ***Informationen in Antwort auf Anforderungen im Rahmen der Strafverfolgung oder der nationalen Sicherheit liefern zu können***"[8].

Daraus kann gefolgert werden, dass offenbar durchaus eine Bereitschaft seitens der Anbieter besteht, eine Telekommunikationsüberwachungsmaßnahme zu unterstützen bzw. den Ermittlungsbehörden Informationen zur Überwindung eventueller, in den jeweiligen „Produkten" angelegter „Hürden" zukommen zu lassen.

Das eine umfangreiche Aus- und Verwertung der Datenströme nicht nur theoretisch möglich ist, sondern in der Praxis der Telekommunikationsüberwachung auch erfolgt, zeigt z.B. die Schilderung der Erkenntnisse einer repressiven Telekommunikationsüberwachung aus dem Jahr 2004 (!) im Tatbestand einer Entscheidung des OLG Stuttgart[9] aus dem Jahr 2008 (!):

> *„Danach konnten **anhand der Telefon- bzw. DSL-Überwachung** im Zeitraum ab Mitte Januar 2004 häufige **Besuche** des Angeklagten [...] **auf verschiedenen Internetseiten** der Ansar wie www.a...8m.com oder www.an...8m.com festgestellt werden, auf denen u. a. eine Vielzahl von Anschlagsbekennungen eingestellt waren. Im Juli 2004 habe A. zudem die islamistischen Internetseiten www.su...org und www.ra...com besucht, auf denen zumindest zeitweise auch Links zu Internetseiten der Ansar geschaltet waren. Seit 26. Oktober 2004 habe der Angeklagte regelmäßig die Seite www.O.com aufgesucht und dort **verschiedene Videos**, vorwiegend zu Geiselnahmen und Geiseltötungen oder -enthauptungen **angesehen**. Beispielsweise habe er am 26. Oktober das Video „Ansar al sunnah army captures 11 iraqi soldiers", am 27. Oktober das Video „2 turks beheading", am 28. und 30. Oktober das Video „11 Iraqi Hostages by ansar al Sunnah", am 30. Oktober **auch das Video** „Osama bin laden video tape", am 3., 4. und 5. November 2004 das Video „Ansar al sunnah army beheading video of Iraqi officer", am 22. und 25. November das Video „Ansar al Sunnah shoots 2 Iraqis" **angeklickt**."*

[8] *Rötzer*, „Neue NSA-Dokumente enthüllen die Zusammenarbeit von Microsoft mit der NSA", Telepolis v. 12.7.2013, abrufbar unter: http://www.heise.de/-3399676 - Ausdruck anbei als **Anlage 2**.
[9] OLG Stuttgart, Urteil v. 15.7.2008 - 5-2 StE 2/05 – BeckRS 2009, 26901 – Hervorhebung nur hier.

Das Gewinnen derartiger Erkenntnisse ist nur durch vollständige Auswertung des vollständigen „Surfverhaltens“ der jeweiligen „Zielperson“ möglich.

Im Rahmen der Telekommunikationsüberwachung wird also in der Praxis jeder Webseitenaufruf, jede Suchanfrage bei einer Suchmaschine, jeder Aufruf einer Datei, eines Videos, einer Audio-, Bild- oder Textdatei, kurz: jeder Klick, jede Bewegung im Internet ausgewertet. Es werden – insbesondere in Anbetracht der heutigen Nutzungsgepflogenheiten (hierzu noch unter: A.III) sog. Smartphones – also in ganz erheblichem Umfang „Mensch-zu-Maschine“-Informationen erhoben, die einen tiefen Einblick in das Leben und die Gedankenwelt der Zielperson (und aller Anschlussnutzer) gestatten.

Das dies in der Praxis nicht nur zufällig, sondern ganz gezielt erfolgt, mag auch folgender Auszug aus dem Sachverhalt einer Entscheidung des OLG Hamburg verdeutlichen:

> *„In einem durch die StA Hamburg wegen des Verdachtes von 3 Betäubungsmittelverbrechen geführten Ermittlungsverfahrens hat das LG H. mit Beschwerdebeschlüssen vom 17. 8., 14. 9. und 26. 10. 2007 gem. § 100a StPO* ***die Überwachung und Aufnahme des Telekommunikationsverkehrs „einschließlich der gesamten DSL-Daten, mithin sämtlicher Telekommunikationsformen wie Internet etc.”*** *bezüglich eines näher bezeichneten Anschlusses des Beschuldigten zu 1. bis (zuletzt) 26. 11. 2007 angeordnet.“*[10]

In einem Nichtannahmebeschluss der 3. Kammer des Zweiten Senats zum Az. 2 BvR 1454/13 (hierzu noch unten) finden sich die folgenden Feststellungen:

> *„Im Zuge von Akteneinsicht und weiteren Auskünften durch die Staatsanwaltschaft erhielt er Kenntnis davon, dass über seinen streitgegenständlichen DSL-Anschluss* ***insgesamt 129.000 Aufrufe von HTML-Seiten*** *im Überwachungszeitraum registriert wurden. Auf Anfrage des Prozessbevollmächtigten des Beschwerdeführers*

[10] OLG Hamburg, Beschluss v. 12.11.2007 - 6 Ws 1/07 – zit. nach NStZ 2008, 478 – Hervorhebung nur hier.

> *erläuterte die Staatsanwaltschaft, dass durch Vorlage eines Beschlusses nach § 100a StPO der Provider verpflichtet sei, eine* ***Kopie der von ihm übermittelten Impulse, zu denen auch HTML-Seiten*** *gehörten, an die Polizei auszuleiten. [...]* ***Das Landeskriminalamt Baden-Württemberg gab mit Schreiben vom 27. Juni 2012 eine Stellungnahme zur durchgeführten Internetüberwachung ab. Darin wurde unter anderem dargestellt, dass sämtliche ausgeleiteten Rohdaten über eine verschlüsselte Verbindung zur TKÜ-Anlage übermittelt und dort nach den Vorgaben der Technischen Richtlinien als Rohdaten entgegengenommen und gespeichert würden. Zur Auswertung würden die Rohdaten vom TKÜ-System automatisiert dekodiert und dem Auswerter zur Verfügung gestellt.*** *Die Staatsanwaltschaft gab ebenfalls eine Stellungnahme ab. Aus ihrer Sicht sei das Abrufen von Internetseiten als Telekommunikation im Sinne des § 100a StPO zu bewerten und eine Verletzung des Kernbereichs des Grundrechts auf informationelle Selbstbestimmung nicht ersichtlich.*"

Im Zusammenhang mit einer Telekommunikationsüberwachungsmaßnahme nach § 23a ZFdG finden sich in einer Entscheidung des OLG Köln[11] folgende Ausführungen:

> *„Das Zollkriminalamt macht geltend, dass aus technischen Gründen eine Löschung nur der geschützten Kommunikation nicht früher möglich gewesen sei.* ***Die internetbasierten Kommunikationsdaten würden in einem Rohdatenstrom übermittelt, der in der Folge dekodiert und damit in E-Mails, VoIP-Daten, Internet-Surfsessions u. ä. aufgeteilt werden.*** *Erst mit der Dekodierung würden die Daten sichtbar bzw. auswertbar. Das Löschen bestimmter Teile des Rohdatenstroms sei nicht möglich. Der Löschung des gesamten Rohdatenstroms stehe entgegen, dass hierdurch auch andere, für die Maßnahme erforderliche Daten gelöscht würden.*"

Der „*Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2017*" des Bundesamtes für Justiz[12] ist zu entnehmen, dass im Jahr 2017 eine gezielte

[11] OLG Köln, Beschluss v. 22.3.2013 - 6 Wx 16/12 – BeckRS 2013, 6733 – Hervorhebung nur hier.

[12] Abrufbar unter https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html - beigefügt als **Anlage 3**.

Überwachung der „*Internettelekommunikation*“ in bundesweit **9.508 Fällen** durchgeführt wurde.

c. Insbesondere: Cloud Computing

Telekommunikationsüberwachungsmaßnahmen beschränken sich nicht nur auf die Überwachung des „Surfverhaltens“, also letztlich das Abrufen von Webseiten im Internet. Durch eine Überwachung des Datenverkehrs im Internet wird zudem *jede* Datei erfasst, die bewusst oder unbewusst durch den Nutzer „in die Cloud“ – also auf einen externen Speicherplatz – geladen wird. [13] Sie ist Bestandteil des im Rahmen einer Telekommunikationsüberwachung ausgeleiteten Rohdatenstroms bzw. der Überwachungskopie.

Eine Überwachung und Aufzeichnung der Datenströme zwischen Geräten der Zielperson und den von ihr genutzten Clouddiensten (z.B. iCloud, Dropbox, etc.) wird von namhaften Praktikern wie *RiBGH a.D. Dr. Jürgen-Peter Graf* als im Rahmen einer „normalen“ Telekommunikationsüberwachung „*überwachungsfähige Telekommunikation*“ angesehen.[14] Auch *Bundesanwalt beim BGH a. D. Michael Bruns* hält die Überwachung der „*Recherche im Internet zur Informationsbeschaffung oder den Datenverkehr zwischen Datenspeicher im Netz („Cloud-Computing“ […]) und dem Zugriffsberechtigten*“ [15] im Rahmen einer „normalen“ Telekommunikationsüberwachung für zulässig.

Die Nutzung von „Cloud-Computing“-Dienstleistungen ist inzwischen gang und gäbe:

Im Rahmen von sog. Software as a Service (SaaS) [16] werden Anwendungen über das Internet in der „Cloud“ und nicht mehr „lokal“ auf dem informationstechnischen System selbst genutzt. So kann sich z.B. der Nutzer eines Webmaildienstes wie Google Mail, gmx oder web.de über das Internet bei „seinem“ Webmaildienst anmelden und ohne Nutzung eines lokal installierten E-Mail-Programmes E-Mails entwerfen, sichern und natürlich senden. Die Nutzung von Textverarbeitung, Tabellenkalkulation oder

[13] Hierzu bereits *Obenhaus*, NJW 2010, 651.
[14] *Graf*, in: BeckOK StPO, § 100a Rn. 227c.
[15] *Bruns*, in: KK-StPO, § 100a Rn. 4 – zu § 100a StPO.
[16] Zu den einzelnen Cloud Services z.B. https://aws.amazon.com/de/types-of-cloud-computing/.

Präsentationssoftware sowie Bildbearbeitung kann vollständig über das Internet „abgewickelt" werden[17]. Hierbei müssen freilich permanent Daten zwischen Nutzer und SaaS-Anbieter über das Internet ausgetauscht werden. Diese Daten sind Bestandteil des im Rahmen einer Überwachungskopie übermittelten Rohdatenstroms.

Im Rahmen von sog. Infrastructure as a Service (IaaS) ist insbesondere die Nutzung von Datenspeichermöglichkeiten in der Cloud weit verbreitet. Nutzer eines Apple-Smartphones erhalten beispielsweise im Rahmen der Einrichtung der sog. iCloud derzeit 5 Gigabyte Speicherplatz kostenfrei. *„Sie können diesen Speicher für Ihre iCloud-Backups verwenden, zum Speichern von Fotos und Videos in iCloud-Fotos und um Ihre Dokumente in iCloud Drive auf dem neuesten Stand zu halten."*[18] – wird die Funktionalität beworben. Wird sie genutzt, kann von jedem mit dem jeweiligen Gerät erstellten Foto oder Video automatisiert eine Kopie über die Internetverbindung in den Clouddatenspeicher geladen werden. Diese Kopien sind Teil des Rohdatenstroms. Im Rahmen einer Systemsicherung (sog. Backup) wird gar das gesamte System über das Internet auf den Cloudspeicherplatz gespiegelt. Wenn ein solches „Cloud-Backup" im Rahmen einer TKÜ ausgeleitet wird, ist es möglich, dieses auf ein neues Gerät einzuspielen und somit (so z.B. bei Apple Endgeräten möglich[19]) ein Duplikat des für die Kommunikation verwendeten Endgeräts - mit allen darauf enthaltenen Information - zu erhalten.

d. Zudem: Überwachung der Maschine-zu-Maschine-Kommunikation

Auch so genannte Smart-Home-Geräte wie z.B. Sprachassistenten (Amazon Alexa, Google Home, Apple Homepod) kommunizieren permanent mit der jeweiligen Anbietercloud über den Anschluss des Nutzers und leiten diesen betreffende Daten über das Internet weiter. [20] Gleiches gilt für die über das Internet gesendeten Videobilder privater Überwachungskameras (z.B. sog. IP-Babycam) oder die Daten, die sog. Wearables[21] (z.B. eine sog. Fitness-Uhr) an den Server der Hersteller von Software bzw. Hardware übermittelt. Da der einzige unmittelbar menschliche Bezug zu dieser Form der Telekommunikation die ursprüngliche Inbetriebnahme des jeweiligen Gerätes ist und die

[17] Z.B. Microsoft Office 365.
[18] https://support.apple.com/de-de/HT204247.
[19] Vgl. https://support.apple.com/de-de/HT204184.
[20] Vgl. *Blechschmitt*, MMR 2018, 361 (362) .
[21] Ausführlich *Kopp/Sokoll*, NZA 2015, 1352.

weitere Kommunikation der Geräte untereinander automatisiert erfolgt, wird hier von „Maschine-zu-Maschine-Kommunikation“ gesprochen.

Perspektivisch werden mit Verbreitung des sog. Internet der Dinge („Internet of Things“ oder kurz IoT) eine große Zahl von Alltagsgeräten – vom Fernseher bis zur Waschmaschine – über das Internet und damit über den jeweiligen Telekommunikationsanschluss des Nutzers „kommunizieren“. Die damit verbundene „Maschine-zu-Maschine-Kommunikation“ wird als Telekommunikation i.S.d. § 3 Nr. 22 TKG angesehen.[22] Die im Rahmen dieser „Maschine-zu-Maschine-Kommunikation“ generierten und ausgetauschten Daten sind ebenfalls Gegenstand von Telekommunikationsüberwachungsmaßnahmen, da sie Bestandteil der „Überwachungskopie“ sind.

Wie selbstverständlich wird in einer Antwort der Bundesregierung auf eine kleine Anfrage zum Thema „*Wanzen im Wohnzimmer – Überwachung durch Sprachassistenten und smarte Geräte auf Bundesebene*“ die Auffassung vertreten:

> „*Soweit über das vernetzte Gerät Telekommunikation erfolgt, findet § 100a StPO Anwendung.*“[23]

Es gibt keine Anzeichen dafür, dass bezüglich der präventiven Telekommunikationsüberwachung in Nordrhein-Westfalen eine andere Position vertreten wird.

e. Weitere Überwachungsmethode: WLAN-Catching

In der Praxis der modernen Telekommunikationsüberwachung findet neben der Überwachung und Aufzeichnung durch Ausleitung von Überwachungskopien mit Hilfe von Telekommunikationsdiensteanbietern das Verfahren des sog. WLAN-Catching, d.h. die Überwachung lokaler Funknetzwerke (WLAN) Anwendung. Hierbei wird ohne aktives

[22] *Grünwald/Nüßing*, MMR 2015, 378 (379 f.).
[23] BT-Drs. 19/11478, S. 3 – Antwort auf Frage 5. Bemerkenswert auch die Antwort auf Frage 21.

Eingreifen in den Netzwerkverkehr der im WLAN anfallende Datenverkehr zu Überwachungszwecken heimlich und von außen mitgeschnitten (sog. Sniffing).[24]

> *„Ausgeleitet und gespeichert wird bei einer solchen Maßnahme grundsätzlich also der gesamte laufende Internetdatenverkehr (z.B. auch das Aufrufen von medialen Webseiten im WWW, Anfragen bei Suchmaschinen oder die Nutzung von Angeboten des Online-Banking oder e-Commerce). Erfasst wird daher das gesamte Surfverhalten des Nutzers. Von einer solchen Maßnahme betroffen sind ebenfalls solche Datenpakete, die lediglich innerhalb des lokalen Netzwerks (ohne Nutzung des Internet-Netzwerks) zirkulieren, [...]. Denkbar wären etwa Druckaufträge an den lokalen Netzwerkdrucker.“*[25]

Graf weiß zu berichten:

> *„Angesichts dieser gerade auch in Privathaushalten immer stärker verbreiteten Funktechnik* [Anm.: gemeint ist WLAN]*, welche mit den hierfür verwendeten Endgeräten (Router) neben dem Zugang ins Internet vielfach auch die Möglichkeit zu kabellosen Telefonaten mit entsprechendem Equipment ermöglichen, machen entsprechende technische Hilfen zur Ermittlung der diese Dienste in Anspruch nehmenden Teilnehmer bei dem Verdacht erheblicher Straftaten notwendig. Hinzu kommt, dass immer häufiger mit diesen Funknetzen Wohnungsgrenzen überwunden werden, so dass einem Beschuldigten äußerlich nicht sichtbar die Möglichkeit geboten sein kann, mit Unterstützung von Nachbarn und der Benutzung deren Funknetze Überwachungsmaßnahmen zu umgehen.“*[26]

Graf berichtet weiter, dass derzeit *„der Einsatz solcher Geräte aber noch nicht sehr häufig*“ sei und verweist auf die Antwort der Bundesregierung auf eine Kleine Anfrage aus dem Jahr 2012. Aus dieser ergibt sich, dass das BKA Telekommunikationsüberwachungen mittels WLAN-Catcher durchführt:

---

[24] *Ulbrich*, Die Überwachung lokaler Funknetzwerke („WLAN-Catching“), S. 142 f.
[25] *Ulbrich*, Die Überwachung lokaler Funknetzwerke („WLAN-Catching“), S. 143.
[26] *Graf*, in: BeckOK-StPO, 34. Edition – Juli 2019, § 100a Rn. 223.

„Von 2007 bis 2011 kam der WLAN-Catcher des BKA insgesamt 16 mal zum Einsatz."[27]

In Nordrhein-Westfalen stellt sich die Situation ausweislich der Antwort der nordrhein-westfälischen Landesregierung auf eine Große Anfrage aus dem Jahr 2014[28] wie folgt dar:

„Die nordrhein-westfälische Polizei verfügt über einen W-LAN-Catcher beim Landesamt für Zentrale Polizeiliche Dienste Nordrhein-Westfalen (LZPD NRW). Im Rahmen von Verfahren nordrhein-westfälischer Strafverfolgungsbehörden wurde der W-LAN-Catcher auf der Grundlage richterlicher Anordnungen bislang für folgende Behörden eingesetzt:

Tabelle 5: Zuordnung Jahr - Behörde – Summe W-LAN-Catcher Einsätze

Jahr	***Behörde***	***Anzahl***
2013	*PP Essen*	*1*
2013	*PP Köln*	*1*

"

Als Rechtsgrundlage werden in selbiger Antwort die §§ 100a, 100g StPO angeführt.[29]

Daraus kann gefolgert werden, dass die Überwachung und Aufzeichnung der Telekommunikation zu repressiven Zwecken bereits heute in Nordrhein-Westfalen auch mit dem WLAN-Catcher realisiert wird.

Es ist anzunehmen, dass ein Einsatz des vorhandenen WLAN-Catchers auch zu präventiv-polizeilichen Zwecken auf Basis von § 20c PolG NRW erfolgt bzw. erfolgen wird.

[27] BT-Drs. 17/8544, S. 16.
[28] NRW LT-Drs. 16/6051, S. 20.
[29] NRW LT-Drs. 16/6051, S. 21.

2. Quellen-Telekommunikationsüberwachung (§ 20c Abs. 2 PolG NRW)

Durch § 20c Abs. 2 PolG NRW wird eine sog. Quellen-Telekommunikationsüberwachung gestattet („*Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird...*"). Ziel ist es, das Mitlesen und Mithören der Inhalte verschlüsselter Telekommunikation zu ermöglichen („*...um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen*"), bei denen eine Entschlüsselung auf anderem Wege bzw. durch andere Methoden scheitert.

Hierzu müssen sämtliche Kommunikationsinhalte vor der Verschlüsselung bzw. nach der Entschlüsselung ausgeleitet werden. Dies soll technisch durch einen Zugriff auf dem informationstechnischen System (der „Quelle" der Telekommunikation) erfolgen.

a. Vorgehensweise

Zur Durchführung einer Quellen-Telekommunikationsüberwachung muss – wie bei einer Online-Durchsuchung – eine Softwarelösung[30] eingesetzt werden, mit Hilfe derer ein Zugriff auf das Zielsystem ermöglicht wird (sog.„Trojanersoftware").

Hierzu ist es erforderlich, auf dem informationstechnischen System der Zielperson (in der Regel einem Smartphone) die Trojanersoftware heimlich zu installieren (sog. Infiltration), um dann aus der Ferne auf das informationstechnische System zugreifen zu können.

Die Installation erfolgt technisch in der Regel durch Ausnutzen eines Programmierfehlers, einer sog. Sicherheitslücke in einer Software auf dem von der Zielperson genutzten System. Hierbei kann es sich um das Betriebssystem oder auch eine Anwendungssoftware handeln. Der Zielperson wird z.B. eine unverdächtig erscheinende E-Mail zugesandt (oder ein Datenträger übergeben). Sobald diese oder ihr Anhang geöffnet wird, wird die

[30] Eine gewisse Marktführerstellung hat hierbei offenbar die Software FinSpy des Anbieters FinFisher, vgl. *Holland*, FinSpy: Deutsche Überwachungssoftware gegen türkische Opposition eingesetzt, heise.de v. 15.5.2018 - https://www.heise.de/newsticker/meldung/FinSpy-Deutsche-Ueberwachungssoftware-gegen-tuerkische-Opposition-eingesetzt-4049677.html - Ausdruck als **ANLAGE 4** anbei.

Trojanersoftware bei bestehender Internetverbindung unbemerkt auf das Zielsystem geladen und installiert.[31]

Vor der Installation muss eine solche Sicherheitslücke entweder eigenständig ermittelt oder entsprechende Informationen über diese Schwachstellen von Dritten „beschafft" werden. Für den Ankauf von Informationen über offene Sicherheitslücken gibt es entsprechende „Schwarzmärkte". Hauptnachfrager sind nach Erkenntnissen der Gesellschaft für Informatik e.V. (i.W. „GI") Cyberkriminelle, die diese für die Installation sog. Ransomware (also eine Software, die einen Computer infiziert, sperrt und dann „Lösegeld" dafür verlangt, ihn zu entsperren) ausnutzen wollen.[32]

Die Nutzung der Sicherheitslücken ist nur zeitlich beschränkt sinnvoll möglich. Sobald die Hersteller die betreffenden Sicherheitsdefizite in ihren Softwareprodukten oder Betriebssystemen beseitigen können[33], ist ein Zugriff ausgeschlossen. Dementsprechend ist es, soll die Sicherheitslücke für Zwecke der Quellen-Telekommunikationsüberwachung tauglich sein, erforderlich, diese den Anbietern der lückenhaften Software *nicht* mitzuteilen. Damit ein effektiver Zugriff auf ein möglichst breites Portfolio von Betriebssystemen (z.B. Windows, Linux, iOS, Android, MacOS) und Anwendungssoftware (z.B. Microsoft Office, Adobe PDF) möglich ist, müssen möglichst viele Sicherheitslücken ermittelt, vorgehalten und genutzt werden. Der Bedarf kann de facto nur durch einen Ankauf von Informationen zu (unbekannten) Sicherheitslücken und Möglichkeiten zur Ausnutzung auf dem „freien Markt" gedeckt werden.

Wird eine Sicherheitslücke nicht geschlossen, kann sie nicht nur von den Strafverfolgungsbehörden, sondern auch von jedem anderen (aus)genutzt werden.

---

[31] Vgl. z.B. *Gierow*, FINSPY: Neuer Staatstrojaner-Exploit in RTF-Dokument gefunden, golem.de v. 13.9.2017 - https://www.golem.de/news/finspy-neuer-staatstrojaner-exploit-in-rtf-dokument-gefunden-1709-130025.html - Ausdruck als **ANLAGE 5** anbei.

[32] *Federrath*, Stellungnahme der GI zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen v. 6. und 8.2.2018 - abrufbar unter https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen/2018/GI-Stellungnahme_Neuausrichtung_HessVS_2018-02-08.pdf - Ausdruck als **ANLAGE 6** anbei.

[33] Das Schließen einer Sicherheitslücke erfolgt über einen sog. Patch, der über die (häufig automatisch ausgeführte) Aktualisierungsfunktion der Software auf dem System eingespielt wird.

Dies war z.B. im Jahr 2017 der Fall, als eine wohl von der amerikanischen NSA „vorgehaltene" Sicherheitslücke von Cyberkriminellen zur Verbreitung des Schadprogramms „WannaCry" genutzt wurde. Dieses Schadprogramm infizierte im Mai 2017 über eine Sicherheitslücke im Windows-Betriebssystem innerhalb weniger Tage weltweit eine große Zahl informationstechnischer Systeme und legte sie lahm. Betroffen waren neben vielen privaten Nutzern z.B. die Deutsche Bahn AG, der japanische Autohersteller Nissan, der französische Autohersteller Renault sowie Banken, Geldautomaten und Schulen. [34] Auch lebenswichtige Einrichtungen wie z.B. Krankenhäuser waren betroffen.[35] Die Folgen des Angriffs, dessen Umfang auf Millionen von Infektionen geschätzt wird, dauern bis heute an.[36]

b. Insbesondere: Limitierung des Zugriffs auf „laufende Kommunikation"

Nach den Vorgaben des *Gerichts* ist bei Quellen-Telekommunikationsüberwachungsmaßnahmen durch „*technische Vorkehrungen*" sicherzustellen, dass „*sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt*"[37]. Dies wurde in einer späteren Entscheidung dahingehend konkretisiert, dass die zur Quellen-Telekommunikationsüberwachung genutzte Software so ausgestaltet sein müsse, dass sie *„hinreichend abgesichert auch gegenüber Dritten – den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern [...] – inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.*"[38]

Eine Trojanersoftware zur Durchführung einer Quellen-Telekommunikationsüberwachung darf dementsprechend weder beabsichtigt noch unbeabsichtigt persönlichkeitsrelevante Informationen erheben, die nicht Inhalte und Umstände der laufenden Telekommunikation betrifft.

---

[34] *Biermann*, WannaCry: Großer Schaden für 31.000 Dollar, Zeit Online v. 14.05.2017, https://www.zeit.de/digital/datenschutz/2017-05/wannacry-ransomware-cyberattacke-bitcoin-windows-microsoft - Ausdruck als **ANLAGE 7** anbei.
[35] Vgl. z.B. *Wittmann*, Erpresser-Software lähmt 40 Kliniken in Großbritannien, Berliner Morgenpost v. 12.5.2017, https://www.morgenpost.de/politik/article210553117/Krankenhaeuser-in-England-durch-Hacker-Angriff-lahmgelegt.html - Ausdruck als **ANLAGE 8** anbei.
[36] *Gierow*, MS17-010: Noch immer Millionen Wanna-Cry-Infektionen aktiv, golem.de v. 14.5.2018, https://www.golem.de/news/ms17-010-noch-immer-millionen-wanna-cry-infektionen-aktiv-1805-134360.html - Ausdruck als **ANLAGE 9** anbei.
[37] BVerfGE 120, 274 (309 - Rn. 190).
[38] BVerfGE 141, 220 (311f. - Rn. 234).

Es ist jedoch technisch nicht möglich, derartige Vorkehrungen zu treffen und somit die verfassungsrechtlichen Anforderungen zu erfüllen.[39]

Eine Quellen-Telekommunikationsüberwachung zielt darauf ab, auf Kommunikationsinhalte vor deren Verschlüsselung zuzugreifen. Es muss damit aus technischer Sicht – notwendigerweise – gerade nicht die „laufende Telekommunikation" überwacht werden.

Die Telekommunikation kann erst dann als „laufend" betrachtet werden, wenn sie vom Absender unwiderruflich und ohne Möglichkeit der Rückholung dem Informationsmittler (z.B. dem Messengerdienstanbieter) technisch „übergeben" wurde, z.B. durch Anklicken des „Absendebutton". Die Trojanersoftware greift indes bereits vor diesem Zeitpunkt auf die Inhalte zu. Es werden bereits Entwürfe von Nachrichten, die mehr oder weniger kurz vor dem Absenden erstellt wurden (und ggf. dann gar nicht mehr abgesendet werden) erhoben.[40]

Diese Problematik wurde in der öffentlichen Sachverständigenanhörung des Innenausschusses des Nordrhein-Westfälischen Landtages am 13. November 2018 von der Sachverständigen *Bröckling* anschaulich verdeutlicht:

> *„Eine Quellen-Telekommunikationsüberwachung können Sie sich so vorstellen: Sie haben den Messenger-Dienst. Entweder bekommen Sie als Polizeibeamter die Tastaturanschläge – Sie sehen was geschrieben wird – oder Sie bekommen Screenshots – Sie sehen, was im Messenger passiert.*
> *Nun stellen Sie sich vor, dass ich mein Handy nehme und beginne, eine Nachricht zu tippen. Sie wird für einen Moment angezeigt. Dann entschließe ich mich, die*

[39] *Kurz/Neumann/Rieger/Engling*, „Stellungnahme zur „Quellen-TKÜ" nach dem Urteil des Bundesverfassungsgerichts vom 20.4.2016 - 1 BvR 966/09", S. 6 ff., https://www.ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf - Ausdruck als **ANLAGE 10** anbei.

[40] *Hornung*, Stellungnahme zur öffentlichen Anhörung zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen - Drucks. 19/5412 - sowie dem Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN - Drucks. 19/5782 - S. 6 (i.W. „*Hornung*, Stellungnahme").

> *Nachricht doch nicht zu senden; ich lösche sie wieder. Es ist nie zu einer Kommunikation gekommen. Es war nie laufende Kommunikation, weil ich diese Nachricht nie abgeschickt habe. Es war immer nur ein Entwurf auf meinem Endgerät. Trotzdem würde es definitiv mitgelesen werden. Wie soll das denn technisch verhindert werden? – Wir sehen hier ein grundlegendes Problem in diesem Gesetzentwurf: Es wird versucht, etwas umzusetzen, was technisch nicht machbar ist."*[41]

Zudem muss eine Software zur Durchführung einer Quellen-Telekommunikationsüberwachung denknotwendigerweise weitere Daten erheben und weiterleiten, die weder laufende noch ruhende Kommunikation – und auch keine Umstände derselben – darstellen. So muss die Trojanersoftware beispielsweise erfassen (und weiterleiten), wann das überwachte informationstechnische System ein- und ausgeschaltet wird, ob es – unabhängig von einem konkreten Kommunikationsvorgang – mit dem Internet verbunden ist, ob und welche Kommunikationsprogramme – ebenfalls unabhängig von einem konkreten Kommunikationsvorgang – geöffnet oder geschlossen wurden. Da stets die Möglichkeit besteht, dass ein informationstechnisches System und die darauf vorgehaltenen Kommunikationsprogramme von verschiedenen Personen genutzt werden, muss die Trojanersoftware den Zugriff verschiedener Nutzer protokollieren. Zudem wird, um nicht in rechtswidriger Weise eine Telekommunikationsüberwachung außerhalb Deutschlands durchzuführen, eine permanente Erhebung und Übermittlung des Standorts des Geräts erforderlich sein.

Somit ist eine Überwachung der Telekommunikationsaktivitäten „an der Quelle" faktisch nur im Wege einer Online-Durchsuchung möglich.

III. Tatsächliche Nutzungsgepflogenheiten

Im Rahmen der durch § 20c PolG NRW ermöglichten Überwachung von internetfähigen Telekommunikationsendgeräten, insb. der allgegenwärtigen Smartphones mit ihren umfangreichen internetgebundenen Funktionalitäten (Foto, Navigation, Ausführen von diversen Anwendungsprogrammen etc.) ist es möglich, ein umfangreiches

[41] NRW LT APr 17/438, S. 13.

Persönlichkeitsprofil einer von einer Telekommunikationsüberwachungsmaßnahme betroffenen Person zu erstellen.

Nicht erst in Folge einer „Infiltration" dieser Geräte, sondern bereits im Rahmen einer die Datenströme erfassenden Telekommunikationsüberwachung können mehr und umfangreichere Informationen über die betroffene Person und ihre Persönlichkeit aufgezeichnet werden, als diese ihren intimsten Gesprächspartnern oder z.B. einem Tagebuch preisgeben würde.

Die Überwachung der Nutzung eines Smartphones über die Telekommunikationsüberwachung – und erst recht die Quellen-Telekommunikationsüberwachung – macht dessen Nutzer zum schutzlosen, gläsernen Objekt staatlicher Beobachtung.

Inzwischen nutzen in Deutschland rund 57 Millionen Menschen ein Smartphone[42]. Solche Geräte werden nicht – wie dies zum Zeitpunkt der sog. Online-Durchsuchungs-Entscheidung des *Gerichts* vor nunmehr elf Jahren bei PCs der Fall war – vorwiegend als Arbeitsgeräte genutzt, sondern dienen ganz überwiegend persönlichen und persönlichsten Zwecken.

Smartphones sind für ihre Nutzer intimer und intensiv genutzter Begleiter vom Aufstehen bis zum Zubettgehen. Smartphonebesitzer im Alter zwischen 18 und 24 Jahren nutzen im Schnitt über fünfzig Mal am Tag ihr Gerät.[43]

Die inzwischen in jedem Smartphone eingebaute Foto- und Videotechnik wird von 90 Prozent der Smartphonebesitzer auch genutzt.[44] Die Einsatzmöglichkeiten der Geräte sind vielfältig, faktisch in aller Regel aber privater Natur, wie etwa zur Herstellung von Fotos im familiären Bereich. Weit verbreitet ist auch das sog. Sexting, also das Erstellen

[42] Bitkom, Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen), Statista 2019 - Ausdruck als **ANLAGE 11** anbei.
[43] *Deloitte*, Ziemlich bester Smartphone-Freund, Statista 2018 - Ausdruck als **ANLAGE 12** anbei.
[44] Bitkom Research Januar 2017, Anteil der befragten Smartphone-Nutzer, die die folgenden Funktionen mit ihrem Smartphone nutzen, Statista 2019- Ausdruck als **ANLAGE 13** anbei.

und Austauschen erotischer Selbstportraits mit dem Smartphone über das Internet.[45] Sobald ein Foto oder Video erstellt wird, wird es nicht nur in digitaler Form lokal gespeichert. Regelmäßig wird zudem automatisch eine Kopie unter Nutzung der Internetverbindung an einen externen Speicherdienst (sog. Cloud-Diensteanbieter – z.B. Apple iCloud, GoogleDrive) gesendet und dort abgelegt. Gerätespeicher und Anbietercloud werden typischerweise als dauerhafte Foto- und Videoarchive genutzt.

Ebenfalls regelmäßig (ca. 74 % der Nutzer) werden Suchmaschinen über das Smartphone aufgerufen. Auch hier dominiert die private Nutzung. Bei der Suche nach Antworten (und Hilfe) in privaten und privatesten Angelegenheiten, wie zum Beispiel der Behandlung und Diagnose von Krankheiten ist für einen Großteil der Nutzer die Abfrage von Suchmaschinen und der Besuch der dort zu findenden Webseiten selbstverständlich.[46]

Über Telekommunikationsendgeräte werden auch die unterschiedlichsten sozialen Netzwerke und Internetforen zur Interaktion und Kommunikation mit Bekannten, Freunden und dem oder den Geschlechtspartnern genutzt. Darüber hinaus dienen soziale Netzwerke und Internetforen dem Austausch mit „gleichgesinnten" Personen in unterschiedlichsten Kontexten. Die weit verbreitete Möglichkeit der anonymen Nutzung dieser Foren und Netzwerke ermöglicht es den Teilnehmern sich frei und ohne Selbstzensur und Angst vor Repressalien über die sie interessierenden Themen auszutauschen und ihre Meinung frei zu äußern.

Die in einem Smartphone enthaltene GPS-Funktion wird regelmäßig (64 %) [47] zu Navigationszwecken bzw. zur Orientierung mit Hilfe von sog. Kartenapps (z.B. Google Maps) verwendet. Nicht nur der Standort des Smartphones wird dabei über das Internet an den jeweiligen Anbieter weitergeleitet. Wie die Süddeutsche Zeitung berichtet, sammelt und sendet z.B. die Applikation Google Maps weitaus mehr Nutzerdaten:

---

[45] Über 50 % der erwachsenen Smartphonenutzer haben bereits einmal ein erotisches Selbstporträit erstellt und weitergeleitet, vgl. *Döring*, „Sexting. Aktueller Forschungsstand und Schlussfolgerungen für die Praxis", in: Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V., „Gewalt im Netz", S. 15 (19) - mit weiteren Nachweisen und umfassender Darstellung des Phänomens. - Kopie der zitierten Seite als **ANLAGE 14** anbei.

[46] Bitkom Research 2016, Habe Sie schon einmal Krankheitssymptome in eine Internet-Suchmaschine eingegeben?, Statista 2018 - Ausdruck als **ANLAGE 15** anbei; Civey, Informieren Sie sich online über Ihre Symptome, bevor Sie zum Arzt gehen?, Statista 2018 - Ausdruck als **ANLAGE 16** anbei.

[47] Bitkom Research Januar 2017, Anteil der befragten Smartphone-Nutzer, die die folgenden Funktionen mit ihrem Smartphone nutzen, Statista 2019- Ausdruck als **ANLAGE 13** anbei.

> „*Die Handys sendeten unter anderem den aktuellen Akkustand, die Gerätenummern aller Bluetooth-Gadgets in der Nähe der Handys und natürlich die GPS-Koordinaten an Google. Außerdem versuchten die Handys herauszufinden, was die Nutzer gerade taten und schickten Wahrscheinlichkeitswerte an Google, zum Beispiel: Mit einer Wahrscheinlichkeit von 58 Prozent geht der Nutzer zu Fuß.*“[48]

Für über 20 Prozent[49] der Nutzer ist ihr Smartphone Begleiter bei der Suche nach (potentiellen) Lebens- oder Geschlechtspartnern (sog. Dating). Die Dating-Applikation Tinder ist im August 2019 die zweiterfolgreichste Applikation für Smartphones der Marke Apple iPhone gewesen, die Dating-Applikation LOVOO folgte auf dem achten Platz.[50]

Unabhängig davon, welche konkreten Dienste genutzt werden: Nutzer von mobilen, internetfähigen Endgeräte sind dank Flatrate heutzutage „always on“, d.h. permanent mit dem Internet verbunden. Dies trifft insbesondere – aber nicht nur – auf die Nutzer zu, die heute noch zu den „Kindern und Jugendlichen“ gezählt wurden:

> „*Der Medien- und Internetkonsum von Kindern und Jugendlichen wird immer mobiler. Ins Internet „zu gehen“ ist den Kindern von heute völlig fremd, sie sind „always on“ – egal wo und egal wann*“.[51]

Ist eine Person aber „*always on*“, dann generiert ihr genutztes Endgerät permanent Daten, die über das Internet ausgetauscht werden.

---

[48] *Strathmann*, Google weiß, wo Sie sind, zeit.de v. 9.2.2018 - https://www.sueddeutsche.de/digital/digitale-privatsphaere-google-weiss-wo-sie-sind-1.3859023 - Ausdruck als **ANLAGE 17** anbei.

[49] Bitkom Research Januar 2017, Anteil der befragten Smartphone-Nutzer, die die folgenden Funktionen mit ihrem Smartphone nutzen, Statista 2019- Ausdruck als **ANLAGE 13** anbei.

[50] Priori Data, Ranking der erfolgreichsten iPhone-Apps nach Umsatz in Deutschland im August 2019 (in 1.000 US-Dollar), Statista 2019 - Ausdruck als **ANLAGE 18** anbei.

[51] *Achim Berg*, Vize-Präsident des Branchenverbandes BITKOM anlässlich der Vorstellung der Studie „Kinder & Jugend in der digitalen Welt“ – zitiert nach: https://www.bitkom.org/Presse/Presseinformation/Jung-digital-und-immer-online-Fuer-die-Generation-Z-gilt-mobile-first.html - Ausdruck als **Anlage 19** anbei.

Durch den heimlichen Zugriff auf die über ein Smartphone stattfindende Telekommunikation (zur Praxis der Telekommunikationsüberwachung siehe oben A.II.1) wird der zugreifenden Stelle mit Blick auf die Art der Informationen, die abgerufen werden können, aber auch mit Blick auf den Umfang der abrufbaren Informationen, technisch unvermeidbar ein Einblick in die engste Persönlichkeitssphäre des Betroffenen gewährt.

Selbst durch eine Kombination von „herkömmlichen" heimlichen Maßnahmen können keine derart umfassenden Einblicke in die Privat- und Intimsphäre, insbesondere die Gedankenwelt der betroffenen Personen gewonnen werden.

IV. Beschwerdeführer*innen

Alle Beschwerdeführer*innen nutzen und unterhalten Telekommunikationsanschlüsse (sowohl „fest" als auch mobil) zur Kommunikation und Internetnutzung mittels Smartphones und mit dem Internet verbundenen PCs, Laptops und Tablets. Über diese kommunizieren sie mit anderen Personen – teils auch verschlüsselt.

Alle Beschwerdeführer*innen tragen ihre Smartphones in der Regel stets bei sich und nutzen die eingebauten Funktionen wie Kamera, GPS-Funktion und Mikrofon sowie unterschiedliche Programme/Apps (z.B. zur Navigation, Spiele, Notizbuch, Soziale Netzwerke, E-Mail). Insbesondere nutzen die Beschwerdeführer*innen die Möglichkeit, sich über das Smartphone im Internet mittels Suchmaschinen und anschließendem Besuch gefundener Informationsangebote (Webseiten, Videos, Texte etc.) über die sie im jeweiligen Moment bewegenden Fragestellungen kundig zu machen. Diese Fragestellungen umfassen, wie bei der ganz überwiegenden Mehrheit der Internetnutzer auch, gesundheitliche Probleme/Vorsorge, Fragestellungen zu Sexualität und Partnerschaft, politische und religiöse Themen.

Alle Beschwerdeführer*innen überlassen ihre in der Regel permanent mit dem Internet verbundenen informationstechnischen Systeme und Smartphones bei Bedarf (und Vertrauen) anderen Personen zur Mitnutzung. Ebenso nutzen sie die Möglichkeit des Internetzugangs über informationstechnische Systeme von Dritten (z.B. WLAN-Zugang bei Freunden/Verwandten aber auch von kommerzielle Anbietern wie z.B. Internetcafés)

bzw. geben anderen Personen die Möglichkeit ihren Telekommunikations-/Internetanschluss zu nutzen (z.B. über WLAN, Tethering-Funktion des Smartphones/PC).

Sämtliche Beschwerdeführer*innen nutzen zudem unterschiedliche, mit dem Internet verbundene Geräte. Zudem nutzen sie sog. Software as a Service und Infrastructure as a Service Cloud Computing Dienstleistungen wie z.B. Webmail-Programme, Online-Text- und Bildbearbeitungsprogramme sowie sog. Cloudspeicher (z.B. iCloud und Dropbox).

1. [redacted]

Die Beschwerdeführerin zu 1, [redacted], ist Referentin beim Komitee für Grundrechte und Demokratie e.V. Das Grundrechtekomitee setzt sich öffentlich unter anderem gegen ein Verbot der Roten Hilfe ein, für Gefangenenrechte, für eine Entmilitarisierung und gegen eine Ausweitung staatlicher Befugnisse, beispielsweise im Bereich der Sicherheitsbehörden. Zudem vertritt es die Forderung nach einer Abschaffung des Verfassungsschutzes.

[redacted] betätigt sich zudem als Journalistin. Sie schreibt regelmäßig für die anarchistische Zeitung „Graswurzelrevolution".

Schließlich ist [redacted] aktiv in der Klimabewegung „Ende Gelände", die den sofortigen Kohleausstieg und einen Systemwandel fordert. „Ende Gelände" organisiert Massenaktionen des zivilen Ungehorsams gegen Braunkohleinfrastruktur und bringt regelmäßig mehrere tausend Leute dazu, sich auf Schienen für den Kohletransport zu setzen oder Bagger im Braunkohletagebau zu blockieren. Die Klimabewegung „Ende Gelände" wird vom Bundesamt für Verfassungsschutz als „*linksextremistisch beeinflusste Kampagne*" bezeichnet[52] und offenbar beobachtet. Im Verfassungsschutzbericht NRW aus dem Jahr 2017 heißt es:

[52] *Bundesamt für Verfassungsschutz*, „Linksextremisten instrumentalisieren „Klimaschutz"-Proteste", Online-Beitrag ohne Datum auf https://www.verfassungsschutz.de/de/aktuelles/schlaglicht/schlaglicht-2018-08-linksextremisten-instrumentalisieren-klimaschutz-proteste - Ausdruck als **Anlage 20** anbei.

> *„Bei Ende Gelände selbst handelt es sich um ein europaweites Sammelbündnis zivildemokratischer und linksextremistischer Organisationen, Bündnisse und Netzwerke. Es wird aufgrund der intensiven aktionsorientierten Einflussnahme und Mitwirkung der linksextremistischen Interventionistischen Linken (IL) als Scharnier zum zivildemokratischen Spektrum genutzt.“*[53]

Im Zusammenhang mit den Aktivitäten von „Ende Gelände“ ist die Beschwerdeführerin in den Fokus des polizeilichen Interesses geraten. Im Rahmen einer Versammlung von „Ende Gelände“ in Erkelenz im Jahr 2015 ermittelte die Polizei gegen sie wegen angeblichem Landfriedensbruch. Die Staatsanwaltschaft erhob Anklage, [redacted] wurde vom Amtsgericht Erkelenz (Az. 27 Cs-720 Js 358/15-152/16) freigesprochen. Die Beschwerdeführerin beteiligt sich auch weiterhin an Aktivitäten und Aktionen von „Ende Gelände“ und anderen Klimaschutzgruppen in NRW.

Im Zusammenhang mit ihrer beruflichen Tätigkeit steht [redacted] zudem in Kontakt mit JVA-Insassen, mit Menschen in forensischen Einrichtungen und mit Einzelpersonen, Vereinen (beispielsweise dem Rechtshilfeverein AZADI e.V.[54] und Rote Hilfe e.V.) oder Gruppen (beispielsweise der Interventionistischen Linken oder dem VVN-BdA), die in den Verfassungsschutzberichten benannt und als extremistisch eingestuft werden.

Daher ist nicht auszuschließen, dass sie auch mit Personen in Kontakt steht, denen Straftaten im Sinne des § 8 Abs. 4 PolG NRW vorgeworfen werden oder bei denen der Vorwurf der Planung einer Begehung der dort genannten „terroristischen Straftaten“ zumindest möglich erscheint.

Auf Grund der vorgenannten Tätigkeiten im politisch linken Spektrum erscheint es zudem wahrscheinlich, dass die Beschwerdeführerin bereits jetzt Zielperson einer Telekommunikationsüberwachungsmaßnahme oder einer Quellen-Telekommunikationsüberwachungsmaßnahme nach § 20c Abs. 1 Nr. 2 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 2 PolG NRW ist.

---

[53] Verfassungsschutzbericht NRW 2017, S. 68.

[54] Der „AZADI Rechtshilfefonds für Kurdinnen und Kurden in Deutschland e.V,“ wird im Kapitel „Sicherheitsgefährdende und extremistische Bestrebungen von Ausländern (ohne Islamismus)“ in: Bundesministerium des Innern, für Bau und Heimat, Verfassungsschutzbericht 2018, S. 269 beschrieben.

Jedenfalls ist es mit Blick auf die von [redacted] gepflegten Kontakte und Freundschaften sehr wahrscheinlich, dass sie als Anschluss-/Endgeräteüberlasserin i.S.d. § 20c Abs. 1 Nr. 4 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 4 PolG NRW Zielperson einer (Quellen-)Telekommunikationsüberwachungsmaßnahme war, ist oder wird. Zudem ist es hochwahrscheinlich, dass sie von einer solchen Maßnahme als „andere Person" i.S.d. § 20c Abs. 1 Satz 2 PolG NRW betroffen ist.

2. [redacted]

Die Beschwerdeführerin zu 2., [redacted], ist seit vielen Jahren Umweltaktivistin. Sie ist bundesweit aktiv, unter anderem auch in Nordrhein-Westfalen[55]. Während ihrer dortigen Aktivitäten hält sie sich dort auf und wohnt bei einem Freund in Münster.

Sie wurde auf Grund dieser Aktivitäten immer wieder zu Zwecken der Straftatenverhütung heimlich überwacht[56], in Gewahrsam genommen[57] und war Ziel bzw. Gegenstand von Maßnahmen des unmittelbaren Zwangs. Insbesondere wurden gegen die Beschwerdeführerin Strafverfahren wegen der auch im hier angegriffenen § 8 Abs. 4 PolG NRW genannten Delikte (z.B. § 315, § 316b StGB) eingeleitet.

Auch das Gericht – genauer die 2. Kammer des Zweiten Senats – war bereits unter dem Aktenzeichen 2 BvR 1754/14[58] mit einer rechtswidrigen Ingewahrsamnahme auf Grund einer Aktion der Beschwerdeführerin befasst.

Das Landeskriminalamt NRW hielt offenbar im Jahr 2016 die Aufbewahrung von Daten über die Beschwerdeführerin die *„auf der Grundlage des Kriminalpolizeilichen Meldedienstes „Politisch motivierte Kriminalität" (KPMD-PMK)"* nach dem PolG NRW

[55] Vgl. Schreiben des LKA NRW v. 27.9.2016 – Az. ZA 2.2-57.03.01.-444/16 – Ausdruck als **Anlage 21** anbei.
[56] Vgl. den Vermerk der PI Lüneburg v. 6.11.2006 sowie Benachrichtigungsschreiben v. 7.12.2006 – Ausdrucke als **Anlage 22** anbei.
[57] Vgl. z.B. VG Gelsenkirchen - 17 K 3055/12; LG Essen, Urteil v. 15.12.2016 - 4 O 113/16; AG Essen, Beschluss v. 27.4.2017 – 71 XIV 178/17; OVG NRW, Beschluss v. 8.12.2011 – 5 A 1045/09 - Kopien anbei als **Anlagenkonvolut 23**.
[58] BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 20.4.2017 - 2 BvR 1754/14.

erfasst wurden „*zur Vorbeugung von Straftaten von erheblicher und überregionaler Bedeutung*“ für erforderlich und übermittelte diese wohl an die Verbunddatei „INPOL-Fall ‚Innere Sicherheit‘ (IFIS)‘.[59]

In dieser Datei wurde die Beschwerdeführerin ausweislich einer Auskunft durch das BKA als sog. „relevante Person“ geführt.[60] Eine Person wird als „relevant“ angesehen, wenn

> *„sie innerhalb des extremistischen/terroristischen Spektrums die Rolle einer Führungsperson, eines Unterstützers/Logistikers oder eines Akteurs einnimmt und objektive Hinweise vorliegen, die die Prognose zulassen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche im Sinne des § 100a der Strafprozessordnung (StPO) fördert, unterstützt, begeht oder sich daran beteiligt,*
> *oder*
> *es sich um eine Kontakt- oder Begleitperson eines Gefährders, eines Beschuldigten oder eines Verdächtigen einer politisch motivierten Straftat von erheblicher Bedeutung, insbesondere einer solchen im Sinne des § 100a StPO, handelt.*“[61]

Dies vorausgeschickt ist es sehr wahrscheinlich, dass die Beschwerdeführerin bereits jetzt Zielperson einer Telekommunikationsüberwachungsmaßnahme oder einer Quellen-Telekommunikationsüberwachungsmaßnahme nach § 20c Abs. 1 Nr. 1 oder Nr. 2 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 1 oder Nr. 2 PolG NRW ist oder in naher Zukunft wird.

Zudem ist es sehr wahrscheinlich, dass sie als Nachrichtenmittlerin oder als Anschluss-/Endgeräteüberlasserin bzw. als Überlasserin eines informationstechnischen Systems welches zur verschlüsselten Kommunikation genutzt wird, jedenfalls aber als „andere Person“ von einer (Quellen-)Telekommunikationsüberwachungsmaßnahme betroffen war oder ist.

---

[59] Schreiben des LKA NRW v. 27.9.2016 – Az. ZA 2.2-57.03.01.-444/16 – Ausdruck als **Anlage 21** anbei.
[60] Widerspruchsbescheid des BKA v. 10.9.2015 – Az. ZV 15 5391.05 – 3/15 – Ausdruck als **Anlage 24** anbei.
[61] So die Definition der *BReg* – BT Drs. 17/5136, S. 3.

3. [redacted]

Der *Beschwerdeführer zu 3*, [redacted], ist Autor einer Vielzahl anarchistischer Aufsätze sowie in vielen linkspolitischen Projekten und Einrichtungen aktiv. Er ist Mitglied der vom Verfassungsschutz beobachteten Roten Hilfe, die mitunter als „linksextremistisch“ und „verfassungsfeindlich“ eingeschätzt wird.[62] Früher war er auch Mitglied der vom Verfassungsschutz beobachteten anarchistisch syndikalistischen Jugend.

Aufgrund dieser politischen Hintergründe und der vielfachen „Polizeikontakte“ im Zusammenhang mit seiner Beteiligung an Demonstrationen (u.a. als Anmelder und Ansprechpartner) und Aktionen (zuletzt insbesondere im Zusammenhang mit den Protestaktionen im Hambacher Forst) geht der Beschwerdeführer davon aus, dass er bereits jetzt heimlich überwacht wird. Er hält es zudem für hochwahrscheinlich, dass er aus vorgenannten Gründen auch Zielperson einer Maßnahme nach § 20c PolG NRW werden könnte oder bereits ist.

Jedenfalls ist es mit Blick auf die von [redacted] gepflegten Kontakte und Freundschaften sehr wahrscheinlich, dass er als Anschluss- bzw. Endgeräteüberlasser i.S.d. § 20c Abs. 1 Nr. 4 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 4 PolG NRW Zielperson einer (Quellen-)Telekommunikationsüberwachungsmaßnahme war oder ist. Zudem ist es hochwahrscheinlich, dass er von einer solchen Maßnahme als „andere Person“ i.S.d. § 20c Abs. 1 Satz 2 PolG NRW betroffen ist.

4. [redacted]

Der *Beschwerdeführer zu 4*, [redacted], ist seit 1976 mit unterschiedlichsten Kommunikationsmedien politisch arbeitender Künstler. Seit den frühen 80er-Jahren ist es sein Anliegen, Menschen digital zu 'ermündigen'. Zu diesem Zweck beschäftigt er sich intensiv mit den Möglichkeiten moderner digitaler Technologien und deren

[62] Vgl. Antwort der *BReg* auf Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter der Fraktion DIE LINKE. – Drucksache 19/3333 – BT Drs. 19/3553, S. 5.

Vernetzungsmöglichkeiten. Diese Beschäftigung beinhaltet Elemente des Erfindens, des Entdeckens, des Erforschens und des Umsetzens.

Im Zusammenhang mit dieser Tätigkeit ist er immer wieder zur Zielperson polizeilicher Überwachungs- und Ermittlungstätigkeiten wegen (angeblicher) Straftaten geworden, die auch in § 8 Abs. 4 PolG NRW als „terroristische Straftaten" definiert sind. Einige Zeit nachdem er mit der Beschwerdeführerin zu 6. begonnen hatte, sog. MailBox-Netzwerke aufzubauen, führte der Staatsschutz Bielefeld, KK ST 2 (unter Mitwirkung des LKA Nordrhein-Westfalen) eine Hausdurchsuchung durch, da über das Netzwerk eine angebliche Bombenbauanleitung abrufbar war. Das Verfahren gegen ihn wurde eingestellt. Weitere Kontakte und Ermittlungen folgten. Die Tätigkeit der Vernetzung hat der Beschwerdeführer indes nie aufgegeben. Seit vielen Jahren betreibt er mit der Beschwerdeführerin zu 6. sogenannte Tor-Exit-Server. Das sind Anonymisierungsserver, die innerhalb eines globalen Netzwerkes dafür sorgen, dass Menschen ihr Recht auf anonyme Nutzung des Internet in Anspruch nehmen können, da dieses Netzwerk verschleiert, wer auf welche Inhalte zugreift. So kann, wenn das Tor-Netzwerk zum Beispiel von einem investigativ arbeitenden Journalisten genutzt wird, der Betreiber einer Internetplattform, die dieser Journalist aufruft, nicht feststellen, von welchem Anschluss der Aufruf erfolgt. Für den Plattformbetreiber würde es immer so aussehen, als sei es der Beschwerdeführer selbst – also der Betreiber des Servers –, der auf die Internetplattform zugreift. Genauso, wie Kriminelle und Terroristen eine öffentliche Straße anonym nutzen können, können Kriminelle und Terroristen auch die Anonymisierungsstrukturen des Tor-Netzwerkes nutzen. Auch deren Kommunikationsverhalten kann über den Tor-Exit-Server des Beschwerdeführers geleitet werden – mithin sieht es so aus, als sei dieser der Nutzer, da die zugehörige IP-Adresse auf seinen Namen eingetragen ist. Aus diesem Grund ist der Beschwerdeführer bereits häufig Verdächtiger schwerster Straftaten gewesen.[63]

Da das Tor-Netzwerk bzw. der von ihm auf seinem Namen betriebene Tor-Exit-Server voraussichtlich auch von Kriminellen und Terroristen genutzt wird, um zum Beispiel anonym Waffen im Internet bzw. im sog. „Darknet" zu beschaffen, sich dort zu Straftaten zu verabreden, etc. befürchtet er, dass er nunmehr zudem Zielperson von präventiv-

[63] Die Verfahren wurden stets eingestellt.

polizeilichen Telekommunikations- bzw. Quellen-Telekommunikationsmaßnahmen nach § 20c Abs. 1 bzw. Abs. 2 PolG NRW wird bzw. eventuell sogar bereits ist.

5. [redacted]

Die *Beschwerdeführerin zu 5*, [redacted], arbeitet für Digitalcourage e.V. als Campaignerin und Redakteurin. Insbesondere im Zusammenhang mit der Organisation und Durchführung von Aktionen und Demonstrationen in Bündnissen, denen auch Organisationen angehören, die dem sog. linksaktivistischen Bereich zugeordnet werden (z.B. Ende Gelände), steht sie in Kontakt zu Personen, denen entweder bereits die in § 8 Abs. 4 PolG NRW genannten Straftaten vorgeworfen wurden oder bei denen ein entsprechender Vorwurf hochwahrscheinlich ist.

Gleiches gilt für die mit [redacted] im Rahmen ihrer Recherchetätigkeit in Kontakt stehenden Hinweisgeberinnen und Hinweisgeber. Beispielhaft sei der Kontakt zu vom Verfassungsschutz beobachteten Organisationen und Personen bzw. als „linksextremistisch" eingeschätzten Gruppierungen und Personen im Zusammenhang mit Kampagnen und Aktionen gegen die Verschärfung des Polizeigesetzes NRW (namentlich: „Bündnis Polizeigesetz NRW stoppen!" - #NOPOLGNRW) erwähnt.[64]

Mit Blick das Gesagte hält es [redacted] für sehr wahrscheinlich, dass sie jedenfalls als Anschluss- bzw. Endgeräteüberlasserin i.S.d. § 20c Abs. 1 Nr. 4 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 4 PolG NRW Zielperson einer (Quellen-) Telekommunikations-überwachungsmaßnahme war oder ist, jedenfalls aber von einer solchen Maßnahme als „andere Person" i.S.d. § 20c Abs. 1 Satz 2 PolG NRW betroffen ist.

6. [redacted]

Die *Beschwerdeführerin zu 6*, [redacted], ist Mitglied im Vorstand des Digitalcourage e.V. In dieser Tätigkeit recherchiert sie sehr viel, sowohl telefonisch als auch im Internet, unter anderem für den Datenschutz-Negativpreis „BigBrotherAwards".

[64] Dieses Bündnis wird aktiv von den aus **Anlage 25** ersichtlichen Organisationen unterstützt - abrufbar unter https://polizeigesetz-nrw-stoppen.de/das-buendnis/.

Hierbei erhält sie vertrauliche Informationen aus Behörden, zivilgesellschaftlichen Organisationen und Unternehmen. Die Informantinnen und Informanten bewegen sich mitunter im Bereich der in § 8 Abs. 4 PolG NRW genannten Straftaten.

Die Beschwerdeführerin, die Ehrenmitglied im Chaos Computer Club ist, betreibt darüber hinaus mit dem Beschwerdeführer zu 4. einen Tor-Server über den Dritte anonym über das Internet kommunizieren und anonym Internetdienste aufrufen können. Diese Möglichkeit wird – wie bereits dargelegt – mitunter zu illegalen Zwecken ausgenutzt. Die „digitale Spur" (sog. IP-Adresse) führt technikbedingt auch zur Beschwerdeführerin als Zugangsvermittlerin.

Es ist daher ebenso wie beim Beschwerdeführer zu 4. wahrscheinlich, dass sie unmittelbar oder als vermeintliche Nachrichtenmittlerin bzw. Anschlussüberlasserin Ziel der hier angegriffenen Maßnahmen wird.

Da auch bei der Beschwerdeführerin bereits wegen angeblichen Verbreitens einer vermeintlichen „Bombenbauanleitung" über elektronische Netze eine Hausdurchsuchung durchgeführt wurde[65], hat sie die begründete Befürchtung, dass sie Zielperson der hier angegriffenen Maßnahmen nach § 20c PolG NRW wird bzw. gegebenenfalls bereits ist.

V. Prozessbevollmächtigter

Der Prozessbevollmächtigte erfüllt die in § 22 Abs. 1 BVerfGG niedergelegten Anforderungen. Er ist Professor für Öffentliches Recht an der Hochschule für Wirtschaft und Recht Berlin (HWR Berlin) [66], also einer deutschen Hochschule. Er hat im Jahr 2005 die Befähigung zum Richteramt im Sinne des § 5 Abs. 1 DRiG erworben und war mehrere Jahre als Rechtsanwalt zugelassen und tätig.

[65] Auch hier wurde das Verfahren eingestellt.
[66] https://www.hwr-berlin.de/hwr-berlin/ueber-uns/personen/589-jan-dirk-roggenkamp/ (letzter Besuch 29. Oktober 2019).

B. Rechtsschutzbegehren

Die Beschwerdeführer*innen wenden sich mit der Verfassungsbeschwerde gegen § 20c PolG NRW sowie § 8 Abs. 4 PolG NRW in der Fassung des „Gesetzes zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden“ vom 18. Dezember 2018 (GV. NRW. S. 741, ber. 2019 S. 23), in Kraft getreten am 29. Dezember 2018 bzw. des „Gesetzes zur Stärkung der Sicherheit in Nordrhein-Westfalen - Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen“ vom 13. Dezember 2018 (GV. NRW. S. 684, ber. 2019 S. 23), in Kraft getreten am 20. Dezember 2018, die sie für mit dem Grundgesetz unvereinbar und nichtig erachten.

Die Beschwerdeführer*innen rügen die Verletzung ihrer Grundrechte aus Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 sowie Art. 10 Abs. 1 GG.

C. Zulässigkeit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist zulässig.

I. Grundrechtsträger

Die Beschwerdeführer*innen sind natürliche Personen und damit Träger der hier als verletzt gerügten Grundrechte.

II. Beschwerdebefugnis

Die Beschwerdeführer*innen sind beschwerdebefugt. Durch die Regelungen werden sie mit hinreichender Wahrscheinlichkeit selbst, unmittelbar und gegenwärtig in ihren Grundrechten betroffen.

1. Unmittelbar

Die Beschwerdeführer*innen sind durch die angegriffenen Regelungen unmittelbar beschwert. Ihnen steht die Verfassungsbeschwerde unmittelbar gegen die angegriffenen gesetzlichen Regelungen zu. Diese sind zwar vollzugsbedürftig, nach der Rechtsprechung des *Gerichts* gilt indes:

> *„Die Verfassungsbeschwerde kann sich jedoch ausnahmsweise unmittelbar gegen ein vollziehungsbedürftiges Gesetz richten, wenn der Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil es ihn nicht gibt (vgl. BVerfGE 67, 157 [170]) oder weil er keine Kenntnis von der Maßnahme erlangt (vgl. BVerfGE 100, 313 [354]). In solchen Fällen steht ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zu wie in jenen Fällen, in denen die grundrechtliche Beschwer ohne vermittelnden Vollzugsakt durch das Gesetz selbst eintritt (vgl. BVerfGE 30, 1 [16 f.]; 67, 157 [169 f.]; 100, 313 [354]).“*[67]

Diese Voraussetzungen sind vorliegend erfüllt. Die angegriffenen Maßnahmen werden heimlich durchgeführt. Der Betroffene erfährt von diesen weder vor noch während der

[67] BVerfGE 109, 279 (306 f. - Rn. 96).

Überwachung. Die Inanspruchnahme fachgerichtlichen Rechtsschutzes ist dementsprechend nicht möglich. Eine nachträgliche Benachrichtigung ist zwar grundsätzlich vorgesehen, steht der Zulässigkeit der Verfassungsbeschwerde aber nicht entgegen:

> *„Ihre Erhebung unmittelbar gegen das Gesetz ist nicht nur dann zulässig, wenn nach der gesetzlichen Regelung die Betroffenen zu keinem Zeitpunkt Kenntnis von einem heimlichen Vollzugsakt erhalten, sondern darüber hinaus auch dann, wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber auf Grund weit reichender Ausnahmetatbestände auch langfristig abgesehen werden kann. Unter diesen Umständen ist ebenfalls nicht gewährleistet, dass der Betroffene effektiven fachgerichtlichen Rechtsschutz erlangen kann (vgl. MVVerfG, LKV 2000, 345 [346]).“*[68]

Derart weitreichende Ausnahmetatbestände von der nachträglichen Unterrichtung liegen hier vor. Nach § 33 Abs. 3 PolG NRW kann eine Benachrichtigung vollständig unterbleiben, „*soweit dies im überwiegenden Interesse einer betroffenen Person liegt*“. Bereits aus diesem Grund kann die Mitteilung an die Betroffenen auf unabsehbare Zeit ausgeschlossen sein. Zudem erfolgt eine Benachrichtigung ausweislich § 33 Abs. 2 Satz 1 PolG NRW erst, „*sobald dies ohne Gefährdung des Zwecks der Maßnahme, des Bestandes des Staates, von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, möglich ist*“. Eine Zurückstellung der Benachrichtigung ist demnach auch langfristig möglich. Das verdeutlicht § 33 Abs. 4 Satz 1 und 2 PolG NRW. Danach ist zunächst nach sechs Monaten eine richterliche Entscheidung über die Zurückstellung einzuholen (Satz 1), sodann nur noch jährlich (Satz 2). Schließlich kann die Benachrichtigung bei Maßnahmen nach § 20c PolG NRW „*unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen sind und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben.*“ Es ist unklar, wann eine derartige „unerhebliche“ Betroffenheit vorliegt. Es besteht dadurch stets die Gefahr, dass eine Benachrichtigung unterbleibt, weil – für den Betroffenen nicht nachvollziehbar, da dies ihm ja unbekannt bleibt – eine „erhebliche“ Betroffenheit verneint wird.

---

[68] BVerfGE 109, 279 (307 - Rn. 97).

2. Selbst und gegenwärtig

Die Beschwerdeführer*innen werden durch die angegriffenen Befugnisse zur Durchführung einer Telekommunikationsüberwachung sowie einer Quellen-Telekommunikationsüberwachung in eigenen Grundrechten und gegenwärtig verletzt.

Da die angegriffenen Regelungen bereits jetzt einen Eingriff gegenüber jedermann erlauben, ist mit einiger Wahrscheinlichkeit anzunehmen, dass die Beschwerdeführer*innen von den durch die angegriffenen Regelungen gestatteten (heimlichen) Maßnahmen betroffen werden oder sogar bereits sind.

Nach der Rechtsprechung des *Gerichts* gilt in diesen Fällen:

> *„Die Möglichkeit der eigenen und gegenwärtigen Betroffenheit ist grundsätzlich erfüllt, wenn der Bf. darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird (vgl. BVerfGE 67, 157 [169f.] = NJW 1985, 121; BVerfGE 100, 313 [354] = NJW 2000, 55). Der geforderte Grad der Wahrscheinlichkeit wird davon beeinflusst, welche Möglichkeit der Bf. hat, seine Betroffenheit darzulegen (vgl. BVerfGE 100, 313 [355f.] = NJW 2000, 55). So ist bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt (dazu vgl. BVerfG [1. Kammer des Ersten Senats], NVwZ 2001, 1261 = NJW 2002, 1037 L = DVBl 2001, 1057) oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann. Darlegungen, durch die sich der Bf. selbst einer Straftat bezichtigen müsste, dürfen zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden.“*[69]

Die hier gegenständlichen Maßnahmen der Telekommunikations- und der Quellen-Telekommunikationsüberwachung sollen der Abwehr gegenwärtiger Gefahren und der Bekämpfung des (internationalen) Terrorismus dienen[70].

[69] BVerfGE 109, 279 (307f. - Rn. 99).
[70] NRW LT-Drs. 17/2351, S. 2.

Mögliche Adressaten sind nicht nur (vermeintliche) Verhaltens- oder Zustandsstörer (§ 20c Abs. 1 Nr. 1 PolG NRW) oder Personen bei denen die Begehung einer sog. terroristischen Straftat (§ 8 Abs. 4 PolG NRW) „prognostiziert" wird (§ 20c Abs. 1 Nr. 2 PolG NRW). Eine Überwachung und Aufzeichnung der Telekommunikation sowie - im Fall des Abs. 2 – auch eine Quellen-Telekommunikationsüberwachung darf sich auch auf Personen erstrecken, die gerade keine Störer sind und auch keine Straftatbegehung planen, vgl. § 20c Abs. 1 Nr. 3 und Nr. 4. Zudem darf nach § 20c Abs. 1 Satz 2 PolG NRW eine (Quellen-)Telekommunikationsüberwachung auch durchgeführt werden, wenn „*andere Personen unvermeidbar betroffen werden*". Nach § 20c Abs. 2 PolG NRW darf zudem zum Zweck der Quellen-Telekommunikationsüberwachung „*mit technischen Mitteln*" in jedes „*von der betroffenen Person genutzte informationstechnische Systeme eingegriffen*" werden.

Alle Beschwerdeführer*innen haben Ihren Lebensmittelpunkt in Nordrhein-Westfalen bzw. halten sich regelmäßig längere Zeit dort auf.

Sie nutzen – wie dargelegt – sowohl eigene als auch fremde Telekommunikationsanschlüsse (sowohl Festnetz als auch Mobilfunk sowie WLAN-Zugänge) und umfänglich und insbesondere zu privaten Zwecken eine Vielzahl mit dem Internet bzw. dem „Telekommunikationsnetz" verbundene Endgeräte bzw. informationstechnische Systeme (z.B. Smartphones, PC, Laptop, sowie mit den jeweiligen Geräten verbundene Kameras und Mikrofone).

Alle Beschwerdeführer*innen teilen ihre Telekommunikationsanschlüsse, Endgeräte und mit dem Internet verbundenen informationstechnischen Systeme auch mit Dritten bzw. nutzen mit dem Internet verbundene informationstechnische Systeme Dritter.

Sie gebrauchen diese informationstechnischen Systeme sowie die Telekommunikationsanschlüsse und mit dem Internet verbundenen Endgeräte sowohl zur (verschlüsselten) privaten Kommunikation, z.B. über sog. Messengerdienste wie Signal oder Threema sowie zum Austausch von Daten aller Art.

Darüber hinaus nutzen alle Beschwerdeführer*innen ihre Internetzugänge bzw. die Zugänge Dritter für private und privateste Dinge (z.B. Suchanfragen bei persönlichen Problemen, Fragen zu Sexualität und Gesundheit, religiösen und politischen Fragen, etc.). Sie nutzen unterschiedliche Internetdienste, insbesondere sog. Cloud Computing Anwendungen (z.B. zur Sicherung des lokalen Datenspeichers – sog. Backup oder zur Synchronisation der genutzten Geräte).

Es besteht stets die Möglichkeit, dass die Beschwerdeführer*innen zufällig von einer der hier angegriffenen Maßnahmen erfasst werden.

Zudem besteht die Möglichkeit, dass die informationstechnischen Systeme der Betroffenen durch die bewusste Offenhaltung von unbekannten Sicherheitslücken zum Zweck der Infiltration beeinträchtigt werden.

Im Kontext der verfassungsrechtlichen Überprüfung der präventiv-polizeilichen Telekommunikationsüberwachung nach dem Nds. SOG a.F. hat das *Gericht* festgehalten:

> „*Die Möglichkeit, Objekt einer Maßnahme der Telekommunikationsüberwachung aufgrund der angegriffenen Regelung zu werden, besteht praktisch für jedermann. Sie kann nicht nur den möglichen Straftäter selbst oder dessen Kontakt- und Begleitpersonen erfassen, sondern auch Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen in Verbindung stehen.*“[71]

Das gilt auch für die durch § 20c PolG NRW zugelassenen Telekommunikationsüberwachungsmaßnahmen bzw. Quellen-Telekommunikations-überwachungsmaßnahmen.

Konkretere Darlegungen für die Frage der eigenen und gegenwärtigen Betroffenheit sind mit Blick auf mögliche Nachteile für die Beschwerdeführer*innen nicht möglich. Es sei jedoch auf die Erläuterungen der Beschwerdeführer*innen zu ihrer persönlichen Situation hingewiesen (oben A.IV). Aus diesen wird ersichtlich, dass diese unmittelbar

[71] BVerfGE 113, 348 (363f. - Rn. 77).

eine Telekommunikations- oder Quellen-Telekommunikationsüberwachung zu befürchten haben.

Insbesondere besteht die hinreichende Wahrscheinlichkeit, dass die Aktivitäten der Beschwerdeführer*innen als „*individuelles Verhalten*“ interpretiert werden, welches vermeintlich „*die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 8 Absatz 4 begehen werden*“.

Es besteht jedenfalls enger Kontakt zu Personen, bei denen die hinreichende Wahrscheinlichkeit besteht, dass diese entsprechenden Überwachungsmaßnahmen ausgesetzt sind, da sie vermeintlich „extremistischen“ oder gar als „terroristisch“ eingestuften Organisationen angehören bzw. bei denen die Möglichkeit des Vorwurfs der Planung/Durchführung „terroristischer“ Straftaten nicht fernliegt. Da nicht auszuschließen ist, dass diese Personen zumindest auch „*Telekommunikationsanschluss oder Endgerät*“ bzw. die „*informationstechnischen Systeme*“ der Beschwerdeführer*innen nutzen, besteht eine hohe Wahrscheinlichkeit, dass diese – auch ohne selbst hierzu unmittelbar Anlass gegeben zu haben – Objekt einer der hier angegriffenen Maßnahmen zu werden.

Zudem besteht jederzeit die Möglichkeit, im Zuge einer Kontaktaufnahme mit den vorgenannten Personenkreisen wenigstens Drittbetroffener einer der angegriffenen Maßnahmen zu werden.

III. Subsidiarität

Auch der Grundsatz der Subsidiarität der Verfassungsbeschwerde ist gewahrt. Es kann den Beschwerdeführer*innen nicht zugemutet werden, einzelne Vollzugsakte und die Benachrichtigung hierüber abzuwarten, die – wie bereits oben unter C.II.1 dargelegt - gegebenenfalls niemals erfolgt.

IV. Frist

Die Verfassungsbeschwerde ist fristgemäß, nämlich innerhalb der Jahresfrist des § 93 Abs. 3 BVerfGG erhoben worden.

Die mit der Verfassungsbeschwerde angegriffenen Regelungen sind gem. Art. 3 des Gesetzes zur Stärkung der Sicherheit in Nordrhein-Westfalen - Sechstes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen vom 13. Dezember 2018 am Tag nach der Verkündung des Gesetzes in Kraft getreten. Die Verkündung im Gesetz- und Verordnungsblatt NRW ist am 19. Dezember 2018 (GV. NRW. S. 684) erfolgt. Die angegriffenen Regelungen sind damit am 20. Dezember 2018 in Kraft getreten[72].

V. Sonstiges

Die vorliegende Verfassungsbeschwerde enthält einen ordnungsgemäßen Antrag gemäß §§ 23 Abs. 1, 93 BVerfGG. Sie genügt den Anforderungen des § 23 Abs. 1 BVerfGG, da sie schriftlich mit Begründung erhoben wurde.

[72] Die Anpassung des § 20c PolG NRW auf Grund des Gesetzes zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und des Gesetzes über Aufbau und Befugnisse der Ordnungsbehörden vom 18. Dezember 2018 (GV. NRW. S. 741, ber. 2019 S. 23), ist am 29. Dezember 2018 in Kraft getreten.

D. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist begründet.

Die Beschwerdeführer*innen werden durch die angegriffenen Regelungen in ihren Grundrechten aus Art. 1 Abs. 1 GG, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10 Abs. 1 GG verletzt.

Mit § 20c PolG NRW (i.V.m. § 8 Abs. 4 PolG NRW) wurde sowohl die präventiv-polizeiliche Telekommunikationsüberwachung als auch die sog. Quellen-Telekommunikationsüberwachung in das Arsenal der landespolizeilichen Befugnisse zur heimlichen Datenerhebung eingeführt.

Sowohl die Befugnis zur Telekommunikationsüberwachung als auch zur Quellen-Telekommunikationsüberwachung sind mit der Menschenwürdegarantie unvereinbar und daher bereits aus diesem Grund verfassungswidrig (hierzu D.I).

Wollte man dies verneinen, stellen beide Maßnahmen einen verfassungsrechtlich ungerechtfertigten Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (hierzu D.II) dar, jedenfalls aber in das Fernmeldegeheimnis (hierzu D.III).

I. Unvereinbarkeit mit der Menschenwürdegarantie, Art. 1 Abs. 1 GG

Sowohl die Befugnis zur präventiv-polizeilichen „herkömmlichen“ Telekommunikationsüberwachung als auch die in Abs. 2 niedergelegte Befugnis zur heimlichen Datenerhebung mittels einer sog. Quellen-Telekommunikationsüberwachung stellen – unter Berücksichtigung der oben (A.II.1) dargestellten aktuellen Praxis der Telekommunikationsüberwachung und der oben (A.III) dargestellten Nutzungsgepflogenheiten moderner Telekommunikationsendgeräte bzw. -anschlüsse - eine nicht zu rechtfertigende Verletzung der durch Art. 1 Abs. 1 GG absolut geschützten Menschenwürde dar.

1. Eingriff

Durch beide Maßnahmen wird ein Zugriff auf und die Erhebung von Informationen gestattet, die der unantastbaren Intimsphäre des Nutzers zuzurechnen sind. Es wird faktisch *stets* ein Einblick in die innerste Gedankenwelt der jeweiligen Zielperson ermöglicht.

Es geht unter Berücksichtigung der heutigen Nutzungsgepflogenheiten (Stichwort: *always on*) nicht mehr – wie noch bei früheren Entscheidungen im Zusammenhang mit der Frage nach der Verfassungsmäßigkeit von Telekommunikationsüberwachungsmaßnahmen – um die Frage, ob eventuell einzelne Gespräche dem Kernbereich privater Lebensgestaltung zuzurechnen sind.

Es geht nicht darum, ob „*auch Tatsachen mit erfasst werden, die auch den Kernbereich des Persönlichkeitsrechts berühren*". Wenn eine Telekommunikationsüberwachung auch – wie es die Praxis und der zweite Senat annimmt - dazu berechtigt und genutzt wird, den gesamten Datenstrom der durch einen Nutzer „ausgelöst" wird permanent zu überwachen, dann ist dies eine Ausforschung der Gedanken- und Gefühlswelt.

Dieser Zugriff auf die Intimsphäre, den unantastbaren Kernbereich privater Lebensgestaltung stellt ob seiner Intensität eine *selbständige Verletzung*[73] der in Art. 1 Abs. 1 GG geschützten Menschenwürde dar.

Die letztlich im Fokus der Telekommunikations- und Quellen-Telekommunikationsüberwachung stehenden Geräte (insb. Smartphones) - sind unabkömmliche persönliche Begleiter. Im Rahmen einer Telekommunikationsüberwachung – und erst recht einer Quellen-Telekommunikationsüberwachung – überwachte und aufgezeichnete Informationen sind regelmäßig nicht nur von „gesteigerter", sondern von höchster Sensibilität.

[73] Vgl. *Di Fabio*, in: Maunz/Dürig, Art. 2 Abs. 1, Rn. 158.

Die ausnahmsweise Gestattung der (offenen!) Verwertung eines Tagebuchs zur Aufklärung einer schweren Straftat wird bislang als „*äußerste Grenze staatlicher Ausforschung der Intimsphäre*“[74] angesehen.

Die Telekommunikationsüberwachung in ihrer heutigen Gestalt (hierzu A.II.1) sowie die Quellen-Telekommunikationsüberwachung, die dem Betroffenen nicht einmal mehr die Möglichkeit belässt, sich durch Verschlüsselung aktiv vor einer Kenntnisnahme zu schützen - überschreitet diese Grenze bei weitem.

Sie gestattet nicht nur die (offene) Überwachung und Aufzeichnung höchstvertraulicher Vorgänge und Informationen, sie erlaubt gewissermaßen die dauerhafte heimliche Überwachung des Verfassens der Tagebucheinträge – insbesondere aber dessen, was der Betroffene nicht einmal seinem Tagebuch anvertrauen würde. Die hier angegriffene Regelung gestattet für sich allein bereits eine Überwachung, die sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden kann.

Sie eröffnet, wie *Prantl* es bezüglich der Neuregelung der Online-Durchsuchung und der Quellen-TKÜ in der StPO zutreffend formuliert, „*die Möglichkeit, Gedanken auszulesen*“[75].

Eine derartig umfassende Maßnahme, mit Hilfe derer über einen längeren Zeitraum nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können, stellt für sich genommen bereits eine Menschenwürdeverletzung dar.[76]

[74] *Herdegen*, in: Maunz/Dürig, Art. 1 Rn. 90.
[75] *Prantl*, Der Staatstrojaner ist ein Einbruch ins Grundrecht, SZ v. 22.6.2017 - https://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917 - Ausdruck als **ANLAGE 26** anbei.
[76] Vgl. BVerfGE 130, 1 (24).

Jede durch § 20c PolG NRW gestattete Maßnahme macht den Kernbereich privater Lebensgestaltung denknotwendigerweise zum Ziel staatlicher Ermittlungen und ist damit absolut auszuschließen.[77]

Es handelt sich sowohl bei der Telekommunikationsüberwachung als auch der Quellen-Telekommunikationsüberwachung nicht lediglich um eine „verletzungsgeneigte Maßnahme", sondern um eine Überwachungsmaßnahme der eine Verletzung des Kernbereichs immanent ist. Es ist technisch nicht möglich, eventuelle nicht kernbereichsrelevante Informationen im Rahmen eines Zugriffs auszufiltern.

2. Unmöglichkeit der Rechtfertigung

Können kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist nach den Ausführungen des *Gerichts* zur vergleichbaren Maßnahme der Online-Durchsuchung

> „*ein Zugriff auf das informationstechnische System jedoch auch dann zulässig,* ***wenn*** *hierbei* ***eine Wahrscheinlichkeit*** *besteht, dass* ***am Rande auch*** *höchstpersönliche Daten miterfasst werden.*"[78]

Dies beansprucht Gültigkeit für jede heimliche Datenerhebungsmaßnahme. Aus den Ausführungen folgt im Umkehrschluss, dass eine heimliche Datenerhebungsmaßnahme dann *nicht* zulässig ist, wenn die Wahrscheinlichkeit besteht, dass *überwiegend* höchstpersönliche Daten erfasst werden.

Wenn aber eine Maßnahme – wie die Telekommunikationsüberwachung und die Quellen-Telekommunikationsüberwachung - regelmäßig und nicht nur in Ausnahmefällen und ganz „*am Rande auch*" den Kernbereich der privaten Lebensgestaltung erfasst, weil – wie oben dargestellt – letztlich das gesamte Verhalten permanent überwacht werden kann, stellt sie per se einen Verstoß gegen die Menschenwürde dar und kann nicht gerechtfertigt werden.

[77] BVerfGE 121, 220 (278 - Rn. 125).
[78] BVerfGE 121, 220 (307 - Rn. 220) zur Online-Durchsuchung - Hervorhebung nur hier.

II. Unvereinbarkeit mit dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)

Sowohl die nach § 20c Abs. 1 PolG NRW gestattete Telekommunikationsüberwachung als auch die nach § 20c Abs. 2 PolG NRW gestattete Quellen-Telekommunikationsüberwachung sind – wenn man dem vorgenannten nicht folgen wollte - *jedenfalls* als verfassungsrechtlich nicht gerechtfertigter Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) zu bewerten.

1. Beurteilungsmaßstab und Eingriff

Der grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zur Durchführung einer Telekommunikationsüberwachung als auch einer Quellen-Telekommunikationsüberwachung muss generell Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme sein und nicht „nur" Art. 10 Abs. 1 GG (sogleich D.II.1.a). Die durch § 20c PolG NRW gestattete Telekommunikationsüberwachung als auch die Quellen-Telekommunikationsüberwachung stellen einen Eingriff in dieses Grundrecht dar.

Die durch § 20c Abs. 2 PolG NRW i.V.m. § 20c Abs. 1 PolG NRW gestattete Quellen-Telekommunikationsüberwachung bewirkt darüber hinaus einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, weil die Vorgabe des *Gerichts* auf wirksame Beschränkung auf die *„Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang"* [79] nicht eingehalten wurde (dazu D.II.1.b).

[79] BVerfGE 120, 274 (309).

Die Quellen-Telekommunikationsüberwachung stellt darüber hinaus stets einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme dar, da die der Infiltration des Zielsystems innewohnende Kompromittierung des Gesamtsystems technisch nicht revidierbar ist (dazu D.II.1.c).

a. Maßstab nicht Art. 10 Abs. 1 GG

Dass die Telekommunikationsüberwachung „nur" an Art. 10 Abs. 1 GG und nicht an den vom *Gericht* zum Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme entwickelten Maßstäben zu messen sei, hat das *Gericht* in der BKAG-Entscheidung mit dem „Gesamtcharakter" der Telekommunikationsüberwachung begründet:

> *„Allerdings ist die Telekommunikationsüberwachung ihrem Gesamtcharakter nach nicht in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Wohnraumüberwachung oder auch die Online-Durchsuchung (vgl. BVerfGE 113, 348 [391]). Sie erfasst Kommunikation aller Art in allen Situationen, die immer technisch vermittelt ist. Höchstvertrauliche Kommunikation ist ein kleiner Teil von ihr, der bei der Überwachung miterfasst zu werden droht, nicht aber -- wie die Überwachung des Rückzugsbereichs der privaten Wohnung -- typusprägend ist. Sie unterscheidet sich insoweit auch von Online-Durchsuchungen. Denn während diese oft gesamthaft über lange Zeit angesammelte Informationen einschließlich höchstprivater Aufzeichnungen erfassen und dabei unter Umständen durch deren Verknüpfung sowie das Nach- oder Mitverfolgen der Bewegungen im Internet auch geheim gehaltene Schwächen und Neigungen erschließen können, bezieht sich die Telekommunikationsüberwachung auf einzelne Akte unmittelbarer Kommunikation. Ihre Kernbereichsnähe beschränkt sich vor allem darauf, dass sie hierbei auch den höchstpersönlichen Austausch zwischen Vertrauenspersonen umfasst (vgl. BVerfGE 129, 208 [247]).*"[80]

[80] BVerfGE 141, 220 (312) – Rn. 238.

aa) Geänderter Gesamtcharakter der Telekommunikationsüberwachung

Diese Annahmen bedürfen angesichts der oben (A.II.1) dargestellten tatsächlichen Praxis der Telekommunikationsüberwachung einer Korrektur, jedenfalls aber einer differenzierten Betrachtung.[81]

Die o.g. Annahmen des *Gerichts* zum „Gesamtcharakter" treffen nämlich nur auf die „klassische" Telekommunikationsüberwachung zu, d.h. die Telekommunikationsüberwachung die sich tatsächlich „nur" auf die Überwachung des kommunikativen Austauschs zwischen zwei natürlichen Personen – also „*einzelne Akte unmittelbarer Kommunikation*" bzw. „*auch den höchstpersönlichen Austausch zwischen Vertrauenspersonen"* beschränkt; die technisch vermittelte „Mensch-zu-Mensch-Kommunikation".

Moderne Formen der Telekommunikationsüberwachung – und damit auch der Quellen-Telekommunikationsüberwachung – beschränken sich aber technisch gerade *nicht* mehr auf die Überwachung einzelner Akte des Austauschs von Nachrichten zwischen zwei (natürlichen) Personen mit Hilfe von Telekommunikationstechnik.

Im Rahmen von Telekommunikationsüberwachungsmaßnahmen kann und wird in der Praxis (ausführlich bereits oben A.II.1) seit Jahren insbesondere auch der vollständige Datenverkehr des überwachten Anschlusses erfasst, überwacht und als Rohdatenstrom ausgeleitet. [82] Überwacht wird also die „Mensch-zu-Maschine-Kommunikation" (die „Internetaktivitäten") sowie die „Maschine-zu-Maschine-Kommunikation" (z.B. Kommunikation der Geräte des Anschlussinhabers bzw. der Zielperson im sog. Internet der Dinge).

Im Rahmen der Quellen-Telekommunikationsüberwachung (§ 20c Abs. 2 PolG NRW) darf zudem noch eine eventuelle Verschlüsselung durch Nutzung von Trojanersoftware oder ähnlichen technischen Mitteln überwunden werden.

---

[81] In diese Richtung auch *Hiéramente*, HRRS 2016, 448 (451).
[82] Siehe bereits BGH, Beschluss vom 23.3.2010 - StB 7/10 – NStZ-RR 2011, 148;

bb) Folgerung

Die in der Praxis anzutreffende Telekommunikationsüberwachung ist nach alledem – um die oben zitierten Ausführungen des Gerichts aufzugreifen - *in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Wohnraumüberwachung oder auch die Online-Durchsuchung*.

Folge der eingangs dargelegten geänderten Nutzungsgepflogenheiten ist es, dass bereits im Rahmen einer Telekommunikationsüberwachung, und erst Recht im Rahmen einer Quellen-Telekommunikationsüberwachung, bei welcher nicht einmal mehr der „Selbstschutz" durch Verschlüsselung möglich ist, nicht nur ein umfangreiches Verhaltens- und Kommunikationsprofil der Zielperson erstellt werden kann. Die überwachende Stelle kann mehr und umfangreichere Informationen über die betroffene Person und ihre Persönlichkeit erhalten, als diese ihren intimsten Gesprächspartnern oder z.B. einem Tagebuch preisgeben würde. Durch eine Telekommunikations- bzw. Quellen-Telekommunikationsüberwachungsmaßnahme werden die betroffenen Personen genauso zu schutzlosen, gläsernen Objekten staatlicher Beobachtung, wie die Zielpersonen einer Online-Durchsuchung. Sie haben einen vergleichbaren „*Gesamtcharakter*".

cc) Maßstab nicht „lediglich" Art. 10 Abs. 1 GG

Eine die o.g. Praxis der Telekommunikationsüberwachung de facto billigende Entscheidung der dritten Kammer des Zweiten Senats findet sich im Nichtannahmebeschluss vom 6. Juli 2016 zum Aktenzeichen 2 BvR 1454/13. Nach dieser ist auch Zulässigkeit der Überwachung und Aufzeichnung der gesamten Internetnutzung – gegenständlich war die Überwachung des „Surfverhaltens" - (lediglich) am Maßstab des Art. 10 Abs. 1 GG zu messen. Damit hat sich der zweite Senat von seiner zuvor vertretenen Auffassung:

> „*Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen* ***an individuelle Empfänger*** *mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 67, 157 [172]; 106, 28 [35 f.]). Die*

> *Beteiligten sollen weitestgehend so gestellt werden, wie sie bei einer Kommunikation unter Anwesenden stünden.*“[83]

entfernt. Im o.g. Nichtannahmebeschluss wird nunmehr vertreten:

> „*Für das Merkmal „Telekommunikation“ kommt es auch i.R.d. Art. 10 Abs. 1 GG aber weder auf die technische Umsetzung der Kommunikation* ***noch auf deren Inhalt und Empfängerkreis an*** *(vgl. BVerfGE 120, 274, 307 [= MMR 2008, 315 m. Anm. Bär]). Auch ist irrelevant, wer Betreiber der Übertragungs- und Vermittlungseinrichtungen ist (vgl. BVerfGE 107, 299, 322); das Grundrecht ist insgesamt „entwicklungsoffen“ (vgl. Guckelberger, in: Schmidt-Bleibtreu, a.a.O., Art. 10 Rdnr. 21; BVerfGE 106, 28, 36).*
>
> *Unabhängig vom Übertragungsweg und der Übermittlungsform ist also* ***allein maßgeblich, dass die Informationen körperlos befördert werden und dass sie am Empfangsort wieder erzeugt werden können.*** *Dies macht ihre Vulnerabilität für heimliche Ausforschungsmaßnahmen aus. Wo dies nicht der Fall ist – es sich entweder um ein körperliches Medium handelt oder der Übermittlungsvorgang wie bei der „Online-Durchsuchung“ bereits abgeschlossen ist – sind andere Verfassungsvorschriften einschlägig, z.B. das Briefgeheimnis und die Grundrechte auf informationelle Selbstbestimmung, auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und auf Unverletzlichkeit der Wohnung.*“

sowie

> „*Art. 10 Abs. 1 GG ist demgegenüber z.B. alleiniger grundrechtlicher Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-TKÜ“, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden TK-Vorgang beschränkt (BVerfG, a.a.O.; zuletzt: BVerfG, U. v. 20.4.2016, a.a.O., Rdnr. 234).* ***Nichts anderes gilt im vorliegenden Fall, da sich die Überwachung auf die laufende Internetkommunikation beschränkt.***“

[83] BVerfGE 115, 166 (182) – Hervorhebung nur hier.

Das steht im Widerspruch zu der Rechtsprechung des ersten Senats zu Umfang und Grenzen des Schutzbereichs des Fernmeldegeheimnisses. In der Entscheidung zur vorbeugenden Telekommunikationsüberwachung nach dem Nds. SOG a.F. hat dieser den Schutzbereich wie folgt umrissen:

> „*Der Schutz des Fernmeldegeheimnisses umfasst den Kommunikationsinhalt und die Kommunikationsumstände. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich* ***Kenntnis vom Inhalt der über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Information*** *zu verschaffen.*“[84]

Bereits hieraus folgt, dass Art. 10 Abs. 1 GG die technikgestützte „zwischenmenschliche Kommunikation“ erfasst, nicht aber die Kommunikation „Mensch - Maschine“ oder gar „Maschine - Maschine“. Das wird in den Ausführungen des ersten Senats in der „Telekommunikationsüberwachung 1“-Entscheidung noch deutlicher, bei welchem explizit auf einen mittels Fernmeldeanlagen abgewickelten *Gedankenaustausch* abgestellt wird:

> „*Das Fernmeldegeheimnis umfaßt zuvörderst den Kommunikationsinhalt. Die öffentliche Gewalt soll grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt des über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Informations- und* ***Gedankenaustauschs*** *zu verschaffen.*“[85]

Ein Gedankenaustausch aber erfordert stets einen menschlichen Kommunikationspartner.

Die Einstufung der Überwachung und Aufzeichnung des gesamten „Rohdatenstroms“ – insb. der Internetaktivitäten - als **Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme**[86] ist geboten, weil

[84] BVerfGE 113, 348 (364).
[85] BVerfGE 100, 313 (358).
[86] Meyer-Goßner/*Schmitt*, StPO, § 100a Rn. 7 – sieht einen „Grundrechtseingriff eigener Art“.

Art. 10 Abs 1 GG „lediglich" die Vertraulichkeit der technikvermittelten Kommunikation von Mensch zu Mensch über Distanz schützen will und soll.[87]

Bei der Überwachung des „Surfverhaltens" ist jedoch – wie bei einer Online-Durchsuchung auch – insbesondere der Aspekt der Vertraulichkeit informationstechnischer Systeme betroffen.[88] In letzter Konsequenz geht es bei der Erhebung der Internetkommunikation um die Überwachung und Aufzeichnung der auf einem informationstechnischen System „*erzeugten, verarbeiteten und gespeicherten Daten*"[89].

Das *Gericht* hat im Jahr 2008 die immense Eingriffsqualität einer Online-Durchsuchung gerade damit illustriert, dass durch eine Infiltration des Rechners des Betroffenen massenhaft sensible Daten über seine Online-Aktivitäten gewonnen werden können. Das *Gericht* erkannte die besondere Schwere des Eingriffs einer Online-Durchsuchung explizit darin, dass dadurch die Möglichkeit bestehe, „*die gesamte Internetkommunikation des Betroffenen über einen längeren Zeitraum mitzuverfolgen*" [90]. Genau das wird mit einer Telekommunikationsüberwachung nach § 20c PolG NRW ermöglicht.

Zudem hat das *Gericht* bereits 2008 festgehalten, dass eine Infiltration des informationstechnischen Systems selbst (z.B. durch eine Trojanersoftware) nicht zwingend erforderlich ist:

> „*Das Grundrecht schützt auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind,* ***aber diese Datenverarbeitungsvorgänge zum Gegenstand haben****.*"[91]

[87] Vgl. auch Nomos-BR/Roggan G-10 - § 1 Rn. 15 der konstatiert: „*Entsprechende Maßnahmen kommen in ihrer Bedeutung einer Online-Durchsuchung jedenfalls nahe*".
[88] In diese Richtung auch *Hiéramente*, HRRS 2016, 448 (451).
[89] BVerfGE 120, 274 (314).
[90] BVerfGE 120, 274 (324).
[91] BVerfGE 120, 274 (315).

Die Telekommunikations- und Quellen-Telekommunikationsüberwachung der Internetaktivitäten stellt eine solche Datenerhebung dar.

Die hier vertretene Einschätzung stützt sich zudem auf Ausführungen des *Gerichts* in der BKAG-Entscheidung. Dort wird konstatiert, dass „*das Nach- oder Mitverfolgen der Bewegungen im Internet auch geheim gehaltene Schwächen und Neigungen erschließen könne*“ und dementsprechend die Qualität einer Online-Durchsuchung habe. Weiter führt das *Gericht* in der BKAG-Entscheidung aus:

> *„Tagebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens, Film- oder Tondokumente werden heute zunehmend in Dateiform angelegt, gespeichert und teilweise ausgetauscht. Weite Bereiche auch der höchstpersönlichen Kommunikation finden elektronisch mit Hilfe von Kommunikationsdiensten im Internet oder im Rahmen internetbasierter sozialer Netzwerke statt.* ***Dabei befinden sich die Daten, auf deren Vertraulichkeit die Betroffenen angewiesen sind und auch vertrauen****, in weitem Umfang nicht mehr nur auf eigenen informationstechnischen Systemen, sondern auf denen Dritter.* ***Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt*** *dementsprechend* ***vor einem geheimen Zugriff auf diese Daten*** *und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen,* ***sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind****, erfasst* ***und Bewegungen der Betroffenen im Netz verfolgt werden.*** *Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.“*[92]

Sowohl das Verfolgen der Bewegungen Betroffener „im Netz“ als auch die heimliche Erhebung auf externe Server ausgelagerter persönlicher Daten (und damit denknotwendigerweise auch der Vorgang der Auslagerung selbst) sind danach als

[92] BVerfGE 141, 220 (304) – Hervorhebung nur hier.

Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einzustufen.[93]

Daraus folgt, dass auch die Telekommunikations- und die Quellen-Telekommunikationsüberwachung – soweit sie sich nicht (durch eine entsprechende gesetzgeberische Klarstellung) auf die Überwachung der Individualkommunikation (Telefonate, Nachrichten in Textform) beschränkt, sondern zu einer vollständigen Überwachung der Datenströme berechtigt – an diesem Grundrecht und nicht an Art. 10 Abs. 1 GG zu messen ist.

Eine andere Bewertung erscheint nur denkbar, wenn die konkrete Befugnis zur Durchführung einer Telekommunikations- bzw. Quellen-Telekommunikationsüberwachung ausdrücklich (!) auf die Erhebung und Verwertung der Inhalte und Umstände dieser Individualkommunikation („Mensch-zu-Mensch") beschränkt wäre.

Die hier gegenständliche Befugnis, „*die laufende Telekommunikation*" einer Person zu überwachen und aufzuzeichnen (§ 20c Abs. 1 Satz 1 PolG NRW) ist – insbesondere unter Berücksichtigung der weiten Interpretation des Telekommunikationsbegriffs des zweiten Senats und der Praxis - zu umfassend (hierzu noch D.II.2.c). Der Gesetzgeber müsste, wollte er „lediglich" Eingriffe in das Fernmeldegeheimnis zulassen, dies hinreichend deutlich machen, indem er beispielsweise ausdrücklich formuliert „*Die Polizei kann ohne Wissen der betroffenen Person die laufende Individualtelekommunikation einer Person überwachen und aufzeichnen ...*" (zur Unbestimmtheit der gestatteten Rechtsfolge sowie zu diesem Formulierungsvorschlag noch unten D.II.2.c).

Das ist nicht geschehen.

Die Gestattung einer Telekommunikationsüberwachung sowie einer Quellen-Telekommunikationsüberwachung die sich auch auf die Überwachung von

[93] Vgl. auch *Braun*, jurisPR-ITR 1/2017, Anm. 2 der zumindest eine gleichlaufende Eingriffsintensität anerkennt.

Kommunikation erstreckt, die über die unkörperliche Übermittlung von Informationen an individuelle menschliche (!) Empfänger mit Hilfe des Telekommunikationsverkehrs hinausgeht[94], ist nach alledem (jedenfalls) als Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme zu bewerten.[95]

b. Quellen-Telekommunikationsüberwachung ist de facto Online-Durchsuchung

§ 20c Abs. 2 PolG gestattet zudem de facto eine Online-Durchsuchung, also einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, da technisch nicht sichergestellt werden *kann*, dass neben der „laufenden Kommunikation" keine weiteren persönlichkeitsrelevanten Informationen erhoben werden (siehe bereits A.II.2.b).

Die Befugnis zur Durchführung einer Quellen-Telekommunikationsüberwachung ist somit auch aus diesem Grund nicht an Art. 10 Abs. 1 GG, sondern am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme messen.[96]

Das Gericht hat mit Blick auf die Durchführung sog. Quellen-Telekommunikationsüberwachungsmaßnahmen bereits im Jahr 2008 ausdrücklich vorgegeben,

> *„Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung* ***ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt****. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."*[97]

Der Versuch des nordrhein-westfälischen Gesetzgebers, die Vorgabe einzuhalten, die Quellen-Telekommunikationsüberwachung auf die Überwachung der Daten aus einem

---

[94] Vgl. BVerfGE 120, 274 (306 f. – Rn. 182).
[95] So auch *Eidam*, NJW 2016, 3511 (3512);
[96] Umkehrschluss zu BVerfGE 141, 220 (309– Rn. 228).
[97] BVerfGE 120, 274 (309 - Rn. 190) - Hervorhebung nur hier.

laufenden Telekommunikationsvorgang zu beschränken schlägt fehl. Nach § 20c Abs. 2 Nr. 1 PolG ist „*durch technische Maßnahmen*“ sicherzustellen, „dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird“.

Im Zusammenhang mit dem gleichlautend formulierten § 20l BKAG a.F. hat das *Gericht* vertreten, dass

> „*Sollten zum gegenwärtigen Zeitpunkt diese Anforderungen nicht erfüllbar sein, liefe die Vorschrift folglich bis auf weiteres leer. Auch dies machte sie jedoch nicht widersprüchlich und verfassungswidrig,* ***weil damit nicht ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können.***“[98]

Das *Gericht* hat, wie der letzte Halbsatz suggeriert, im damaligen Verfahren den Eindruck gewonnen, dass die technische Unmöglichkeit der Beschränkung einer Trojanersoftware auf die Überwachung der laufenden Kommunikation „*in absehbarer Zukunft*“ überwunden werden könnte.

Das ist nicht der Fall.

Es ist seit dem Jahr 2008 nicht gelungen und wird auch in absehbarer (und auch ferner) Zukunft nicht möglich sein, eine Trojanersoftware zu entwickeln, die allein die „laufende Kommunikation“ überwacht.[99] Im Nachgang zur BKAG-Entscheidung des angerufenen Gerichts haben Experten die „*künstliche Trennung zwischen Staatstrojanern, die einerseits auf die gesamte Festplatte zugreifen dürfen, und Staatstrojanern, die andererseits nur Kommunikation ausspionieren dürfen*“ kritisiert und noch einmal eindeutig festgehalten:

> „*Ein Trojaner, der ausschließlich Kommunikation erfassen kann, ist technisch illusorisch.*“[100]

---

[98] BVerfGE 141, 220 (311 f. – Rn. 234) - Hervorhebung nur hier.
[99] Vgl. nochmals *Hornung*, Stellungnahme, S. 6.
[100] Gemeinsame Erklärung des Chaos Computer Clubs (CCC e. V.) und des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.) vom 20.4.2016 – abrufbar unter

Es handelt sich bei § 20c Abs. 2 PolG NRW also nicht nur um eine – nach Auffassung des *Gerichts* zulässige[101] – Gesetzgebung „auf Vorrat", sondern um eine Regelung die eine Maßnahme gestattet, die technisch so niemals umsetzbar sein wird.

Die Regelung läuft also nicht „*bis auf weiteres leer*", sie läuft ad infinitum leer. Sie ist daher (im Umkehrschluss zu den o.g. Ausführungen des Gerichts[102]) „*widersprüchlich und verfassungswidrig*", da „*ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können*".

Insofern das Gericht festhält, dass

> „*das Programm so ausgestaltet* [sein muss]*, dass es - hinreichend abgesichert auch gegenüber Dritten - den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern* [...] *inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.*"[103]

wird § 20c PolG NRW dem nicht gerecht, da diese Vorgabe nicht gesetzlich abgesichert wird. Jedenfalls das aber wäre zur Sicherstellung der Begrenzung auf die Erstreckung der Quellen-Telekommunikationsüberwachung auf die „laufende Kommunikation" erforderlich gewesen.

Zwar muss sich im Antrag nach § 20c Abs. 4 PolG NRW gemäß § 20c Abs. 5 Nr. 4 PolG NRW „*die Bezeichnung des Herstellers und der Softwareversion des einzusetzenden technischen Mittels*" finden. Auch sind nach § 20c Abs. 9 PolG NRW „*Angaben zum Hersteller des zur Datenerhebung eingesetzten Mittels und zur eingesetzten Softwareversion*" zu protokollieren. Zudem enthält § 20c Abs. 3 PolG NRW technische Vorgaben bezüglich der einzusetzenden Software.

---

https://www.ccc.de/updates/2016/staatstrojaner-bka; vgl. auch die oben zitierte Aussage der Sachverständigen *Bröckling* in NRW LT APr 17/438, S. 13..

[101] A.A. *Tomerius*, NVwZ 2015, 412 (414), *Roggan*, LKV 2015, 14 (16 f.).

[102] BVerfGE 141, 220 (311 f. – Rn. 234).

[103] BVerfGE 141, 220 (312).

Es fehlt jedoch jedwede Vorgabe dazu, dass und wie sichergestellt werden soll, dass die Ausgestaltung des Programms den o.g. Anforderungen entspricht.

Wie das *Gericht* festgehalten hat, ist mit der Installation der Trojanersoftware

> „*die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist.*“[104]

Wenn aber unklar bleibt, wer die Einhaltung der „*technischen Vorgaben*“ überwacht, ja die Überprüfung der Einhaltung der Vorgaben faktisch gar nicht möglich ist, fehlt es an einer hinreichenden Absicherung gegen die vorgenannte Gefahr der Ausspähung des gesamten Systems. Die Beurteilung der zureichenden Beschränkung wird dem die Maßnahme anordnenden (und auch dem die Maßnahme ggf. überprüfenden) Gericht schon tatsächlich nicht möglich sein. Sie kann und darf aber nicht in das Belieben der mit der Durchführung der Maßnahmen betrauten Stellen überantwortet werden.

Diese Problematik wurde in der öffentlichen Sachverständigenanhörung des Innenausschusses des Landtags NRW am 13. November 2018 vom Sachverständigen *Gazeas* verdeutlicht:

> „*Es stellt sich hier die Frage: Wie soll ein Richter das überprüfen?*
> *Er kann es faktisch nicht, egal, wie intelligent und begabt dieser Richter ist. Selbst, wenn er technisch versiert ist, kann er es nicht, weil er eben der Software nicht in den Kopf schauen kann. Er kann also selber nicht überprüfen, ob die Software tatsächlich nur das kann, was sie rechtlich darf.*
> *Jetzt haben Sie die Ergänzung im Änderungsantrag vorgesehen, dass im Antrag der Polizei der Hersteller der Software und die Softwareversion genannt werden. Auch das hilft dem Richter nicht, denn die einzige Mehrinformation, die er im Antrag bekommen würde und die Sie übrigens dann nicht für eine Beschränkung im Beschluss vorsehen – da soll das wiederum nicht erscheinen –, ist, dass die Software*

[104] BVerfGE 120, 274 (308 - Rn. 188).

> *XKeyscore Version 4.73 verwendet werden soll. Der Richter ist genauso schlau wie vorher, denn er hat nicht die Möglichkeit zu wissen, was diese Software kann. Da hilft auch nicht der Verweis auf die standardisierte Leistungsbeschreibung des BKA."*[105]

Erforderlich wäre die Benennung einer unabhängigen Stelle gewesen, die die jeweils als Mittel der Wahl auserkorene Software eingehend überprüft. Diesbezüglich wäre zwingend vorzusehen gewesen, dass der überprüfenden Stelle alle dazu erforderlichen Unterlagen (z.B. Programmdokumentation) – einschließlich des Quellcodes – vorgelegt werden, da nur so eine Nachprüfung sinnvoll möglich ist. Der ehemalige Bundesbeauftragte für Datenschutz und Informationsfreiheit *Peter Schaar* hat zutreffend wie folgt ausgeführt[106]:

> „*Ob diese Grenzen [*Anm. die Vorgaben des *Gerichts* zu den Grenzen einer Quellen-Telekommunikationsüberwachung*] eingehalten werden, kann nur durch die Begutachtung und systematisches Testen der Software beurteilt werden. Erforderlich ist hierzu die Vorlage des sogenannten Quellcodes – einen lesbaren, in einer Programmiersprache geschriebenen Text der eingesetzten Software –, damit sich die verantwortliche Stelle nachhaltig über den Umfang der zur Verfügung stehenden programmierten Funktionen überzeugen kann. Auch eine verlässliche und umfassende interne oder externe Datenschutzkontrolle ist nur unter diesen Voraussetzungen möglich.*
>
> *Insbesondere ist ohne die Vorlage des Quellcodes eine sichere Beurteilung einer Software hinsichtlich des Vorhandenseins oder eben Nichtvorhandenseins von Funktionen nicht möglich. Die Übersendung oder Vorlage nur eines umfangreichen ausführbaren Programms (Codes, Binärcodes) reicht zur Beurteilung nicht, denn vor allem das Nichtvorhandensein von Funktionen kann allein anhand eines Binärcodes nicht abschließend bewertet werden.*

[105] NRW LT APr 17/438, S. 20.

[106] BfDI, Bericht gemäß § 26 Abs. 2 Bundesdatenschutzgesetz über Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes, S. 40 f. - abrufbar unter https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf (Ausdruck als **ANLAGE 27** anbei - i.W. „BfDI, Bericht").

> *Auch (mögliche) Seiteneinstiege für Dritte und andere Sicherheitslücken sind allein mit Hilfe des Binärcodes nicht auszuschließen. Gerade bei Überwachungssoftware, mit der in einem rechtstaatlichen Verfahren auch gerichtsverwertbare Daten erhoben werden sollen, sind Fragen nach den Möglichkeiten der Manipulation der Daten von immenser Wichtigkeit. Die Vertraulichkeit und Unversehrtheit der erhobenen Daten sind hier von entscheidender Bedeutung. Dies betrifft nicht nur die Übertragungswege, sondern auch die Speicherung der Daten in jedem Stadium der Überwachungsmaßnahme.*"

Kurz: ohne Vorlage des Quellcodes ist es unmöglich zu überprüfen, wie die Software funktioniert. Zudem ist nicht sichergestellt, dass elementare Anforderungen bezüglich des Datenschutzes erfüllt werden [107], wie sie insbesondere in der Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 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 niedergelegt wurden.

Ohne konkrete Festlegungen bezüglich des „Wie" der Sicherstellung der rechtlichen Anforderungen an die technische Ausgestaltung einer Quellen-Telekommunikationssoftware ist die Niederlegung eben dieser Vorgaben im § 20c PolG NRW mangels Überprüfbarkeit wertlos.

c. Fehlende „Rückholbarkeit"

Die Durchführung einer Quellen-Telekommunikationsüberwachung stellt darüber hinaus stets einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme dar, da die der Infiltration des Zielsystems innewohnende Kompromittierung des Gesamtsystems technisch nicht revidierbar ist.

[107] Das war z.B. bei der bis 2011 verwendeten Staatstrojanersoftware des Unternehmens DigiTask wohl nicht der Fall, vgl. *Beckedahl*, Geleakt: Datenschutzbericht zum Staatstrojaner, netzpolitik.org v. 17. 2. 2018, https://netzpolitik.org/2012/geleakt-datenschutzbericht-zum-staatstrojaner/ Ausdruck als **ANLAGE 28** anbei - der referenzierte Bericht ist unter https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf abrufbar und liegt als **ANLAGE 27** anbei.

Das erkennt auch der Gesetzgeber, wenn er die in § 20c Abs. 3 Nr. 2 PolG NRW niedergelegte Anforderung, dass sichergestellt werden müsse, dass die „*vorgenommenen Veränderungen bei Beendigung der Maßnahme* [...] *automatisiert rückgängig gemacht werden*“ können, unter den Vorbehalt der technischen Machbarkeit („*soweit technisch möglich*“) stellt. Dieser Fall wird stets eintreten, da es nicht möglich ist, eine Software „aus sich heraus“ vollständig zu deinstallieren bzw. „zurückzuholen“[108]. Der Adressat einer polizeilichen Maßnahme – der von dieser unter Umständen nie erfährt (vgl. § 33 Abs. 2, 3 PolG NRW) – behält regelmäßig eine schlimmstenfalls nur deaktivierte Trojanersoftware auf seinem – dann dauerhaft kompromittiertem informationstechnischen Gerät zurück. Bereits dies stellt einen erheblichen Eingriff in die Integrität des informationstechnischen Systems dar.

2. Fehlende verfassungsrechtliche Rechtfertigung

Der Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist – wenn man ihn nicht mit dem oben (D.I) Gesagten prinzipiell für unzulässig halten mag - nur unter strengen Bedingungen verfassungsrechtlich rechtfertigbar bzw. verhältnismäßig.

Diese Bedingungen erfüllt § 20c PolG NRW (i.V.m. § 8 Abs. 4 PolG NRW) nicht, da

1. die Befugnis selbst (sowie der maßgeblich in Bezug genommene § 8 Abs. 4 PolG NRW) nicht den Anforderungen des Bestimmtheitsgebotes genügt (a),
2. die Durchführung von Telekommunikations- und Quellen-Telekommunikationsüberwachungsmaßnahmen nicht lediglich zum Schutz „überragend wichtiger Rechtsgüter“ zugelassen ist (b),
3. die gestattete Rechtsfolge nicht den Anforderungen des Bestimmtheitsgebots genügt (c),
4. der Kernbereichsschutz sowohl auf der Erhebungs- als auch der Verwertungsebene unzureichend ausgestaltet wurde (d),

[108] Vgl. *Arzt*, Stellungnahme 17/936 – zur Stellungnahme zur Anhörung im Innenausschusses des Landtags NRW am 13.11.2018 betreffend Gesetzentwurf der Landesregierung Drs. 17/2351 vom 11.4.2018 und Änderungsantrag CDU und FDP Drs. 17/3865 vom 10.10.2018 (i.W. *Arzt*, Stellungnahme), S. 14.

5. der Schutz Dritter unzureichend ausgestaltet wurde (e), und
6. nicht explizit die Ausnutzung von Sicherheitslücken als Infiltrationsmethode ausgeschlossen wurde (f).

a. Unbestimmtheit der Eingriffsvoraussetzungen

Die Eingriffsvoraussetzungen des § 20c Abs. 1 Nr. 2 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 2 PolG NRW entsprechen nicht den Anforderungen an das Bestimmtheitsgebot und sind deshalb verfassungswidrig.

Es handelt sich sowohl bei der Telekommunikationsüberwachung als auch der Quellen-Telekommunikationsüberwachung um eine Befugnis zur heimlichen Datenerhebung und –verarbeitung, die – wie dargelegt – tief in die Privatsphäre hineinwirkt. Daher stellt der Grundsatz der Normenklarheit und Bestimmtheit „*besonders strenge Anforderungen*“.[109] Das folgt daraus, dass Maßnahmen nach § 20c PolG NRW von den Betroffenen weitgehend nicht wahrgenommen und angegriffen werden können. Ihr Gehalt kann nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden.[110]

aa) Unzureichende „Copy&Paste“-Gesetzgebung

In § 20c Abs. 1 Nr. 2 PolG NRW wurden bei Bestimmung der Eingriffsschwellen Formulierungen aus den Entscheidungsgründen des BKAG-Urteils des *Gerichts* übernommenen[111].

Nach § 20c Abs. 1 Nr. 2 PolG NRW ist eine Telekommunikationsüberwachung bzw. (über die Verweisung in § 20c Abs. 2 PolG NRW) eine Quellen-Telekommunikationsüberwachung bei einer Person zulässig,

> „*deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 8 Absatz 4 begehen wird*“.

[109] BVerfGE 141, 220 (265 - Rn. 94).
[110] Vgl. BVerfGE 141, 220 (265 - Rn. 94).
[111] BVerfGE 141, 220 (272 - Rn. 112).

Die Ausführungen des *Gerichts* weisen allerdings eine beträchtliche Begriffsunschärfe auf und werden in der Literatur nicht einheitlich ausgelegt[112]. Unbestritten ist allenfalls, dass das *Gericht* für heimliche Informationseingriffe bei terroristischen Gefährdungslagen *bereits im Vorfeld konkreter Gefahren* Eingriffsbefugnisse als mit der Verfassung vereinbar ansieht[113], wenn durch einschränkende gesetzliche Formulierungen Sorge getragen wird, dass Maßnahmen nicht auf Grundlage bloßer Vermutungen und von allgemeinem Erfahrungswissen, das auf die Begehung terroristischer Straftaten hindeutet, getroffen werden.

Hierfür hat das *Gericht* dem Gesetzgeber gewissermaßen Hilfestellung geleistet, indem es eine Art Korridor vorgab, der bei der gesetzgeberischen Formulierung von Eingriffsschwellen Anhaltspunkte geben kann. Dass sich das *Gericht* mit den in Rn. 112 getätigten Ausführungen als „Ersatzgesetzgeber" zeigen wollte, ist nicht anzunehmen; hierfür sind die Ausführungen des Gerichts zu ausfüllungsbedürftig[114].

Vielmehr ist der Gesetzgeber (natürlich!) selbst berufen, eine normenklare Umsetzung der Vorgaben zu realisieren.[115]

Der Einwand, dass „*niemand ernstlich vom Gesetzgeber verlangen* [könne], *dass er klüger ist als das BVerfG, wenn dieses in seinen Urteilsgründen bewusst Leitsätze für die zulässige Fassung von Vorfeldtatbefugnissen formuliert*" [116], überzeugt nicht. Das *Gericht* hat deutlich darauf hingewiesen, dass der Gesetzgeber die Prognoseanforderungen hinreichend bestimmt auszugestalten hat [117]. Eine schlichte Übernahme höchstrichterlicher Entscheidungsgründe im Sinne einer „Copy&Paste"-Gesetzgebung ist nicht ausreichend. Der Gesetzgeber muss den ihm vorgegebenen Rahmen eigenständig durch hinreichend normenklare und verständlich formulierte Tatbestandsmerkmale ausfüllen:

> „*Nach den oben dargelegten Maßstäben ist der Gesetzgeber hieran nicht grundsätzlich gehindert und zwingt ihn die Verfassung nicht, Sicherheitsmaßnahmen auf die Abwehr von -- nach tradiertem Verständnis --*

---

[112] Auf etwaige Inkonsistenzen weist etwa *Möstl*, BayVBl. 2018, 156 (157 f.), hin.

[113] Vgl. *Möstl*, BayVBl. 2018, 156 (158)

[114] Anders etwa als in der Entscheidung zur Online-Durchsuchung; BVerfGE 120, 274 LS 2, in der die Eingriffsschwellen mit Hilfe tradierter gefahrenabwehrrechtlicher Begrifflichkeiten (leicht) modifiziert wurden, sodass im Ergebnis kein gesetzgeberischer Gestaltungsspielraum mehr bestand, gab das *BVerfG* in seinem BKA-Urteil nur einen groben Rahmen vor.

[115] So auch die Einschätzung von Vorlage 32 des Gesetzgebungs- und Beratungsdienstes im Landtag Niedersachsen vom 26.10.2018, 81/85/891/1179-85, S. 17; *Gazeas*, Stellungnahme 17/945, S. 13; *Löffelmann*, BayVBl. 2018, 145 (148).

[116] *Möstl*, BayVBl. 2018, 156 (159).

[117] BVerfG, Urt. v. 20.04.2016 - 1 BvR 966/09 –Rn. 164.

> *konkreten Gefahren zu beschränken. Allerdings bedarf es aber auch bei Maßnahmen zur Straftatenverhütung zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist (vgl. BVerfGE 110, 33 [56 f., 61]; 113, 348 [377 f.]; 120, 274 [328 f.]; 125, 260 [330]). In Bezug auf terroristische Straftaten kann der Gesetzgeber stattdessen aber auch darauf abstellen, ob das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft terroristische Straftaten begeht (siehe oben C IV 1 b).* ***Die diesbezüglichen Anforderungen sind normenklar zu regeln.***"[118]

Das ist nicht geschehen.

Was mit den Formulierungen in § 20c Abs. 1 Nr. 2 PolG NRW – gemeint sein soll, ist nicht nachvollziehbar. [119] Welches „*individuelle Verhalten*" genau soll die „*konkrete Wahrscheinlichkeit*" dafür begründen, dass künftig eine Straftat begangen werden soll? Und was bedeutet „*innerhalb eines übersehbaren Zeitraums*"? Es ließen sich unter diesen Wortlaut Zeiträume von mehreren Monaten bis hin zu einigen Jahren subsumieren[120].

Es bleibt schon unklar, für welche praktischen Fallkonstellationen die Normen geschaffen wurden. Das *Gericht* hat hier zwar grobe Anhaltspunkte gegeben: Nicht vom eingriffseröffnenden Tatbestand wäre etwa ein bloßes fundamentalistisches Religionsverständnis des Betroffenen erfasst, währenddessen Überwachungsmaßnahmen gerechtfertigt sein könnten, wenn eine Person aus einem terroristischen Ausbildungslager im Ausland in die Bundesrepublik Deutschland zurückkehrt.[121]

Zur weiteren Erhellung trägt der Gesetzgeber, was seine Aufgabe gewesen wäre, indes nicht bei. Er belässt es bei der unreflektierten Übernahme von Leitsätzen des *Gerichts* und

---

[118] BVerfGE 141, 220 (290 f. – Rn. 164) – Hervorhebung nur hier; darauf weist – unter Benennung von möglichen Lösungsansätzen ausdrücklich *Gazeas*, Stellungnahme 17/945, S. 13f. sowie Stellungnahme 17/662, S. 16 hin.

[119] Kritisch Vorlage 32 des Gesetzgebungs- und Beratungsdienstes im Landtag Niedersachsen vom 26.10.2018, 81/85/891/1179-85, S. 27; vgl. ferner instruktiv *Löffelmann*, BayVBl. 2018, 145, 148; *Gazeas*, Stellungnahme 17/945, S. 12 f.

[120] *Gazeas*, Stellungnahme 17/945, S. 13.

[121] BVerfGE 141, 220 (272 f.).

unternimmt nicht einmal in der Gesetzesbegründung den Versuch Inhalt und Reichweite der gesetzlichen Regelungen auszuloten.

bb) Unverhältnismäßiger Rechtsgüterschutz: Straftatenkatalog in § 8 Abs. 4 PolG NRW

Insbesondere ist auch der durch § 20c Abs. 1 Nr. 2 PolG NRW in Bezug genommene Straftatenkatalog in § 8 Abs. 4 PolG NRW sowohl in seiner Weite als auch als solches zu unbestimmt. Die bezugnehmende Regelung ist wie der § 8 Abs. 4 PolG NRW selbst daher (auch) aus diesem Grund verfassungswidrig.

(1) Zu weite und unbestimmte Fassung des Straftatenkatalogs

(a) Grundlegende Problematik

Die gesetzestechnische Inbezugnahme von Straftatenkatalogen ist bei polizeilichen Vorfeldbefugnissen ungeeignet. Die Prognose der künftigen Begehung von Straftaten – also die Anknüpfung an strafrechtliche Wertungen, anstelle eines schutzgutbezogenen Ansatzes – ist notwendig unscharf und – wie hier – regelmäßig unbestimmt.

So hat das *Gericht* in seiner Entscheidung zur niedersächsischen Telekommunikationsüberwachung festgestellt[122]:

> „*Bei der Vorverlagerung des Eingriffs in eine Phase, in der sich die Konturen eines Straftatbestandes noch nicht abzeichnen, besteht das Risiko, dass der Eingriff an ein nur durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichnetes, in der Bedeutung der beobachteten Einzelheiten noch schwer fassbares und unterschiedlich deutbares Geschehen anknüpft. Sachverhaltsfeststellung und Prognose sind mit vorgreiflichen Einschätzungen über das weitere Geschehen, ebenso wie über die erst noch bevorstehende strafrechtliche Relevanz der festgestellten Tatsachen verknüpft (vgl. BVerfGE 110, 33 [59]). Da der Eingriff sich auf mögliche zukünftige Aktivitäten bezieht, kann er sich häufig nur auf Tatsachen stützen, bei denen noch offen ist, ob sie sich zu einer Rechtsgutverletzung weiterentwickeln (vgl. BVerfGE 110, 33 [59]). Die Situation der Vorfeldermittlung ist insofern durch eine hohe Ambivalenz der potenziellen Bedeutung einzelner Verhaltensumstände geprägt. Die Indizien oder einzelne beobachtete Tätigkeiten können in harmlosen, strafrechtlich unerheblichen Zusammenhängen verbleiben; sie können aber auch der Beginn eines Vorgangs sein, der zur Straftat führt. Sieht der Gesetzgeber in solchen Situationen Grundrechtseingriffe vor,* ***so hat er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die***

[122] BVerfGE 113, 348 (377 f.).

> ***künftige Begehung hindeuten, so bestimmt zu umschreiben, dass das im Bereich der Vorfeldermittlung besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar ist****. Die Norm muss handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist (vgl. BVerfGE 110, 33 [56])".*

Zuzustimmen ist insb. dem *Thüringischen Verfassungsgerichtshof*[123]:

> *„Das Gebot der Normenklarheit und Bestimmtheit setzt dem Gesetzgeber enge Grenzen, bei der Regelung präventiver polizeilicher Befugnisse auf einen Straftatenkatalog zu verweisen.* ***Der Charakter der Gefahrenabwehr als Rechtsgüterschutz verlangt, dass bei der Normierung von Grundrechtseingriffen die zu schützenden Rechtsgüter und die Intensität ihrer Gefährdung in den Blick genommen werden.*** *Nur so lässt sich sicherstellen, dass die polizeilichen Befugnisse im Einzelnen gerechtfertigt sind und zu dem erstrebten Erfolg nicht außer Verhältnis stehen.* ***Durch einen Verweis auf einen Straftatenkatalog geht dieser Zusammenhang zwischen Grundrechtseingriff und Rechtsgüterschutz weitgehend verloren.*** *Zudem ist die Bezugnahme auf Strafrechtsnormen regelmäßig* ***keine geeignete Regelungstechnik****, um einen Sachverhalt unter dem Gesichtspunkt der Gefahrenabwehr zu erfassen. Straftatbestände legen fest, ob ein in der Vergangenheit liegendes, fest umrissenes Verhalten einer bestimmten Person strafbar ist oder nicht. Im Bereich der Gefahrenabwehr hat die Polizei dagegen aus der Beobachtung von Einzelheiten, die oft diffus sind, auf die Gefährlichkeit eines noch nicht klar erkennbaren zukünftigen Geschehens zu schließen.* ***In diesem Stadium sind strafrechtliche Tatbestandsmerkmale ungeeignet, die Voraussetzungen eines polizeilichen Einschreitens festzulegen.*** *Dies gilt in besonderem Maß, wenn die Strafrechtsnormen auf weitere Vorschriften Bezug nehmen. Eine solche Verweisungskette erschwert es, die maßgeblichen Tatbestandsmerkmale zu erkennen und diese den beobachteten Tatsachen zuzuordnen. Gerade bei Überwachungsmaßnahmen unter Zeitdruck besteht ein hohes Risiko, dass sich die Handelnden keine Rechenschaft mehr darüber geben, ob sich die beobachteten Indizien auf konkrete Straftatbestände beziehen lassen. Hinzu kommt, dass hier gefahrenabwehrrechtliche Zielsetzungen verfolgt werden, die einen Bezug auf*

[123] VerfGH Thüringen, Urteil v. 21.11.2012 - VerfGH 19/09 = ZD 2013, 79 (84) m. Anm. von *Petri* und *Popp*.

> *strafrechtliche Beurteilungen problematisch machen, soweit bereits der Versuch oder die Vorbereitungshandlung selbst strafbar ist."*

Vor diesem Hintergrund ist der durch § 20c Abs. 1 Nr. 2 PolG NRW in Bezug genommene Katalog „terroristischer" Straftaten in § 8 Abs. 4 PolG NRW zum einen in Teilen zu weit gefasst. Zum anderen sind die subjektiven und objektiven Anforderungen, die § 8 Abs. 4, 2. HS PolG NRW formuliert, unbestimmt gefasst, ermöglichen keine handhabbare Eingrenzung der Gefahrenprognose auf die Begehung nur schwerer terroristischer Straftaten und eröffnen dem Normanwender einen unangemessen weiten Spielraum bei der Qualifizierung „terroristischer Straftaten", die es durch die streitgegenständlichen Normen zu verhindern gilt. Insgesamt ist kein nachvollziehbares gesetzgeberisches Konzept erkennbar, das sich bei der Aufgabe der Terrorismusbekämpfung unter Einbeziehung der gegenwärtigen Gefährdungslage um eine sinnhafte Balance von Freiheits- und Sicherheitsinteressen bemüht.

(b) Weite der einbezogenen Straftatbestände

Der Gesetzgeber verfolgt ausweislich der Gesetzbegründung das Ziel der Bekämpfung schwerer Formen des Terrorismus, namentlich des „internationalen Terrorismus", womit augenscheinlich islamistische Bestrebungen, etwa solche des sog. Islamischen Staates, gemeint sind[124]. Diesem gesetzgeberischen Anliegen wird der Straftatenkatalog des § 8 Abs. 4 PolG NRW, der unter anderem in § 20c Abs. 1 Nr. 2 PolG NRW in Bezug genommen wird, nicht gerecht.

§ 8 Abs. 4 PolG NRW ist an der Norm des § 129a StGB orientiert formuliert. § 129a StGB normiert indes die Strafbarkeit terroristischer *Vereinigungen*; der Straftatbestand ist nach den Anschlägen des 11. September 2001 stark erweitert worden[125] und erfasst – in verfassungsrechtlich bedenklich unbestimmter Fassung[126] – auch minder schwere Fälle

---

[124] NRW LT-Drs. 17/2351, S. 1.

[125] Das „Gesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union v. 13.6.2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze" v. 20.12.2003 (BGBl. I 2836) hat die mit Gesetz v. 18.08.1976 (BGBl. I 2181) in das StGB eingefügte Norm grundlegend umgestaltet und um zahlreiche Anlasstatbestände in § 129a Abs. 2 StGB erweitert. Nach der Neufassung genügt es insoweit nicht mehr, dass die Zwecke oder Tätigkeit der Vereinigung auf die Begehung der in § 129a Abs. 2 StGB genannten Straftaten gerichtet sind. Vielmehr muss hinzukommen, dass *„eine der […] Taten bestimmt ist, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen kann."*

[126] *Pollähne*, KritJ 2005, 292 (310); *Weigend*, Terrorismus als Rechtsproblem, in: Griesbaum/Hannich/Schnarr (Hrsg.), Strafrecht und Justizgewährung: FS für *Kay Nehm*, 2006, S. 151, 164 f.

terroristischer Bestrebungen, die weit unterhalb des Niveaus liegen, das Fällen islamistischen Terrors gewöhnlich innewohnt. Auch weniger „gefährliche" Zusammenschlüsse z.B. aus dem Bereich des linksaktivistischen Spektrums werden erfasst (vgl. die unter D.II.2.a.bb)(2) genannten Beispiele aus der Rechtsprechung). Ein gefahrenvorsorgendes Konzept gerade gegen Fälle des „internationalen Terrorismus", wie ihn der Gesetzgeber vor Augen hat, konnte durch die vollständige Übernahme der in § 129a StGB genannten Straftaten nicht geschaffen werden.

Auch lässt der Gesetzgeber außer Acht, dass die Strafbarkeit des § 129a StGB gerade von der Manifestierung eines verbrecherischen „Gruppenwillens" abhängt – Strafbarkeit der Gründung einer *Vereinigung*, deren Zwecke oder Tätigkeit darauf gerichtet sind, bestimmte Straftaten zu verüben. Diese Gruppenbetätigung, die eine besondere Gefährlichkeit aufgrund planvollen gemeinsamen Vorgehens indiziert, mag auch die Einbeziehung weniger schwerer Straftaten rechtfertigen, wie sie § 129a Abs. 2 StGB aufführt. Für diese „minder schweren" Straftaten des § 129a Abs. 2 StGB reicht es in im Gegensatz zu den besonders schweren in § 129a StGB genannten Straftaten allein nicht aus, dass sie Betätigungszweck einer Vereinigung sind. Zusätzlich sind strafbegründend besondere subjektive und objektive Merkmale erforderlich, die in § 129a Abs. 2, 2. HS StGB formuliert sind[127].[128]

Diese für die Strafnorm des § 129a StGB nachvollziehbare konzeptionelle Struktur gibt § 8 Abs. 4 PolG NRW auf. Angezeigt ist es zwar, nicht auf das Merkmal einer „Vereinigung" abzustellen. Freilich hätten dann nur Straftaten in Bezug genommen werden dürfen, deren Schwere und Gewicht auch dann im Gefahrenvorfeld eingriffsintensive Maßnahmen der Terrorismusbekämpfung rechtfertigen, wenn sie nicht auch von einem inkriminierten Gruppenwillen getragen sind. Naheliegend wäre es etwa gewesen, im Schwerpunkt lediglich auf die in § 129a Abs. 1 StGB genannten Straftaten abzustellen. Das sind: Mord (§ 211 StGB), Totschlag (§ 212 StGB), Völkermord (§ 6 des Völkerstrafgesetzbuches), Verbrechen gegen die Menschlichkeit (§ 7 des Völkerstrafgesetzbuches), Kriegsverbrechen (§§ 8, 9, 10, 11 oder § 12 des Völkerstrafgesetzbuches) und Straftaten gegen die persönliche Freiheit in den Fällen des § 239a oder des § 239b StGB. Hätte man diesen Straftatenkatalog ggf. um noch *ausgewählte* Verstöße des

[127] Vgl. *Schäfer*, in: Miebach (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, § 129a Rn. 43 m.w.N.
[128] Erforderlich ist, dass „*eine der Taten bestimmt ist, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen kann.*"

Kriegswaffenkontrollgesetzes oder des Waffengesetzes ergänzt (vgl. § 129a Abs. 2 Nr. 5 und 6 StGB), wären die in der Gesetzesbegründung angesprochenen schweren Fälle des internationalen Terrorismus lückenlos erfasst gewesen.

Das ist aber nicht geschehen. Vielmehr wurden umfassend *alle* in § 129a Abs. 2 StGB genannten Straftaten übernommen. Das ist nicht sachgerecht und in seiner Weite unverhältnismäßig.

Allein die Vergehenstatbestände der §§ 303b, 305, 317 StGB führen im Vergleich zu den anderen aufgeführten Taten zu bedenkenswerten *Strafrahmenfriktionen*[129]. Wie *Arzt* treffend feststellt, sind in § 8 Abs. 4 PolG NRW Katalogstraftaten genannt, die den erforderlichen Schutz hochrangiger Rechtsgüter nicht abbilden[130]: Etwa „*die Zerstörung eines Kraftfahrzeuges der Polizei oder Bundeswehr (§ 305a StGB) und sogar der Versuch derselben, die Störung öffentlicher Betriebe (§ 316b StGB), zum Beispiel durch Beschädigung einer hierzu gehörenden Sache auch im Falle von Postdienstleistungen oder dem Verkehr, also z.B. der Diebstahl von Kupferkabeln bei der S-Bahn oder das Anzünden eines Fahrzeuges der Deutschen Post; auch hier ist bereits der Versuch strafbar. Hierzu gehört ferner sogar die Zerstörung eines Telefonverteilerkastens nach § 317 Abs. 1 StGB wie auch der Versuch*".

Der Straftatenkatalog des § 8 Abs. 4 PolG NRW ist unverhältnismäßig ausufernd.

Zudem gibt der Gesetzgeber zu erkennen, dass ihm strafrechtliche Wertungen weitgehend fremd sind, wenn er im Vergleich zu § 129a StGB den Straftatenkatalog in § 8 Abs. 4 Nr. 1 PolG NRW mit der Inbezugnahme von § 227 StGB (Körperverletzung mit Todesfolge) sogar partiell erweitert. Die Aufnahme dieses Straftatbestandes ist so *völlig unsinnig*, dass die Vermutung naheliegt, dass sich der Gesetzgeber nicht bewusst gemacht hat, welche Prognoseleistungen bei der Verhütung terroristischer Straftaten vom Normanwender zu erbringen sind. Körperverletzung mit Todesfolge ist ein erfolgsqualifiziertes Delikt. Der Vorsatz des Täters darf sich nur auf das Grunddelikt, nicht auf die Todesfolge erstrecken[131], weil sonst ein Tötungsverbrechen vorliegt und keine erfolgsqualifizierte Körperverletzung. D.h., dass bzgl. der Todesverursachung zwingend Fahrlässigkeit vorliegen muss. Dies bei noch nicht ins Versuchsstadium gelangten Delikten zu prognostizieren, ist *völlig unmöglich, da zu diesem Zeitpunkt dem potentiellen Täter selbst noch nicht bewusst*. Eine Strafbarkeit nach § 227 StGB setzt zudem zwingend voraus, dass ein Mensch stirbt. Entweder durch eine vorsätzlich begangene

[129] *Fischer*, StGB, 66. Aufl. 2019, § 129a Rn. 10; ebenso *Sternberg-Lieben/Schittenhelm, in:* Schönke/Schröder (Hrsg.), StGB, 30. Aufl. 2019, § 129a Rn. 2a f.
[130] *Arzt*, Stellungnahme 17/936 LT-Drs. S. 5.
[131] BGHSt 2, 223 (225).

Körperverletzung mit fahrlässiger Todesfolge oder – in seltenen, aber nach der Rechtsprechung des *BGH* möglichen Fällen, in denen die Körperverletzung im Versuchsstadium stecken bleibt, aber das Opfer verstirbt (sog. erfolgsqualifizierter Versuch) [132] . Unmöglich ist dagegen ein Versuch der Erfolgsqualifikation, da die Qualifikation nur fahrlässig verursacht sein kann. Der Tötungsversuch wird nämlich durch §§ 211 f., 22 StGB erfasst, die §§ 227, 22 StGB verdrängen. Das bedeutet, dass zum Zeitpunkt der polizeilichen Prognose, der potentielle Täter den Tod des Opfers – der sicher sein muss! – nicht wollen darf und Vorsatz nur hinsichtlich einer etwaigen Körperverletzung bestehen darf. Prognosen in Bezug auf die subjektive Vorstellung eines mutmaßlichen Täters im Gefahrenvorfeld in diese Richtung anstellen zu wollen, ist abwegig.

(c) Untaugliches, da unbestimmtes Korrektiv in § 8 Abs. 4, 2. HS PolG NRW

§ 8 Abs. 4 PolG NRW verlangt für alle dort aufgeführten Straftaten, dass diese „*dazu bestimmt sind, die Bevölkerung auf erhebliche Weise einzuschüchtern, eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen, und sie durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen können*“. Dieser Passus ist wortlautgleich mit § 129a Abs. 2, 2. HS StGB. Zweck der Regelung in § 129a Abs. 2 StGB ist es, die dort in Bezug genommenen, im Vergleich zu den in § 129a Abs. 1 StGB aufgeführten „minderschweren“, Straftaten auf ein zumindest vergleichbares Niveau zu heben[133]. Dass der betreffende Passus in § 8 Abs. 4 PolG NRW sich, unabhängig von ihrer Schwere, auf alle dort genannten Straftaten bezieht, schadet zunächst nicht.

Allerdings ist die Regelung zu unbestimmt gefasst um ihren Zweck zu erfüllen; jedenfalls, wenn eine prospektive Beurteilung der Straftatenbegehung in Rede steht.

Die Qualifizierung als spezifisch terroristische Straftat in § 8 Abs. 4, 2. HS PolG NRW schränkt die eingriffseröffnende Prognose durch zwei zusätzliche Anforderungen an die

[132] BGHSt 48, 34 (37 f.).

[133] *Schäfer*, Miebach (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, § 129a Rn. 43: „*Abs. 2 StGB verlangt für die Strafbarkeit der Organisationstat eine besondere Bestimmung und Eignung der Taten, auf welche die Zwecke oder die Tätigkeit der Vereinigung gerichtet sind. Mit diesen Erfordernissen soll, weil die Katalogtaten des Abs. 2 in ihrer Schwere deutlich hinter denen des Abs. 1 zurückbleiben, ein Gleichgewicht hergestellt werden.*“

beabsichtigten Straftatenbegehung ein, nämlich einer subjektiven („*bestimmt ist …*“) und einer objektiven („*schädigen kann …*“).[134]

(aa) Subjektive Einschränkung: „Besondere Bestimmung der Taten“

Benannt wird das Ziel, die Bevölkerung auf erhebliche Weise einzuschüchtern (1. Alt.), eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder mit Drohung mit Gewalt zu nötigen (2. Alt.) oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen (3. Alt.).

Diese Fülle *unbestimmter Rechtsbegriffe* führt dazu, dass dieser Teil der Vorschrift sowohl unter Bestimmtheitsgesichtspunkten als auch hinsichtlich der Anwendung der Norm in der Praxis besonders problematisch ist[135]. Dies gerade deswegen, weil diese Merkmale auf europäischen Regelungen beruhen, die im deutschen materiellen Strafrecht keine Entsprechung aufweisen[136]; die Gesetzesmaterialien schweigen sich zur Auslegung aus.

Im Strafrecht (§ 129a Abs. 2 StGB) dominiert eine weitgehend am konkreten Einzelfall orientierte Betrachtung, welche quantitativen und qualitativen Voraussetzungen erforderlich sind, damit eines der Ziele des § 129a Abs. 2 StGB bejaht werden kann[137]. Für eine retrospektive Betrachtung mag dies zielführend sein. Wie die kaum bestimmbaren subjektiven Voraussetzungen *prospektiv* bei unklarer Tatsachenlage im Rahmen der Straftatenverhütung fassbar gemacht werden können, ist indes ungeklärt. Die einzelfallorientierte Rechtsprechung zu § 129a StGB gibt nicht viel her. Die Fallzahlen sind bislang äußerst überschaubar.[138]

(bb) Objektive Einschränkung: „Besondere Schädigungseignung“

Daneben wird in § 8 Abs. 4, 2. HS PolG NRW in objektiver Hinsicht gefordert, dass eine Katalogtat eine *besondere Gefährlichkeit* aufweist, indem sie *durch die Art ihrer Begehung oder ihre Auswirkungen einen Staat oder eine internationale Organisation erheblich schädigen kann*. Mit diesem für sich genommen wenig aussagekräftigen Merkmal wird

---

[134] BGH NStZ-RR 2008, 305 (306).

[135] *Pollähne*, KritJ 2005, 292 (310); *Weigend*, Terrorismus als Rechtsproblem, in: Griesbaum/Hannich/Schnarr (Hrsg.), Strafrecht und Justizgewährung: FS für *Kay Nehm*, 2006, S. 151, 164 f.; *Fischer*, StGB, 66. Aufl. 2019, § 129a Rn. 17.

[136] *Schäfer*, in: Miebach (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, § 129a Rn. 46.

[137] *Schäfer*, in: Miebach (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, § 129a Rn. 46.

[138] *Schäfer*, in: Miebach (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, § 129a Rn. 5., berichtet: „*Gem. § 129a verurteilt wurden 2008: 5, 2009: 3, 2010: 4, 2011: 3, 2012: 6, 2013: 2 und 2014: 4 Täter. Ein Schwerpunkt der Ermittlungsverfahren nach § 129a betrifft mittlerweile den Bereich des islamistischen Terrorismus*“.

entweder auf die Durchführung oder die Folgen der Straftat abgestellt; nicht erforderlich ist, dass ein Schaden konkret eintritt[139]. Vielmehr soll genügen, dass die Straftat im Falle ihrer Ausführung – unmittelbar oder durch ihre Auswirkungen – konkret geeignet ist, den besagten Schaden für den Staat herbeizuführen. Hierfür ausreichend ist die realistische Möglichkeit, dass der Schaden *nach den Umständen der vorgestellten Tatbegehung* eintritt; eine – unter Umständen erhöhte – Wahrscheinlichkeit ist nicht erforderlich[140]. Wie aber sollen die „*Umstände der vorgestellten Tatbegehung*" im Gefahrenvorfeld fassbar gemacht werden?

Die Bestimmung eines „Schadens" bei einem Staat oder einer internationalen Organisation ist im Übrigen nicht einfach, da nach dem Wortlaut der Norm unklar bleibt, welche Erfolge der Schädigungshandlung erfasst sind. Die Rechtsprechung hat sich unter Verweis auf den Willen des Gesetzgebers zu einer restriktiven Interpretation entschlossen und steht insbesondere der Einbeziehung von bloßen Vermögensschäden kritisch gegenüber[141]. Im Übrigen *entzieht sich dieses Merkmal einer abstrakten Beschreibung*. Maßgebend sind vielmehr die Umstände des Einzelfalls, die umfassend abgewogen werden müssen[142]. Zu berücksichtigen wären etwa das Ausmaß und die Kontrollierbarkeit der Bedrohungslage sowie die „öffentliche Resonanz"[143].

(2) Präventiver Kontext

Wie in Bezug auf eine Tat, die noch nicht begangen worden ist, sondern verhütet werden soll, beurteilt werden kann, ob sie die bezeichneten subjektiven und objektiven Voraussetzungen erfüllt, erschließt sich nicht[144]. Die Beurteilung, ob die Taten die erforderliche „besondere Bestimmung" aufweisen und vor allem, ob sie die notwendige besondere Schädigungseignung haben, dürfte häufig von den zur Zeit der Gefahrenabwehrmaßnahme noch gar nicht bekannten Umständen abhängen. Zwar verlangt auch der Straftatbestand des § 129a StGB ähnliche Prognoseleistungen. Hier besteht allerdings die zusätzliche Einschränkung, dass die Gründung einer Vereinigung mit entsprechender Zielsetzung bezweckt sein muss. Zudem erfolgt die Beurteilung der

[139] BGHSt 52, 98 (105) = NJW 2008, 86 (89); *Helm* StV 2006, 719 (722).

[140] BGHSt 52, 98 (102) = NJW 2008, 86 (88).

[141] BGH NStZ 2008, 146 (148); BGH NJW 2008, 86 (90).

[142] BGHSt 52, 98 (105) = NJW 2008, 86 (89).

[143] *Schäfer*, in: Miebach (Hrsg.), Münchener Kommentar zum StGB, 3. Aufl. 2017, § 129a Rn. 52.

[144] Ähnlich Kritik beim Gesetzgebungs- und Beratungsdienst des Niedersächsischen Landtags, Vorlage 32 vom 26.10.2018 zu Drs. 18/850, S. 7.

Strafbarkeit, nachdem der zu Grunde liegende Sachverhalt ausermittelt wurde. Häufig wurden auch schon Anlasstaten verübt, die eine sicherere Beurteilung ermöglichen[145].

Aber schon retrospektiv begegnen den bezeichneten Anforderungen immense verfassungsrechtliche Bedenken. So stellen *Miebach/Schäfer*[146] zu § 129a StGB fest:

> „*Die Norm ist insgesamt fraglos noch komplexer, differenzierter und durch die Einfügung zahlreicher nur schwer eindeutig bestimmbarer Rechtsbegriffe vor allem in Abs. 2 sicherlich in der Praxis nicht einfacher handhabbar geworden. Daneben erreicht die Tatbestandsgestaltung des Abs. 2 n.F. und dabei insb. die auffällige Häufung jeweils für sich genommen bereits nur mühevoll eingrenzbarer unbestimmter Rechtsbegriffe den* ***Grenzbereich des hinsichtlich des verfassungsrechtlichen Bestimmtheitsgebots noch Zulässigen****. Dieser Umstand fällt umso stärker ins Gewicht, als die Norm Anknüpfungspunkt zahlreicher Ermittlungsmaßnahmen mit teilw. erheblicher Eingriffsintensität ist.*"

Auch im übrigen Schrifttum wird die hinreichende Bestimmtheit der Norm bezweifelt.[147] Nach hier vertretener Auffassung ist die Unbestimmtheit aufgrund der Häufung unbestimmter Rechtsbegriffe und der teilweise schwer durchschaubaren Kombination von objektiven und subjektiven Elementen – die in § 8 Abs. 4 PolG NRW übertragen wurde - evident.

Dies mögen folgende Beispiele illustrieren: Angenommen, polizeiliche Kräfte finden den Prognoseanforderungen der § 20c Abs. 1 Nr. 2 PolG NRW entsprechend heraus, dass (**1.**) Rechtsextremisten gezielt Brandanschlägen gegen Geschäftsobjekte von Ausländern verüben wollen, um diese erheblich einzuschüchtern und aus einem bestimmten Teilgebiet der Bundesrepublik Deutschland zu vertreiben und (**2.**) Linke Aktivisten einen anstehenden Wirtschaftsgipfels stören und mittels Brandanschlägen gegen Gebäude und Fahrzeuge Gesinnungsgenossen mobilisieren wollen. Kann – wenn eine gegenwärtige Gefahr i.S.d. § 20c Abs. 1 Nr. 1 PolG NRW verneint werden muss – eine Telekommunikationsüberwachung oder gar eine Quellen-

---

[145] Vgl. etwa die Sachverhalte, die folgenden Entscheidungen des BGH zu Grunde liegen, NJW 2006, 1603; NStZ 2008, 146 ff. und NJW 2008, 86 ff.

[146] in: Joecks/Miebach, Münchener Kommentar zum StGB, Bd. 2/2, 2005, § 129a Rn. 18 – Hervorhebung im Original.

[147] Vgl. *Hawickhorst*, § 129a StGB - Ein feindstrafrechtlicher Irrweg zur Terrorismusbekämpfung, 2011, S. 175 ff; 198 ff.; *Weigend*, Terrorismus als Rechtsproblem, in: Griesbaum/Hannich/Schnarr (Hrsg.), Strafrecht und Justizgewährung: FS für *Kay Nehm*, 2006, S. 151, 164 f.; *Fischer*, StGB, 66. Aufl. 2019, § 129a Rn. 17.

Telekommunikationsüberwachung auf Basis von § 20c Abs. 1 Nr. 2 PolG NRW angeordnet werden?

Auf den ersten Blick scheint dies grundsätzlich in beiden Fällen möglich. Es stehen jeweils Straftaten nach § 8 Abs. 4 PolG NRW in Rede, zumindest die dort genannten Brandstiftungsdelikte. Auch die erforderlichen subjektiven, wie objektiven Voraussetzungen ließen sich begründen.

Allerdings differenziert die Rechtsprechung, namentlich der *BGH* in den besagten Fällen feinsinnig zwischen „terroristischem" und bloß „militantem" Tatgeschehen[148]. Nur im zuerst genannten Fall läge die erforderliche *objektive Schadenseignung* einer spezifisch terroristischen Straftat vor („*Geeignetheit* der Tat durch die Art ihrer Begehung oder ihre Auswirkungen einen *Staat* oder eine internationale Organisation *erheblich schädigen zu können*"). Begründet wird die erforderliche Schadenseignung der rechtsextremistisch motivierten Brandanschläge mit deren „*einschneidende[n] Auswirkungen auf die Gesellschaft und das wirtschaftliche Leben*" sowie der „*nachhaltigen und tief greifende[n] Schädigung der inneren Sicherheit, wenn ausländische Mitbürger allein wegen ihrer Herkunft massiv verfolgt werden und sich nicht mehr sicher und geschützt fühlen können*".[149]

Im zweiten Fallbeispiel wurde dagegen die objektive Schädigungseignung der Brandanschläge anlässlich des Weltwirtschaftsgipfels verneint. Diese seien ausschließlich gegen Sachen gerichtet gewesen und würden über ihre Signalwirkung auf Gesinnungsgenossen hinaus *keine ernsthafte Behinderung der staatlichen Tätigkeit bezwecken* und seien deshalb zur Schädigung des Staates nicht geeignet[150].

In einer weiteren Entscheidung hat der *BGH* festgestellt, dass mehrere Brandanschläge (gegen Gebäude und Fahrzeuge staatlicher Institutionen sowie privatwirtschaftlicher Einrichtungen mit einer Gesamtschadenssumme von „nur"[151] 1.000.000 Euro) einer „militanten Gruppe", die diese in Umsetzung „linksextremistischer, gewaltbejahender Ideologie" beging, nicht geeignet sind, um den „*Staat erheblich zu schädigen*" (i.S.d. § 129a Abs. 2 StGB bzw. § 8 Abs. 4 PolG NRW).

[148] Vgl. BGH NJW 2008, 86.
[149] BGH NJW 2006, 1603 (1604).
[150] BGH NStZ 2008, 146 ff.
[151] BGH NJW 2008, 86 (90).

Der *BGH* selbst weist in seinen Entscheidungen darauf hin, dass „*das objektive Element ‚einen Staat erheblich schädigen zu können', für sich ohne Konturen und wenig aussagekräftig"* ist.[152]

Das „objektive" Merkmal der Geeignetheit einer Straftat, den *Staat erheblich zu schädigen*, ist letztlich also völlig ungeeignet, eine Straftat als spezifisch terroristische zu qualifizieren; jedenfalls, wenn es, wie hier, nicht an besonders schwere Straftatbestände anknüpft. Die betreffende Schädigungseignung ist *Einfallstor für eine stark wandelbare, vom jeweiligen politischen Vorverständnis geprägte Entscheidungsfindung*, die in der hochproblematischen Unterscheidung zwischen terroristisch motivierten Straftaten und bloßem „militanten" Taggeschehen gipfelt. Prospektive Einschätzungen hierzu treffen zu wollen ist mit weiteren Unabwägbarkeiten verbunden, die eingriffsintensive grundrechtsverkürzende Maßnahmen nach § 20c Abs. 1 oder 2 PolG NRW nicht rechtfertigen können.

Letztlich führen die in § 8 Abs. 4 PolG NRW in Bezug genommenen allenfalls mittelschweren Straftaten in Kombination mit unzureichend bestimmbaren subjektiven und objektiven Kriterien, die die besagten Straftaten zu spezifisch „terroristischen" machen sollen, zu einer Situation, die es ermöglicht, Angehörige politischer Gruppierungen, deren Tätigkeit auch durch eine gewisse Militanz geprägt ist, mehr oder weniger willkürlich zu terroristischen Gefährdern zu küren und deren Grundrechtsausübung durch Mittel staatlicher Überwachung und Kontrolle bei prospektiv kaum fassbarer Gefahrenlage drastisch einzuschränken.

Dies ist gerade auch den Beschwerdeführern, die der linksaktivistischen Szene angehören bzw. damit enge Kontakte pflegen, nicht zumutbar.

(3) Konzeptionell unzureichende Begegnung terroristischer Gefährdungslagen

Im Nordrhein-Westfälischen Polizeigesetz ist kein gesetzgeberisches Konzept erkennbar, das eingriffsintensive Vorfeldmaßnahmen auf schwere Bedrohungslagen durch den internationalen Terrorismus beschränkt, wie sie das *Gericht* in seiner Entscheidung zum BKAG vor Augen hatte[153].

Durch die Inbezugnahme des verfassungswidrig weit gefassten Straftatenkatalogs in § 8 Abs. 4 PolG NRW, der dem Normanwender aufgrund der Verwendung nahezu inhaltsloser

[152] BGH NJW 2008, 86 (88).
[153] Das ergibt sich etwa aus den illustrierenden Beispielen des Gerichts, BVerfGE 141, 220 (272 – Rn. 112 f.) Dort werden die Einreise aus „einem Ausbildungslager für Terroristen im Ausland" oder ein „fundamentalistischen Religionsverständnis" als potentiell (nicht) anlassgebend für Überwachungsmaßnahmen problematisiert.

Leerformeln unangemessenen Spielraum bei der Kategorisierung spezifisch terroristischer Straftatenbegehung belässt, werden auch aktivistische Protestformen einbezogen, die die tiefgreifenden Überwachungsbefugnisse in § 20c Abs. 1 und 2 PolG NRW nicht rechtfertigen können.

Auch wenn man sich entsprechend der Gesetzesbegründung bei Anwendung der neuen Befugnisse – insbesondere auch der neu geschaffenen „aktionellen Befugnisse" - zur Terrorbekämpfung auf Fälle des internationalen Terrorismus beschränken wollte, so wird doch ein *polizeiliches Befugnisarsenal* geschaffen, das – abhängig vom jeweiligen politischen Vorverständnis – eine unangemessene Ausweitung der Bemakelung als „terroristischer Gefährder" auf politische, religiöse und sonstige (vergleichbar harmlose) Normabweichler mit der Folge drastischer Grundrechtseinschränkungen zulässt.

b. Keine Beschränkung auf „überragend wichtige Rechtsgüter"

Die Durchführung von Maßnahmen die – wie die hier gegenständliche Telekommunikationsüberwachung und Quellen-Telekommunikationsüberwachung - einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme darstellen, darf nur unter der Voraussetzung gestattet werden, dass tatsächliche Anhaltspunkte für eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut vorliegen.[154]

> „*Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.*"[155]

Für alle anderen Rechtsgüter hat das *Gericht* festgehalten:

> „*Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die – wie hier – die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde*

[154] BVerfGE 120, 274 (326, 328); BVerfGE 141, 220 (305).
[155] BVerfGE 120, 274 (326 ff. - Rn. 247).

> *preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken …*“[156]

Der § 20c PolG NRW enthält eine solche Beschränkung auf den Schutz „überragend wichtiger Rechtsgüter“ nicht. Eine (Quellen-)Telekommunikationsüberwachung ist ausweislich § 20c Abs. 1 Nr. 2 PolG NRW bzw. § 20c Abs. 2 i.V.m. Abs. 1 Nr. 2 PolG NRW auch zulässig, wenn das „*individuelle Verhalten*“ des Adressaten bzw. der Zielperson „*die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat nach § 8 Absatz 4 begehen wird*“.

Der § 8 Abs. 4 PolG NRW enthält eine Auflistung einer Reihe von Straftaten die als derartig „terroristische Straftaten“ angesehen werden. Erkennbar handelt es sich – wie bereits soeben ausführlich dargelegt – um eine Übernahme der in § 129a Abs. 1 und 2 StGB genannten Straftaten.

Das Erfordernis der Möglichkeit einer „*existentiellen Bedrohungslage*“ wird bereits im Zusammenhang mit der Auswahl der Straftaten – die, wie dargelegt, zu Teilen nur der mittleren Kriminalität zuzurechnen sind - nicht berücksichtigt:

- So wird beispielsweise auch die „*Störung von Telekommunikationsanlagen*“ (§ 317 Abs. 1 StGB) im Katalog der Straftaten genannt (§ 8 Abs. 4 Nr. 1 PolG NRW). Schutzgut des § 317 StGB – ein abstraktes Gefährdungsdelikt - ist aber die „*Funktionsfähigkeit des öffentlichen Telekommunikationsverkehrs als Universalrechtsgut*“ [157] . An dieser besteht [158] „*besonderes Interesse der Allgemeinheit, um insbesondere familiäre und gesellschaftliche Kontakte zu pflegen, im Notfall erreichbar zu sein, Daten zu übertragen und damit Informationen auszutauschen.*“ Ob eine Störung i.S.d. § 317 StGB bereits – wie vom *Gericht* gefordert - eine (hinreichend konkrete) existentielle Bedrohungslage darstellt, kann auch in den Fällen bezweifelt werden, in denen eine der weiteren

[156] BVerfGE 120, 274 (326 ff. - Rn. 248).
[157] *Wieck-Noodt*, in: Münchener-Kommentar zum StGB, 3. Aufl. 2019, § 317 Rn 1.
[158] So *Wieck-Noodt*, a.a.O. m.w.N.

(unbestimmten – hierzu bereits oben) Voraussetzungen des § 8 Abs. 4 PolG NRW als erfüllt angesehen werden.

- Bezeichnenderweise wäre eine repressive Telekommunikations- oder Quellen-Telekommunikationsüberwachungsmaßnahme zur Aufklärung einer Straftat nach § 317 StGB nicht zulässig, da diese ausweislich § 100a Abs. 2 StPO nicht als schwere Straftat im Sinne des § 100a Abs. 1 StPO angesehen wird. Gleiches gilt für die in § 8 Abs. 4 PolG NRW genannten Straftatbestände (versuchte) Zerstörung wichtiger Arbeitsmittel (§ 305a StGB) sowie die Störung öffentlicher Betriebe (§ 316b StGB).

- Ausdrücklich wird in § 8 Abs. 4 PolG NRW auch der § 315 StGB bei den terroristischen Straftaten „gelistet". Dieser ist nicht nur bei einer Gefährdung von Leib und Leben Dritter, sondern auch bereits bei einer Gefährdung von „fremden Sachen von bedeutendem Wert" einschlägig. Auch hier muss aus der zu verhütenden Straftat keine „existentielle Bedrohungslage" resultieren. Zudem ist insb. auch – in Abweichung zu § 100a Abs. 2 Nr. 1 u StPO – der Abs. 1 sowie der minderschwere Fall nach Abs. 4 aufgeführt.

c. Unbestimmtheit der Rechtsfolge

Insofern der § 20c PolG NRW die „*Überwachung und Aufzeichnung*" der „*Telekommunikation*" gestattet, ist unklar, was hierunter zu verstehen ist. Die Regelung ist unbestimmt und daher verfassungswidrig.

Wie bereits dargelegt wird der Begriff der Telekommunikation in der Praxis offenbar inzwischen dahingehend ausgelegt, dass die Telekommunikationsüberwachung nicht nur die Überwachung von technisch vermittelter „Mensch-zu-Mensch Kommunikation" erfassen soll, sondern auch „Mensch-zu-Maschine"-Kommunikation (z.B. Recherche im Internet) und sogar „Maschine-zu-Maschine"-Kommunikation. Unabhängig davon, dass die hier im Sinne des effektiven Grundrechtsschutzes gebotene weite Interpretation eine Einstufung der Telekommunikationsüberwachung jedenfalls als Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

gebietet, ist dies unter Berücksichtigung des Bestimmtheitsgebotes und der Wesensgehaltslehre verfassungsrechtlich nicht hinnehmbar.

Der Gesetzgeber ist insbesondere bei heimlichen Maßnahmen verpflichtet, der Exekutive nicht nur klar vorzugeben, unter welchen Umständen eine Maßnahme zulässig ist. Er muss auch unzweideutig klarstellen, was der Exekutive bei Vorliegen der gesetzlich festgelegten Voraussetzungen in welchen Grenzen gestattet ist. Das Handeln der Verwaltung muss „*messbar und in gewissem Ausmaß für den Staatsbürger voraussehbar und berechenbar*“ sein.[159]

Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels – der sich anhand der Wandlung des Gesamtcharakters der Telekommunikationsüberwachung eindrücklich zeigt - muss der Gesetzgeber nach ständiger Rechtsprechung des *Gerichts*[160] „*die technischen Entwicklungen aufmerksam beobachten und bei Fehlentwicklungen hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe*“ durch die Exekutive und Judikative „*notfalls durch ergänzende Rechtssetzung korrigierend eingreifen*“. Dies gilt erst recht, wenn eine Befugnis – wie hier – erstmals geschaffen wird.

Diese Vorgabe hat der Gesetzgeber – wenn er (was auch nach Lektüre der Begründung ungeklärt bleibt) nur die Überwachung von technisch vermittelter Individualkommunikation beabsichtigt haben sollte - vorliegend nicht beachtet. Eine Auseinandersetzung mit der Praxis und Rechtsprechung bezüglich der Auslegung des Begriffs „Telekommunikation“ hat zumindest nicht erkennbar stattgefunden.

Eine eindeutige Formulierung der Rechtsfolge wäre möglich gewesen. Möchte der Gesetzgeber lediglich die Überwachung und Aufzeichnung der technisch vermittelten Mensch-zu-Mensch-Kommunikation und nicht der gesamten Telekommunikation im technischen Sinne gestatten, kann er dies – ohne hierbei die Technikoffenheit der Regelung aufzugeben – durch schlichte Klarstellung dahingehend realisieren, dass er

[159] So schon BVerfGE 8, 274 (325).
[160] BVerfGE 112, 304 (316 – Rn. 51); BVerfGE 141, 220 (290 – Rn. 161); BVerfGE 90, 145 (191).

lediglich die „*Überwachung und Aufzeichnung von Individualtelekommunikation*“ gestattet.

Der Begriff Individualkommunikation wird in der Kommunikationswissenschaft als Kommunikationstyp bzw. Kommunikationsform definiert bei der einzelne Individuen miteinander kommunizieren. Individuum wiederum bezeichnet nach dem Duden den „Mensch als Einzelwesen“. Die Einfügung „tele“ verdeutlicht schließlich, dass nicht jedwede, sondern nur die technisch vermittelte Individualkommunikation überwacht und aufgezeichnet werden darf. Soll hingegen sämtliche technisch vermittelte Kommunikation überwacht werden dürfen, könnte dies z.B. durch die Wendung „*Überwachung und Aufzeichnung der gesamten Telekommunikation*“ verdeutlicht werden.

Die Entscheidung, wie umfassend eine „Telekommunikationsüberwachung“ sein darf, darf der Gesetzgeber auch deshalb nicht der Exekutive überlassen, da es einen wesentlichen, einen erheblichen Unterschied mit Blick auf die – in beiden Fällen gegebene – Eingriffsintensität macht, ob „nur“ die technisch vermittelte „Mensch-zu-Mensch-Kommunikation“ oder das gesamte Kommunikationsverhalten einschließlich der Bewegungen und Aktivitäten im Internet und der gesamte Datentransfer auch zu nicht-kommunikativen Zwecken (z.B. Backup von Einzeldateien oder gar des gesamten Systems in der Cloud) überwacht und aufgezeichnet werden darf.

Die derzeitige Regelung ist nach alledem zu unbestimmt und daher verfassungswidrig.

d. Unzureichender Kernbereichsschutz

Die in § 20c Abs. 8 und 9 PolG NRW vorgesehenen Regelungen bleiben verfassungswidrig hinter den verfassungsrechtlichen Anforderungen an die gesetzgeberische Verpflichtung zum Schutz des Kernbereichs privater Lebensgestaltung zurück.

aa) Unzureichender Kernbereichsschutz in der Erhebungsphase

Für die Erhebungsphase bestehen nach dem vorliegenden gesetzgeberischen Regelungskonzept faktisch keine Schutzvorkehrungen, die Eingriffen in den Kernbereich privater Lebensgestaltung wirksam vorbeugen könnten.

§ 20c Abs. 8 Satz 1 PolG NRW läuft völlig leer [161] . Danach ist von einer Telekommunikationsüberwachung als auch einer Quellen-Telekommunikationsüberwachung abzusehen, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie „*allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung"* erlangt werden. Anwendungsfälle, in denen ausschließlich kernbereichsrelevante Telekommunikationsinhalte Gegenstand einer Überwachungsmaßnahme sein könnten, gibt es jedoch bei moderner Telekommunikationsüberwachung nicht. Die entgegenstehende Annahme des *Gerichts*[162] (zum gleichlautenden § 100a Abs. 4 Satz 1 StPO a.F.) ist erkennbar von der Vorstellung getragen, dass eine Telekommunikationsüberwachungsmaßnahme sich stets auf einzelne Akte der Individualtelekommunikation beschränkt. So wird als Beispiel für einen ausschließlichen Kernbereichsbezug die Kommunikation mit engsten Familienangehörigen, Geistlichen, Telefonseelsorgern, Strafverteidigern und Ärzten genannt. „*Soweit ein derartiges Vertrauensverhältnis für Ermittlungsbehörden erkennbar ist, dürfen Maßnahmen der Telekommunikationsüberwachung nicht durchgeführt werden.*" heißt es denn auch in dem Beschluss[163].

Die diesbezüglichen Feststellungen des *Gerichts* sind nicht auf die Telekommunikationsüberwachung heutiger Prägung übertragbar. Diese beschränkt sich gerade nicht mehr auf Individualkommunikation von Mensch zu Mensch. Wie dargelegt ist eine Erfassung kernbereichsrelevanter Inhalte nicht nur am Rande, sondern *typischerweise*, wie bei einer heimlichen Wohnraumüberwachung oder einer Online-Durchsuchung, *zu erwarten*, so dass schon für die Erhebungsphase, ein wirksamer Kernbereichsschutz gesetzlich zu implementieren ist.

Ein Absehen von einer strengeren Regelung ist auf der „Erhebungsebene" *nur dann* zulässig, wenn lediglich „*eine Wahrscheinlichkeit besteht, dass* ***am Rande*** *auch höchstpersönliche Daten* ***miterfasst***"[164] werden.

---

[161] Hierzu *Roggan* HRRS 2013, 153 (154 m.w.N.).
[162] BVerfGE 129, 208 (246 ff.); dagegen *Roggan* HRRS 2013, 153 (155 ff.).
[163] BVerfGE 129, 208 (247).
[164] Vgl. BVerfGE 141, 220 (307 Rn. 220) – zur vergleichbaren Online-Durchsuchung - Hervorhebung nur hier.

Mit Blick auf die oben (A.III) dargestellte Änderung der Nutzungsgepflogenheiten im Umgang mit informationstechnischen Systemen sowie der Ausweitung der Telekommunikationsüberwachung über die technisch vermittelte Individualkommunikation hinaus, hätte es *jedenfalls* einer abgestuften Regelung bedurft:

Auf der Erhebungsebene ist eine Prognose zu erstellen, ob und in welchem Umfang kernbereichsrelevante Daten erfasst werden. Ergibt diese Prognose, dass eine Erhebung kernbereichsrelevanter Daten voraussichtlich in nicht nur unerheblichem Umfang (also nicht nur „*am Rande*") erhoben werden, ist von einer Anordnung und Durchführung der Maßnahme abzusehen. Orientierung kann hier die Regelung in § 18 Abs. 3 PolG NRW geben. Freilich wäre nicht auf die Art der zu überwachenden Räumlichkeiten, sondern vielmehr auf die Art des genutzten Telekommunikationsanschlusses bzw. der genutzten Endgeräte abzustellen. Regelmäßig dürfte bei (auch) privat genutzten Smartphones (bzw. dem entsprechenden Mobilfunkanschluss) oder (auch) privat genutzten Internetzugängen zu prognostizieren sein, dass in ganz erheblichem Umfang kernbereichsrelevante Daten erhoben würden. Ergibt die Prognose hingegen, dass höchstpersönliche Daten doch voraussichtlich nur am Rande erhoben werden (wobei unklar ist, in welchen Fällen dies der Fall sein sollte), wären wirksame Schutzvorkehrungen auf der Stufe der Aus- und Verwertung vorzusehen.

Eine solche Prognoseanforderung enthält § 20c PolG NRW nicht. Im Gegenteil: es ist zu konstatieren, dass der Gesetzgeber nicht einmal die grundlegenden verfassungsrechtlichen Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung umgesetzt hat. Das *Gericht* hat im Zusammenhang mit der verfassungsrechtlichen Bewertung einer Befugnis zur Durchführung einer Online-Durchsuchung festgehalten:

> „*Allerdings ist auch hier vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind,* ***soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt****. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen; können mit deren Hilfe*

> *höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt (vgl. BVerfGE 120, 274 [338])*." [165]

Es ist kein Grund ersichtlich, wieso dies nicht auch für die Telekommunikationsüberwachung moderner Prägung gelten sollte. Gleichwohl findet sich eine solche Vorgabe in der hier angegriffenen Regelung nicht.

Natürlich ist die Wirksamkeit einer derartigen Regelung von künftigen technischen Entwicklungen abhängig. Derzeit ist es „informationstechnisch" nicht möglich im Rahmen einer Telekommunikationsüberwachung ausgeleitete Daten entsprechend zu filtern. Die Frage, ob Informationen zum Kernbereich privater Lebensführung zu rechnen sind oder nicht, setzt einen äußerst komplexen und normativen Abwägungsvorgang voraus, den ein Computerprogramm nicht leisten kann. Mit Blick auf die Rechtsprechung des *Gerichts* ist dies insoweit nicht schädlich, da im Sinne eines Grundrechtsschutzes durch technische Verfahren zunächst nur ein Schutzauftrag besteht, der auf das technisch Mögliche begrenzt ist („*soweit wie informationstechnisch möglich*").

Der Gesetzgeber muss – was hier versäumt wurde - daher zudem sicherstellen, dass diese Verpflichtungen durch erkenn- und nachprüfbare Bemühungen des Normanwenders auch eingehalten werden. Zwingend ist eine explizite Dokumentationspflicht zu normieren, nach der etwaige eingesetzte technische Schutzvorkehrungen in ihrer Funktionsweise und technischen Beschaffenheit zu protokollieren sind; flankiert von einer obligatorischen Kontrollpflicht durch eine unabhängige Stelle (z.B. den oder die jeweiligen Landesbeauftragte(n) für Datenschutz und Informationsfreiheit (i.W. LfDI)) die in die Lage versetzt wird, regelmäßig und engmaschig nachzuprüfen, ob die eingesetzten technischen Schutzvorkehrungen auch dem gegenwärtigen Stand der Technik entsprechen. Nur so kann sichergestellt werden, dass der „technische Kernbereichsschutz" nicht lediglich symbolische, der verfassungsgerichtlichen Rechtsprechung formelhaft Tribut zollende Leerformel bleibt, sondern auch zur praktischen Anwendung kommt.

[165] BVerfGE 141, 220 (307 – Rn. 219).

Zwar sieht § 33b PolG NRW Protokollierungspflichten vor. Diese sind zur Erreichung des Ziels der Sicherstellung des „technischen Kernbereichsschutzes“ jedoch nicht ausreichend. Zu protokollieren ist bei einer Telekommunikations- und Quellen-Telekommunikationsüberwachungsmaßnahme ausweislich § 33b Abs. 1 PolG NRW lediglich „*1. das zur Datenerhebung eingesetzte Mittel, 2. der Zeitpunkt des Einsatzes, 3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen und 4. die Organisationseinheit, die die Maßnahme durchführt.*“. Ergänzend sieht § 20c Abs. 9 Satz 2 PolG NRW vor, dass bei einer Quellen-Telekommunikationsüberwachung nach § 20c Abs. 2 PolG NRW „*1. Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen, nicht nur flüchtigen Veränderungen, 2. Angaben zum Hersteller des zur Datenerhebung eingesetzten Mittels und zur eingesetzten Softwareversion*“ zu protokollieren sind. Eine Pflicht zur Protokollierung der eingesetzten technischen Schutzmechanismen fehlt hingegen. Sie lässt sich auch nicht in die Verpflichtung hineinlesen, zumindest bei der Quellen-Telekommunikationsüberwachung Angaben zu Hersteller und Software zu machen. Allein die Angabe von Hersteller und „Softwareversion“ versetzt (auch – zur entsprechenden Problematik bezüglich der Überprüfung durch den Richter bereits oben D.II.1.b) den oder die jeweilige(n) LfDI nicht in die Lage eine sinnvolle Datenschutzkontrollprüfung vorzunehmen. Nach § 33c PolG NRW muss diese nur „*mindestens alle zwei Jahre*“ „*zumindest stichprobenartig*“ vorgenommen werden. Unabhängig davon, dass bereits dieser Zeitrahmen eine effektive Überprüfung illusorisch erscheinen lässt, wäre diese nur sinnvoll durchführbar, wenn der bzw. die LfDI das „*eingesetzte Mittel*“ bzw. die „*eingesetzte Softwareversion*“ auch umfänglich (anhand des Quellcodes) prüfen und so die Funktionsweise nachvollziehen könnte. Das ist nach der derzeitigen Regelung aber gerade nicht der Fall.

Wieso die Protokollierungspflichten nach § 20c Abs. 9 PolG NRW nur für die Quellen-Telekommunikationsüberwachung ausreichen sollen, ist unklar. Auch die Auswertung (und Speicherung) des der Polizei zugeleiteten Rohdatenstroms wird regelmäßig mit Hilfe von spezieller Software (sog. TKÜ-Applikation) stattfinden. Für eine wirksame Datenschutzkontrolle bedarf es auch bei dieser Maßnahme konkreter Angaben und der Prüfmöglichkeit der eingesetzten Software (einschließlich der Möglichkeit der Sichtung des Quellcodes) durch den bzw. die LfDI.

bb) Unzureichender Kernbereichsschutz in der Verwertungsphase

Die vorhandenen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung auf der Aus- und Verwertungsebene sind unzureichend ausgestaltet. Im Regelfall wird der Polizei im Rahmen einer Telekommunikationsüberwachung eine Überwachungskopie (§ 2 Nr. 14 TKÜV) zugeleitet. Nach § 5 Abs. 2 Satz 1 TKÜV „*hat der Verpflichtete der berechtigten Stelle* [Anm.: nach dem PolG NRW die Polizei] *am Übergabepunkt eine vollständige Kopie der durch die zu überwachende Kennung bezeichneten Telekommunikation bereitzustellen, die über seine Telekommunikationsanlage abgewickelt wird*". Diese Überwachungskopie enthält nicht nur die Inhalte der Individualtelekommunikation, sondern sämtliche Telekommunikation i.S.d. § 3 Nr. 22 TKG sowie zusätzlich die nach § 7 TKÜV bereitzustellenden Daten (wie z.B. die Standortdaten eines mobilen Anschlusses, § 7 Abs. 1 Nr. 7 TKÜV sowie Verkehrsdaten). Was aber mit dieser umfangreichen Überwachungskopie – die die Zeichnung eines umfassenden Persönlichkeitsbildes der Zielperson erlaubt - geschehen darf, regelt § 20c Abs. 8 PolG NRW nur kursorisch. Klargestellt wird in § 20c Abs. 8 Satz 3 – 7 PolG, dass durch eine Telekommunikations- bzw. Quellen-Telekommunikationsüberwachungsmaßnahme erlangte Erkenntnisse aus dem Kernbereich nicht verwertet werden dürfen und Aufzeichnungen hierüber zu löschen sind. Zudem enthält die Regelung Dokumentationspflichten.

Das ist unzureichend und wird dem tiefgreifenden Eingriffsniveau der Maßnahme nicht gerecht.

Wenn der Gesetzgeber die Telekommunikationsüberwachung nicht auf die Überwachung der technikgestützten Individualkommunikation von Mensch zu Mensch reduziert, sondern eine Überwachung des gesamten Sprach- und Datenverkehrs gestattet, dann ist diese Form der Telekommunikationsüberwachung als auch der Quellen-Telekommunikationsüberwachung – wie dargelegt – in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Wohnraumüberwachung oder auch die Online-Durchsuchung. Dementsprechend ist es nicht gerechtfertigt, an den Kernbereichsschutz weniger strenge Anforderungen als an die letztgenannten Maßnahmen zu stellen. Vielmehr bedarf es hier, wie vom Gericht für Maßnahmen der Online-Durchsuchung gefordert, *in jedem Fall* einer Sichtung durch eine unabhängige

Stelle, die kernbereichsrelevante Informationen *vor* ihrer Kenntnisnahme und Nutzung durch die Polizei herausfiltert.[166]

Die vorliegende Regelung sieht – über § 20c Abs. 8 Satz 9 i.V.m. § 18 Abs. 4 PolG NRW – lediglich für automatische Aufzeichnungen und Zweifelsfälle eine vorgelagerte Prüfung durch ein Gericht vor. Damit bleibt der Gesetzgeber verfassungswidrig weit hinter dem erforderlichen Mindestmaß an Schutzvorkehrungen auf der Verwertungsebene zurück.

e. Zu weite Überwachungsmöglichkeit Dritter

Die Befugnis wird mit Blick auf die Möglichkeit der heimlichen Überwachung und Aufzeichnung der Telekommunikation Dritter (§ 20c Abs. 1 Nr. 3 und Nr. 4 PolG NRW) sowie der Durchführung einer Quellen-Telekommunikationsüberwachung auf bzw. über informationstechnische Systeme Dritter (§ 20c Abs. 2 Satz 1 PolG NRW) verfassungswidrig weit ausgestaltet.

Maßnahmen die, wie die nach § 20c Abs. 1 bzw. § 20c Abs. 2 i.V.m. Abs. 1 PolG NRW gestatteten, dermaßen tief in die Privatsphäre eindringen wie eine Online-Durchsuchung oder Wohnraumüberwachung, dürfen sich grundsätzlich „*nur gegen diejenigen als Zielperson richten, die für die drohende oder dringende Gefahr verantwortlich sind*“[167].

Für den Fall der Online-Durchsuchung hat das *Gericht* beschieden, dass diese „*auf informationstechnische Systeme Dritter erstreckt werden* [kann], *wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert* ***und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht***.“[168]

Das muss entsprechend für die Gestattung von Telekommunikationsüberwachungsmaßnahmen wie sie § 20c PolG NRW gestattet gelten.

---

[166] Vgl. BVerfGE 141, 220 (307 ff.); BVerfGE 120, 274 (338 f.).
[167] BVerfGE 141, 220 (273 – Rn. 115).
[168] BVerfGE 141, 220 (274 – Rn. 115) – Hervorhebung nur hier.

Ein Überwachen und Aufzeichnen des Rohdatenstroms eines Telekommunikationsanschlusses einer dritten Person kann nicht schon – wie es § 20c Abs. 1 Nr. 4 PolG NRW gestattet – zulässig sein, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass die Zielperson deren Telekommunikationsanschluss oder Endgerät benutzen wird. Gesetzlich niedergelegte Mindestanforderung muss es zudem jedenfalls sein, dass ein Zugriff auf den Anschluss der Zielperson *allein* nicht ausreichend ist.

Zudem fordert das *Gericht* selbst für heimliche Überwachungsmaßnahmen gegenüber Dritten von vermeintlich geringerer Intensität, dass diese nicht dazu dienen dürfen, herauszufinden, ob sich überhaupt (weitere) Ermittlungsansätze finden lassen. Aus diesem Grund bedürfe es „*zusätzlicher Anhaltspunkte, dass der Kontakt* [zu der dritten Person] *einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Gefahr dienlich sein wird*“ [169] . Das hiermit postulierte Erfordernis der erhöhten Erfolgswahrscheinlichkeit findet sich jedoch nicht im Normtext wieder.

Nach § 20c Abs. 1 Nr. 4 PolG NRW ist es vielmehr möglich, die Telekommunikation aller Familienmitglieder und Freunde/Bekannten der Zielperson zu überwachen und aufzuzeichnen, da bereits der Umstand der familiären bzw. freundschaftlichen Verbundenheit als Tatsache im Sinne des § 20c Abs. 1 Nr. 4 PolG NRW gelten dürfte, die die Annahme rechtfertigt, dass die Zielperson „das Endgerät“ oder den „Telekommunikationsanschluss“ eines Freundes oder eines Familienmitglieds benutzt. Gleiches gilt für die Überwachung des Telekommunikationsanschlusses von Örtlichkeiten (Café, Universität, etc.), die die Zielperson regelmäßig frequentiert. Wird dort – wie heutzutage üblich – ein WLAN-Zugangspunkt bereitgestellt, liegt es nahe, dass die Zielperson diesen auch „benutzen“ wird. Die Ausleitung des Rohdatenstroms dieser Örtlichkeit könnte technisch nicht lediglich auf die Kommunikation und die Internetaktivitäten der Zielperson beschränkt werden. Technisch notwendig wäre die Ausleitung der Daten aller Nutzer des Telekommunikationsanschlusses.

Die Ausdehnung der Befugnis zur Telekommunikations- und Quellen-Telekommunikationsüberwachung auf Dritte in § 20c Abs. 1 Nr. 4 PolG NRW ist daher zu

[169] BVerfGE 141, 220 (274 – Rn. 116).

weit gefasst. Sie wäre – wenn sie überhaupt für zulässig befunden würde - auf Fälle zu begrenzen gewesen, in denen 1. die Überwachung des Anschlusses der Zielperson allein nicht ausreichend ist, und 2. eine erhebliche Wahrscheinlichkeit besteht, dass die Überwachung der Aufklärung der Gefahr dienlich ist.

Insoweit das angerufene *Gericht* eine dem § 20c Abs. 1 **Nr. 3** PolG NRW ähnliche Regelung (§ 20l Abs. 1 Nr. 3 und 4 BKAG a.F.) noch als „*bei verfassungskonformer Auslegung mit Art. 10 Abs. 1 GG vereinbar*" angesehen hatte, kann das nicht als Placet für Neuregelungen gelten. Klargestellt wurde bezüglich der Regelung im BKAG a.F., dass die Telekommunikationsüberwachung nicht „*ins Blaue hinein*" auf alle Personen erstreckt werden dürfe, die mit der Zielperson Nachrichten ausgetauscht haben, sondern „*eigene, in der Anordnung darzulegende Anhaltspunkte*" voraussetze, „*dass der Nachrichtenmittler von der Zielperson in die Tatdurchführung eingebunden wird und somit eine besondere Tat- oder Gefahrennähe aufweist*"[170]. Zumindest die Regelung über den Inhalt der Anordnung der Maßnahme, § 20c Abs. 6 PolG, hätte diese Vorgabe reflektieren müssen (so z.B. die Regelung in Niedersachsen: § 33a Abs. 5 Nr. 5 NPOG).

Eine Quellen-Telekommunikationsüberwachungsmaßnahme darf schließlich ausweislich § 20c Abs. 2 Satz 1 PolG NRW „*in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person* ***genutzte*** *informationstechnische Systeme eingegriffen*" wird. Eine weitere Differenzierung nach eigenen informationstechnischen Systemen und solchen Dritter Personen erfolgt in verfassungswidriger Weise nicht. Das wäre aber, entsprechend dem oben Gesagten, erforderlich gewesen. Insbesondere wäre – entsprechend den o.g. Vorgaben des Gerichts zur Online-Durchsuchung auf informationstechnischen Systemen Dritter - ein Zugriff nur dann zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson das fremde informationstechnische System in ermittlungsrelevanter Weise nutzt und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht.

[170] Dies umsetzend z.B. Art. 42 Abs. 1 Nr. 2 BayPAG.

f. Schranken-Schranke: nationale (und internationale) IT-Sicherheit

Die Regelung des § 20c Abs. 2 PolG NRW ist auch insofern verfassungswidrig, als sie pauschal einen Eingriff in informationstechnische Systeme mittels „technischer Mittel" gestattet, ohne die technischen Wege der Infiltration dergestalt zu begrenzen, dass eine Gefährdung der IT-Sicherheit Dritter zumindest nicht gefördert wird.

Nach dem vorliegenden Regelungskonzept ist zum Zweck der Infiltration des informationstechnischen Zielsystems eine Ausnutzung noch unbekannter Sicherheitslücken in Betriebssystemen und Anwendungssoftware erforderlich. Die Informationen über diese Sicherheitslücken müssen ermittelt und vor den betroffenen Softwareherstellern verheimlicht werden, damit diese die Lücken nicht schließen. Die hieraus resultierenden und bewusst in Kauf genommenen Gefahren für die nationale (und internationale) IT-Sicherheit stehen zu dem Zweck in krassem Missverhältnis, ja können sogar das Gegenteil des Zwecks befördern, indem Sie terroristisch motivierte „Cyber-Angriffe" fördern. Es besteht die hinreichende Wahrscheinlichkeit, dass die unbekannten Sicherheitslücken den „falschen" Personen bekannt werden bzw. unabhängig von den staatlichen Stellen entdeckt werden. Die Folge wäre, dass hierdurch mitunter lebenswichtige IT-Infrastrukturen Schaden nehmen (zum Vorfall „WannaCry" siehe bereits oben A.II.2.a).

Der Gesetzgeber hat, trotz eines entsprechender Hinweise durch Sachverständige in diesem und anderen Gesetzgebungsverfahren zu ähnlichen Regelungen [171] sowie eindeutiger Warnungen von Experten in der Literatur[172] ohne nähere Begründung von einer Ausnahmeregelung abgesehen, nach welcher eine Ausnutzung unbekannter Sicherheitslücken zum Zweck der Infiltration des Zielsystems unzulässig ist.

Es wurde offenbar übersehen, dass eine entsprechende Verpflichtung bereits unmittelbar aus dem Recht auf Gewährleistung (!) von Integrität und Vertraulichkeit informationstechnischer Systeme folgt. Dieses ist nicht nur Abwehrrecht des Bürgers

[171] Vgl. *Arzt*, Stellungnahme, S. 17; *Gazeas*, Stellungnahme, S. 18 – jeweils mit Verweis auf die substantiierte Darstellung der Problematik bei *Buermeyer*, Stellungnahme zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, BT A-Drs. 18(6)334, S. 21f..
[172] Eingehend z.B. *Pohlmann*, DuD 2018, 37 – 44.

gegen den Staat. Es enthält auch einen verfassungsrechtlichen Schutz- und Gewährleistungsauftrag zur Verwirklichung der Wertvorstellungen des Grundrechts.[173]

Diesem Schutzauftrag wäre durch einen expliziten Ausschluss der Ausnutzung unbekannter Sicherheitslücken zum Zweck der Durchführung der Maßnahmen nachzukommen gewesen. Das ist indes nicht geschehen.

III. Unvereinbarkeit mit dem Fernmeldegeheimnis, Art. 10 Abs. 1 GG

Sollte das *Gericht* nicht der Auffassung folgen, dass der § 20c PolG NRW (i.V.m. § 8 Abs. 4 PolG NRW) zumindest am Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme zu messen ist, sondern „nur" einen Eingriff in Art. 10 Abs. 1 GG darstellt, stellt sich die Regelung gleichwohl als verfassungswidrig dar.

Wenn der angerufene Senat des *Gerichts* der Auffassung des zweiten Senats[174] folgen sollte, nach welchem auch die (ggf. monatelange) Überwachung der – weit verstandenen - „Internetkommunikation" (d.h. des gesamten ein- und ausgehenden Datenverkehrs) einer Zielperson im Rahmen einer Telekommunikations- oder Quellen-Telekommunikationsüberwachung „nur" an Art. 10 Abs. 1 GG zu messen sei, bedürfte es einer Neujustierung der verfassungsrechtlichen Anforderungen an die vorzusehenden gesetzlichen Schutzvorkehrungen bei Eingriffen in das Fernmeldegeheimnis.

Diese wären den Anforderungen an Schutzvorkehrungen im Zusammenhang mit Eingriffen in das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme bzw. Art. 13 Abs. 1 GG anzugleichen.

Nicht (mehr) zu überzeugen vermag – wie bereits dargelegt – die Einschätzung des *Gerichts*[175], dass „*die Telekommunikationsüberwachung ihrem Gesamtcharakter nach nicht in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt* [sei] *wie die Wohnraumüberwachung oder auch die Online-Durchsuchung*" und das dem insbesondere „*durch weniger strenge Anforderungen an den Kernbereichsschutz Rechnung* [ge]*tragen*" werden könne. In keinem Fall kann und darf die Entscheidung über das Ob und den

[173] So die wohl h.M. *Derin/Golla*, NJW 2019, 1111 (1114); *Roßnagel/Schnabel*, NJW 2008, 3534 (3535); *Kutscha*, NJW 2008, 1042 (1044); *Heckmann*, in: Heckmann, jurisPK-Internetrecht, 6. Aufl. 2019, Kap. 5 Rn. 139f.
[174] BVerfG, Nichtannahmebeschluss v. 6.7.2016 – 2 BvR 1454/13 – Rn. 41.
[175] BVerfGE 141, 220 (312 f.).

Umfang der Telekommunikationsüberwachung den Ermittlungsbehörden überlassen werden.[176] Die Einbindung unabhängiger Stellen – also insbesondere der Gerichte – wäre in gleichem Umfang wie bei der Gestattung einer Online-Durchsuchung oder einer Wohnraumüberwachung vorzusehen.

Das die hier angegriffene Regelung der Telekommunikationsüberwachung und der Quellen-Telekommunikationsüberwachung die verfassungsrechtlichen Anforderungen die an Maßnahmen zu stellen sind, die ihrem Gesamtcharakter nach in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt sind, wie die Wohnraumüberwachung oder die Online-Durchsuchung, nicht erfüllt, wurde bereits oben dargelegt.

Es bleibt darauf hinzuweisen, dass auch die Telekommunikations- und Quellentelekommunikationsüberwachung nach herkömmlichem – auf die technisch vermittelte Individualkommunikation zwischen Menschen – beschränkten Verständnis einen schwerwiegenden Eingriff in Art. 10 Abs. 1 GG darstellt. Die Befugnis zur Telekommunikationsüberwachung bzw. zur Quellen-Telekommunikationsüberwachung nach § 20c PolG NRW (i.V.m. § 8 Abs. 4 PolG NRW) ist, auch wenn man sie „lediglich" als Eingriff in Art. 10 Abs. 1 GG ansehen wollte, dennoch aus den unter D.II.2 dargelegten Gründen verfassungswidrig. Insbesondere entspricht § 20c PolG NRW nicht den hohen Anforderungen an die Bestimmtheit und Klarheit einer einen solch schwerwiegenden Eingriff gestattenden Regelung. Die Darlegungen und Ausführungen unter D.II.2.a und D.II.2.c gelten entsprechend.

Sollten die durch § 20c PolG NRW gestatteten Maßnahmen „nur" als Eingriff in Art. 10 Abs. 1 GG angesehen werden, dürften sie sich dennoch nicht in der hier vorgesehenen Weise auf Dritte erstrecken. Die oben unter D.II.2.e hierzu gemachten Ausführungen gölten entsprechend.

Nach alledem ist § 20c PolG NRW (i.V.m. § 8 Abs. 4 PolG NRW) auch mit dem Art. 10 Abs. 1 GG verfassungsrechtlich unvereinbar.

Prof. Dr. jur. Jan Dirk Roggenkamp

[176] So aber BVerfG, Nichtannahmebeschluss v. 6.7.2016 – 2 BvR 1454/13 – Rn. 48f.