# DIE KRIMINALPOLIZEI

Zeitschrift der Gewerkschaft der Polizei

Ausgabe 4/2022

Baden-Württemberg

Bundespolizei

Bundeskriminalamt

Niedersachsen

Saarland

Freistaat Sachsen

Sachsen-Anhalt

## Gesetzliche Änderungen im Sexualstrafrecht

## Verwertbarkeit von Encrochat-Kommunikationsinhalten

## Der Verdeckte Ermittler im LVwG SH

www.kriminalpolizei.de

# Editorial

## Liebe Leserinnen, liebe Leser,

das Jahr neigt sich dem Ende zu und vor Ihnen liegt mit dem Heft 4/2022 bereits die Weihnachtsausgabe der „Kriminalpolizei".

In den zurückliegenden Monaten hat uns die Coronakrise weiter beschäftigt, wenngleich die Gefahren der Pandemie insbesondere durch den menschenverachtenden russischen Angriffskrieg in der Ukraine sowie die damit verbundenen und die gesamte Welt treffenden Auswirkungen in den Hintergrund gedrängt wurden. Mit unserer Zeitschrift haben wir auch diese besondere Ausgangssituation berücksichtigt, denn dadurch ist die vielschichtige polizeiliche Aufgabenwahrnehmung unmittelbar beeinflusst worden.

In der letzten Ausgabe dieses Jahres geht es zunächst, thematisch aufbauend auf einem Fortsetzungsbeitrag in der „Kriminalpolizei" 2/2021 und 3/2021, um das Sexualstrafrecht. **Prof. Dr. Dennis Bock** und **Cathrin Lebro** setzen sich mit den durch das Gesetz zur Bekämpfung sexualisierter Gewalt gegen Kinder vom 16.6.2021 (BGBl. I 2021, 1810 ff.) und punktuell durch das Gesetz zur Änderung des Strafgesetzbuches vom 14.9.2021 (BGBl. I 2021, 4250 ff.) vorgenommenen Änderungen auseinander und sparen dabei nicht mit Kritik. In ihrem Fazit kommen die Autoren unter anderem zur Feststellung, dass der Gesetzgeber es bedauerlicherweise versäumt habe, die sorgfältig ausgearbeiteten Empfehlungen der eingesetzten Reformkommission umzusetzen, und stattdessen überwiegend auf eine generalpräventive Wirkung gesetzt habe, was unter Berücksichtigung vorliegender kriminalpolitischer Erkenntnisse äußerst zweifelhaft erscheine. Dennis Bock ist Inhaber des Lehrstuhls für Deutsches und Internationales Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht an der Christian-Albrechts-Universität zu Kiel, Direktor des dortigen Instituts für Kriminalwissenschaften sowie Richter am Schleswig-Holsteinischen Oberlandesgericht. Der Beitrag ist gemeinsam mit der an seinem Lehrstuhl tätigen studentischen Mitarbeiterin Cathrin Lebro entstanden.

Zur Verwertbarkeit von Encrochat-Kommunikationsinhalten nehmen **Dr. Sören Pansa** und **Dr. Marius Heller** Stellung. Sören Pansa ist als Oberstaatsanwalt bei der Generalstaatsanwaltschaft Schleswig-Holstein und Marius Heller als Staatsanwalt bei der Staatsanwaltschaft bei dem Landgericht Kiel tätig. Die Autoren gehen dabei insbesondere auf eine aktuelle Entscheidung des Bundesgerichtshofs vom 2.3.2022 (5 StR 457/21) ein, in der in diesem Kontext ausdrücklich kein Beweisverwertungsverbot aus rechtshilfespezifischen Gründen, nationalem Verfassungsrecht sowie den Vorgaben der Europäischen Menschenrechtskonvention (EMRK) festgestellt worden ist. Zudem gehen sie davon aus, dass sich die inzwischen herausgebildeten Handlungsroutinen in Zukunft auch für die Auswertung erlangter Daten aus mit Encrochat vergleichbaren Krypto-Netzwerken wie „SkyECC" und „ANOM" als nützlich erweisen dürften. Angesichts der wegweisenden Entscheidung des Bundesgerichtshofs dürften wohl der Verwertbarkeit auch dieser Daten keine Bedenken entgegenstehen.

Der in der Abteilung 3 (Staatsschutz) des Landeskriminalamtes Schleswig-Holstein tätige **KK Lasse Dähling** beschäftigt sich mit der Implementierung der Rechtsfigur des Verdeckten Ermittlers in das allgemeine Polizeirecht des Landes Schleswig-Holstein durch Gesetzesänderung vom 26.2.2021 (GVOBl. 2021, 222). Mit der überfälligen Einfügung des § 185 Abs. 1 Nr. 3 LVwG SH sind nunmehr auch hier Datenerhebungsmaßnahmen durch den Einsatz von Polizeivollzugsbeamten unter einer ihnen verliehenen, auf Dauer angelegten Legende möglich. Berechtigt weist der Autor jedoch auch darauf hin, dass es im Zuge einer anzustrebenden Harmonisierung der hoheitlichen Befugnisnormen wünschenswert gewesen wäre, sowohl inhaltlich als auch systematisch-redaktionell im Gleichklang mit den Gefahrenabwehrgesetzen anderer Länder vorzugehen. Im Einzelfall eingebrachte Hinweise auf die „Wesensmerkmale des (Sicherheits-) Föderalismus" greifen in diesem Zusammenhang erkennbar zu kurz.

Weitere Fachbeiträge setzen sich mit dem Verzicht auf die öffentliche Ordnung im bereichsspezifischen Versammlungsrecht, den Herausforderungen bei der Anwendung kindgerechter Kriterien für das Strafverfahren, der Prävention von Delikten im Sinne des § 184b StGB, der Cyberkriminalität und den Risiken der digitalen Sphäre sowie der Virtualisierung und Meinungsbildung in der rechtsextremistischen Szene auseinander. Für die Bearbeitung dieser Themen konnten unter anderem **Prof. Michael Knape, Josefine Barbaric, PD a.D. Rainer Becker** und **Prof. Dr. Mirko Faber, Dr. Viktoria Schäfer** und **Dr. Yvonne Zimmermann** sowie **RA Marcel Auber** gewonnen werden.

Ein Grußwort des neu gewählten Bundesvorsitzenden der Gewerkschaft der Polizei, eine strafrechtliche Rechtsprechungsübersicht, Aktuelles aus dem Netz und Rezensionen runden unsere Zeitschrift schließlich ab.

Liebe Leserinnen und Leser, wir wünschen Ihnen eine anregende Lektüre und sind auf Ihre Rückmeldungen gespannt. Zugleich wünschen wir Ihnen und Ihren Familien ein frohes Weihnachtsfest, einige erholsame Tage zwischen den Jahren sowie ein glückliches, erfolgreiches und gesundes Jahr 2023. Wir hoffen auf ruhigere Zeiten und freuen uns auf den weiteren Austausch mit Ihnen.

Für das Redaktionsteam

Ihr

Hartmut Brenneisen

# Grußwort

## Liebe Leserinnen und Leser, liebe Kolleginnen und Kollegen,

das Motto unseres vergangenen Bundeskongresses „Für uns. Für morgen“ ist uns nach wie vor präsent – und es ist uns eine Verpflichtung. Vor diesem Hintergrund, aktiv und unterwegs zu sein, ist der Maßstab, an dem wir uns messen lassen wollen. Ich selbst, als neu gewählter Bundesvorsitzender der Gewerkschaft der Polizei (GdP), ebenso wie meine Kolleg:innen im neu konstituierten Geschäftsführenden Bundesvorstand der GdP.

Die Delegierten des Kongresses haben, getreu dem sehr treffenden Kongressmotto, wichtige Weichen für die gewerkschaftliche Arbeit der kommenden Jahre gestellt. Mit mir hat der Bundeskongress den jüngsten Bundesvorsitzenden der Geschichte der GdP an die Spitze des neunköpfigen Teams des GBV gewählt. Und auch sonst hat sich der Geschäftsführende Bundesvorstand der GdP durch das Votum der Delegierten personell deutlich verjüngt – ohne dabei jedoch an Kompetenz und Gestaltungswillen einzubüßen.

Ich bin sehr glücklich, unserer Organisation vorstehen zu dürfen und werde, ebenso wie meine GBV-Kolleg:innen, meine Kraft und mein Engagement darin setzen, den Belangen der rund 200.000 Polizeibeschäftigten, die in unserer Organisation zusammengeschlossen sind, eine hörbare Stimme und ein wahrnehmbares Gesicht zu verleihen.

Auch inhaltlich hat der Bundeskongress wichtige Weichen gestellt. Wir im Bundesvorstand haben von unseren Mitgliedern klare Arbeitsaufträge zu vielen für die GdP relevanten Themenbereichen bekommen. Besonders freue ich mich, dass wir auch für die Kriminalpolizei richtungsweisende Beschlüsse gefasst haben. Denn die aktuellen Herausforderungen für die Kolleg:innen in diesem Bereich, bedingt durch die Globalisierung, gesellschaftliche Veränderungen, Digitalisierung und digitale Vernetzung, sind immens. Und deshalb werden wir uns als Gewerkschaft der Polizei hier auch verstärkt einmischen. Mit hohem Sachverstand und Engagement. Das Themenspektrum, dem sich der Bundesvorstand auf Grundlage der Kongressergebnisse in den nächsten vier Jahren widmen wird, reicht angesichts dessen richtigerweise vom Grundsatzthema der notwendigen konstruktiven Einmischung bei der Frage, wie mit der politisch forcierten Freigabe von Cannabis als Genussmittel umzugehen und worauf dabei aus Sicht der Polizeibeschäftigten zu achten ist, über die Notwendigkeit, Kripo-Laufbahnen attraktiver zu gestalten bis hin zur Forderung, die Kriminalitätsbekämpfung durch eine intensivierte Zusammenarbeit von Bund und Ländern zu stärken.

Wenn ich auf die gewerkschaftliche Arbeit blicke, die hier vor uns liegt, bin ich sehr froh, dass wir uns im Bundesvorstand auf die fachliche Expertise unserer Mitgliedschaft sowie der kriminalpolizeilichen Fachwelt verlassen können. Gerne ermöglichen wir als GdP daher auch zukünftig das Erscheinen unserer Zeitschrift „Die Kriminalpolizei“, deren 40-jähriges Erscheinungsjubiläum wir im Jahre 2023 feiern werden. Und auch darüber hinaus verfügt unsere GdP über eine belastbare organisatorische Struktur, die uns im Bundesvorstand mit kriminalpolizeilicher Expertise berät. An der Spitze dieser Struktur sehe ich zuvorderst unsere Fachausschüsse in den Ländern und im Bund. Diese erfüllen die wichtige Aufgabe, die kriminalpolizeiliche Expertise der GdP zu bündeln und zu kanalisieren. Unser Fachausschuss auf Bundesebene wird uns im Bundesvorstand auch in den kommenden Jahren sehr direkt mit kriminalfachlichem Rat und gewerkschaftlichem Tatendrang zur Seite stehen. Ich bin mir sicher, wir können uns auf das funktionierende Teamplay mit unserer Mitgliedschaft verlassen: Ich als Bundesvorsitzender ebenso wie mein Stellvertreter Alexander Poitz aus Brandenburg, der im Geschäftsführenden Bundesvorstand in den nächsten Jahren die Themenverantwortung für Kriminalpolitik ausüben wird.

Packen wir es an!

Ihr/Euer

Jochen Kopelke
(Bundesvorsitzender der GdP)

Bildrechte: GdP / Kay Herschelmann.

## STÄNDIGE EHRENAMTLICHE MITARBEITER*INNEN

### Baden-Württemberg

**Landespolizeipräsident a. D. Gerhard Klotter**

**Polizeipräsident Martin Schatz,**
Polizeipräsidium Hochschule für Polizei BW

**Polizeipräsident a. D. Thomas Köber**

**Polizeipräsident a. D. Ekkehard Falk**

**Polizeipräsident a. D. Hartmut Grasmück**

**Polizeipräsident Reinhard Renter,**
Polizeipräsidium Offenburg

### Bayern

**Ltd. Kriminaldirektor a. D. Gunter Hauch**

**Erster Kriminalhauptkommissar Gerold Wiesbacher,**
Fortbildungsinstitut der Bayerischen Polizei, Fachbereich Kriminalistik/Kriminologie

**Kriminaldirektor Bernd Hackl,**
Leiter der KPI Rosenheim

### Berlin

**Prof. Dr. Claudius Ohder,**
Hochschule für Wirtschaft und Recht, Fachbereich 5

**Kriminaldirektor Oliver Tölle,**
Hochschule für Wirtschaft und Recht, Fachbereich 5 Berlin

**Kriminalhauptkommissar Thomas Spaniel,**
Gesamtpersonalrat (GPR)

### BKA

**Holger Münch,**
Präsident des Bundeskriminalamtes

**Leitende Kriminaldirektorin a. D. Sabine Wenningmann**

**Leitender Wissenschaftlicher Direkor Dr. Peter Frodl,**
Bundeskriminalamt/KT 1

**Leitender Kriminaldirektor Nikolaus Speicher,**
Vorsitzender Gesamtpersonalrat im Bundeskriminalamt

### Bremen

**Ltd. Kriminaldirektorin Andrea Wittrock,**
Leiterin ZPD, Polizei Bremen

**Kriminaldirektor Jörg Seedorf,**
Ortspolizeibehörde Bremerhaven

**Kriminalhauptkommissar Lüder Fasche,**
Gesamtpersonalrat Bremen und Landesvorsitzender der GdP

### Bundespolizei

**Erster Polizeihauptkommissar Edgar Stoppa,**
Bundespolizeiakademie Lübeck

**Präsident der Bundespolizeidirektion Pirna Jörg Baumbach**

**Polizeidirektor Helgo Martens,**
Leiter der KrimB Bundespolizeiinspektion Hamburg

**Erster Polizeihauptkommissar Jürgen Lindemann,**
Bundespolizeidirektion Berlin

### Hamburg

**Kriminaloberrat André Bunkowsky,**
Polizei Hamburg

### Hessen

**Kriminaloberkommissar Lars-Germann Elsebach,**
Polizeipräsidium Nordhessen

### Mecklenburg-Vorpommern

**LKD Thomas Krense,**
Ministerium für Inneres und Europa, Leiter der Abteilung 5/Verfassungsschutz (m.d.W.d.D.b.)

**Inspekteur der Polizei a. D. Rudolf Springstein**

**Polizeidirektor a. D. Rainer Becker**

### Niedersachsen

**Direktor der Polizei a. D. Wolfgang Rösemann**

**Kriminaldirektor Uwe Lietzau,**
PI Braunschweig

**Polizeidirektor a. D. Volker Feige**

### Nordrhein-Westfalen

**Kriminalhauptkommissar Dipl. Verw. Wirt Dietrich Voß,**
Kriminalprävention/Opferschutz

**Leitender Kriminaldirektor a.D. Jürgen Kleis**

**Erster Kriminalhauptkommissar Frank Schniedermeier**

**Kriminaldirektor Jürgen Dekker**

**Erster Kriminalhauptkommissar Michael Maatz**

### Rheinland-Pfalz

**Inspekteur der Polizei Jürgen Schmitt,**
Ministerium des Innern und für Sport

**Generalstaatsanwalt Dr. Jürgen Brauer,**
Generalstaatsanwaltschaft Koblenz

**Leitender Oberstaatsanwalt Harald Kruse,**
Staatsanwaltschaft Koblenz

**Polizeipräsident Rainer Hamm,**
Polizeipräsidium Mainz

**Matthias Bongart,**
Geschäftsführer Landesbetrieb Daten und Information

**Kriminaldirektor Gerald Gouasé,**
Leiter der Kriminaldirektion Mainz

**Kriminaldirektor a. D. Klaus Mohr**

### Saarland

**Direktor a. D. Dr. Helmut Albert,**
Ministerium für Inneres, Bauen und Sport, Leiter Abteilung V - Verfassungsschutz

**Generalstaatsanwalt a. D. Ralf-Dieter Sahm**

**Landespolizeivizepräsident a. D. Hugo Müller**

**Polizeioberrat Norbert Meiners,**
Landesinstitut für präventives Handeln

**Kriminaloberrätin Nadine Weiler-Kunz,**
Dozentin an der Fachhochschule für Verwaltung

**KOK David Bohnenberger,**
LPP 214 (Brandermittlungen/ Umweltkriminalität)

### Sachsen

**Prof. Dr. med. Jan Dreßler,**
Leiter des Instituts für Rechtsmedizin, Universität Leipzig

**Prof. Dr. Christine Erfurt, a. D.**

**Kriminalhauptkommissar Kai Martin,**
Polizeirevier Chemnitz-Nordost

### Sachsen-Anhalt

**Leitender Kriminaldirektor Sirko Eckert,**
Landeskriminalamt

**Landespolizeidirektor Karl-Albert Grewe,**
Ministerium für Inneres und Sport

**Landespolizeidirektor a. D. Rolf-Peter Wachholz**

### Schleswig-Holstein

**Ministerialdirigent a. D. Jörg Muhlack**

**Landespolizeidirektor Michael Wilksen,**
Landespolizeiamt

**Leitender Polizeidirektor Ralph Garschke,**
Landespolizeiamt

**Leitender Kriminaldirektor Rainer Bretsch,**
Ministerium für Inneres, Kommunales, Wohnen und Sport

**Polizeidirektor Frank Ritter,**
Polizeidirektion Itzehoe

**Kriminaldirektor Michael Raasch,**
Polizeidirektion Flensburg

### Thüringen

**Präsident Jens Kehr,**
Landeskriminalamt Thüringen

| | |
|---|---|
| **Editorial** | **1** |
| **Grußwort**<br>des Bundesvorsitzenden der GdP | **2** |
| **Gesetzliche Änderungen im Sexualstrafrecht**<br>Von Prof. Dr. Dennis Bock und Cathrin Lebro, Kiel | **5** |
| **„Vertrauen ist gut" – Von der Verwertbarkeit erlangter Daten bezüglich sogenannter Kryptohandys**<br>Von Oberstaatsanwalt Dr. Sören Pansa und Staatsanwalt Dr. Marius Heller, Schleswig/Kiel | **10** |
| **Der Verdeckte Ermittler im LVwG SH – Eine überzeugende Ergänzung?**<br>Von KK Lasse Dähling, Kiel | **15** |
| **Zum Verzicht auf die öffentliche Ordnung im VersFG BE und im VersG NRW**<br>Von Prof. Michael Knape und Prof./LRD a.D. Hartmut Brenneisen, Berlin/Preetz | **18** |
| **Polizeien und Kinderschutz – Herausforderungen bei der Anwendung kindgerechter Kriterien für das Strafverfahren**<br>Von Josefine Barbaric, Salach | **21** |
| **Führungsaufsicht: Prävention von Delikten gemäß § 184b StGB**<br>Von PD a.D. Rainer Becker und Prof. Dr. Mirko Faber, Nordenham/Güstrow | **25** |
| **Cyberkriminalität und Risiken in der „digitalen Sphäre"**<br>Von Dr. Viktoria Schäfer und Dr. Yvonne Zimmermann, Montabaur | **27** |
| **Virtualisierung und Meinungsbildung im Rechtsextremismus**<br>Von RA Marcel Auber, Ludwigsburg | **31** |
| **Strafrechtliche Rechtsprechungsübersicht**<br>Von EPHK & Ass. jur. Dirk Weingarten, Wiesbaden | **34** |
| **Aktuelles aus dem Netz**<br>Von EKHK Christian Zwick, Ludwigshafen | **36** |
| **Buchrezensionen** | **8,13,19,26** |


## IMPRESSUM


**Herausgeber:**
GdP Gewerkschaft der Polizei, Bundesgeschäftsstelle Berlin,
Stromstraße 4, 10555 Berlin, Telefon: 030 / 39 99 21-0, Fax: -200

**Redaktion:**

**Fachlicher Teil:**
Prof./LRD a.D. Hartmut Brenneisen, Verantwortlicher Redakteur
E-Mail: brenneisen@kriminalpolizei.de
KD Frank Wimmel, Redakteur
E-Mail: wimmel@kriminalpolizei.de
EPHK Ass. jur. Dirk Weingarten, Redakteur
E-Mail: weingarten@kriminalpolizei.de
EKHK Christian Zwick, Redakteur
E-Mail: zwick@kriminalpolizei.de
c/o VERLAG DEUTSCHE POLIZEILITERATUR GmbH
Anzeigenverwaltung
Ein Unternehmen der Gewerkschaft der Polizei
Betriebsstätte Worms, Rheinstraße 1, 67547 Worms, Telefon 0 62 41 / 84 96-0

**Gewerkschaftspolitischer Teil:**
Jochen Kopelke, GdP-Bundesvorsitzender,
c/o GdP-Bundesgeschäftsstelle, Stromstraße 4, 10555 Berlin,
Telefon: 030 / 39 99 21-110, Fax: -211

**Namentlich gekennzeichnete Artikel müssen nicht die Meinung der Redaktion wiedergeben.**
Manuskripte bitte ausschließlich an die Redaktion senden. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Nachdruck, Vervielfältigungen usw. sind nur mit Quellenangabe und nach schriftlicher Genehmigung des Verlages gestattet.

**Verlag und Anzeigenverwaltung:**
VERLAG DEUTSCHE POLIZEILITERATUR GMBH
Anzeigenverwaltung
Ein Unternehmen der Gewerkschaft der Polizei

Forststraße 3 a, 40721 Hilden,
Telefon: 02 11 / 7 10 4-0, Fax: -174, av@vdp-polizei.de
Betriebsstätte Worms: Rheinstraße 1, 67547 Worms,
Telefon: 0 62 41 / 84 96-0, Fax: -70, avworms@vdp-polizei.de

Geschäftsführer: Bodo Andrae, Joachim Kranz
Anzeigenleitung: Antje Kleuker

**Erscheinungsweise und Bezugspreis:**
Vierteljährlich im letzten Quartalsmonat

Einzelbezugspreis 3,50 Euro incl. 7 % MwSt. zzgl. Versandkosten, Jahresabonnement 12,– Euro incl. 7 % MwSt. zzgl. Versandkosten. Aufgrund des kriminalfachlichen Inhalts der Zeitschrift „Die Kriminalpolizei" kann diese nur an Personen und Institutionen ausgeliefert werden, die entsprechendes berufliches Interesse an der Zeitschrift nachweisen. „Die Kriminalpolizei" darf nicht in Lesezirkeln geführt werden. Bestellungen nur an den Verlag.

**Herstellung:**
Print Media Group GmbH,
St.-Reginen-Platz 5, 59069 Hamm,
Telefon: 0 23 85 / 931-100, Fax 0 23 85 / 931-199, info@pmg.de

**ISSN 0938-9636**

Internet-Adresse: **www.kriminalpolizei.de**

# Gesetzliche Änderungen im Sexualstrafrecht

Von Prof. Dr. Dennis Bock und Cathrin Lebro, Kiel[1]

## 1 Einführung

Kaum ein Deliktsbereich im Strafgesetzbuch unterlag in den vergangenen Jahrzehnten einem so starken Wandel wie das Sexualstrafrecht.[2] Angesichts der hohen medialen Aufmerksamkeit und der gesellschaftlichen Brisanz der Thematik waren und sind die Straftaten gegen die sexuelle Selbstbestimmung im 13. Abschnitt des Strafgesetzbuches immer wieder Gegenstand von Reformbestrebungen. Obgleich erst durch das 49. StrÄndG vom 21.1.2015[3] sowie das 50. StrÄndG v. 4.11.2016[4] weitreichende Änderungen, Erweiterungen und Umstrukturierungen des Abschnitts vorgenommen wurden, setzte der damalige Bundesjustizminister Heiko Maas im Jahr 2015 eine Reformkommission zur Untersuchung der (weiteren) Reformbedürftigkeit des Sexualstrafrechts ein. Diese attestierte in ihrem 2017 vorgelegten Abschlussbericht das Erfordernis einer grundlegenden Neuordnung und Neusystematisierung des 13. Abschnitts des Strafgesetzbuches.[5] Vorgeschlagen wurde dabei etwa die Streichung von Tatbeständen sowie die Einführung eines minder schweren Falles auch für den schweren Kindesmissbrauch.[6] Nachdem aber im Jahr 2020 die bekanntgewordenen Kindesmissbrauchsfälle von Staufen, Bergisch-Gladbach, Lüdge und Münster die mediale Aufmerksamkeit erregten, häuften sich die politischen Forderungen nach härteren Strafen.[7] Der Gesetzgeber gab diesem öffentlichen Druck nach, und so trat am 1.7.2021 das Gesetz zur Bekämpfung sexualisierter Gewalt gegen Kinder[8] in Kraft, in dem die kritischen Stimmen der Sachverständigen weitgehend unberücksichtigt blieben.[9] Eine weitere – punktuelle – Änderung des Sexualstrafrechts erfolgte noch durch das am 14.9.2021 verabschiedete Gesetz zur Strafbarkeit der Verbreitung und des Besitzes von Anleitungen zu sexuellem Missbrauch von Kindern.[10]

Der folgende Beitrag nimmt diese Reformen zum Anlass, um anknüpfend an den im vergangenen Jahr erschienenen systematischen Überblick zu den Straftaten gegen die sexuelle Selbstbestimmung[11] die wichtigsten Änderungen in Bezug auf das Sexualstrafrecht darzustellen.

Hinzuweisen ist darauf, dass angesichts des Ruhens der Verjährung gem. § 78b I Nr. 1 StGB bis zur Vollendung des 30. Lebensjahres des Opfers auch die früheren Gesetzesfassungen aktuell noch praktische Bedeutung haben. Schließlich gilt für *„Altfälle“* gem. § 2 I StGB grundsätzlich das Tatzeitrecht, wenn nicht § 2 III StGB die Anwendung eines späteren Gesetzes vorschreibt.[12]

## 2 Gesetz zur Bekämpfung sexualisierter Gewalt gegen Kinder vom 16. Juni 2021

Der deutsche Gesetzgeber sieht die Bekämpfung sexualisierter Gewalt gegen Kinder als eine der wichtigsten gesellschaftspolitischen Herausforderung dieser Zeit und als zentrale Aufgabe des Staates an.[13] Mit Blick auf den technischen Wandel und der damit einhergehenden veränderten Art der gegen die Kinder gerichteten Straftaten habe sich das Gefährdungspotenzial für Kinder in der virtuellen und realen Welt gleichermaßen erhöht.[14] Angesichts der gestiegenen Fallzahlen im Bereich des sexuellen Missbrauchs von Kindern und der Verbreitung, des Besitzes und der Besitzverschaffung von Kinderpornographie bestünde ein gesteigerter politischer Handlungsbedarf.[15] Zur Verwirklichung des Ziels, Kinder vor sexuellem Missbrauch zu schützen, enthält das Gesetz zur Bekämpfung sexualisierter Gewalt gegen Kinder in erster Linie eine Verschärfung des Strafrechts, um potentielle Täter abzuschrecken.[16] Daneben sieht es weitreichende Maßnahmen in den Bereichen Strafverfolgung, Prävention und Qualifizierung der Justiz vor.[17]

### 2.1 Änderungen im Strafgesetzbuch

#### 2.1.1 §§ 174 ff. StGB

Unter Berücksichtigung einiger Vorschläge der Reformkommission[18] sind zunächst die §§ 174 ff. StGB, die den sexuellen Missbrauch von Schutzbefohlenen sowie den Missbrauch institutioneller Abhängigkeit erfassen, geändert worden.

#### 2.1.1.1 § 174 StGB

Durch die Gesetzesänderung wurde in § 174 StGB die Altersschutzgrenze der Tatopfer auf 18 Jahre vereinheitlicht, indem das Schutzalter in § 174 I Nr. 1 StGB auf 18 Jahre heraufgesetzt und § 174 I 2 StGB entsprechend angepasst wurde. Zuvor wurde bei einem Missbrauch im Rahmen von Erziehungs-, Ausbildungs- oder Betreuungsverhältnissen zwischen Personen unter 16 Jahren und Personen zwischen 16 und 18 Jahren differenziert. Während bei den Personen unter 16 Jahren bereits das Bestehen eines Abhängigkeitsverhältnisses den Missbrauch indizierte, musste i.Ü. ein Ausnutzen dieses Abhängigkeitsverhältnisses hinzukommen. Zudem wurde jeweils ein Satz in die Absätze 1 und 2 eingefügt, der auch Tathandlungen unter Einbeziehung Dritter unter Strafe stellt. Strafbar macht sich demnach auch, wer den Schutzbefohlenen dazu bestimmt, dass er sexuelle Handlungen an oder vor einer dritten Person vornimmt oder von dieser an sich vornehmen lässt. Zuletzt wurde der Anwendungsbereich des Straftatbestands von § 174 III StGB, der Handlungen ohne körperlichen Kontakt zwischen Schutzbefohlenen und dem Opfer betrifft,[19] ausgeweitet, indem das einschränkende Tatbestandsmerkmal der Erregungsabsicht für § 174 III Nr. 2 StGB gestrichen wurde.

#### 2.1.1.2 §§ 174a-c StGB

Der Tatbestand des § 174a StGB, der den sexuellen Missbrauch von Gefangenen, behördlich Verwahrten oder Kranken und Hilfsbedürftigen in Einrichtungen unter Strafe stellt, wurde ebenfalls um Tathandlungen unter Einbeziehung Dritter erweitert.[20] Gleiches gilt für den sexuellen Missbrauch unter Ausnutzung einer Amtsstellung nach § 174b StGB sowie den sexuellen Missbrauch unter Ausnutzung eines Beratungs-, Behandlungs- oder Betreuungsverhältnisses nach § 174c StGB.[21]

### 2.1.2 §§ 176 ff. StGB

Während die §§ 174 ff. StGB nur kleinere Änderungen erfahren haben, wurden die Normen der §§ 176 ff. StGB, die den sexuellen Missbrauch von Kindern, also Personen unter 14 Jahren, zum Gegenstand haben, grundlegend umgestaltet und mit erheblichen Strafschärfungen und z.T. auch Straferweiterungen versehen.

#### 2.1.2.1 Systematische Umgestaltung

Ziel der systematischen Neuordnung der §§ 176 ff. StGB war es, die Übersichtlichkeit innerhalb der Straftatbestände zu verbessern.[22]

#### 2.1.2.1.1 § 176 StGB

Die Vorschrift des § 176 StGB stellt den sexuellen Missbrauch von Kindern unter Strafe und erfasst im Gegensatz zu der Vorgängerregelung nur noch Tatbestandsvarianten mit Körperkontakt zum Kind und die zugehörigen Vorfeldhandlungen.[23] Die Tathandlungen des § 176 I, II StGB a.F. gehen inhaltlich unverändert in § 176 I Nr. 1, 2 StGB auf. Das zuvor in § 176 V i.V.m. § 176 I, II StGB a.F. geregelte Anbieten eines Kindes und das Versprechen des Nachweises eines Kindes für eine Tat nach § 176 I Nr. 1, 2 StGB n.F. findet sich nun in § 176 I Nr. 3 StGB n.F. [24] Aus Verhältnismäßigkeitsgründen sieht § 176 II StGB für Fälle einvernehmlicher sexueller Handlungen annähernd gleichaltriger Personen eine Regelung vor, nach der im Einzelfall von einer Strafverfolgung abgesehen werden kann.

**Beispiel**: Die 14-jährige A gibt ihrem 13-jährigen Freund B einen Zungenkuss.

Mit der Kriminalisierung von Handlungen, die für die sexuelle Entwicklung von Kindern bzw. Jugendlichen wichtig sind, würde der gesetzgeberische Zweck der §§ 176 ff. StGB, nämlich die Möglichkeit des Kindes zur ungestörten Ausbildung der sexuellen Selbstbestimmung, konterkariert.[25] Der Abs. 2 soll daher einen Freiraum sexueller Selbsterprobung mit (annähernd) Gleichaltrigen sicherstellen.[26]

#### 2.1.2.1.2 § 176a StGB

Der zuvor als *„Schwerer sexueller Missbrauch von Kindern"* umschriebene § 176a StGB wurde völlig neu gefasst und beinhaltet nun den sexuellen Missbrauch von Kindern ohne Körperkontakt mit dem Kind. In § 176a StGB finden sich die bisher in § 176 IV Nr. 1, 2, 4, V StGB a.F. geregelten Tatalternativen, die sog. *„Hands-off-Delikte"*.[27] Mit der eigenständigen Regelung in einem eigenen Tatbestand soll dem unterschiedlichen Unrechtsgehalt von Tathandlungen mit und ohne Körperkontakt Rechnung getragen werden.[28] Zudem wurde § 176a I Nr. 1 um die Tatvariante ergänzt, in der der Täter die sexuelle Handlung vor einem Kind von einer dritten Person an sich vornehmen lässt. Hierdurch wurde die aufgrund der Unrechtsäquivalenz von Vornehmen und Vornehmenlassen wenig konsequente Lücke geschlossen und damit einer Empfehlung der Reformkommission nachgekommen.[29]

#### 2.1.2.1.3 § 176b StGB

§ 176b StGB wurde neu gefasst und regelt in einem eigenständigen Tatbestand die zuvor von § 176 IV Nr. 3 StGB a.F. erfasste Strafbarkeit des sog. Cybergroomings, also Tathandlungen zur Vorbereitung von sexualisierter Gewalt gegen Kinder.[30] Experten äußern diesbezüglich nach wie vor Kritik an der Verlagerung der Strafbarkeit weit ins Vorfeld sexueller Handlungen. Es sei unverständlich, warum die Vorbereitung eines sexuellen Kindesmissbrauchs strafbar sein solle, die Vorbereitung eines Mordes dagegen nicht.[31]

#### 2.1.2.1.4 §§ 176c, b StGB

Die §§ 176b, c StGB entsprechen weitestgehend den Regelungen der §§ 176a, 176b StGB a.F. Während § 176b StGB (Schwerer sexueller Missbrauch von Kindern) unterschiedliche Qualifikationstatbestände enthält, handelt es sich bei dem sexuellen Missbrauch von Kindern mit Todesfolge nach § 176b StGB um eine Erfolgsqualifikation.

#### 2.1.2.2 Strafschärfungen

Großes Aufsehen hat unter den Experten die Anhebung der Strafrahmen der §§ 176, 176a StGB erregt.[32] Der Strafrahmen des § 176 StGB wurde von sechsmonatiger bis zehnjähriger Freiheitsstrafe auf Freiheitsstrafe von einem bis fünfzehn Jahren erhöht und damit zu einem Verbrechen hochgestuft (§ 12 I StGB). Dies führt dazu, dass zum einen in materiellrechtlicher Hinsicht der Anwendungsbereich des § 30 StGB eröffnet und somit auch eine Vorfeldbestrafung möglich ist, und zum anderen in prozessrechtlicher Hinsicht eine Einstellung von Verfahren wegen des Verdachts des sexuellen Missbrauchs gegen Kinder aus Gründen der Opportunität wegen Geringfügigkeit nach den §§ 153, 153a StGB ausgeschlossen ist.[33] In § 176a StGB wurde der Strafrahmen von drei Monaten bis zu fünf Jahren auf sechs Monate bis zehn Jahre Freiheitsstrafe angehoben. Bei den übrigen Tatbeständen blieben die Strafrahmen weitgehend unverändert. Hervorzuheben ist in Bezug auf § 176b StGB aber noch, dass die Mindeststrafe für bestimmte Taten nach § 176 I Nr. 1, 2 StGB von einem Jahr auf zwei Jahre erhöht und die Regelung für minder schwere Fälle (§ 176a IV StGB a.F.) gestrichen wurde. Der Gesetzgeber begründet die Strafschärfungen zuvorderst mit der gestiegenen Zahl bekanntgewordener Fälle des sexuellen Missbrauchs von Kindern und erhofft sich einen besseren Schutz von Kindern sexualisierter Gewalt durch Abschreckungsprävention.[34] Dabei verschließt er sich aber kriminalpolitischen Erkenntnissen und ist insofern dem – berechtigten – Vorwurf einer *„symbolischen ad-hoc-Gesetzgebung"*[35] ausgesetzt.[36] Zugleich soll stärker als bisher das besonders schwere Unrecht der Tat widergespiegelt werden.[37] Unter dem Aspekt der besonderen Wehrlosigkeit der Tatopfer und der psychischen Langzeitfolgen solcher Taten, mag die Einordung als schwerstes Unrecht und der damit einhergehenden Gestaltung des Strafrahmens gerechtfertigt sein.[38]

### 2.1.3 § 184b StGB

Neben dem sexuellen Missbrauch von Kindern wurde auch der Tatbestand des § 184b StGB, der die zentrale Norm für Erscheinungsformen der Kinderpornographie darstellt,[39] neu gefasst und dabei der Strafrahmen enorm angehoben.

#### 2.1.3.1 Strafschärfungen

Nunmehr werden unterschiedslos alle Umgangsformen mit tatsächlicher und wirklichkeitsnaher Kinderpornographie, namentlich das Verbreiten, der Besitz und die Besitzverschaffung, als Verbrechen ausgestaltet.[40] Dabei sind die Strafrahmen der ersten drei Absätze gestaffelt. Bei der Verbreitung kinderpornographischer Inhalte droht gem. § 184b I StGB eine Freiheitsstrafe von einem Jahr bis zu zehn Jahren (zuvor: Freiheitsstrafe von drei Monaten bis zu fünf Jahren). Mit Freiheitsstrafe nicht unter zwei Jahren werden gem. § 184b II StGB Täter bestraft, die gewerbsmäßig oder als Mitglied einer Bande bestimmte kinderpornographische Inhalte verbreiten (zuvor: Freiheitsstrafe von sechs Monaten bis zu zehn Jahre). Massiv angehoben wurde der Besitz und die Besitzverschaffung von kinderpornographischen Inhalten nach § 184b III StGB auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren (zuvor: Freiheitsstrafe bis zu drei Jahren oder Geldstrafe).

Anlass der Strafschärfungen war eine aus Sicht des Gesetzgebers zu milde Sanktionspraxis der Gerichte sowie gestiegene Fallzahlen, aus denen eine zu geringe Abschreckungswirkung gefolgert wurde.[41] Ziel ist es, das Unrecht dieser Taten stärker widerzuspiegeln und eine der Schwere der Tat entsprechende Bestrafung zu ermöglichen. Zugleich sollen potentielle Täter von einer Straftatbegehung bereits im Vorfeld abgeschreckt und somit die Anzahl der Straftaten reduziert werden.[42]

In der Tat ist die Zahl der registrierten Taten nach § 184b StGB seit Jahren angestiegen.[43] Der Ansatz, dieser Problematik allein durch eine Verschärfung des Strafrahmens Herr zu werden, greift jedoch zu kurz und hat sich auch in der Vergangenheit nicht als probates Mittel erwiesen.[44] So beruht der massive Anstieg der Deliktszahlen nicht nur auf der ständigen Verfügbarkeit moderner Kommunikationsmittel, sondern auch auf einer insgesamt bei den Sexualdelikten deutlich angestiegenen Wahrnehmungs-, Anzeige- und Verfolgungsbereitschaft.[45] Hinzu kommt das Phänomen, dass zunehmend Kinder oder Jugendliche selbst entsprechende Inhalte herunterladen oder gar selbst erstellen und verbreiten.[46] Letztere Tatgruppe dem Bereich der Schwerstkriminalität zuzuordnen, scheint kaum angemessen.

Besonders kritisch zu würdigen ist zudem die Anhebung des Strafrahmens für den Besitz und die Besitzverschaffung von kinderpornographischen Inhalten gem. § 184b III StGB. Der Gesetzgeber rechtfertigt die Verschärfung damit, dass die Täter durch ihre Nachfrage den Markt für Kinderpornographie befeuerten und sich folglich am Missbrauch kindlicher Opfer mitschuldig machten.[47] Auch wenn dies einleuchtet, ist es schwer verständlich, dass etwa der nach § 184b III StGB strafbare bloße Besitz eines einzigen Bildes mit der *„sexuell aufreizenden Wiedergabe … des unbekleideten Gesäßes eines Kindes“* derselben Strafdrohung wie eine sexuelle Handlung mit Körperkontakt (§ 176 I StGB) unterliegt.[48] Angezeigt wäre viel mehr eine differenzierende Betrachtung nach Tätertypen und Handlungsweisen.[49]

#### 2.1.3.2 Privilegierung, § 184b I 2 StGB

Zur Wahrung der Verhältnismäßigkeit enthält § 184b I 2 StGB noch einen Vergehenstatbestand (Freiheitsstrafe von drei Monaten bis zu fünf Jahren) und privilegiert darin Taten nach § 184b I Nr. 1, 2 StGB, soweit lediglich fiktive, also erkennbar künstliche Kinderpornographie, betroffen ist.[50] Hierunter fallen z.B. kinderpornographische Comics, Zeichnungen, Inhalte in virtuellen Welten oder Erzählungen. Mangels Beteiligung eines realen Kindes bestünde nicht in gleicher Weise die Befürchtung einer Nachahmung der Konsumenten,[51] sodass hier etwa eine Geldstrafe über § 47 II StGB oder Einstellungen gem. § 153a StPO möglich sind.[52] Problematisch ist aber, dass angesichts des technischen Fortschritts in der Datenverarbeitung die Grenzen zwischen *„wirklichkeitsnaher“* und *„fiktiver“* Kinderpornographie verschwimmen und daher z.B. Formate der *„virtuellen Realität“* kaum zuverlässig einzuordnen sind.[53]

#### 2.1.3.3 § 184b V, VI StGB

Zuletzt wurde der Tatbestandsausschluss des § 184b V StGB a.F. für eine bessere Übersichtlichkeit und einfachere Zitierung in zwei Absätze aufgeteilt.[54] § 184b V StGB schließt die Strafbarkeit für Handlungen nach § 184b I 1 Nr. 2, III StGB aus, die ausschließlich der rechtmäßigen Erfüllung von staatlichen Aufgaben (Nr. 1), Aufgaben, die sich aus Vereinbarungen mit einer zuständigen staatlichen Stelle ergeben (Nr. 2) oder dienstlichen oder beruflichen Pflichten (Nr. 3) dienen. In § 184b VI StGB wird die Strafbarkeit nach § 184b I Nr. 1 und 4 StGB für bestimmte *„dienstliche Handlungen i.R.v. strafrechtlichen Ermittlungsverfahren“* ausgeschlossen.

### 2.1.4 § 184l StGB

Im Zuge der Gesetzesänderung wurde zudem mit § 184l StGB ein neuer Tatbestand geschaffen, der das Inverkehrbringen, den Erwerb und auch den Besitz von Sexpuppen mit kindlichem Erscheinungsbild pönalisiert.[55] Anlass waren wohl Funde solcher Sexpuppen i.R.d. Ermittlungen bei den Missbrauchsfällen von Bergisch-Gladbach und Münster.[56] Es handelt sich hierbei um ein abstraktes Gefährdungsdelikt, dem die Erwägung zu Grunde liegt, dass kindliche Sexpuppen die Neigungen von Missbrauchstätern bestärken und die Hemmschwelle, entsprechende Fantasien an echten Kindern auszuüben, senken könnte.[57] Gleichsam ist es aber auch möglich, dass ein Umgang mit kindlichen Sexpuppen die sexuellen Fantasien potentieller Täter mit pädophilen Neigungen befriedigt und insofern die Hemmschwelle erhöht.[58] In Anbetracht dessen, dass z.B. der Besitz entsprechender *„erwachsener“* Sexpuppen nicht pönalisiert wird, um eine mittelbare Förderung der Begehung von Straftaten nach § 177 StGB zu verhindern,[59] steht letztlich hinter der Gesetzesinitiative der Wille, ein unmoralisches Verhalten, die Pädophilie, zu bestrafen.[60] Tatobjekt ist die körperliche Nachbildung eines Kindes oder eines Körperteils eines Kindes, die nach ihrer Beschaffenheit zur Vornahme sexueller Handlungen bestimmt ist. Hierunter fallen i.d.R. Sexpuppen mit kindlichem Erscheinungsbild.[61] Wirklichkeitsgetreu muss die Nachbildung nicht sein.[62] Tathandlungen sind das Herstellen, Anbieten oder Bewerben (Nr. 1), das Handeltreiben oder

Verbringen (Nr. 2), sowie das Veräußern, Abgeben oder sonstige Inverkehrbringen ohne Handeltreiben (Nr. 3). Sie entsprechen im Wesentlichen § 184b I Nr. 3 und 4 StGB.[63]

**Beispiel**: A schenkt B eine Sexpuppe mit kindlichem Erscheinungsbild und macht sich somit nach § 184b I Nr. 3 Var. 2 StGB strafbar.

Für Fälle, in denen das Tatobjekt erworben, besessen oder ins Inland verbracht wird, normiert § 184l II StGB einen Qualifikationstatbestand.[64] Hier reicht die Strafe bis zu drei Jahren Freiheitsstrafe, während § 184l I StGB einen Höchststrafrahmen von fünf Jahren Freiheitsstrafe normiert. § 184l III StGB stellt den Versuch der § 184l I Nr. 2 und 3 StGB unter Strafe. In § 184l IV StGB wird der Tatbestand nach dem Vorbild des § 184b V StGB für Fälle ausgeschlossen, in denen durch die Tathandlung staatliche Aufgaben (z.B. Strafverfolgung) wahrgenommen werden bzw. dienstliche Pflichten erfüllt werden.[65] Eine Strafbarkeit nach § 184l StGB kommt gem. § 184l I 2 StGB nur in Betracht, wenn die Tat nicht nach § 184b StGB mit schwerer Strafe bedroht ist (formelle Subsidiarität). Der Gesetzgeber ist folglich davon ausgegangen, dass Sexpuppen zugleich pornographische Inhalte nach § 184b StGB sein können, wobei unklar geblieben ist, welche Fälle dies sein könnten.[66]

## 2.2 Strafprozessuale Begleitmaßnahmen

Zur Bekämpfung sexualisierter Gewalt gegen Kinder wurden zudem einige Maßnahmen zur Effektivierung der Strafverfolgung getroffen. So ist zum einen durch eine Änderung des § 112 III StPO die Anordnung von Untersuchungshaft unter erleichterten Voraussetzungen bei schwerem sexuellem Missbrauch gegen Kinder möglich.[67] Zum anderen besteht künftig gem. § 100a I, II Nr. 1 lit. g StPO die Möglichkeit zur Durchführung einer Telekommunikationsüberwachung auch bei Ermittlungen wegen Sichverschaffens oder Besitzes von Kinderpornographie nach § 184b III StGB.[68] Zuletzt kann nun bei sämtlichen Formen des schweren sexuellen Missbrauchs von Kindern sowie bei der Verbreitung kinderpornographischer Inhalte eine Onlinedurchsuchung angeordnet werden (vgl. § 100b I Nr. 1, II Nr. 1 lit. e, f StPO).

# 3 Strafbarkeit der Verbreitung und des Besitzes von Anleitungen zu sexuellem Missbrauch von Kindern

Durch das Gesetz zur Strafbarkeit der Verbreitung und des Besitzes von Anleitungen zu sexuellem Missbrauch von Kindern[69] wurde die Vorschrift des § 176e StGB eingeführt, die die Verbreitung und den Besitz von Anleitungen zu sexuellem Missbrauch von Kindern unter Strafe stellt.

## 3.1 Rechtspolitischer Hintergrund und geschützte Rechtsgüter

Die Einführung des § 176e StGB beruht auf dem stetigen Anstieg der Fallzahlen des sexuellen Missbrauchs in den letzten Jahren sowie der Beobachtung, dass im Internet (insbesondere im Darknet) vermehrt Anleitungen aufzufinden sind, wie sexueller Missbrauch vorbereitet, durchgeführt und verschleiert werden könne.[70] Solche *„Missbrauchsanleitungen"* könnten die Hemmschwelle potentieller Täter absenken und ihre Bereitschaft zur Begehung von Straftaten nach den §§ 176-176d StGB fördern. Zudem seien

## REZENSION

**Fischer, Strafgesetzbuch mit Nebengesetzen, Kommentar. 69. Auflage 2022**

Der Kommentar zum Strafgesetzbuch mit Nebengesetzen von Dr. Thomas Fischer dürfte jedem Juristen und jedem Polizeibeamten ein Begriff sein. Der von Otto Schwarz begründete und Eduard Dreher sowie Herbert Tröndle fortgeführte Handkommentar gehört zu den unverzichtbaren Standardwerken in Praxis und Studium. Die jährliche Neuauflage sorgt für eine besondere Aktualität.
Thomas Fischer, der das Werk seit der 50. Auflage herausgibt, ist Rechtsanwalt, Vorsitzender Richter am Bundesgerichtshof a.D. und Honorarprofessor an der Universität Würzburg.
Inhaltlich überzeugt der praxisgerechte und zugleich wissenschaftlich fundierte Kommentar auf ganzer Linie. Durch seine ausgezeichnete Strukturierung schafft er in kurzer Zeit einen umfassenden Überblick über Rechtsprechung und Lehrmeinungen, verliert sich aber nicht in verzichtbaren Einzelfragen. Den Kommentierungen sind der Normtext, eine Übersicht sowie Hinweise auf das einschlägige Schrifttum vorangestellt, so dass sich der Leser schnell und unkompliziert zurechtfinden kann und eine vertiefende Auseinandersetzung mit der Thematik ermöglicht wird. Als ausgesprochen positiv herauszustellen ist die Ausgewogenheit und Objektivität der Kommentierung. Der Autor legt den Schwerpunkt erkennbar auf die Rechtsprechung, vernachlässigt jedoch keineswegs relevante Literaturmeinungen.
Die 69. Auflage liegt mit dem Gesetzesstand vom November 2021 vor. Berücksichtigt werden seit der Vorauflage 13 Änderungsgesetze, durch die zahlreiche Normen neu eingefügt, aufgehoben oder modifiziert wurden. Exemplarisch hervorgehoben werden sollen nur die Neufassungen des § 238 StGB (Nachstellung) und des § 261 StGB (Geldwäsche). Daneben liegt der ausgewiesene Schwerpunkt der Neuauflage erneut auf der Einarbeitung der aktuellen Rechtsprechung und Literatur.
Aufgrund seiner Informationsfülle, Zuverlässigkeit und Aktualität ist der Kommentar für alle am Strafverfahren Beteiligten eine wichtige Grundlage und ohne Einschränkungen zu empfehlen.

Hartmut Brenneisen, Preetz/Worms

| | |
|---|---|
| **Herausgeber und Autor:** | **Thomas Fischer** |
| **Titel:** | **Strafgesetzbuch mit Nebengesetzen** |
| **Auflage:** | **69. Auflage 2022** |
| **Format:** | **2912 Seiten, 12,8 x 19,4 cm, Hardcover** |
| **Preis:** | **99,00 Euro** |
| **ISBN:** | **978-3-406-77219-1** |
| **Verlag:** | **Verlag C. H. Beck oHG** |

derartige Anleitungen durch die bestehenden Strafvorschriften, z.B. § 184b StGB (Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte), § 111 StGB (Öffentliche Aufforderung zu Straftaten), § 131 StGB (Gewaltdarstellung) oder § 140 StGB (Belohnung und Billigung von Straftaten) nur unzureichend erfasst.[71] Neben der Verhütung von Straftaten und der Schließung von Strafbarkeitslücken verfolgt die Vorschrift ferner das Ziel, eine Störung des Öffentlichen Friedens zu verhindern, wenn unter Nutzung menschenverachtender Sprache in derartigen Missbrauchsanleitungen Kinder als Objekte sexuellen Missbrauchs objektiviert werden.[72] Demnach schützt die Vorschrift sowohl den Schutz des Individualrechtsguts der sexuellen Selbstbestimmung als auch das Kollektivrechtsgut des Öffentlichen Friedens.[73] Sprachlich orientiert sich das abstrakte Gefährdungsdelikt an § 130a StGB.[74]

## 3.2 Tatbestand

### 3.2.1 § 176e I StGB

Tatgegenstand des § 176e I StGB ist ein Inhalt i.S.d. § 11 III StGB, der geeignet ist, als Anleitung zu einer rechtswidrigen Tat nach §§ 176-176d StGB zu dienen und zusätzlich dazu bestimmt ist, die Bereitschaft anderer zur Begehung solcher Taten zu fördern oder zu wecken. Anleitung ist nach der Gesetzesbegründung eine *„Schilderung, die Kenntnisse zu Möglichkeiten der Tatvorbereitung oder Tatausführung vermittelt."*[75] Sie muss keine Aufforderung an den Adressaten oder eine Billigung der Begehung beinhalten, sondern es genügt bereits, wenn sie die inhaltliche Vermittlung der Art und Weise, sexuellen Missbrauch an Kindern vorzubereiten, durchzuführen oder zu verschleiern, enthält.[76] Der Inhalt soll bereits dann als Anleitung geeignet sein, wenn er die Vorbereitung, die abstrakte Durchführung oder das Nachtatverhalten beschreibt. Konkrete Handlungsanweisungen sind nicht erforderlich.[77]

**Beispiel**: A gibt dem B Hinweise, wie man am besten zu einem Kind Kontakt aufnimmt, ohne Rückschlüsse auf die eigene Identität zuzulassen.

Zusätzlich muss der Inhalt aber aus objektiver Sicht dazu bestimmt sein, die Bereitschaft anderer zur Begehung von Taten nach §§ 176-176d StGB zu fördern oder zu wecken. Dabei braucht das Fördern und Wecken der Bereitschaft aber nicht das alleinige Ziel sein. Diesbezüglich genügt Eventualvorsatz.[78] Wie bei § 130a StGB reicht bereits das Hervorrufen einer generellen subjektiven Geneigtheit zur Begehung der Taten aus, ein konkreter Tatentschluss muss nicht hervorgerufen werden.[79] Die Tathandlungen des Verbreitens und des öffentlich Zugänglichmachen orientieren sich an den Begrifflichkeiten des § 130a StGB.[80]

### 3.2.2 § 176e II StGB

§ 176e II StGB enthält zwei Tatvarianten. Nach § 176e II Nr. 1 StGB macht sich strafbar, wer einen Inhalt, der geeignet ist, als Anleitung zu einer Tat nach §§ 176-176d StGB zu dienen, verbreitet oder öffentlich zugänglich macht. Im Unterschied zu § 176 I StGB ist hier keine objektive Bestimmtheit zur Anleitung erforderlich, so dass für sich betrachtet *„neutrale"* Inhalte, wie z.B. eine medizinische Abhandlung über die Besonderheiten der Geschlechtsorgane eines Kindes,[81] erfasst werden.[82] Als Ausgleich muss der Täter in der Absicht handeln, die Bereitschaft anderer zur Begehung solcher Taten zu fördern oder zu wecken. § 176e II Nr. 2 StGB setzt voraus, dass der Täter öffentlich bzw. in einer Veranstaltung eine Anleitung zu solchen Taten gibt und in der Absicht handelt, die Bereitschaft Dritter zu wecken oder zu fördern. Hierunter fallen gerade auch nicht verkörperte Äußerungen, v.a. Reden.[83]

### 3.2.3 § 176e III StGB

§ 176e III StGB qualifiziert Fälle, in denen der Täter den Inhalt i.S.d. § 176e I StGB tatsächlich abruft, besitzt, einer anderen Person zugänglich macht oder dieser den Besitz an ihm verschafft. Der im Vergleich zu § 176e I StGB (Freiheitsstrafe bis zu drei Jahren oder Geldstrafe) niedrigere Strafrahmen (Freiheitsstrafe mit bis zu zwei Jahren oder Geldstrafe) rechtfertigt sich aus der unterschiedlichen Größe der Empfängergruppe und dem damit einhergehenden geringeren abstrakten Gefährdungspotential.[84] Für Straftaten nach § 176e III StGB ermöglicht § 176e VI StGB die Einziehung der Tatgegenstände (§§ 74 ff. StGB). Sie ist der Regelung des § 184b VII StGB nachgebildet.[85]

### 3.2.4 § 176e IV, V StGB

Die § 176e IV, V StGB enthalten nach dem Vorbild der § 184b V, VI StGB Tatbestandsausschlüsse für Tathandlungen, die der Erfüllung rechtmäßiger Aufgaben bzw. dienstlichen Pflichten (§ 176e IV StGB) und bestimmten Aufgaben im strafrechtlichen Ermittlungsverfahren (§ 176e V StGB) dienen. Verdeckte Ermittler können sich dadurch zur Identifizierung einzelner Täter und Betreiber von kriminellen Handelsplattformen im Internet mit computergenerierten Bildern Zutritt zu kinderpornographischen Foren verschaffen, die oftmals als *„Eintrittskarte"* verlangt werden (sog. *„Keuschheitsprobe"*).[86]

## 4 Fazit

Im Zuge der letzten Gesetzesänderungen hat der Gesetzgeber zumindest punktuell eine systematisch sinnvolle Neuordnung der Straftaten gegen den sexuellen Missbrauch von Kindern vorgenommen.[87] Bedauerlicherweise hat er es aber verpasst, die sorgfältig ausgearbeiteten Empfehlungen der Reformkommission umzusetzen, v.a. was die Streichung von Straftatbeständen angeht.[88] Angeheizt von der politischen Debatte und medienwirksamen Fällen wurde stattdessen in kurzer Zeit ein Reformpaket auf den Weg gebracht und trotz zahlreicher kritischer Stellungnahmen umgesetzt, das die Anhebung von Strafrahmen und die Ausdehnung der Strafbarkeit als Allzweckwaffe für die Bekämpfung von sexuellem Missbrauch ansieht und auf generalpräventive Abschreckung setzt. Ob dies zum Ziel führt, scheint unter Berücksichtigung kriminalpolitischer Erkenntnisse äußerst zweifelhaft.[89] Insofern bleibt zu hoffen, dass bei dem nächsten Gesetzesvorhaben die von den Sachverständigen geäußerten Bedenken ernst genommen und entsprechend berücksichtigt werden. Eine rein symbolische Strafrechtspolitik hilft weder Täter noch Opfer.

Bildrechte: Redaktion.

## Anmerkungen

1 Prof. Dr. Dennis Bock ist Inhaber des Lehrstuhls für Deutsches und Internationales Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht an der Christian-Albrechts-Universität zu Kiel und Direktor des dortigen Instituts für Kriminalwissenschaften sowie Richter am Schleswig-Holsteinischen Oberlandesgericht. Frau Cathrin Lebro ist studentische Mitarbeiterin am Lehrstuhl von Prof. Dr. Bock.

2 S. für einen Überblick der Gesetzesänderungen Renzikowski, in: MK-StGB, 4. Aufl. 2021, Vor § 174 Rn. 89 ff.

3 BGBl. I 2015, S. 10.

4 BGBl. I 2016, S. 2460.

5 BMJV (Hrsg.), Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 180 ff., 343; näher zu möglichen Änderungen Bezjak ZStW 130, 328 ff.; Laubenthal FS Fischer, 2018, 435 ff.

6 Vgl. Renzikowski/Schmidt KriPoZ 2018, 325 ff.

7 Vgl. Spiegel Online v. 8.6.2020, abrufbar unter: https://www.spiegel.de/politik/deutschland/kindesmissbrauch-in-muenster-herbert-reul-wir-werden-garantiert-nie-alle-erwischen-a-02e52d17-b2f6-4637-8720-533e79fa985b (zuletzt abgerufen am 22.7.2022).

8 BGBl. I 2021, S. 1810 ff.

9 Vgl. Hoven/Obert JA 2021, 441 ff.

10 BGBl. I 2021, S. 4250 ff.
11 Bock/Lebro Die Kriminalpolizei Nr. 2 2021, 4 ff.; Nr. 3 2021, 8 ff.
12 LPK-StGB, 9. Aufl. 2022, Vor 174 ff., Rn. 5.
13 BT-Drs. 19/27928, S. 2.
14 BT-Drs. 19/27928, S. 2.
15 Vgl. BT-Drs. 19/23676, S. 2.
16 BT-Drs. 19/27928, S. 2.
17 Näher hierzu BT-Drs. 19/27928, S. 25 ff.
18 Vgl. BMJV (Hrsg.), Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 158, 324 f., 335.
19 Vgl. Fischer, StGB, 69. Aufl. 2022, § 174 Rn. 13.
20 Ziegler, in: BeckOK StGB, 53. Ed., Stand: 1.5.2022, § 174a Rn. 1.
21 Ziegler, in: BeckOK StGB, 53. Ed., Stand: 1.5.2022, § 174b Rn. 1, § 174c Rn. 1.
22 Vgl. Bussweiler ZRP 2021, 84, der an der Erreichung dieses Ziels zweifelt.
23 Hoven/Obert JA 2021, 441 (444).
24 BT-Drs. 19/23707, S. 38.
25 Vgl. BT-Drs. 19/23707, S, 38.
26 BT-Drs. 19/23707, S, 38.
27 Ziegler, in: BeckOK StGB, 53. Ed., Stand: 1.5.2022, § 176a Rn. 1; zur Begrifflichkeit s. Bussweiler ZRP 2021, 84.
28 BT-Drs. 19/23707, S, 39.
29 BT-Drs. 19/23707, S. 39; Hoven/Obert JA 2021, 441 (446); BMJV (Hrsg.), Abschlussbericht der Reformkommission zum Sexualstrafrecht, 19.7.2017, S. 108; Bezjak, in: Abschlussbericht der Reformkommission, 841 (849).
30 LPK-StGB, 9. Auf. 2022, § 176b Rn. 1.
31 So etwa Schönke/Schröder/Eisele, 30. Aufl. 2019, StGB § 176 Rn. 14.
32 Vgl. Renzikowski KriPoZ 2020, 308 (312); Hörnle ZIS 2020, 440 (443); Kreuzer KriPoZ 2020, 263 (266); Stellungnahme des Deutschen Richterbundes, September 2020, S. 3 f.; Stellungnahme des Deutschen Anwaltvereins, September 2020, S. 9; Luczak/Martens DRiZ 2020, 382 f.
33 LPK-StGB, 9. Aufl. 2022, § 176 Rn. 1; BT-Drs. 19/23707, S. 38.
34 Vgl. BT-Drs. 19/23707, S. 1, 21, 60.
35 Eisele LTO v. 6.7.2020, https://www.lto.de/recht/hintergruende/h/lambrecht-bekaempfung-kindesmissbrauch-kinderpornografie-strafen-gewalt-bmjv-muenster-verbrechen (zuletzt abgerufen am 22.7.2022).
36 Vgl. Eisele, in: Schönke/Schröder/Eisele, StGB, 30. Aufl. 2019, StGB Vor §§ 174 ff. Rn. 9; Kreuzer KriPoZ 2020, 263 (264); Renzikowski KriPoZ 2020, 308 (312); Stellungnahme des Deutschen Anwaltvereins, September 2020, S. 9.
37 Vgl. BT-Drs. 19/23707, S. 60.
38 So Hoven/Obert JA 2021, 441 (443); kritisch Hörnle ZIS 2020, 440 (441).
39 LPK-StGB, 9. Aufl. 2022, § 184b Rn. 1.
40 Bussweiler ZRP 2021, 84 (86).
41 BT-Drs. 19/23707, S. 20 f., 41.
42 Vgl. BT-Drs. 19/23707, S. 41.
43 Vgl. PKS 2019 Tatziffer 143200.
44 Vgl. Laue NJOZ 2020, 1441 ff.
45 Vgl. Fischer, StGB, 69. Aufl. 2022, § 184b Rn. 2a.
46 Vgl. Fischer, StGB, 69. Aufl. 2022, § 184b Rn. 2a; Bussweiler, ZRP 2021, 84 (86).
47 Vgl. BT-Drs. 19/23707, S. 41.
48 Vgl. Renzikowski KriPoZ 2020, 308 (315).
49 Näher zu Lösungsansätzen Bussweiler ZRP 2021, 84 ff.
50 Vgl. BT-Drs. 19/23707, S. 41.
51 Vgl. BT-Drs. 19/23707, S. 41.
52 Vgl. Fischer, StGB, 69. Aufl. 2022, § 184b Rn. 46.
53 So Fischer, StGB, 69. Aufl. 2022, § 184b Rn. 14.
54 Vgl. BT-Drs. 19/23707, S. 41.
55 Vgl. Fischer, StGB, 69. Aufl. 2022, § 184l Rn. 2.
56 Plenarprotokoll 19/187 Deutscher Bundestag 187. Sitzung am 30.10.2020, S. 23561.
57 Fischer, StGB, 69. Aufl. 2022, § 184l Rn. 2 f.; Renzikowski KriPoZ 2020, 308 (315 f.).
58 So Fischer, StGB, 69. Aufl. 2022, § 184l Rn. 3.
59 Vgl. Fischer, StGB, 69. Aufl. 2022, § 184l Rn. 3.
60 So Renzikowski KriPoZ 2020, 308 (315 f.) m.w.N; kritisch zur Einführung des Delikts auch Frommel NK 2021, 150 ff.
61 BT-Drs. 19/23707, S. 42; LPK-StGB, 9. Auf. 2022, § 184l Rn. 2.
62 BT-Drs. 19/23707, S. 42
63 Renzikowski KriPoZ 2020, 308 (315).
64 LPK-StGB, 9. Auf. 2022, § 184l Rn. 5.
65 LPK-StGB, 9. Auf. 2022, § 184l Rn. 7.
66 Vgl. Fischer, StGB, 69. Aufl. 2022, § 184l Rn. 8.
67 Vgl. BT-Drs. 19/23707 S. 46.
68 Vgl. BT-Drs. 19/23707, S. 45.
69 BGBl. I 2022, S. 4250.
70 Vgl. BT-Drs. 19/31115, S. 11.
71 Vgl. BT-Drs. 19/31115, S. 11.
72 Vgl. BT-Drs. 19/31115, S. 11.
73 Fischer, StGB, 69. Aufl. 2022. § 176e Rn. 2.
74 LPK-StGB, 9. Aufl. 2022, § 176e Rn. 1.
75 BT-Drs. 19/31115, S. 12.
76 BT-Drs. 19/31115, S. 12.
77 BT-Drs. 19/31115, S. 12.
78 BT-Drs. 19/31115, S. 12.
79 BT-Drs. 19/31115, S. 12.
80 LPK-StGB, 9. Aufl. 2022, § 176e Rn. 4.
81 BT-Drs. 19/31115, S. 12.
82 Fischer, StGB, 69. Aufl. 2022, § 176e Rn. 8.
83 Ziegler, in: BeckOK StGB, 53. Ed., Stand: 1.5.2022, § 176e Rn. 11.
84 BT-Drs. 19/31115, S. 13.
85 Ziegler, in: BeckOK StGB, 53. Ed., Stand v. 1.5.2022, § 176e Rn. 20.
86 Näher zu verdeckten Ermittlungen wegen §§ 176e, 184b StGB s. Soiné NStZ 2022, 321 ff.
87 So Hoven/Obert JA 2021, 441 (448); kritischer Bussweiler ZRP 2021, 84 f.
88 Näher hierzu BMJV (Hrsg.), Abschlussbericht der Reformkommission zum Sexualstrafrecht, 2017, S. 180 ff., 343; näher zu möglichen Änderungen Bezjak ZStW 130, 328 ff.; Laubenthal FS Fischer, 2018, 435 ff.
89 Vgl. zur mangelnden Wirksamkeit präventiver Strafschärfungen Laue NJOZ 2020, 1441.

# „Vertrauen ist gut" – Von der Verwertbarkeit erlangter Daten bezüglich sogenannter Kryptohandys

Von Oberstaatsanwalt Dr. Sören Pansa und Staatsanwalt Dr. Marius Heller, Schleswig/Kiel[1]

## 1 Einleitung

Im Frühjahr 2020 brandete ein Ruf wie Donnerhall über die Flure der Landeskriminalämter und Staatsanwaltschaften: *„ENCROCHAT"*. Eine genaue Vorstellung, was genau sich dahinter verbarg, dürften die meisten dabei nicht gehabt haben. Aber man hatte viel gehört: Angeblich überwachungssichere Mobiltelefone, welche von Kriminellen genutzt wurden, die jedoch sehr unvorsichtig vorgegangen sein sollen. Hierzu muss gesagt werden, dass bis zu diesem Zeitpunkt Telekommunikationsüberwachungen, insbesondere bezüglich des Betäubungsmittelhandels eher ernüchternd verliefen. Dies resultierte zum einen aus dem typischerweise konspirativen Vorgehen der Beteiligten. Zum anderen aus der bereits seit Längerem zunehmenden Nutzung sog. Messenger-Dienste, welche eine Überwachung stark

erschwerten. Hierauf hat der Gesetzgeber am 17. August 2017 durch die Schaffung der *„Online-Durchsuchung"* i.S.d. § 100b StPO und der *„Quellen-Telekommunikationsüberwachung"* i.S.d. § 100a Abs. 1 S. 2 StPO reagiert.[2] Doch bereits die erste oberflächliche Sichtung der Encrochat-Kommunikationsinhalte machte die zuletzt durchwachsene Entwicklung der Telekommunikationsüberwachung schlagartig vergessen. So hatten die Nutzer in vollkommenen Vertrauen auf die Qualität ihrer Mobiltelefone tatsächlich meist nicht nur Betäubungsmittel fotografiert, sondern oftmals auch gleich den Abholer samt Ausweisdokumenten, denn der Verkäufer musste schließlich wissen, wem er die große Tasche in die Hand drücken sollte. Im Anschluss an die Auswertung der Daten folgten in der gesamten Bundesrepublik Deutschland zunächst Vollstreckungen zahlreicher Untersuchungshaftbefehle und anschließend rechtskräftige Verurteilungen zu teils langjährigen Freiheitsstrafen. Daraufhin äußerten sich zahlreiche Strafverteidiger bezüglich der Verwertbarkeit der Daten, welche, wenig überraschend, einhellig abgelehnt wurde.[3] Der 5. Strafsenat des Bundesgerichtshofes hat inzwischen ausführlich zu dem Themenkomplex *„Encrochat"* Stellung genommen.[4] Ein gebührender Anlass, sich nunmehr einen umfassenden Überblick über den gegebenen Sachverhalt und die hiermit verbundenen rechtlichen Probleme zu verschaffen.

## 2 Sachverhalt

Am 15. Juli 2021 hat das Landgericht Hamburg einen Angeklagten wegen Verstößen gegen das Betäubungsmittelgesetz zu einer Freiheitsstrafe von 5 Jahren verurteilt. Maßgeblich für die Überzeugungsbildung des Landgerichts war dabei die Kommunikation des Angeklagten, welche dieser über das verschlüsselte Nachrichtensystem EncroChat geführt hat. Den in Frankreich durchgeführten Ermittlungsmaßnahmen zur Erlangung der relevanten EncroChat-Kommunikation lag folgender verfahrensrechtlicher Sachverhalt zugrunde:

In den Jahren 2017 und 2018 stellten französische Behörden in mehreren nicht im Zusammenhang stehenden Ermittlungsverfahren – in denen es überwiegend um den Handel mit Betäubungsmitteln im Kilogrammbereich ging – fest, dass die Tatverdächtigen jeweils über sog. Kryptohandys verfügten, die über eine sog. EncroChat-Architektur verschlüsselt waren. Aufgrund der Verschlüsselung war eine Auswertung dieser Mobiltelefone nicht möglich. Nach ersten Ermittlungsergebnissen wurden die Kryptohandys mit folgenden Produktmerkmalen beworben: *„Garantie der Anonymität, personalisierte Android Plattform, doppeltes Betriebssystem, allerneueste Technik, automatische Löschung von Nachrichten (‚Advanced Burn'), schnelles Löschen (‚Panic Wipe'), Unantastbarkeit (‚Tamper Proofing'), Kryptografie-Hardwaremodul"*. Folgende Anwendungen waren auf dieser Art von Telefonen verfügbar: *„EncroChat (Instant-Secure Messaging Kunde), EncroTalk (Chiffrierung der Sprachkonversationen auf IP), EncroNotes (Chiffrierung der lokal auf dem Gerät gespeicherten Notizen)"*. Telefonieren oder das Internet benutzen, konnte man mit diesen Geräten hingegen nicht. Kommunikation war nur zwischen Kunden von EncroChat möglich. Über offizielle Vertriebskanäle konnten derartige Telefone nicht erworben werden. Auf Internetplattformen wurden entsprechende Geräte für 1.610 Euro angeboten, wobei dieser Preis eine Nutzerlizenz für die Dauer von sechs Monaten beinhaltete. Ein existierendes Unternehmen *„EncroChat"* war ebenso wenig zu lokalisieren wie diesbezüglich verantwortlich handelnde Personen oder ein Unternehmenssitz.

In Frankreich leitete die Staatsanwaltschaft Lille im November 2018 aufgrund des wiederholten Auftauchens[5] dieser Geräte ein Ermittlungsverfahren u.a. wegen des Verdachts einer kriminellen Vereinigung ein und fand heraus, dass die verschlüsselte Kommunikation zwischen EncroChat-Nutzern über einen im französischen Roubaix betriebenen Server lief. Nach Einholung eines richterlichen Beschlusses wurden am 21. Dezember 2018 und im Oktober 2019 die Daten des Servers kopiert und in der Folgezeit ausgewertet. Hierbei ergab sich, dass 66.134 SIM-Karten eines niederländischen Anbieters im System eingetragen waren, die in einer Vielzahl europäischer Länder verwendet wurden. Eine Dechiffrierung mehrerer tausend *„Notizen"* von EncroChat-Nutzern belegte, dass diese zweifelsfrei mit illegalen Aktivitäten wie Betäubungsmittelhandel mit bis zu 60 kg Kokain in Verbindung standen. Dabei belegten die Notizen das Handeltreiben in einer ungewohnt offenen Weise, da die Nutzer von einer Abhörsicherheit und *„Unverletzlichkeit"* ihrer Telefone ausgegangen waren.

Am 30. Januar 2020 genehmigte das Gericht in Lille auf Antrag der Staatsanwaltschaft den Einsatz einer Datenabfangeinrichtung sowohl auf dem Server als auch auf den mit diesem Server verbundenen Endgeräten, wobei die Installation dieser *„Trojanersoftware"* in Einklang mit der französischen Strafprozessordnung durch den damit beauftragten Generaldirektor für innere Sicherheit unter Rückgriff auf der Geheimhaltung der Nationalen Verteidigung unterliegende Staatsmittel ausgeführt werden sollte. Mangels anderer Ermittlungsmöglichkeiten, den Chiffrierungsschutz zu umgehen, genehmigte das Gericht in Lille am 20. März 2020 darüber hinaus u.a. eine Umleitung aller Datenströme (DNS-Umleitung) des Servers in Roubaix ab dem 1. April 2020. Zur Begründung hatte die Staatsanwaltschaft Lille darauf verwiesen, die bisherigen Ermittlungen hätten bestätigt, dass EncroChat-Geräte für kriminelle Zwecke verwendet würden und es aufgrund der Unmöglichkeit, die Endgeräte zu *„analysieren"*, nur die Installation einer Datenabfangeinrichtung ermöglichen könne, die Chiffrierung zu umgehen.

Das durch den technischen Dienst für die justiziellen Abfangmaßnahmen entwickelte Softwaretool wurde sodann durch die französischen Behörden per *„Ferninjektion"* eingebracht, wobei auf Mittel zurückgegriffen wurde, die der Geheimhaltung der nationalen Verteidigung unterliegen. Dabei wurde bekannt, dass von der Datenabfangmaßnahme 32.477 Nutzer in 121 Ländern betroffen waren. Von den 380 in Frankreich aktiven Telefonen wurden nach ersten Erkenntnissen jedenfalls 63,7% für kriminelle Zwecke verwendet. Die übrigen Geräte waren entweder teils inaktiv oder noch nicht ausgewertet.

Am 7. April 2020 wurden die Ermittlungen auf Transport, Besitz, Erwerb, Anbieten oder Abgabe von Betäubungsmitteln und den Besitz und Erwerb von Waffen ohne Genehmigung ausgedehnt, nachdem die ausgewerteten Gespräche und die Überprüfung der ausgetauschten Fotos das ganze Ausmaß des von den Nutzern betriebenen Betäubungsmittelhandels offenlegten. Ein durch das Abfangen der Daten erlangter Leitfaden zur Vermarktung der chiffrierten Telefone enthielt folgende Hinweise: a) Es soll vorzugsweise in Kryptowährung gezahlt werden, b) Man soll sich gegenüber der Polizei bedeckt halten und insbesondere vermeiden, durch mengenmäßig zu große Lieferungen aufzufallen. Ein Verkäufer der Mobiltelefone wies insbesondere darauf hin, dass die Polizei die Telefone nicht lokalisieren könne, sie nicht abgehört werden und nicht genutzt werden könnten, wenn sie *„in schlechte Hände"* fielen. Insgesamt gingen Staatsanwaltschaft und Gericht in Auswertung der im ersten Monat erlangten Daten von einem *„nahezu ausschließlich kriminelle(n) Klientel"* der EncroChat-Nutzer aus.[6]

Anhand dieser Erkenntnisse wurden die aufgrund der richterlichen Anordnung zeitlich begrenzten technischen Maßnahmen zunächst für einen Monat ab 1. Mai 2020 und darauffolgend für weitere vier Monate ab 1. Juni 2020 – jeweils mit richterlichem Beschluss – verlängert und die Deliktstatbestände, derentwegen ermittelt wurde, erweitert.

Dem Bundeskriminalamt wurden in der Folgezeit über Europol Erkenntnisse zugleitet, wonach in Deutschland eine Vielzahl

schwerster Straftaten, insbesondere Einfuhr und Handeltreiben mit Betäubungsmitteln in nicht geringen Mengen von EncroChat-Nutzern begangen würden. Bei der Generalstaatsanwaltschaft Frankfurt am Main, Zentralstelle zur Bekämpfung der Internetkriminalität, wurde ein Verfahren gegen Unbekannt u.a. wegen des Verdachts von Betäubungsmittelstraftaten eingeleitet. In diesem Verfahren erging am 2. Juni 2020 eine an Frankreich gerichtete Europäische Ermittlungsanordnung mit dem Antrag, die Deutschland betreffenden EncroChat-Daten zu übermitteln und deren unbeschränkte Verwendung in deutschen Strafverfahren zu erlauben. Beides genehmigte ein französisches Gericht am 13. Juni 2020. Die im Rahmen des Rechtshilfeersuchens übermittelten Informationen könnten dabei von den deutschen Behörden im Rahmen eines jeden Ermittlungsverfahrens und im Hinblick auf ein jedwedes Gerichts-, Strafverfolgungs- oder Untersuchungsverfahren oder Urteil verwendet werden.[7]

Auf Bitte der französischen Behörden übermittelte Europol der Generalstaatsanwaltschaft Frankfurt am Main die zwischen dem 1. April 2020 und dem 30. Juni 2020 auf den EncroChat-Servern erfassten Daten, die sich auf Geräte bezogen, die zu einer Auslösung von Mobilfunkantennen auf deutschem Boden geführt hatten. In diesem Zeitraum wurden auch die Landeskriminalämter, der Zoll und die Bundespolizei über das Vorliegen der EncroChat-Daten informiert. Mit Zustimmung der Generalstaatsanwaltschaft Frankfurt am Main wurden ihnen die Daten zur Verfügung gestellt, um eine gemeinsame Auswerte- und Ermittlungstätigkeit unter der Sachleitung der Generalstaatsanwaltschaft Frankfurt am Main zu realisieren. Die Schwierigkeit bestand dabei darin, die Identität der Nutzer der Krypto-Handys zu ermitteln, da bisher ja ausschließlich deren *„Nicknames“* bekannt waren. Dabei wurden die Nutzer anhand ihrer Geodaten den örtlich zuständigen Ermittlungsbehörden vorläufig zugeordnet. Durch eine solche Zuordnung sollte zunächst die Erstbearbeitung eines Nutzers erfolgen und der Datenbestand koordiniert gesichtet werden. Eine endgültige Festlegung der örtlichen und sachlichen Zuständigkeiten erfolgte erst nach inhaltlicher Auswertung der EncroChat-Daten. Für die inhaltliche Auswertung war es in der Folgezeit in einer Vielzahl von Verfahren erforderlich, mehrere zigtausend Chatzeilen in die deutsche Sprache zu übersetzen. Sodann mussten die Chatverläufe akribisch mit erheblichem Aufwand nach Anhaltspunkten für eine Identifizierung des jeweiligen Nutzers durchsucht werden. Eine Identifizierung konnte dabei vielfach durch versandte Lichtbilder (der Person des Nutzers selbst, ihrer PKW, Strafzettel, Wohnungen etc.) oder durch Hinweise auf den Wohnort, die persönlichen/familiären Verhältnisse sowie verbüßte Freiheitsstrafen erfolgen. Es kann dabei nicht oft genug betont werden, dass hierbei eine effektive Bearbeitung nur möglich war, da keine der involvierten Ermittlungsbehörden starr auf örtlichen Zuständigkeiten beharrte. Denn die Taten eines Nutzers erstreckten sich typischerweise auf zahlreiche Städte. Ferner waren oftmals mehrere Personen beteiligt, welche ebenfalls an unterschiedlichen Orten aufhältig waren. Insofern kann der Encrochat-Komplex wohl als eines der erfolgreichsten Beispiele deutscher Strafverfolgung bezeichnet werden, an welchem Ermittlungsbehörden nahezu aller Bundesländer beteiligt waren.

## 3 Erwägungen des Bundesgerichtshofes

Im Weiteren werden die rechtlichen Erwägungen des Bundesgerichtshofs hinsichtlich der Verwertbarkeit der erlangten EncroChat-Daten dargestellt.

### 3.1 Rechtsgrundlage für die Verwertung der Daten

Der Bundesgerichtshof stellt seiner Entscheidung voran, dass die verfassungsgemäße Rechtsgrundlage für die Verwertung von Beweisen im Strafprozess § 261 StPO (Grundsatz der freien richterlichen Beweiswürdigung) bildet. Dies gilt unabhängig davon, ob diese Beweise im Inland oder auf sonstige Weise – etwa im Wege der Rechtshilfe – erlangt worden sind. Eine ausdrückliche Regelung, dass im Wege der Rechtshilfe aus dem Ausland erlangte Daten nur eingeschränkt verwendet werden dürfen, enthält das deutsche Recht nicht, insbesondere ist § 100e Abs. 6 StPO hierauf nicht unmittelbar anwendbar.[8]

Ein von der Revision des Angeklagten in Einklang mit großen Teilen des Schrifttums und vereinzelter Rechtsprechung[9] geltend gemachtes Beweisverwertungsverbot hinsichtlich der erlangten EncroChat-Daten besteht nach Auffassung des Bundesgerichtshofs unter keinem rechtlichen Gesichtspunkt. Ein solches ergibt sich weder aus rechtshilfespezifischen Gründen (vgl. 3.2) noch aus nationalem Verfassungs- oder Prozessrecht (vgl. 3.3). Auch die Vorgaben der Europäischen Menschenrechtskonvention (EMRK) stehen einer Beweisverwertung nicht entgegen (vgl. 3.4).

### 3.2 Kein Beweisverwertungsverbot aus rechtshilfespezifischen Gründen

Im Rahmen der Entscheidung erfolgen umfangreiche Ausführungen bezüglich eines potentiellen Beweisverwertungsverbotes unter rechtshilfespezifischen Aspekten. Hierbei handelt es sich zwar um eine vergleichsweise spezielle Materie, welcher Staatsanwälten und Polizeibeamten bei der täglichen Arbeit noch eher selten begegnen. Dessen ungeachtet soll im Folgenden auf die wesentlichen Problempunkte eingegangen werden. Denn zum einen nimmt die internationale Zusammenarbeit von Ermittlungsbehörden (glücklicherweise) stetig zu, weshalb auch die praktische Relevanz der diesbezüglichen Vorschriften exponentiell steigt. Zum anderen werden diese vom Bundesgerichtshof dargestellten Grundsätze auch für zukünftige vergleichbare Verfahren vollumfängliche Gültigkeit beanspruchen können.

Zunächst soll aufgrund der für einige Leser wohl eher unbekannten Materie kurz auf die Grundsätze der internationalen Zusammenarbeit in Strafsachen innerhalb der Europäischen Union eingegangen werden. Prägend für diese ist das Prinzip gegenseitiger Anerkennung strafjustizieller Entscheidungen der Mitgliedstaaten.[10] Hieraus folgen zahlreiche Aspekte, welche eine Rechtshilfe innerhalb der Europäischen Union stark vereinfachen. Etwa eine grundsätzlich bestehende gegenseitige Unterstützungspflicht. Sowie ein weitreichender Verzicht auf die sachliche Überprüfung ausländischer Entscheidungen. Am 3. April 2014 sind diese Grundsätze in der Richtlinie über die Europäische Ermittlungsanordnung (RL-EEA) manifestiert worden - 2014/41/EU -, deren Vorschriften der deutsche Gesetzgeber in den §§ 91a ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG) am 22. Mai 2017 im Wesentlichen übernommen hat.[11] Seitdem kooperien die Mitgliedstaaten mittels der Europäischen Ermittlungsanordnung, wie es auch die Bundesrepublik Deutschland und Frankreich auf die beschriebene Weise im Juni 2020 getan haben. Der Bundesgerichtshof befasste sich daher mit der Frage, ob die Übermittlung der Encrochat-Daten an die Bundesrepublik Deutschland von den bezeichneten Rechtsgrundlagen getragen wird.

Zunächst wird dabei auf einen möglichen Verstoß gegen den sog. orde-public-Grundsatz eingegangen, welcher unter anderem in § 91b IRG und § 73 IRG Eingang gefunden hat. Dieser besagt im Wesentlichen, dass eine Rechtshilfe zu unterbleiben hat, wenn eine solche gegen elementare rechtstaatliche Grundsätze verstoßen,

insbesondere eine erhebliche Grundrechtsverletzung darstellen würde.[12] Der Bundesgerichtshof führt diesbezüglich aus, dass allein aufgrund der beschriebenen Verwendung der Encrochat-Kryptohandys ein Anfangsverdacht gegen die Nutzer wegen schwerer Straftaten aus dem Bereich der Betäubungsmittelkriminalität gegeben war. Insofern habe gerade keine rechtswidrige verdachtslose Telekommunikationsüberwachung stattgefunden. Vielmehr waren die französischen Ermittlungsbehörden angesichts der Verdachtslage und aufgrund des staatlichen Auftrags zum Schutz der Bürger vor den von organisierter Betäubungsmittelkriminalität ausgehender Gefahren sowie des verfassungsrechtlichen Gebots einer funktionsfähigen Strafrechtspflege zur Vornahme von Ermittlungsmaßnahmen befugt. Grundlegende Rechtsstaatsdefizite oder Verstöße gegen menschen- bzw. europarechtliche Grundwerte wären hierin nicht zu erkennen.[13]

Des Weiteren käme auch ein Verstoß gegen Art. 31 RL-EEA und dessen Umsetzung in § 91g Abs. 6 IRG in Betracht. Art. 31 RL-EEA sieht eine Pflicht zur Benachrichtigung des von einer grenzüberschreitenden Telekommunikationsüberwachung betroffenen Zielstaates durch den überwachenden Staat vor. Der Zielstaat soll dann innerhalb von 96 Stunden entscheiden können, ob die Maßnahmen abgebrochen und die gewonnenen Erkenntnisse durch den überwachenden Staat nicht oder nur eingeschränkt verwendet werden dürfen. Im konkreten Fall wäre daher fraglich, ob Frankreich die Bundesrepublik Deutschland unmittelbar von den Maßnahmen bezüglich der EncroChat-Server hätte unterrichten müssen, jedenfalls soweit hiervon auch Nutzer auf dem Gebiet der Bundesrepublik Deutschland betroffen waren. Der Bundesgerichtshof lässt dahinstehen, ob es sich bei der Infiltration der Server überhaupt um eine mitteilungsbedürftige Telekommunikationsüberwachung gehandelt haben könnte. Ferner wird ausgeführt, dass ein Individualschutz des Art. 31 RL-EEA hinsichtlich betroffener Bürger wohl lediglich bezüglich einer Verwendung der erlangten Daten in etwaigen französischen Ermittlungsverfahren bestehen würde. Denn nur vor einer nicht gewollten Datenverwendung außerhalb des von der Telekommunikationsüberwachung betroffenen Zielstaates soll die Mitteilungspflicht des Art 31 RL-EEA schützen.[14] Letztlich lässt der Bundesgerichtshof aber auch dies dahinstehen. Denn selbst wenn Art. 31 RL-EEA individualschützender Charakter zukäme, würde ein etwaiger Verstoß nicht zu einem Beweisverwertungsverbot bezüglich der an die Bundesrepublik Deutschland übermittelten Daten führen. Dem Strafverfahrensrecht lässt sich kein allgemein geltender Grundsatz entnehmen, wonach jeder potentielle Verstoß gegen Rechtsnormen ein strafprozessuales Verwertungsverbot nach sich zieht. Ob ein solches eingreift, ist vielmehr jeweils nach den Umständen des Einzelfalls, insbesondere nach der Art des Verbots und dem Gewicht des Verstoßes, unter Abwägung der widerstreitenden Interessen zu entscheiden. Maßgeblich beeinflusst wird das Ergebnis der Abwägung einerseits durch das Ausmaß des staatlichen Aufklärungsinteresses,

## REZENSION

**Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar. 65. Auflage 2022**

Der nunmehr in der 65. Auflage vorliegende Kommentar bietet ausgesprochen überzeugende Erläuterungen zur zielgerichteten Lösung aller strafprozessualen Fragestellungen an. Die Darstellungen orientieren sich unmittelbar an den Erfordernissen der Praxis, sind jedoch zugleich auch wissenschaftlich fundiert. Neben der Strafprozessordnung werden die für das Strafverfahren einschlägigen Vorschriften des Gerichtsverfassungsgesetzes sowie weiterer Rechtsnormen erläutert bzw. ergänzend aufgenommen. Dies gilt z.B. für die praxisrelevanten Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) sowie die Anordnung über Mitteilungen in Strafsachen (MiStra).

Seit mehreren Jahren trägt Prof. Dr. Bertram Schmitt die Verantwortung für das Werk, der Prof. Dr. Lutz Meyer-Goßner abgelöst hat. Bertram Schmitt ist Richter am Internationalen Strafgerichtshof, Richter am Bundesgerichtshof (zur Wahrnehmung der Tätigkeit beim IStGH beurlaubt) und Honorarprofessor an der Universität Würzburg. Der Kommentar ist unter der fachlichen Mitarbeit von Marcus Köhler, Richter am Bundesgerichtshof und Lehrbeauftragter an der Universität Leipzig, entstanden, der u.a. die für die Polizei besonders relevanten Bestimmungen der §§ 94 bis 111q sowie §§ 158 bis 163g StPO bearbeitet hat.

Inhaltlich überzeugt das Werk auf ganzer Linie. Durch seine sehr gute Strukturierung schafft es in kurzer Zeit einen umfassenden Überblick über Rechtsprechung und fachspezifische Literatur, verliert sich aber nicht in verzichtbaren Einzelmeinungen. Den Kommentierungen sind der Normtext und eine Übersicht vorangestellt, so dass sich der Leser schnell zurechtfinden kann. Ein maßvoll eingesetzter Fettdruck lässt wichtige Stichworte und die Jahreszahlen der Rechtsprechungsnachweise leichter finden. Als ausgesprochen positiv herauszustellen ist die Ausgewogenheit der Ausführungen, die den Schwerpunkt erkennbar auf die Rechtsprechung legen, relevante Literaturmeinungen jedoch nicht vernachlässigen.

Die vorliegende Auflage befindet sich hinsichtlich Gesetzgebung, Rechtsprechung und Schrifttum auf dem Stand vom März 2022. Berücksichtigt wurden so z.B. das Gesetz zur Fortentwicklung der StPO vom 25.6.2021 (BGBl. I 2021, 2099) mit zahlreichen Neuerungen und Anpassungen. Aus der Judikatur ist insbesondere auf die Entscheidung des BGH zur Verwertbarkeit von Encrochat-Daten (BGH v. 2.3.2022, 5 StR 457/21-juris) und den Nichtannahmebeschluss des BVerfG zur Unzulässigkeit konkludenter Absprachen im Strafverfahren (BVerfG v. 29.4.2021, 2 BvR 1543/20-juris) hinzuweisen.

In der Gesamtschau ist der Kommentar als unverzichtbares Standardwerk anzusehen. Aufgrund seiner überzeugenden Informationsfülle und Aktualität durch jährliches Erscheinen ist er für alle am Strafverfahren Beteiligten eine wichtige Grundlage. Dies gilt auch für Polizeivollzugsbeamte in Theorie und Praxis.

Hartmut Brenneisen, Preetz/Worms

| | |
|---|---|
| **Autoren:** | **Bertram Schmitt, Marcus Köhler** |
| **Titel:** | **Strafprozessordnung mit GVG und Nebengesetzen** |
| **Auflage:** | **65. Auflage 2022** |
| **Format:** | **2758 Seiten, DIN A 5, Hardcover** |
| **Preis:** | **105,00 Euro** |
| **ISBN:** | **978-3-406-78383-8** |
| **Verlag** | **Verlag C.H. Beck oHG** |

dessen Gewicht im konkreten Fall vor allem unter Berücksichtigung der Verfügbarkeit weiterer Beweismittel, der Intensität des Tatverdachts und der Schwere der Straftat bestimmt wird. Andererseits ist das Gewicht des in Rede stehenden Verfahrensverstoßes von Belang, das sich vor allem danach bemisst, ob der Rechtsverstoß gutgläubig, fahrlässig oder vorsätzlich begangen wurde.[15] Dabei muss beachtet werden, dass die Annahme eines Verwertungsverbots, auch wenn die Strafprozessordnung nicht auf Wahrheitserforschung um jeden Preis gerichtet ist, eines der wesentlichen Prinzipien des Strafverfahrensrechts einschränkt, nämlich den Grundsatz, dass das Gericht die Wahrheit zu erforschen und dazu die Beweisaufnahme von Amts wegen auf alle relevanten Tatsachen und Beweismittel zu erstrecken hat. Daran gemessen bedeutet ein Beweisverwertungsverbot eine Ausnahme, die nur nach ausdrücklicher gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist.[16] Dies kommt etwa in Betracht, bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen, bei denen die grundrechtlichen Sicherungen planmäßig oder systematisch außer Acht gelassen werden.[17] Im Rahmen der erforderlichen Abwägung führt der Bundesgerichtshof dann prägnant aus: *„Es geht um die Aufklärung besonders schwerwiegender Straftaten, nämlich Verbrechen nach § 29a Abs. 1 Nr. 2 BtMG, die im Höchstmaß mit Freiheitsstrafe von 15 Jahren bedroht sind. Andere Beweismittel stehen hier für die Überführung des Angeklagten in den von seinem Geständnis nicht erfassten Fällen nicht zur Verfügung, so dass ohne die Verwertung dieser Beweismittel eine Überführung des Angeklagten in den relevanten Fällen nicht möglich wäre. Die EncroChat-Protokolle sind als Beweismittel besonders ergiebig, da darin offen über Drogengeschäfte in erheblichem Umfang kommuniziert wird. Demgegenüber fiele ein etwaiger individualschutzbezogener Rechtsverstoß […] nicht entscheidend ins Gewicht“.*

Zuletzt soll bezüglich dieses Themenkomplexes eine mögliche Verletzung des Art. Art 6 RL-EEA problematisiert werden. Art. Art 6 RL-EEA sieht u.a. vor, dass mittels einer Europäische Ermittlungsanordnung nur Maßnahmen erbeten werden können, welche in einem vergleichbaren innerstaatlichen Fall unter denselben Bedingungen angeordnet werden könnten. Der Bundesgerichtshof erklärt diese Regelung in der gegebenen Konstellation jedoch für nicht anwendbar. Denn es handele sich lediglich um die Übermittlung der durch einen anderen Mitgliedstaat aufgrund eigener Ermittlungstätigkeit nach dessen nationalem Recht bereits erlangten Beweismittel. Die Durchführung einer Ermittlungsmaßnahme wäre also seitens der Bundesrepublik Deutschland gerade nicht erbeten worden; vielmehr wäre diese ja bereits seitens der französischen Behörden erfolgt. Der Anordnungsstaat müsse in Konstellationen, in welchen auf die erlangten Erkenntnisse eines anderen Staates zugegriffen werden soll, lediglich prüfen, ob der Erlass der Europäischen Ermittlungsanordnung für die Zwecke des Verfahrens unter Berücksichtigung der Rechte der Verfahrensbeteiligten notwendig und verhältnismäßig ist. Diese Voraussetzung erfüllt dabei die Europäische Ermittlungsanordnung der Generalstaatsanwaltschaft Frankfurt am Main von Juni 2020, da insbesondere unter Berücksichtigung der sehr hohen Kosten für Erwerb und Nutzung von EncroChat-Handys klare Anhaltspunkte dafür vorlagen, dass die Beweismittel sich auf schwerste Straftaten aus dem Bereich der organisierten Kriminalität bezogen, deren Aufklärung ohne Zugriff auf die in Frankreich erlangten Informationen ansonsten kaum möglich gewesen wäre.[18]

## 3.3 Kein Beweisverwertungsverbot aus nationalem Verfassungsrecht

Ein Beweisverwertungsverbot ergibt sich nach den Ausführungen des Bundesgerichtshofs auch nicht unmittelbar aus deutschem Verfassungsrecht. Ein absolutes Beweisverwertungsverbot unmittelbar aus den Grundrechten, kann überhaupt nur im absoluten Kernbereich privater Lebensgestaltung bestehen, was bei der Planung und Durchführung von Straftaten hingegen nicht der Fall ist.[19]

Die Verwertung personenbezogener Informationen wie der EncroChat-Kommunikation greift zwar grundsätzlich in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Dabei hängt die durch die Verwertung der Daten liegende Eingriffsintensität maßgeblich davon ab, welchen Grad an Persönlichkeitsrelevanz die betroffenen Daten haben und auf welchem Weg sie erlangt wurden.[20] Bei wie hier erlangten Daten, die mit einen Eingriff in das von Art. 10 GG geschützte Fernmeldegeheimnis einhergehen, muss von Verfassungs wegen der Verhältnismäßigkeitsgrundsatz besonders beachtet werden.

Im Rahmen innerstaatlicher Ermittlungen wird der Grundrechtseingriff durch die unterschiedlichen Voraussetzungen für verschiedene Ermittlungsmaßnahmen bereits bei der Anordnung der Maßnahme selbst limitiert (etwa Beschränkung auf besonders schwere Straftaten oder Fälle qualifizierten Verdachts). Kann diese Beschränkung in Fällen wie dem vorliegenden nicht geleistet werden, weil hier durch einen anderen Mitgliedstaat (Frankreich) in originärer Anwendung seines nationalen Rechts in die Grundrechte Betroffener eingegriffen wird, sind die dadurch möglichen Unterschiede bei den Eingriffsvoraussetzungen auf der Ebene der Beweisverwendung zu kompensieren.[21]

Zu diesem Zweck greift der Bundesgerichtshof in seiner Entscheidung sodann auf die in den strafprozessualen Verwendungsbeschränkungen verkörperten Wertungen zurück, die insoweit als verfassungsrechtliche Schutzmechanismen für die Beweisverwertung dienen. Demnach dürfen aufgrund der Bedeutung der französischen Ermittlungsmaßnahmen in Anlehnung an die Verwendungsschranke mit dem höchsten Schutzniveau – § 100e Abs. 6 Nr. 1 StPO[22] – derart erlangte Daten zur Überführung solcher besonders schwerer Straftaten verwendet werden, für deren Aufklärung die eingriffsintensivsten Ermittlungsmaßnahmen des deutschen Strafverfahrensrechts – namentlich eine Online-Durchsuchung gem. § 100b StPO oder eine akustische Wohnraumüberwachung gem. § 100c StPO – hätten angeordnet können.[23]

Die im vorliegenden Fall in Rede stehenden Verbrechen erfüllen die Voraussetzungen für eine Beweisverwertung nach dieser gebotenen strikten Verhältnismäßigkeitsprüfung. Die Vorwürfe wiegen auch im Einzelfall schwer, da es jeweils um den Handel mit Betäubungsmitteln im Kilogrammbereich geht und die Erforschung des Sachverhalts ohne dieses Beweismittel nicht möglich wäre.

Weiter betont der Bundegerichtshof, es wäre unter verfassungsrechtlichen Aspekten gerade nicht geboten, dass das deutsche Strafprozessrecht eine entsprechende Ermittlungsmaßnahme vorsieht. Die bloße Nichteinhaltung deutschen Rechts bei einer ausländischen Ermittlungsmaßnahme kann nicht per se ein unselbstständiges Beweisverwertungsverbot begründen.[24] Die Einhaltung rechtstaatlicher Mindeststandards wird in solchen Fällen – wie vorstehend ausgeführt – insbesondere durch eine strikte Verhältnismäßigkeitsprüfung unter (entsprechender) Anwendung besonderer nationaler Verwendungsvorbehalte gewährleistet.[25]

## 3.4 Kein Verstoß gegen Vorgaben der Europäischen Menschenrechtskonvention (EMRK)

Schließlich führt der Bundesgerichtshof aus, dass die Verwertung der EncroChat-Daten auch mit den Regelungen der EMRK vereinbar ist. Insbesondere sind zu einem Beweisverwertungsverbot führende Verstöße gegen Art. 8 EMRK (Recht auf

Achtung des Privat- und Familienlebens) sowie Art. 10 EMRK (Freiheit der Meinungsäußerung) bei einer durch einen Richter angeordneten Maßnahme bezüglich der gegenständlichen schweren Straftaten nicht festzustellen.[26]

## 4 Resümee

Die Entscheidung des Bundesgerichtshofes ist absolut zu begrüßen und in ihren Formulierungen erfreulich deutlich. Es wäre aber wohl auch kaum dem *„Bürger von der Straße"* zu vermitteln, wenn derartige Daten, welche sich nahezu ausschließlich auf schwerste Straftaten beziehen, und die geeignet sind, diese unmittelbar zu beweisen, nicht seitens der Ermittlungsbehörden verwertet werden dürften. Ferner muss es diesen möglich sein, bezüglich technischer Aufrüstungsmaßnahmen krimineller Organisationen reagieren zu können. Denn insbesondere dieser Ermittlungskomplex hat wieder einmal nachhaltig verdeutlicht, wie umfassend die Beteiligten bereits technische Neuerungen genutzt und wie wenig sie ihr Handeln an Landesgrenzen ausgerichtet haben. Die Bekämpfung derartiger krimineller Netzwerke setzt daher entschlossenes Vorgehen der Ermittlungsbehörden, einen steten überregionalen bzw. internationalen Austausch der jeweiligen Erkenntnisse und die Koordinierung der Ermittlungshandlungen voraus. Von der Bereitschaft zu überobligatorischem Einsatz ganz zu schweigen. All dies haben die beteiligten Behörden in beeindruckendem Maße bezüglich des *„Encrochat-Komplexes"* umgesetzt und so sicherlich einige Wirkungstreffer im Bereich des internationalen Betäubungsmittelhandels landen können. Die dabei eingeübten Handlungsroutinen dürften sich auch in naher Zukunft bei der Auswertung der erlangten Daten aus den mit Encrochat vergleichbaren Krypto-Netzwerken *„SkyECC"*[27] und *„ANOM"*[28] als nützlich erweisen. Angesichts dieses wegweisenden Beschlusses des Bundesgerichtshofes dürften der Verwertbarkeit auch dieser Daten in deutschen Strafprozessen keine Bedenken entgegenstehen.

## Anmerkungen

1 Dr. Sören Pansa ist bei der Generalstaatsanwaltschaft Schleswig-Holstein und Dr. Marius Heller bei der Staatsanwaltschaft bei dem Landgericht Kiel tätig. Der Beitrag gibt ausschließlich die persönliche Auffassung der Verfasser wieder.
2 BGBl. I 2017, 3202ff.
3 Vgl. statt vieler Gerhard/Michalke, NJW 2022, 655; Strate HRRS 2022, 15; Nadeborn/Albrecht, NZWiSt 2021, 420.
4 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 –, zitiert nach juris; inzwischen hat der 4. Strafsenat des Bundesgerichtshofes diese Entscheidung inhaltlich bestätigt: Beschluss vom 5. Juli 2022 - 4 StR 61/22 -, zitiert nach juris.
5 Nach einer im Jahr 2019 durch das Bundeskriminalamt durchgeführten Abfrage sollen im Zeitraum von Oktober 2018 bis September 2019 etwa 75% der bekannt gewordenen Kryptohandys in Deutschland solche des Anbieters EncroChat gewesen sein.
6 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 18, zitiert nach juris.
7 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 22, zitiert nach juris.
8 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 25, zitiert nach juris.
9 Derin/Singelnstein, NStZ 2021, 449; dies., StV 2022, 130; Erhard/Lödden, StraFo 2021, 366; Gebhard/Michalke, NJW 2022, 655; Wahl, ZIS 2021, 452; LG Berlin, Beschluss vom 1. Juli 2021 – [525 KLs] 254 Js 592/20 [10/21], NStZ 2021, 696.
10 Hierzu zusammenfassend: BGH, Beschluss vom 23. April 2020 – 1 StR 15/20 –, NJW 2020, 3185 (3188).
11 BGBl. I 2017, S. 31ff.
12 Vgl. hierzu umfassend Gleß/Wahl/Zimmermann in Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, 6. Aufl. 2020, § 73 IRG Rn. 1 ff.
13 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 36ff., zitiert nach juris.
14 So auch Wahl, ZIS 2021, 452 (457).
15 Vgl. statt vieler BGH, Urteil vom 20. Oktober 2021 – 6 StR 319/21 –, zitiert nach juris.
16 BGH, Urteil vom 18. April 2007 – 5 StR 546/06 –, BGHSt 51, 285.
17 BGH, Beschluss vom 21. April 2016 – 2 StR 394/15 –, StV 2016, 539.
18 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 46ff., zitiert nach juris.
19 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 62, zitiert nach juris.
20 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 64, zitiert nach juris.
21 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 68, zitiert nach juris.
22 Die Vorschrift des § 100e Abs. 6 StPO ist nach ihrem Wortlaut auf die vorliegende Konstellation nicht anwendbar, da die in Rede stehenden Daten nicht nach den §§ 100b, 100c StPO, sondern durch eigenständige Maßnahmen nach französischem Prozessrecht erlangt wurden.
23 Für diese Prüfung ist dabei auf den Erkenntnisstand im Zeitpunkt der Verwertung der Beweisergebnisse abzustellen, auf die Rekonstruktion der Verdachtslage im Anordnungszeitpunkt kommt es indes nicht an, BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 70, zitiert nach juris; a. A. LG Berlin, Beschluss vom 1. Juli 2021 – [525 KLs] 254 Js 592/20 [10/21], NStZ 2021, 696.
24 BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, Rn. 72 f, zitiert nach juris.
25 Ob für den Fall eines – hier nicht ersichtlichen – sog. *„Befugnis-Shoppings"*, also eines Rechtshilfeersuchens zwecks bewusster Umgehung strengerer inländischer Anordnungsvorrausetzungen, eine andere Bewertung vorzunehmen wäre, hat der BGH offengelassen, vgl. BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, Rn. 75, zitiert nach juris.
26 BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 77, zitiert nach juris.
27 Vgl. OLG Celle, Beschluss vom 15. November 2021 – 2 HEs 24 - 30/21 –, NdsRpfl 2022, 87.
28 Vgl. OLG Frankfurt, Beschluss vom 22. November 2021 – 1 HEs 427/21 –, NJW 2022, 710.

# Der Verdeckte Ermittler im LVwG SH – Eine überzeugende Ergänzung?

Von KK Lasse Dähling, Kiel[1]

## 1 Einleitung

Mit der Novellierung des Landesverwaltungsgesetzes Schleswig-Holstein (LVwG SH) im Februar 2021 hat der Gesetzgeber wichtige Regelungen im Bereich des Polizeirechts neu erfasst und strukturiert.[2] Nach mehr als dreijähriger Vorbereitung sind diverse Rechtsgrundlagen neu geschaffen, konkretisiert oder nach aktueller Rechtsprechung grundrechtskonform ausgestaltet worden, um den heutigen Anforderungen an die polizeiliche Gefahrenabwehr gerecht zu werden. So ist beispielsweise der *„finale Rettungsschuss"* gem. § 258 Abs. 1 S. 2 LVwG SH normiert sowie die Möglichkeit des Einsatzes von Distanz-Elektroimpulsgeräten (DEIG) gem. § 258a LVwG SH und körpernah getragener Aufnahmegeräten *(„Bodycams")* gem. § 184a LVwG SH geschaffen worden. Auch die elektronische Aufenthaltsüberwachung *(„Fußfessel")* gem. § 201b LVwG SH hat Einzug in das schleswig-holsteinische Polizeirecht gehalten.

Neben den oben genannten Bestimmungen wurden auch wesentliche Regelungen im Bereich der verdeckten Maßnahmen erneuert. Diese finden regelmäßig in Bereichen der Schwerstkriminalität wie z.B. organisierter Kriminalität oder politisch bzw. religiös motivierter Kriminalität Anwendung.[3] Hier können häufig aufgrund der abgeschotteten Personenkreise und deren konspirativen Verhalten mit offenen polizeilichen Maßnahmen nicht ausreichend Informationen zur Gefahrenlage erhoben werden, gleichzeitig jedoch gebietet die Gefahrenlage für gewichtige Rechtsgüter den Einsatz solch eingriffsintensiver Maßnahmen. Insbesondere bei Sachverhalten in der Terrorismusabwehr, zu denen oft noch keine strafbare Handlung vorliegt, wohl aber die Gefahr eines extremistisch motivierten Anschlags hinreichend begründet werden kann[4], sind solch verdeckte Maßnahmen daher vielfach wichtige Quellen der Datenerhebung, um die Gefahr abzuwenden. Sowohl die neu geschaffene Möglichkeit der Unterbrechung der Telekommunikation gem. § 185b LVwG SH als auch die nun umfangreiche Ausgestaltung der Rechtsgrundlage zum Einsatz von Vertrauenspersonen (VP) gem. § 185c LVwG SH (welche vor der Novellierung allenfalls rudimentär gefasst war) können dabei geeignete Mittel zur Abwendung der Gefahr sein. Hier wurde zusammen mit der Anpassung der gesamten Normen der verdeckten Maßnahmen im Sinne des Urteils des BVerfG zum BKAG[5] ein großes Stück Normenklarheit und Grundrechtsschutz geschaffen.

## 2 Verdeckter Ermittler als Datenerhebungsmaßnahme gem. § 185 LVwG SH

Daran schließt sich auch die Neueinfügung des Verdeckten Ermittlers (VE) an. Dieser wurde mit der Novellierung in § 185 Abs. 1 Nr. 3 LVwG SH als *„Polizeivollzugsbeamtin oder Polizeivollzugsbeamten unter einer ihr oder ihm verliehenen, auf Dauer angelegten Legende“*[6] legal definiert und reiht sich damit in die besonderen Mittel der Datenerhebung des § 185 LVwG SH als spezielle Ermächtigungsgrundlage ein.[7] Anders als ein *„undercover agent“*, der komplett in die Szene eintaucht[8], soll ein VE für eine bestimmte Zeit im Rahmen eines klar definierten Auftrags verdeckt Daten erheben.[9]

Die Maßnahme unterliegt (allein schon aus der Systematik heraus) denselben Eingriffsvoraussetzungen wie die anderen in § 185 LVwG SH normierten Maßnahmen, z.B. der längerfristigen Observation. Es müssen damit gem. § 185 Abs. 2 LVwG SH Tatsachen vorliegen, die einen Schaden für die dort genannten Rechtsgüter erwarten lassen und die Maßnahme zur Sachverhaltsaufklärung unerlässlich machen.

Über die bereits vor der Novellierung genannten Rechtsgüter Leib, Leben und Freiheit von Personen sowie gleichgewichtige Sach- und Vermögenswerte und die Umwelt sind nun auch der Bestand und Sicherheit des Bundes bzw. eines Landes genannt.

Dieser Ausfluss aus dem Urteil des BVerfG zum BKAG ist vor dem Hintergrund der stetig anhaltenden Gefahr terroristischer Bedrohungen in Deutschland[10] durchweg zu begrüßen, da Täter von terroristischen Anschlägen regelmäßig das Sekundärziel verfolgen, durch eine möglichst öffentlichkeitswirksame Tat den Bestand oder die Sicherheit des Staates zu erschüttern.[11] Auch wenn aus der Gefahr eines einzelnen Anschlags sicherlich nicht immer zwangsläufig auf eine Gefahr für den Bestand des Bundes geschlossen werden kann,[12] ist doch allen extremistischen Strömungen die Ablehnung bzw. Abschaffung der freiheitlich demokratischen Grundordnung und die damit verbundene Implementierung einer anderen Staatsordnung gemein.[13] Somit könnte nun bei einer solchen Gefahrenlage auch auf das langfristig verfolgte Ziel abgestellt werden, insbesondere wenn möglicherweise noch kein detaillierter Anschlagsplan besteht, aber schon der Tatentschluss mit entsprechender Motivation gefasst wurde.

Demonstrative Proteste gegen die Novellierung des LVwG SH.

## 3 Problematik des Einsatzes in Wohnungen

In § 185 Abs. 4 LVwG SH werden Einzelheiten zum Einsatz von VE näher ausgestaltet. So dürfen für den Aufbau bzw. die Aufrechterhaltung der Legende eines VE Urkunden ausgestellt, verändert und gebraucht werden, wenn es für den Einsatz unerlässlich ist. Auch darf der VE unter der Legende (z.B. mit diesen Urkunden) am Rechtsverkehr teilnehmen.

Ihm wird außerdem gestattet, unter der Legende Wohnungen zu betreten, solange er das Einverständnis des Berechtigten hat und er das Zutrittsrecht nicht über eine Täuschung, die über die Legende hinausgeht, erhalten hat.[14]

Ob aus der Ermächtigung des Betretens von Wohnungen auch die Erlaubnis zur Datenerhebung in der betretenen Wohnung folgt, ist nicht vollends ersichtlich und kann in der praktischen Umsetzung rechtliche Unsicherheiten bergen. Gerade in einem geschützten, nicht-öffentlichen Umfeld wie der eigenen Wohnung können dem VE unter Umständen Informationen anvertraut werden, die er ansonsten an anderen Orten nicht erhalten würden. Eine Aussparung von Wohnung beim Einsatz von VE wäre daher vollkommen lebensfremd.

Doch auch wenn unter teleologischen Gesichtspunkten die konkludente Erlaubnis zur Datenerhebung in Wohnungen unter den genannten Voraussetzungen angenommen werden kann,[15] würde hier eine Klarstellung ein deutliches Mehr an Rechtssicherheit bringen. Insbesondere vor dem systematischen Hintergrund, dass im vorangestellten Absatz 3 explizit die Datenerhebung mit den Mitteln aus § 185 Abs. 1 LVwG SH (zu denen eben auch der Einsatz von VE zählt) behandelt wird und die Eingriffsschwelle für diese Fälle deutlich erhöht wird, wäre ein Hinweis über die Nicht-Anwendung des § 185 Abs. 3 LVwG SH für den VE wünschenswert gewesen.

## 4 Systematik, Anordnungskompetenz

Aus systematischer Betrachtung wäre auch insgesamt (unabhängig von dem Problem der Datenerhebung in Wohnungen) die Einfügung einer eigenständigen Norm für den Einsatz von VE statt einer Integration in den § 185 LVwG SH klarer gewesen.

Die Mehrzahl der anderen Bundesländer[16] hat die Ermächtigungsgrundlage entweder in einer eigenen Norm gefasst oder zumindest eine gemeinsame Norm mit dem Einsatz von VP geschaffen, womit der Maßnahme des VE-Einsatzes als komplexes, wichtiges Mittel der verdeckten Datenerhebungen Rechnung getragen werden kann. Die Einführung einer eigenständigen Bestimmung hat der schleswig-holsteinische Gesetzgeber im Rahmen der Novellierung aber lediglich mit dem Einsatz von VP vollzogen, welcher nun in § 185c LVwG SH geregelt wird. Unter anderem als Ausfluss aus dem Parlamentarischen Untersuchungsausschuss des

schleswig-holsteinischen Landtags zum *„Subway-Verfahren"* wurden hier insbesondere die Voraussetzungen und Verfahrensweisen zur Anwerbung, der Dokumentation und justiziellen Kontrolle in bisher nicht dagewesenem Umfang ausgestaltet.[17]

Angesichts gleicher Eingriffsschwelle, gleicher Anordnungskompetenz und ähnlicher Verfahrensweisen in der Umsetzung erscheint es umso weniger nachvollziehbar, dass nicht auch für den Einsatz von VE eine eigene Norm (oder zumindest eine gemeinsame Bestimmung mit dem Einsatz von VP) geschaffen wurde. An dieser Stelle wurde eine wichtige Chance verpasst, auf systematische Weise zwei wesensverwandte Maßnahmen sinnvoll miteinander zu kombinieren und widerspruchsfrei in die Reihe der anderen verdeckten Maßnahmen einzugliedern.

Der Einsatz des VE steht wiederum folgerichtig gem. § 186 Abs. 1 Nr. 4 LVwG SH unter Richtervorbehalt. Bei Gefahr im Verzug kann die Maßnahme auch durch die Leitung des Landespolizeiamts, Landeskriminalamts, Polizeidirektion oder einer besonders beauftragten Person angeordnet werden. Eine richterliche Bestätigung muss dann unverzüglich eingeholt werden, nach drei Tagen tritt ansonsten die polizeiliche Anordnung außer Kraft.

Dies wird grundsätzlich der hohen Eingriffsintensität der Maßnahme[18] gerecht, muss doch davon ausgegangen werden, dass dem VE im Zweifelsfall höchstpersönliche Lebenssachverhalte aus der Intim- und Privatsphäre im Vertrauen offenbart werden. Auch faktische Filter wie die Verschriftlichung durch den VE-Führer oder die Aufnahmefähigkeit des VE selbst können nicht darüber hinwegtäuschen, dass sich der Verantwortliche nach Bekanntwerden des Einsatzes oft einem massiven Vertrauensverlust ausgesetzt sieht, was oft langfristige Auswirkungen für den Verantwortlichen haben kann. Auch vor dem Hintergrund der historischen Erfahrungen mit verdeckt ermittelnden Angehörigen von Sicherheitsbehörden (u.a. den Mitarbeitern des Ministeriums für Staatssicherheit in der Deutschen Demokratischen Republik) erscheint der Richtervorbehalt sowohl für den VE als auch für den Einsatz von VP angemessen.

Die Maßnahme kann gem. § 186 Abs. 3 LVwG SH auf höchstens sechs Monate befristet werden, danach muss ein Antrag auf Verlängerung erfolgen, andernfalls ist die Maßnahme zu beenden. Hier hat der Gesetzgeber erkannt, dass eine Differenzierung bei den Fristen der verdeckten Maßnahmen angezeigt ist, da der erfolgreiche Einsatz eines VE inklusive gründlicher Vorbereitung des Beamten deutlich zeitintensiver ist als beispielsweise eine Observation.[19] Ob dabei sechs Monate ausreichend sind, kann strittig diskutiert werden, denn besonders bei im entsprechenden Milieu eingebundenen, konspirativ agierenden Verantwortlichen kann der Aufbau eines Vertrauensverhältnisses mitunter Jahre dauern. Andererseits wird die Frist aber (auch im Vergleich mit den anderen verdeckten Maßnahmen) durchaus der hohen Eingriffsintensität gerecht und schützt den Bürger vor *„jahrelangem Auskundschaften"* im Sinne einer *„Geheimpolizei"*.[20]

Die neu formulierten Dokumentationspflichten stellen hingegen eindeutig einen Gewinn im Sinne des Grundrechtsschutzes dar und bedienen das Urteil des BVerfG zum BKAG vollumfänglich.

Besondere Protestform bei einer angezeigten/angemeldeten Versammlung.

## 5 Kernbereichsschutz

Ebenfalls Ausfluss des Urteils des BVerfG zum BKAG[21] sind die in § 186a LVwG SH normierten Vorschriften zum Schutz des Kernbereichs, welche auch für den Einsatz von VE entsprechend einschlägig sind. Diese sind zwar für einen effektiven Schutz dieses *„letzten unantastbaren Bereichs menschlicher Freiheit"*[22] unabdingbar, bergen jedoch bezogen auf den Einsatz eines VE Schwierigkeiten in der praktischen Umsetzung.

Eine weitere Problematik dürfte der Umgang mit unfreiwillig[23] erhobenen Informationen aus dem Kernbereich sein. Besonders im Fall eines langjährig aufgebauten, engen Vertrauensverhältnisses (welcher noch eher beim Einsatz von VP vorkommen dürfte) erscheint es nicht völlig abwegig, dass dem VE auch Sachverhalte anvertraut werden, die in der Gesamtbetrachtung zum Kernbereich gezählt werden müssen.[24] Während die nachträgliche Betrachtung in Grenzfällen schon die Problematik von erneuten Gesprächen über dieses Thema nach sich ziehen dürfte, ist der Umgang des VE mit klaren Fällen des Kernbereichsschutzes in der konkreten Situation aus Sicht des Autors ein bislang kaum geregelter Graubereich. Hier kann die Empfehlung von Frister, VE (beim strafprozessualen Einsatz) müssten die Wahrnehmung *„höchstpersönlicher Inhalte vermeiden"*[25], nur begrenzt überzeugen.

Es wäre eine konkret auf die Maßnahme bezogene Klarstellung sinnvoll, denn im Gegensatz zu den technisch basierten Maßnahmen wie der Telekommunikationsüberwachung oder der Wohnraumüberwachung, bei denen im Falle eines Tangierens des Kernbereichs die Maßnahme sofort unterbrochen werden kann, ist dies beim VE nicht so abrupt möglich, ohne zumindest die Maßnahme (wenn nicht sogar Leib und Leben des Beamten) zu gefährden.

## 6 Fazit

In der Gesamtbetrachtung ist die Einfügung einer Ermächtigung für den Einsatz von VE im LVwG SH zu begrüßen, da die Maßnahme als wichtiges Mittel der Schwerstkriminalität das Portfolio der bereits bestehenden verdeckten Datenerhebungsmaßnahmen sinnvoll erweitert. Damit hält diese Maßnahme in Schleswig-Holstein als letztem Bundesland Einzug ins Polizeirecht. Je nach Betrachtungsweise könnte man hier von einem Zugewinn an Harmonisierung zwischen den Bundesländern oder einem längst überfälligen Schritt sprechen.

Gerade im Zuge einer angestrebten Harmonisierung wäre es jedoch vorteilhaft gewesen, sowohl inhaltlich als auch systematisch-redaktionell im Gleichklang mit anderen Bundesländern vorzugehen. Neben den tatbestandlichen Voraussetzungen und den Anforderungen an die Verhältnismäßigkeit als auch in Bezug auf die Anordnungskompetenzen und -fristen besteht ein föderaler *„Flickenteppich"*, in den sich auch Schleswig-Holstein einreiht, auch wenn Pietsch dies in anderem Sachzusammenhang als *„Wesensmerkmal des (Sicherheits-)Föderalismus"* betrachtet.[26]

Beispielhaft seien hier die Anordnungsfristen der verschiedenen Länder genannt. Diese reichen von drei Monaten[27] bis zu

einem Jahr[28], teilweise wird auch gar keine Frist definiert[29]. Eine fachliche Begründung für die Auswahl bestimmter Fristen ist jeweils nicht ersichtlich, sondern dürfte sich vielmehr an den jeweiligen politischen Mehrheitsverhältnissen orientieren. Für eine effiziente, länderübergreifende polizeiliche Gefahrenabwehr wären jedoch einheitliche Rahmenbedingungen, besonders für solch eingriffsintensive verdeckte Maßnahmen, eine wesentliche Verbesserung im Sinne einer wehrhaften Demokratie.

Gerade für die Praxis bleibt daher abzuwarten, ob sich die neue Rechtsgrundlage mit ihren Verfahrensvorschriften als praktikabel erweist oder ob sich im Zuge erster Erfahrungen Nachbesserungsbedarf ergibt.

Bildrechte. Redaktion.

## Anmerkungen

1 Der Autor ist in der Abteilung 3 (Staatsschutz) des Landeskriminalamtes Schleswig-Holstein und nebenamtlich für die Fachgruppe Rechtswissenschaften im Fachbereich der Polizei an der FHVD des Landes tätig.
2 LT-Drucksache 19/2118.
3 Graulich, in: Bäcker/Denninger/Graulich, 2021, Handbuch des Polizeirechts, 7. Auflage, Teil E, Rn. 681.
4 BVerfGE 120, 274 (328 f.); Graulich, in: Bäcker/Denninger/Graulich, 2021, a.a.O., Teil E, Rn. 683.
5 BVerfGE 141, 220.
6 Teilweise auch *„verdeckt ermittelnde Personen“*, vgl. § 16 Abs. 2 HSOG.
7 Vgl. zur Rechtsfigur Schmidbauer, in: Schmidbauer/Steiner, 2020, Polizeiaufgabengesetz, Polizeiorganisationsgesetz, 5. Auflage, Art. 37, Rn. 1.
8 In Deutschland unzulässig, vgl. Köhler, in: Meyer-Goßner/Schmitt, 2022, Strafprozessordnung, 65. Auflage, § 110a, Rn. 4a.
9 Kingreen/Poscher, 2020, Polizei- und Ordnungsrecht, 11. Auflage, S. 239 f.
10 Für das Beispiel islamistischer Terrorismus s. Bundesministerium des Innern, 2021, Verfassungsschutzbericht 2021, S. 177; Bundeskriminalamt, 2021, Politisch motivierte Kriminalität. Bundesweite Fallzahlen, S. 22.
11 Zur vergleichbaren Regelung im BKAG siehe auch BT-Drucksache 16/10121, S. 25.
12 Roth, in: Schenke/Graulich/Ruthig, 2019, Sicherheitsrecht des Bundes, 2. Auflage, § 4 BVerfSchG, Rn. 57; anders zur „Sicherheit“ des Bundes und der Länder vgl. VG Berlin v. 7.4.2011, Az. 2 K 39.10; Roewer, 1987, Nachrichtendienstrecht der Bundesrepublik Deutschland, § 3 BVerfSchG, Rn. 31.
13 Kailitz, 2004, Politischer Extremismus in der Bundesrepublik Deutschland: Eine Einführung, S. 212.
14 Vgl. zum Eingriff in Art. 13 Abs. 1 GG Graulich, in: Bäcker/Denninger/Graulich, 2021, a.a.O., Teil E, Rn. 743; Roggan, in: Graulich, 2019, Festschrift, S. 115 (120).
15 Womöglich *„wesenstypische ermittlungstaktische Maßnahme“* nach Graulich, in: Bäcker/Denninger/Graulich, 2021, a.a.O., Teil E, Rn. 744.
16 Eigenständige Normen siehe Art. 37 BayPAG, § 35 BbgPolG, § 47 BremPolG, § 29 HmbPolDVG, § 36a NPOG, § 20 PolG NRW; gemeinsame Norm mit VP-Einsatz siehe § 26 ASOG Bln, § 16 HSOG, § 18 SOG LSA; anders siehe § 49 BWPolG, § 34 RlpPOG, § 38 SächsPolG, § 33 SOG M-V; § 31 SPolDVG; § 34 ThürPAG.
17 LT-Umdruck 19/4576, S. 8 f.; LT-Drucksache 19/3684 (Abschlussbericht 1. Parlamentarischer Untersuchungsausschuss 19. Wahlperiode), zu den Schlussfolgerungen hinsichtlich der Führung von Vertrauenspersonen u.a. S. 406 ff., zur Gesamtschlussfolgerung hinsichtlich des Umgangs mit Quellen und Vertraulichkeitszusagen z.B. Alternative Meinung 1, S. 904 ff.
18 BVerfGE 141, 220 (290, 294).
19 Anders z.B. § 33a Abs. 5 S. 5 NPOG.
20 Graulich, in: Bäcker/Denninger/Graulich, 2021, a.a.O., Teil E, Rn. 742.
21 BVerfGE 141, 220.
22 BVerfGE 6, 32 (Elfes-Urteil).
23 Ein VE-Einsatz zur gezielten Erhebung von Daten aus dem Kernbereich wäre ohnehin unzulässig, vgl. BVerfGE 141, 220 Rn. 126; BT-Drucksache 18/11163, S. 115; Roggan, 2019, GSZ, S. 112 ff.
24 Zur strafprozessualen Verwertungsverbot vgl. Frister, in: Bäcker/Denninger/Graulich, 2021, a.a.O., Teil F, Rn. 338.
25 Frister, in: Bäcker/Denninger/Graulich, 2021, a.a.O., Teil F, Rn. 338.
26 Pietsch, KriPoZ 2022, S. 36 (u.a. unter Hinweis auf Frommel, NK 2020, S. 123); zur Kritik an dieser Auffassung vgl. Brenneisen, Die Kriminalpolizei 2/2022, S. 23; ders., DP 4/2022, S. 30.
27 § 49 Abs. 6 S. 3 BWPolG; § 31 Abs. 3 S. 2 SPolDVG; § 34 Abs. 4 S. 2 RlpPOG; § 33a Abs. 5 S. 5 NPOG; § 18 Abs. 5 S. 4 SOG LSA (kein Richtervorbehalt vorhanden, lediglich Vorbehalt des Innenministeriums); § 34 Abs. 4 S. 5 ThürPAG; § 28 Abs. 3a S. 5 BPolG; § 45 Abs. 5 S. 3 BKAG.
28 § 26 Abs. 4 S. 11 ASOG Bln.
29 § 16 Abs. 5 HSOG; § 35 Abs. 4 BbgPolG; § 38 Abs. 6 SächsPolG.

# Zum Verzicht auf die öffentliche Ordnung im VersFG BE und im VersG NRW

**Von Prof. Michael Knape und Prof./LRD a.D. Hartmut Brenneisen, Berlin/Preetz[1]**

Sowohl im VersFG BE als auch im VersG NRW ist auf das Schutzgut der öffentlichen Ordnung verzichtet worden.[2] Aufgrund der Vielfalt von Lagen bei oder im Zusammenhang mit Versammlungen stellt sich die Frage, ob dies ein kluger Schachzug des jeweiligen Gesetzgebers war.

## 1 Bedeutung der öffentlichen Ordnung

Auf den ersten Blick mag diese Frage wegen mangelnder Bestimmtheit dieses klassischen Schutzgutes des allgemeinen wie besonderen Polizei- und Ordnungsrechts, damit zugleich auch kraft fehlender Gesetzmäßigkeit der Verwaltung, bejaht werden können.[3] Denn unter *„öffentlicher Ordnung“* wird die von der Verkehrssitte geprägte Gemeinschaftsordnung, die allgemeine Verkehrssitte oder der Zustand des von der Verkehrssitte geregelten Zusammenlebens der Menschen in der staatlichen Gemeinschaft verstanden.[4] Wenn daher von der Gesamtheit der *„ungeschriebenen Normen“* die Rede ist, handelt es sich trotz § 118 I OWiG[5] nicht um Rechtsnormen im förmlichen Sinne. Nur so lässt sich nämlich die öffentliche Ordnung trennscharf von der öffentlichen Sicherheit abgrenzen, zu der u.a. die gesamte Rechtsordnung gehört.[6]

Schutzwürdig ist seit jeher eine *„ungeschriebene Regel“* daher nur, wenn sie nicht geltenden Rechtsnormen widerspricht und auch nur dann, wenn sie das Verhalten des

einzelnen in der Öffentlichkeit betrifft, nicht dagegen wenn sie sich auf seine Privatsphäre bezieht.[7] Dieser Aspekt steht keinesfalls im Widerspruch zu § 2 III VersFG BE, wonach *„dieses Gesetz sowohl für öffentliche als auch für nichtöffentliche Versammlungen gilt"*. In diesem Zusammenhang wird vor allem auf die Frage des zugelassenen Personenkreises in der jeweiligen Versammlung und deren Ausstrahlung nach außen in die Öffentlichkeit – trotz eines möglicherweise geschlossenen Teilnehmerkreises bei nichtöffentlichen Versammlungen – und nicht etwa auf die Privatsphäre des einzelnen Teilnehmers abgestellt.[8]

Kommen z.B. am 20. April mehrere Personen der rechten Szene in einer Wohnung zusammen, um Hitlers Geburtstag zu gedenken, handelt es sich um eine nichtöffentliche Versammlung in geschlossenen Räumen, insoweit also um eine sog. *„geschlossene"* Versammlung. Hier liegt die Gefahr – soweit durch diese Personenzusammenkunft überhaupt öffentliche Interessen berührt werden – ausschließlich im Bereich der öffentlichen Ordnung; geltende Rechtsnormen werden durch die Versammlung nicht verletzt.[9]

Zu beachten ist jedoch, dass gerade das BVerfG in einer Vielzahl von Entscheidungen des Versammlungsrechts[10] dieses Schutzgut heranzog; es brachte die öffentliche Ordnung bei Versammlungen unter freiem Himmel abgestuft in Ansatz. Das Gericht bestätigte zwar ausdrücklich den Grundsatz für Versammlungsverbote, die ebenso wie Auflösungen im Wesentlichen nur zum Schutz elementarer Rechtsgüter der öffentlichen Sicherheit in Betracht zu ziehen sind, so dass insoweit eine Gefährdung der öffentlichen Ordnung im Allgemeinen nicht genügte.[11] Gleichwohl relativierte es diese Auffassung aber insbesondere für Beschränkungen in zeitlicher und räumlicher Hinsicht sowie zum Verlauf der Veranstaltung.

## 2 Praktische Anwendungsfälle

Die öffentliche Ordnung schied demnach als Schutzgut unterhalb der Schwelle eines Versammlungsverbots nicht aus.[12] Dies galt z.B. für das Mitführen von Reichskriegsflaggen des Kaiserreichs, soweit sich die Gefahr für dieses Rechtsgut aus der Art und Weise der Versammlungsdurchführung ergibt,[13] aber auch für rechtsextremistische Demonstrationen am Holocaust-Gedenktag,[14] wobei die Verlegung auf einen anderen Tag als zeitliche Beschränkung einzuordnen ist.[15] Das BVerfG ließ somit beschränkende Maßnahmen zum Schutz der öffentlichen Ordnung immer dann zu, wenn diese sich nicht auf die Verhinderung bestimmter Inhalte der kollektiven Meinungskundgabe erstreckten, sondern auf die Art der Zusammenkunft und kollektiven Meinungskundgabe, etwa wenn durch provokatives oder aggressives Auftreten ein Einschüchterungseffekt oder ein Klima der Gewaltbereitschaft erzeugt wurde.[16] So stellt z.B. das Auftreten des sog. *„Schwarzen Blocks"* der militanten Autonomen, soweit nicht nach wohl heute allgemeiner Auffassung vorrangig ein Verstoß gegen das Uniformverbot gem. §§ 9 II, 27 I Nr. 6 VersFG BE[17] (Bußgeldtatbestand) bzw. gegen das Gewalt- und Einschüchterungsverbot (sog. *„Militanzverbot"*) gem. §§ 18 I Nr. 1, 27 VIII Nr. 1 VersG NRW (Straftatbestand) einschlägig ist,[18] auch eine Gefahr für die öffentliche Ordnung dar,[19] weil von diesem ein bedrohlicher Gesamteindruck ausgeht, der einem geordneten menschlichen Zusammenleben widerspricht.[20]

## REZENSION

**Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, Kommentar. 17. Auflage 2022**

Die 17. Auflage des „Jarass/Pieroth" ist von Prof. Dr. Hans D. Jarass und Prof. Dr. Martin Kment bearbeitet worden, der mit der 16. Auflage den Mitbegründer des Werkes Prof. Dr. Bodo Pieroth abgelöst hat.
Hans D. Jarass ist Direktor des ZIR-Forschungsinstituts für deutsches und europäisches Recht an der Westfälischen Wilhelms-Universität Münster und Martin Kment Lehrstuhlinhaber für Öffentliches Recht und Europarecht, Umweltrecht und Planungsrecht an der Universität Augsburg.
Der Kommentar, der zur Reihe „Gelbe Erläuterungsbücher" zählt, ist ein zuverlässiges und mit 69,00 Euro zudem recht preiswertes Hilfsmittel für jeden, der schnelle und zuverlässige Antworten auf verfassungsrechtliche Fragestellungen sucht. Er präsentiert in komprimierter Form die Rechtsprechung des BVerfG und der übrigen obersten Bundesgerichte. Das einschlägige Schrifttum wird hingegen nur in Ansätzen berücksichtigt. Es geht den Autoren ausdrücklich darum, Kommentare, Handbücher und Fachaufsätze zu erschließen und damit eine fundierte Handreichung für eine vertiefende Auseinandersetzung mit Auslegungsfragen des Grundgesetzes zu geben. Entsprechend wird auf die Ausweisung älterer Quellen auch bewusst verzichtet und insoweit auf die Vorauflagen des Werkes verwiesen.
Jedem Grundgesetzartikel ist eine Kurzübersicht an ausgewählter Literatur vorangestellt. Es folgt bei längeren Kommentierungen ein Inhaltsverzeichnis, das die schnelle und zielgerichtete Recherche ermöglicht.
Die 17. Auflage befindet sich hinsichtlich Rechtsprechung und Schrifttum auf dem (veröffentlichten) Stand vom Januar 2022.
Durch einen stringenten Aufbau, der sich insbesondere im Grundrechtsteil an rechtswissenschaftlichen Falllösungen orientiert, die Kompaktheit und Aktualität ist der Kommentar für Praktiker, Lehrende und Studierende gleichermaßen gut geeignet. Dies gilt gerade auch für den Polizeivollzugsdienst, für den verfassungsrechtliche Fragen von besonderer Bedeutung sind.

Hartmut Brenneisen, Preetz/Worms

| | |
|---|---|
| **Autoren:** | **Hans D. Jarass, Martin Kment** |
| **Titel:** | **Grundgesetz für die Bundesrepublik Deutschland, Kommentar** |
| **Auflage:** | **17. Auflage 2022** |
| **Format:** | **1429 Seiten, 12,8 x 19,4 cm, Hardcover** |
| **Preis:** | **69,00 Euro** |
| **ISBN:** | **978-3-406-78378-4** |
| **Verlag:** | **Verlag C. H. Beck oHG** |

## 3 Pro-russische Versammlungen

Vom Regelungsbereich beider Gesetze nicht erfasst ist z.B. die Motorradfahrt der pro-russisch-nationalistischen Rockergruppierung *„Nachtwölfe"*, die jedes Jahr am 9. Mai das russische Ehrendenkmal in Berlin-Treptow ansteuert.[21] Diese demonstrative Aktion stellt zweifelsohne nur eine unmittelbare Gefährdung der öffentlichen Ordnung dar. Die Fahrt in typischer Rockerstaffelung als *„paramilitärisches Auftreten"* i.S.d. § 18 I Nr. 2 VersG NRW zu klassifizieren, kommt nicht in Betracht.[22] Daran ändert bei bestehender Rechtslage auch die Tatsache nichts, dass sich diese Rockergruppierung mit den politischen sowie militärischen Zielen des russischen Präsidenten *Putin* ohne *„Wenn und Aber"* identifiziert, dessen völkerrechtswidrigen Angriffskrieg gegen die Ukraine gutheißt und sie ihre Anwesenheit gerade an diesem Tag in Berlin als Machtdemonstration der russischen Föderation in Deutschland verstanden wissen will.

Des Weiteren sind bei friedlichen pro-russischen Protesten keine gerichtsfesten Beschränkungen der zuständigen Versammlungsbehörden[23] möglich, soweit Teilnehmer beabsichtigen, Flaggen der russischen Föderation in geringer Anzahl mitzuführen.[24] Dass die Mehrheit der in Deutschland lebenden Bevölkerung dies unter Beachtung der jeweils herrschenden ethischen und sozialen Anschauungen ablehnt, liegt auf der Hand, besitzt dem Grunde nach aber keine rechtliche Relevanz.[25]

Falls solche Versammlungen jedoch auf das Billigen des von Russland gegen die Ukraine geführten Angriffskriegs sowie auf Verhaltensweisen abzielen, die dazu bestimmt und geeignet sind, Gewaltbereitschaft zu vermitteln und damit den *„öffentlichen Frieden zu stören"*, sind Beschränkungen nach dem VersFG BE und VersG NRW zulässig,[26] wenn z.B. das massenweise Zeigen russischer Flaggen geplant ist, obwohl diese für sich genommen keinem Verbotstatbestand unterfallen.[27] Entscheidend ist also stets der Eindruck, der mit der Demonstration vermittelt werden soll.

Weist in Berlin die Senatsverwaltung für Inneres, Digitalisierung und Sport darauf hin, bei derartigen Versammlungen sei *„eine Verstärkung der Traumatisierung oder gar erst ein Hervorrufen eines Traumas"* von Geflüchteten aus der Ukraine zu berücksichtigen, wird insoweit auf das Schutzgut der öffentlichen Ordnung abgestellt.[28] Deshalb kann von der Versammlungsbehörde keine beschränkende Verfügung nach § 14 I VersFG BE – abgesehen von Fällen gem. § 14 I i.V.m. § 14 II Nr. 1 VersFG BE[29] – wirksam erlassen werden; nichts anderes gilt im Land NRW.

Anders stellt sich die Rechtslage dar, soweit Teilnehmende beabsichtigen, z.B. an ihren Fahrzeugen zusätzlich das weiße *„Z"*-Symbol anzubringen. Dies kann durch beschränkende Verfügung verboten werden, weil ein Straftatbestand erfüllt ist.[30] Bei Fahrzeugen mit wenigen Flaggen der russischen Föderation ohne *„Z"*-Symbol bleibt der Polizei/Versammlungsbehörde nur Raum zu deeskalierenden Kooperationsgesprächen im Rahmen des Konfliktmanagements vor und während des Versammlungseinsatzes, um drohende oder bestehende Konfrontation zielgruppenorientiert zu verhindern (§§ 3 IV, 4 I VersFG BE; § 3 VersG NRW).[31]

## 4 Gesetze auf dem Prüfstand

Die CDU bereitet im Land Berlin einen Änderungsantrag des VersFG BE vor; das Tatbestandsmerkmal *„öffentliche Ordnung"* soll im Gesetz wieder aufgenommen werden.[32] Zudem ist aus der Koalition heraus eine spätere Evaluation auf der Grundlage praktischer Erfahrungen und dann vorliegender Rechtsprechung angekündigt worden.[33] Damit dürfte auch der Verzicht auf die öffentliche Ordnung auf den Prüfstand gestellt werden. Vergleichbares gilt für das Land Nordrhein-Westfalen. In der aktuellen Koalitionsvereinbarung ist für Ende 2023 im Zuge der Berichtspflicht nach § 34 VersG NRW eine *„unabhängig(e) und wissenschaftlich(e)"* Evaluierung ausdrücklich festgeschrieben worden.[34]

## Anmerkungen

1 Professor Michael Knape ist Direktor beim Polizeipräsidenten a.D.; Hartmut Brenneisen ist Professor, Ltd. Regierungsdirektor und Polizeidirektor a.D.; beide Autoren sind heute als Redakteure, Gutachter, Lehrbeauftragte sowie Herausgeber und Autoren von Fachpublikationen tätig.

2 Vgl. § 14 I VersFG BE sowie § 13 I u. II VersG NRW; vergleichbar auch § 13 I VersFG SH u. § 13 I u. IV VersammlG LSA; zur Thematik siehe Knape/Brenneisen, Versammlungsfreiheitsgesetz Berlin (VersFG BE), 2021, Rn. 17 zu § 3, Rn. 13 zu § 10, Rn. 3, 13, 35 u. 36 zu § 14, Rn. 12 zu § 16 mit Hinw. auf § 9 MEVersG u. weiteren Erläuterungen; ferner Brenneisen, DEUTSCHE POLIZEI 4/2022, 30 (31); ders., DIE KRIMINALPOLIZEI, 2/2022, 23 (24 [Fn. 19]).

3 Vgl. Knape/Schönrock, Allgemeines Polizei- und Ordnungsrecht für Berlin, 11. Aufl. (2016), Rn. 137 zu § 25 ASOG Bln; dies. ausführlich zum Schutzgut der öffentlichen Ordnung, Rn. 24 ff. zu § 1 ASOG Bln.

4 Vgl. Gürtler/Thoma, in: Göhler/Gürtler/Seitz/Bauer/Thoma, OWiG, 18. Aufl. (2021), Rn. 10 zu § 118 mit weiteren Nachw.; dazu Knape/Schönrock, a.a.O., Rn. 24 zu § 1 ASOG Bln.

5 In § 118 I OWiG ist die *„öffentliche Ordnung"* zwar Tatbestandsmerkmal, erfährt dadurch jedoch keine formal-gesetzliche Konturierung i.S.d. öffentlichen Sicherheit, unabhängig davon, dass bei Verletzung der Bußgeldnorm als geschriebenes Recht der Verstoß im Bereich der öffentlichen Sicherheit liegt; normativ vergleichbarer Aufbau mit Tatbestandsmerkmalen der öffentlichen Ordnung in der Befugnisnorm des § 14 II VersFG BE , so dass die Gefahr im Bereich der öffentlichen Sicherheit liegt; keine korrespondierende Vorschrift dazu mit Tatbestandsmerkmalen der öffentlichen Ordnung im VersG NRW.

6 Vgl. schon Drews/Wacke/Vogel/Martens, Gefahrenabwehr, 9. Aufl. (1986), § 16, S. 245; dazu auch PrOVGE 91, 139 (140); ferner Knape/Schönrock, a.a.O., Rn. 17 zu § 1 ASOG Bln mit Hinw. auf BVerwGE 64, 55 (58 f.) und BVerwGE 82, 34 (40).

7 Vgl. schon Drews/Wacke/Vogel/Martens, a.a.O.; ergänzend dazu Schumann, Grundriss des Polizei- und Ordnungsrechts, (1978), S. 23.

8 Vgl. dazu Knape/Brenneisen, a.a.O., Rn. 23 ff. zu § 2 VersFG BE.

9 Betreten und Durchsuchung von Wohnungen ist zwar entspr. § 19 MEPolG 1977 in allen 16 Polizeigesetzen der Länder geregelt, kommt aber bei Versammlungen in geschlossenen Räumen nur unter strenger Beachtung der sog. Transformationsklausel z.B. des § 10 II VersFG BE, § 9 II VersFG SH bzw. § 9 II VersG NRW als Ausdruck der verfassungssystematischen Schranken aus Art. 8 I GG und zugleich unter strenger Beachtung des verfassungsmäßigen Übermaßverbots in Betracht; insoweit sind also unter versammlungsgesetzlichen Kautelen nur jene Befugnisnormen des allgemeinen Polizei- und Ordnungsrechts der Länder tatbestandsmäßig, die mit § 19 I Nr. 3 MEPolG korrespondieren.

10 Basierend auf § 15 I BVersG, der die öffentliche Sicherheit und die öffentliche Ordnung als Schutzgüter normiert.

11 Vgl. Knape/Schönrock, a.a.O., Rn. 29 mit Hinw. auf BVerfGE 69, 315 (353).

12 Vgl. Knape/Schönrock, a.a.O., mit weiteren Hinw. auf die Rspr. des BVerfG; dies ist für jene Länder wichtig, in denen heute noch das BVersG – z.B. in Brandenburg, Hamburg oder M-V – gilt; Voraussetzung ist jedoch stets, dass der jeweilige Sachverhalt nicht bereits in den Schutzbereich der öffentlichen Sicherheit fällt.

13 BVerfG v. 19.12.2007 – 1 BvR 2793/04; OVG Lüneburg v. 13.11.2020 – 11 ME 293/20; OVG Bremen v. 23.10.2020 – 1 B 331/20; v. 16.10.2020 –1 B 323/20; vorg. VG Bremen v. 15.10.2020 – 5 V 2212/20.

14 Keine rechtsextremen Aufzüge am Holocaust-Gedenktag: vgl. BVerfG v. 26.1.2001 – 1 BvQ 9/01, NJW 2001, 1409; dazu schon Pewestorf, Polizei- und Ordnungsrecht, 2. Aufl. (2017), Rn. 53 zu § 1 ASOG Bln; ferner Knape/Brenneisen, a.a.O., Rn. 30 ff. zu § 14 VersFG BE, hier kraft gesetzlicher Regelung nunmehr unter dem Regime einer Gefährdung für die öffentlichen Sicherheit.

15 Vgl. Knape/Schönrock, a.a.O., Rn. 29 ff. (31) zu § 1 ASOG Bln mit umfangreichem Rspr.-Nachw.; Aufmärsche, die nunmehr gem. § 14 II Satz 1 Nr. 3 sowie dessen Anl. In § 14 II Nr. 1 VersFG BE bzw. § 19 I Satz 1 Nr. 1 u. Satz 3 VersG NRW der deutlich engeren, d.h. normenklareren öffentliche Sicherheit unterliegen.

16 Vgl. Knape/Schönrock, a.a.O., Rn. 29 zu § 1 ASOG Bln.

17 Vgl. Knape/Brenneisen, a.a.O., Rn. 25 zu § 9 VersFG BE (Fn. 53) u.a. mit Hinw. auf Kniesel, in: Kniesel/Braun/Keller, Versammlungsgesetze, 18. Aufl. (2019), Teil II, Rn. 17 zu § 3 BVersG.

18 Dem folgend liegt der Verstoß im Bereich der öffentlichen Sicherheit.

19 Man denke z.B. an den G8-Gipfel v. 6.-8.6.2007 in M-V (Heiligendamm) oder an den G20-Gipfel am 7./8.7.2017 in Hamburg, Länder, in denen noch heute das BVersG gilt.

20 Vgl. Knape/Schönrock, a.a.O., Rn. 31 zu § 1 ASOG Bln. Uneinigkeit besteht in Teilen von Lehre und Schrifttum darüber, ob der sog. *„Schwarze Block"* der militanten Autonomen unter die o.a. Vorschriften des BVersG, VersFG BE u. VersG NRW fällt, damit dem Regime der öffentlichen Sicherheit zuzuordnen ist, weil die Bestimmungen des VersFG BE und VersG NRW explizit auf den einschränkend interpretierten Regelungszweck des bundesrechtlichen *„Uniformverbots"* nach § 3 I BVersG abstellen; dieser Zweck rechtfertigt trotz potenzieller Unfriedlichkeit politisch motivierter Aufmachung kein undifferenziertes generelles Verbot, zumal die verfassungsrechtlich verbürgte Gestaltungsfreiheit auch für Bekleidung anerkannt sei; dazu Enders, in: Dürig-Friedl/Enders, Versammlungsrecht, 2. Aufl. (2022), Rn. 14 zu Art. 7 BayVersG; Kniesel, a.a.O., Teil II, Rn. 1 zu § 3 BVersG (widersprüchlich Kniesel, a.a.O., oben Fn. 17); dazu Drs. BE 18/2764, S. 33, in welcher der Gesetzgeber trotz weit gefassten, klaren Wortlauts des § 9 II VersFG BE nur auf das Uniformverbot i.S.d. § 3 I BVersG abstellt; ein darüber hinaus gehendes *„Einschüchterungsverbot"* sei durch die Norm nicht statuiert; dann aber läge die Gefahr, soweit nicht zugleich auch elementare Rechtsgüter der öffentlichen Sicherheit unmittelbar gefährdet sind, bei sog. *„Schwarzen Blöcken"* als Kombination von gleichartiger Bekleidung und militant-aggressiver Wirkung im Bereich der öffentlichen Ordnung.

21 Für die Tage des 8./9.5.2022 erließ die Polizei Berlin am 4.5.2022 als zuständige Versammlungsbehörde für insgesamt 15 Orte, gestützt auf § 17 I ASOG Bln u. § 14 I i.V.m. II Nr. 1 VersFG BE, eine unter mehreren Aspekten rechtlich problematische Allgemeinverfügung (§ 35 Satz 2 VwVfG i.V.m. § 1 I VwVfG Bln) mit zahlreichen Verboten. So wurde v. 8.5., 06.00 Uhr, bis zum 9.5., 22.00 Uhr, die Versammlungsfreiheit u.a. insofern beschränkt, als das Zeigen sowjetischer, russischer u. ukrainischer Flaggen untersagt war. Ob das Zeigen ukrainischer Flaggen verboten werden kann, darf bezweifelt werden; vgl. dazu Tölle, in: DER TAGESSPIEGEL v. 9.5.2022, S. 7, mit Hinw. darauf, dass *„es überhaupt nicht sichtbar sei, wie sie die öffentliche Sicherheit oder Ordnung stören können"*. Ein Kläger bekam am 9.5. im vorläufigen Rechtsschutzverfahren nach § 80 V Satz 1 Alt. 2 VwGO mit Beschl. des VG Berlin – 1 L 172/22, openJur 2022, 9520, 2. lit. b *„grünes Licht"*, sich zusammen mit zwei anderen am Abend des 9.5. v. 21.30 bis 22.00 Uhr vor dem Deutsch-Russischen Museum in Karlshorst mit ukrainischen Flaggen unter Abspielen und Singen ukrainischer Militärlieder aufzuhalten; die Richter der Kammer erkannten hierin keine Gefahr/Verletzung der partiell im Lichte der Rspr. des BVerfG normierten öffentlichen Ordnung, insoweit einer nunmehr dem Regime der öffentlichen Sicherheit gem. § 14 II Satz 2 Nr. 1 VersFG BE zuzuordnenden Fallvariante; vgl. Knape/Brenneisen, a.a.O., Rn. 35 (mit Fn. 104) und 36 zu § 14 VersFG BE; eine tatbestandsmäßig korrespondierende Vorschrift im VersG NRW existiert nicht, so dass dessen Mittel-Generalklausel gem. § 13 I Satz 1 u. 2, anders als § 14 II VersFG BE ausschließlich fußend auf die unmittelbare Gefahr für die öffentliche Sicherheit ohne weitere Tatbestandsmerkmale in Hinblick auf die öffentliche Ordnung in Ansatz gebracht werden muss; das OVG Berlin-Brandenburg änderte mit Beschl. v. 9.5. – 1 S 35/22 die Entscheidung des VG Berlin i.S.d. Regelungen der Allgemeinverfügung; welche Rolle § 17 I ASOG Bln, eine Befugnisnorm des allgemeinen Polizei- und Ordnungsrechts, im Rahmen der Verfügung im Verhältnis zu den dort genannten Normen des spezielleren VersFG BE spielte, bleibt unklar.

22 Sofern diese militante Rockertruppe z.B. auch das Land NRW durchqueren würde.

23 Im Land Berlin die Polizei Berlin; vgl. dazu Knape/Brenneisen, a.a.O., Rn. 14 zu § 3 u. § 31 VersFG BE.

24 Z.B. unter dem Demonstrationsthema: *„Gegen Diskriminierung russischer Bürger in Deutschland"*, wobei wenige Flaggen an mitgeführten Fahrzeugen befestigt werden sollen; weder eine unmittelbare Gefährdung der öffentlichen Sicherheit (§ 14 I VersFG BE = § 13 I Satz 1 u. 2 Vers NRW) noch die Gefahr der Störung des öffentlichen Friedens (§ 14 II Satz 1 Nr. 1 VersFG BE) oder eine Gewaltbereitschaft vermittelnde Durchführung (§ 14 II Satz 2 Nr. 1 VersFG BE) kommen insoweit in Betracht.

25 Ein Bußgeldverfahren wegen Verstoßes gem. § 118 I OWiG kommt ebenfalls nicht zum Tragen, da nicht tatbestandsmäßig.

26 Betroffen ist hierbei der Verlauf einer Versammlung, vgl. dazu § 13 I Satz 2 Var. 2 VersG NRW.

27 Vgl. VG Berlin v. 23.4.2022 – 94 L 1/22 (1 L 158/22), S. 3 ff.: zahlenmäßige Beschränkung russischer Flaggen – ein Exemplar pro 25 Teilnehmenden bei ca. 500 Personen – gem. § 14 I i.V.m. § 14 II Satz 1 Nr. 1 VersFG BE: Eine massenweise Verwendung solcher Flaggen kann je nach der konkreten Gestaltung der Versammlung zu einem suggestiv-militanten Erscheinungsbild der Versammlung führen und dadurch die *„Billigung eines Angriffskriegs"* (unten Fn. 30) – Siegeszug –, mithin die *„Störung des öffentlichen Friedens"* hervorrufen; zum Begriff *„öffentlicher Friede"* vgl. Knape/Brenneisen, a.a.O., Rn. 27 zu § 14 VersFG BE; im VersG NRW kann einer solchen Gefahr mit einem suggestiv-militanten Erscheinungsbild der Versammlung durch beschränkende Verfügung der Versammlungsbehörde aufgrund der Mittel-Generalklausel gem. § 13 I Satz 1 u. 2 begegnet werden.

28 Zu prüfen ist jedoch, ob die genannten Effekte womöglich den (objektiven) Tatbestand der Körperverletzung erfüllen (§§ 223 f. StGB); dann läge die Gefahr im Bereich der öffentlichen Sicherheit. In solchen Fällen sollte auf die unreflektierte Erwähnung der öffentlichen Ordnung verzichtet werden: Drews/ Wacke/Vogel/Martens, a.a.O., S. 246.

29 Vgl. VG Berlin, a.a.O. (oben Fn. 27).

30 Das *„Z"*, ein russisches Militärzeichen, steht für *„Sieg"*. Es verkörpert zugleich die *„Billigung eines Angriffskriegs"*, insoweit des Kriegs Russlands gegen die Ukraine. Dieses Zeichen, öffentlich zur Schau gestellt, erfüllt den Straftatbestand gem. §§ 140 I Nr. 2 i.V.m. 138 I Nr. 5 letzte Alt. StGB und kann von der zuständigen Versammlungsbehörde verboten werden; dazu zählen auch Verbrechen der Aggression nach dem Völkerstrafgesetzbuch; vgl. OVG Magdeburg v. 27.4.2022 – 3 M 45/22, LS 2 u. S. 5 f. S. 5 f. (= DVBl 2022, 740 ff., LS 2 u. S. 742) zum Tragen der mit weißem Aufdruck *„mmmhhh Z-itronenlimonade"* beschriebenen T-Shirts bei einer Versammlung, das den objektiven Tatbestand der o.a. Strafvorschriften erfüllt, so dass die abzuwehrende Gefahr in Gestalt der Unverletzlichkeit der Rechtsordnung im Bereich der öffentlichen Sicherheit liegt.

31 Zur Abgrenzung zwischen dem *„Z"*-Symbol und den *„Sankt-Georgs-Band"* vgl. auch OVG Münster v. 6.5.2022 – 15 B 584/22; vorg. VG Köln v. 6.5.2022 – 20 L 771/22.

32 Vgl. Siebert, in: BERLINER MORGENPOST v. 12.4.2022, S. 13.

33 PlPr BE 18/72, S. 8589 – Schlüsselburg.

34 Koalitionsvereinbarung von CDU und GRÜNEN 2022 – 2027, S. 84.

# Polizeien und Kinderschutz –

## Herausforderungen bei der Anwendung kindgerechter Kriterien für das Strafverfahren

Von Josefine Barbaric, Salach[1]

### 1 Einleitung

Kinderschutz ist im besten Fall ein Standard und nicht nur ein Ziel. Tatsächlich ist mir dieser Satz mal in einer Fortbildungsveranstaltung für Mitarbeitende des institutionellen Hilfesystems in Mecklenburg-Vorpommern in den Sinn gekommen. Erst Tage später begriff ich, wie weitreichend seine Bedeutung dem Grunde nach ist. Der Schutz für Kinder vor sexualisierter Gewalt ist in Deutschland bei Weitem kein Standard – nicht mal ein flächendeckendes Ziel. Obwohl gerade Kinder eine besonders vulnerable Personengruppe in unserer Gesellschaft darstellen und sie dadurch besonders schutzbedürftig sind. Doch die jährliche Auswertung der Polizeilichen Kriminalstatistik (PKS) zeigt deutlich, dass gerade Kinder häufig Opfer von Gewalt, insbesondere von sexuell motivierten Gewalttaten werden.[2] Dies wiederum zeigt deutlich, dass wirksame und nachhaltige Präventionsmaßnahmen zur Aufklärung und zum Schutz für Kinder vor Gewalt, insbesondere vor sexualisierter Gewalt flächendeckend fehlen. Genau hier versagt der Kinderschutz bereits seit vielen Jahren. Und seit vielen Jahren appelliere ich genau deshalb an Politik und Gesellschaft diesen Missstand zu korrigieren. Der Schutz für Kinder vor sexualisierter Gewalt wird im besten Fall getragen von einer angemessenen moralischen Haltung, auch bei den Polizeien.

Und wenn die Gesellschaft das Kind nicht vor dieser perfiden und in allen Maßen destruktiven Gewalt hat schützen können, dann ist es ihre Verantwortung, alles dafür zu tun, dass das Verbrechen an dem Kind sichtbar gemacht wird, und die Täterperson die volle Härte des Gesetzes zu spüren bekommt. Selbstverständlich müssen alle Ressourcen und Kapazitäten für ein kindgerechtes Ermittlungs- und Strafverfahren zur Verfügung gestellt werden. Alles andere ist beschämend.

Und die bundesweite Lage ist beschämend. Und falls Sie sich nun genau an dieser Stelle fragen sollten, wer die Verfasserin

überhaupt ist, dass sie sich eine solch kritische Meinung anmaßt, so sollten Sie wissen, dass ich Gewalt, insbesondere sexualisierter Gewalt selbst in meiner Kindheit und Jugendzeit erlebt habe. Das liegt nunmehr 34 Jahre zurück und ich schaue in die Gegenwart und frage mich, was nun hat sich seither für den Schutz für Kinder vor Gewalt, insbesondere vor sexualisierter Gewalt tatsächlich zum Guten verändert? Die Antwort ist bedauerlicherweise so überschaubar, wie die Maßnahmen selbst: nichts! Seien Sie also versichert: ich weiß, worüber ich schreibe.

## 2 Chefsache, auch an der Basis?

Der sexuelle Kindesmissbrauch wurde 2019 vom nordrhein-westfälischen Innenminister Herbert Reul (CDU) zur Chefsache erklärt.[3] Eine vorbildliche und zugleich stringente Haltung, die man im politischen Raum ja sonst eher vermisst. Doch was bringt es, wenn diese notwendige moralische Einstellung nicht etwa an der Basis ankommt, bspw. bei den Mitarbeitenden der Strafverfolgungsbehörden, wozu ich die Polizeien und Staatsanwaltschaften zähle. Ich möchte hierzu gerne ein Beispiel aus NRW anführen. Ganz regelmäßig reichen wir über unseren Verein Beschwerde für hilfesuchende Eltern und ihre von sexuellem Missbrauch betroffenen Kinder bei den zuständigen Staatsanwaltschaften ein, da zu beobachten ist, dass Verfahren in den Deliktbereichen § 176 bis § 184 StGB regelmäßig durch Staatsanwaltschaften nach § 170 Abs. 2 StPO eingestellt werden.

## 3 Ein Beispiel aus NRW

Es handelt sich hierbei um Fälle aus dem gesamten Bundesgebiet, viele allerdings aus NRW. So habe ich in meiner Funktion als Vorständin von *„Nein, lass das! e.V."* in einem besonders absurden Fall Herrn Innenminister Reul (CDU) und Herrn Justizminister Biesenbach (CDU) über die Vorgehensweise der zuständigen Polizei und Staatsanwaltschaft in Kenntnis gesetzt. Begründeter Verdacht § 176a StGB eines 3-jährigen Jungen in einer Kindertageseinrichtung in NRW durch einen festangestellten Mitarbeiter. Das Ermittlungsverfahren wurde, wie oben beschrieben, von der zuständigen Staatsanwaltschaft eingestellt. Das Kind erzählte so gut es eben konnte seinen Eltern von den *„Spielen"* des Logopäden. Die Eltern nahmen die Erzählungen ihres Kindes ernst und wandten sich an die Polizei. Eine Anzeige würde sich nicht lohnen, da es zu wenig Beweise gäbe, erklärte man den Eltern auf dem Polizeirevier. Die Eltern blieben jedoch hartnäckig und bestanden darauf, dass die Anzeige aufgenommen wird. Es wurde ihnen im weiteren Verlauf eine Kriminalbeamtin zugewiesen, die von beiden Elternteilen als wenig kooperativ, motiviert und zugewandt beschrieben wurde, weshalb die Eltern sich an den Vorgesetzten wandten. Auch in diesem Gespräch fühlten sich die Eltern mit ihrem Anliegen nicht angemessen ernst genommen. Die Mutter bspw. fragte auf mein Anraten hin, warum nicht noch andere Kinder aus dieser Gruppe befragt wurden, um abzuklären ob möglicherweise noch weitere Kinder betroffen sind. *„Ob einen nicht vollwertigen Zeugen oder zehn, spielt am Ende auch keine Rolle."* Daraufhin habe ich, auf Wunsch der Eltern, mit diesem LKA-Beamten telefoniert. Er bestätigte diese von ihm getätigte Aussage und es war ihm sichtlich unangenehm.

Erinnern Sie sich noch an den letzten Satz des ersten Abschnitts meiner Einleitung? An dieser Stelle möchte ich gerne an eine gemeinsame Veröffentlichung aus dem Jahr 2020 mit Rainer Becker, Polizeidirektor a.D., und Dr. Verena Kolbe, Fachärztin für Rechtsmedizin, für die Gewerkschaft der Polizei (GdP) erinnern, die in Anlehnung an genau solche Rückmeldungen und Erfahrungen entstanden ist.

## 4 Diese Checkliste kann beim Helfen helfen

### 4.1 Machen

Eine sofortige *„Sicherstellung"* des Tatortes sowie eine kriminaltechnische Untersuchung auf eventuelle Spuren. Informatorische Befragungen an den möglichen Tatorten durchführen, um sich einen allgemeinen Überblick über den möglichen Tathergang und die in Frage kommenden Täter machen zu können und um gegebenenfalls weitere betroffene Kinder identifizieren zu können. Auf Suggestivfragen verzichten. Die Gefahr der Manipulation sollte sowohl beim Kind als auch dem anzeigenden Erwachsenen ausgeschlossen sein. Der *„Vorgang"* sollte stets ernst genommen werden. Unter Umständen ist der ermittelnde Beamte die einzige Instanz, die helfen kann. Kinder können den sexuellen Missbrauch nicht allein beenden. Sie sind auf die Hilfe von begleitenden erwachsenen Menschen und der Polizei angewiesen. Auch dem anzeigenden Erwachsenen fällt es häufig enorm schwer, sich zu entscheiden, die Polizei einzuschalten. Im Gespräch sollte keinesfalls ein Generalverdacht gegen den begleitenden Erwachsenen erhoben werden. Zum Beispiel wegen des Verdachts auf eine sogenannte Bindungsintoleranz. Das verunsichert nur unnötig. Bei dem Gefühl eigener Unsicherheit sollte eine Kollegin oder ein Kollege hinzugezogen werden. Auch eine Anfrage bei einer spezialisierten Beratungsstelle für Betroffene von sexueller Gewalt ist hilfreich. Zudem braucht es eine vertraute und warme Gesprächsatmosphäre für die Befragung des betroffenen Kindes und des anzeigenden Erwachsenen. Natürlich können auch anzeigende Erwachsene selbst verunsichert oder vielleicht traumatisiert sein.

Also: sensibel und ruhig vorgehen. Signale, dass man den Aussagen des Kindes sowie der Begleitperson Glauben schenkt, sollten zu jeder Zeit gesendet werden.[4] Unsere Beschwerde wurde an die zuständige Oberstaatsanwältin zur Prüfung weitergegeben. Mit einem abschließenden Schreiben an unseren Verein versuchte man nun, die Einstellung des Verfahrens zu begründen. Um den Unsinn zu verdeutlichen, erlaube ich mir, zwei Passagen aus diesem Schreiben zu zitieren:

*„Das bloße Zeigen des Geschlechtsteils gegenüber einem Kind allein begründet einen hinreichenden Tatverdacht wegen sexuellen Missbrauchs von Kindern (§ 176 Abs. 4 Nr. 1 des Strafgesetzbuches - StGB) nicht, da eine sexuelle Handlung im Sinne der Vorschrift nach ihrem äußeren Erscheinungsbild einen Bezug zu Sexualität aufweisen muss. Ist die Handlung als solche nicht offensichtlich sexuell, kommt es auf die objektiven Rahmenbedingungen aus der Sicht des Beobachters an, der alle Einzelheiten des Geschehens wahrnimmt (zu vgl. Homle in: Münchener Kommentar zum StGB, 4. Auflage 2021, § 184h Rn. 3 m.w.N.). Handlungen, die äußerlich neutral sind und keinerlei Hinweis auf das Geschlechtliche enthalten, sind daher auch dann keine sexuelle Handlung, wenn sie*

Kind nach Misshandlung.

Vernachlässigtes Kind.

*einem sexuellen Motiv entspringen (zu vgl. Eisele in: Schönke/Schröder, StGB, 30. Aufl. 2019, § 184h Rn. 6 m.w.N.). Können die äußeren Umstände einer mutmaßlichen Tatbegehung – wie hier – nicht näher eruiert werden, ist ein hinreichender Tatverdacht insoweit nicht zu begründen."*

Offen gesprochen, da hat wohl jemand nicht gut aufgepasst, denn sexueller Missbrauch beginnt häufig mit dem Zeigen der eigenen Genitalien durch die Täterpersonen (Exhibitionismus). Das Kind gab, seinen Eltern gegenüber, kindgerechte und gewichtige Anhaltspunkte. Doch das Kind wurde zu keiner Zeit, weder durch die zuständige Polizei noch durch die Staatsanwaltschaft (Ermittlungsrichter), angehört. Und das wurde wie folgt von der Oberstaatsanwaltschaft begründet:

*„Von seltenen Ausnahmefallen abgesehen, dürften Kinder erst ab einem Alter von etwa vier Jahren überhaupt als Zeugen in Betracht kommen (zu vgl. Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017 Rn. 1411 m.w.N.). Soweit schon Dreijährige zu Erlebnisberichten und zur Beantwortung altersgerechter Fragen in der Lage sein sollen (ebd.), muss jedenfalls eine Beeinflussung durch Dritte, die zur Verfälschung eigener Wahrnehmungen des Kindes und insoweit zur Beeinflussung seiner Aussage geeignet sind, ausgeschlossen bzw. jedenfalls nachvollzogen werden können. Dies ist hier nicht möglich."*

Ein Beispiel: Wenn ein 3-jähriges Kind regelmäßig den Penis des Vaters, Onkels, Opas, Ersatzvaters oder Bruders in den Mund nehmen muss, möglicherweise bis zur vollständigen Ejakulation der Täterperson, dann sind wir im Bereich des schweren sexuellen Missbrauchs an einem Kind (§ 176c StGB), was seit 1. Juli 2021 einen Verbrechenstatbestand darstellt. Doch wie kann dieses Verbrechen an dem Kind nun sichtbar gemacht und aufgeklärt werden?

Sind äußere Verletzungsspuren zu erkennen? Die Antwort ist überschaubar: nein! Was bleibt, sind unter Umständen einzig und allein Hinweise durch Aussagen, die das Kind bestenfalls alters- und entwicklungsspezifisch geben kann. Doch im hier geschilderten Fall hat es weder die zuständige Polizei, sowie die Staatsanwaltschaft noch die überprüfende Oberstaatsanwaltschaft in NRW interessiert. Das ist auch kein tragischer Einzelfall, weshalb ich in diesem Beitrag auch auf eine weit verbreitete und grundsätzliche ignorante und misstrauische Haltung des Strafverfolgungssystems kindlichen betroffenen Zeugen gegenüber eingehen möchte.

## 4.2 Wie aussagetüchtig sind kindliche Zeugen?

Seit vielen Jahren eine zähe und kontroversgeführte Diskussion zwischen Ermittlungsbehörden, Juristen und Psychologen. Offen gesprochen, ich kann es nicht mehr hören. Man weiß heute: Je mehr sich ein Kind sprachlich ausdrücken kann, umso mehr ist es in der Lage, Gesetzmäßigkeiten zu erkennen, zu verallgemeinern und zu ordnen und zu erinnern. Kurzum: Es kommt auf die individuelle Entwicklungsreife eines Kindes an, wie gut es sich an Ereignisse erinnern und sie wiedergeben kann. Weshalb solche Pauschalisierungen nur wenig zur Aufdeckung solcher Verbrechen beitragen. Im Gegenteil! Es entsteht der Eindruck, man wolle sich nicht die Mühe machen.

## 4.3 Sexueller Kindesmissbrauch – Chefsache auch an der Basis?

Die Fachwelt ist sich einig, dass gerade im Deliktbereich des sog. sexuellen Kindesmissbrauchs ein enorm hohes Dunkelfeld existiert. Perfide Verbrechen, die im Verborgenen stattfinden, zwischen Täterperson und betroffenem Kind, ohne Publikum, ohne Zeugen. So wirkt es schon grotesk, dass Täterpersonen das Blaue vom Himmel lügen dürfen, nicht mal persönlich zum Vernehmungstermin erscheinen müssen, hingegen ein betroffenes und möglicherweise schwer traumatisiertes Kind den Ermittlungsbehörden und dem gesamten Rechtssystem beweisen muss, dass ein Mensch eine Täterperson ist. Sollte es nicht eher umgekehrt sein? Sollte es nicht im Interesse unserer Gesellschaft sein, sicherzustellen, dass von einem Menschen keine Gefahr für andere Menschen, vor allem für Kinder ausgeht?

Viele Hürden für ein betroffenes Kind, finden Sie nicht auch? Genau deshalb braucht es gut geschulte und sensible Ermittlungsbeamte/innen und ein gutes und verlässliches Zusammenspiel der Strafverfolgungsbehörden.

Nun sprechen Kinder nicht grundsätzlich über sexuelle Übergriffe/sexualisierte Gewalt. Es müssen günstige Rahmenbedingungen zusammenwirken, damit ein Kind sich offenbaren kann. Die Chancen hierfür sind gut, wenn die Täterperson nicht aus dem engsten familiären Umfeld kommt, und das Kind gut an seine Eltern gebunden ist und ihnen vertraut. Weitere wichtige Voraussetzungen hierfür sind zudem, dass die Eltern gut auf ihr Kind eingehen und es zum Sprechen aktivieren können. Es ist von elementarer Bedeutung, dass sich das betroffene Kind beschützt fühlt und sich drauf verlassen kann, ernst genommen zu werden. Widersinnig, dass oben genannten Eltern nicht selten unterstellt wird, sie hätten ihre Kinder durch eine mögliche Suggestiv-Befragung beeinflusst. Nicht selten jedoch werden betroffene Kinder in der Vernehmung durch Ermittlungsbeamte/innen selbst suggestiv beeinflusst: *„Bist Du Dir sicher, dass Du Dir das nicht nur einbildest?" „Das hat der XY bestimmt nicht mit Absicht gemacht." „Meinst Du nicht auch, dass war ein Versehen?"*

Tadelnswerte Unwissenheit, Kenntnislosigkeit oder einfach nur Gedankenlosigkeit – es ist in hohem Maße abträglich, denn solch eine unprofessionelle Herangehensweise wird immer zur zusätzlichen Belastung für die ohnehin schon belasteten und betroffenen Kinder und ihre schützenden Eltern/Bezugspersonen.

Was bringt es demnach, wenn denjenigen, die maßgeblich dazu beitragen können, einem betroffenen Kind und seinen schützenden Bezugspersonen ein Gefühl von ehrlicher Bereitschaft zu vermitteln, ganz regelmäßig genau das Gegenteil davon tun. Wie kann das sein? Möglicherweise aus einem Gefühl der Unsicherheit und Hilflosigkeit heraus, weil die notwendigen Qualifikationen und die damit einhergehenden Handlungssicherheiten fehlen. Hinzu kommt ein bedrückender Personalnotstand, auch bei den Polizeien bundesweit und flächendeckend, der zu Überlastung einzelner Beamten/Beamtinnen führt.

Das aber darf nicht zum Problem für von sexualisierter Gewalt betroffenen Kindern werden. Dem Grunde nach sollte

man niemanden mehr daran erinnern müssen, welchen Stellenwert der sog. sexuelle Kindesmissbrauch mittlerweile in unserer Gesellschaft erlangt hat. Ein Verbrechensbereich, der seit vielen Jahren massiv ansteigt und sich zudem durch ein enorm hohes Dunkelfeld auszeichnet. Der nordrheinwestfälische Innenminister Herbert Reul trat bereits im Februar dieses Jahres mit der Veröffentlichung der Fallzahlen der Polizeilichen Kriminalstatistik (PKS) für Nordrhein-Westfalen an die Öffentlichkeit. Ein Großteil der Straftaten seien enorm zurückgegangen und auf einem so niedrigen Niveau wie zuletzt in den 1980er Jahren. Doch der sog. sexuelle Kindesmissbrauch und der Deliktbereich der sog. Kinderpornografie seien so hoch wie noch nie.

Wenn Sie mich fragen, dann lässt das tief blicken und der Umstand, dass die Zahlen von Jahr zu Jahr, bundesweit ansteigen, ist nicht einzig und allein darauf zurückzuführen, dass der Ermittlungsdruck erhöht werden konnte und damit mehr Fälle aus dem Dunkelfeld aufgedeckt werden konnten. Laut Holger Münch, Präsident des Bundeskriminalamtes (BKA), kann seit Jahren nur etwa jeder zehnte Hinweis ausländischer Provider überhaupt ausermittelt werden. Die Causa *„Verkehrsdatenspeicherung“*, die lange ausgesessen wurde und nun unsinnigerweise durch *„Quick-Freeze“* ersetzt werden soll. Ich fasse an dieser Stelle zusammen: Hohes Dunkelfeld, schlechte personelle Ausstattungen der Polizeien und Staatsanwaltschaften bundesweit, insbesondere der Polizeien in Baden-Württemberg, die auf Bundesebene das traurige Schlusslicht abbilden.

## 5 Praxisleitfaden zur Anwendung kindgerechter Kriterien für das Strafverfahren

Der Nationale Rat, der sich aus unterschiedlichen Vertreterinnen/Vertreter aus Politik, Zivilgesellschaft, Fachpraxis sowie aus Mitgliedern des Betroffenenrates der Unabhängigen Beauftragten für Fragen des sexuellen Kindesmissbrauchs (UBSKM) zusammensetzt, hat sich im Dezember 2019 konstituiert, mit dem Ziel, den Schutz für Kinder und Jugendliche vor sexualisierter Gewalt und Ausbeutung zu stärken. Im Juli 2021 wurde hierzu ein Praxisleitfaden zur Anwendung kindgerechter Kriterien für das Strafverfahren herausgegeben.[5] Da heißt es zu kindgerechten Kriterien für die Polizei wie folgt:

- **Besondere Schutzbedürftigkeit beachten:** Ist die Zeugin oder der Zeuge zugleich die oder der Verletzte, so führe ich die sie oder ihn betreffenden Verhandlungen, Vernehmungen und sonstigen Untersuchungshandlungen stets unter Berücksichtigung ihrer oder seiner besonderen Schutzbedürftigkeit durch, § 48a Abs. 1 StPO.
- **Beschleunigungsgebot:** Während des gesamten Verfahrens achte ich auf das Beschleunigungsgebot: Bei Taten zum Nachteil einer oder eines minderjährigen Verletzten führe ich die sie oder ihn betreffenden Verhandlungen, Vernehmungen und sonstigen Untersuchungshandlungen besonders beschleunigt durch, soweit dies unter Berücksichtigung der persönlichen Verhältnisse der oder des Zeugen sowie der Art und Umstände der Straftat zu ihrem oder seinem Schutz oder zur Vermeidung von Beweisverlusten geboten ist, § 48a Abs. 2 StPO.
- **Kindgerechte Information und psychosoziale und rechtliche Begleitung des Kindes im Verfahren:** Im Rahmen der Vernehmung/Anhörung von Kindern belehre ich die Betroffenen in angemessener, kindgerechter Form. Ich kenne die rechtlichen und sozialpädagogischen Unterstützungsmöglichkeiten für Minderjährige und kann sie den Sorgeberechtigten und den Minderjährigen gut und in einfacher Sprache vermitteln; insbesondere ist mir bekannt, wie die psychosoziale Prozessbegleitung arbeitet und in welchen Fällen sie obligatorisch oder fakultativ den verletzten Minderjährigen beigeordnet werden kann. Ich kenne die länderspezifischen Besonderheiten. In geeigneten Fällen gebe ich den Betroffenen z. B. die Broschüre „Ich habe Rechte“ des Bundesministeriums der Justiz und für Verbraucherschutz mit.

Im Weiteren werden folgende kindgerechte Kriterien für die Staatsanwaltschaften vorgestellt:

- **Polizeien und Kinderschutz:** Die Polizei jedenfalls ist die erste Instanz der Strafverfolgungsbehörde die mit von sexualisierter Gewalt betroffenen Kindern und ihren Elternteilen/Bezugspersonen in Kontakt kommt. Weshalb ihr eine herausragend große Bedeutung und Verantwortung zufällt. Es braucht dringend angemessene Studieninhalte für Polizeianwärterinnen/Anwärter und verpflichtende Fortbildungen fertiger Polizeibeamtinnen/Beamte.

## 6 Zum Abschluss

Zudem spreche ich mich seit vielen Jahren für Kinderschutzbeauftragte in jeder größeren Polizeiwache in Deutschland aus. Polizeibeamtinnen/Beamte, die eine angemessene Zusatzqualifikation absolviert haben und die wissen, warum der oben vorgestellte Praxisleitfaden unbedingt verbindlich angewendet werden muss. Für mich zeigt sich regelmäßig, dass gerade bei den Polizeien und Staatsanwaltschaften eklatante und schwerwiegende Fehler gemacht werden, die sich im weiteren Verlauf enorm belastend auf die betroffenen kindlichen Zeugen und ihre schützenden und begleitenden Elternteile/Bezugspersonen auswirken und die am Ende möglicherweise dazu führen können, dass Verfahren eingestellt werden. Sie geben mir sicher Recht, wenn ich schreibe, dass hierdurch niemanden geholfen wird. Noch schlimmer: Täterpersonen können unbemerkt weitere Verbrechen an weiteren Kindern begehen. Je jünger die Kinder, umso größer die Wahrscheinlichkeit, dass Ermittlungsverfahren der Staatsanwaltschaften eingestellt werden, kleine Kinder, denen die Aussagetüchtigkeit ja ohnehin vollständig abgesprochen wird.

Ich komme nun zum Schluss und möchte trotz aller Verbitterung zuversichtlich nach vorne schauen und drauf hoffen, dass mein Beitrag von Ihnen, den Leser/innen dieser Zeitschrift nicht als stumpfsinniges Fingerpointing abgetan wird, sondern vielmehr als Ansporn und Motivation die eigene moralische Haltung und Arbeitsweise zu hinterfragen und möglicherweise zu korrigieren, um damit einen wichtigen Beitrag für eine flächendeckende Anwendung kindgerechter Kriterien für das Strafverfahren zu gewährleisten. Der Schutz für Kinder vor sexualisierter Gewalt ist eine gesamtgesellschaftliche Verantwortung, doch die Polizeien in Deutschland können viel dazu beitragen, dass Kinderschutz im Ermittlungsverfahren ein Standard wird und nicht nur ein Ziel bleibt. Vielen Dank!

QR-Code zu der „Checkliste, die beim Helfen helfen kann“ der GdP:

SCAN ME

Bildrechte: ProPK.

## Anmerkungen

1 Josefine Barbaric ist Referentin *„Sexueller Missbrauch an Kindern“*, Trainerin für Gewaltprävention, Buchautorin und Vorstand *„Nein, lass das! e.V.“*
2 Polizeiliche Kriminalstatistik *„Kindliche Gewaltopfer in Deutschland“*, 2021.
3 https://www.im.nrw/kampf-gegen-kindesmissbrauch-300-euro-erschwerniszulage-0.
4 Gewerkschaft der Polizei, Bundesvorstand, www.gdp.de, 31. März 2020.
5 Praxisleitfaden Nationaler Rat.

# Führungsaufsicht: Prävention von Delikten gemäß § 184b StGB „Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte“

**Von PD a.D. Rainer Becker und Prof. Dr. Mirko Faber, Nordenham/Güstrow[1]**

## 1 Einleitung

Seit Juli 2021 sind sexualisierte Gewalt gegen Kinder und nahezu sämtliche Tatvarianten rund um die sog. Kinderpornografie zu besonders verwerflichen Straftaten (= Verbrechen) geworden und mit einer Mindeststrafandrohung von einem Jahr Freiheitsstrafe bewehrt.[2] In diesem Zusammenhang weisen die Verfasser darauf hin, dass gemäß § 181b StGB das Gericht nun auch in den Fällen des § 184b StGB *„Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte“* Maßnahmen der Führungsaufsicht anordnen kann (§ 68 Abs. 1 StGB). Wer während der Führungsaufsicht gegen eine bestimmte Weisung der in § 68b Abs. 1 StGB bezeichneten Art verstößt und dadurch den Zweck der Maßregel gefährdet, wird gemäß § 145a StGB mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Die Tat wird nur auf Antrag der Aufsichtsstelle (§ 68a StGB) verfolgt. Vor dem Hintergrund der explodierenden Zahlen, insbesondere in Zusammenhang mit Delikten gemäß § 184b StGB, stellt diese Regelung einen Fortschritt dar.[3] In Bezug auf die Anwendung der durch die §§ 145a, 68b, 181b StGB eröffneten Möglichkeiten wird sicherlich je nach Einzelfall zu differenzieren sein. Maßstab für die Anordnung der Führungsaufsicht nach § 68 Abs. 1 StGB ist eine prognostische Entscheidung des Gerichts dahingehend, ob die Gefahr der Begehung weiterer Straftaten besteht.[4] Kriterien könnten z.B. sein, inwieweit es sich um einen Ersttäter oder Wiederholungstäter handelt. Bei Ersttätern sollte besonders erörtert werden, wieviel strafbares Material bei ihnen gefunden wurde, wie *„aggressiv“* das ausgewertete Material war, mit wie vielen Personen sie dies geteilt hatten und ob sie ggf. auch selbst beweisbar aktiv sexuellen Missbrauch betrieben haben.

## 2 Maßnahmen der Einflussnahme

Die Strafvollstreckungskammer kann der verurteilten Person Weisungen für ihre künftige Lebensführung erteilen. Die Führungsaufsichtsstelle überwacht im Einvernehmen mit dem Gericht das Verhalten der verurteilten Person und die Erfüllung der Weisungen.[5] Dazu kann die Führungsaufsichtsstelle gemäß der in § 463a Abs. 1–3 StPO eingeräumten Kompetenzen von sämtlichen öffentlichen Behörden Auskünfte einholen, Ermittlungen anstellen oder solche durch andere Behörden im Rahmen ihrer Zuständigkeit vornehmen lassen.[6]

Weisungen können z.B. sein:

- den Wohn- oder Aufenthaltsort oder einen bestimmten Bereich nicht ohne Erlaubnis der Aufsichtsstelle zu verlassen,
- sich nicht an bestimmten Orten aufzuhalten, die der unter Aufsicht stehenden Person Gelegenheit oder Anreiz zu weiteren Straftaten bieten können,
- zu der verletzten Person oder bestimmten Personen oder Personen einer bestimmten Gruppe, die Gelegenheit oder Anreiz zu weiteren Straftaten bieten können, keinen Kontakt aufzunehmen, mit ihnen nicht zu verkehren, sie nicht zu beschäftigen, auszubilden oder zu beherbergen,
- bestimmte Tätigkeiten nicht auszuüben, die sie nach den Umständen zu Straftaten missbrauchen kann,
- bestimmte Gegenstände, die Gelegenheit oder Anreiz zu weiteren Straftaten bieten können, nicht zu besitzen, bei sich zu führen oder verwahren zu lassen,
- Kraftfahrzeuge oder bestimmte Arten von Kraftfahrzeugen oder von anderen Fahrzeugen nicht zu halten oder zu führen, die sie nach den Umständen zu Straftaten missbrauchen kann,
- sich zu bestimmten Zeiten bei der Aufsichtsstelle, einer bestimmten Dienststelle oder der Bewährungshelferin oder dem Bewährungshelfer zu melden,
- jeden Wechsel der Wohnung oder des Arbeitsplatzes unverzüglich der Aufsichtsstelle zu melden,
- sich im Fall der Erwerbslosigkeit bei der zuständigen Agentur für Arbeit oder einer anderen zur Arbeitsvermittlung zugelassenen Stelle zu melden,
- keine alkoholischen Getränke oder andere berauschende Mittel zu sich zu nehmen, wenn aufgrund bestimmter Tatsachen

Gründe für die Annahme bestehen, dass der Konsum solcher Mittel zur Begehung weiterer Straftaten beitragen wird, und sich Alkohol- oder Suchtmittelkontrollen zu unterziehen, die nicht mit einem körperlichen Eingriff verbunden sind,

- sich zu bestimmten Zeiten oder in bestimmten Abständen bei einer Ärztin oder einem Arzt, einer Psychotherapeutin oder einem Psychotherapeuten oder einer forensischen Ambulanz vorzustellen oder
- die für eine elektronische Überwachung ihres Aufenthaltsortes erforderlichen technischen Mittel ständig in betriebsbereitem Zustand bei sich zu führen und deren Funktionsfähigkeit nicht zu beeinträchtigen.

Die letztgenannte Weisung meint konkret die sog. elektronische Fußfessel, die einen besonders schwerwiegenden Eingriff in die private Lebensgestaltung beinhaltet. Deshalb ist diese Weisung nur unter bestimmten Voraussetzungen möglich.

## 3 Eine Kontrolle der Kommunikationsmittel des Betroffenen?

Bezugnehmend auf die Feststellung, dass die Führungsaufsichtsstelle von sämtlichen öffentlichen Behörden Auskünfte einholen und selbst Ermittlungen anstellen oder von anderen Behörden vornehmen lassen kann, stellt sich die Frage, ob und wie hierbei ggf. auch die im Besitz der Betroffenen befindlichen Kommunikationsmittel (effektiv) begrenzt oder sogar unangekündigt stichprobenhaft kontrolliert werden können.

Ein Vergleich mit der sog. Razzien-Kontrolle aus dem Polizeirecht, bei der die Polizei sogar ohne richterliche Anordnung an *„gefährlichen"* Orten bei allen Personen, die sich dort aufhalten, die Identität feststellen und sie und ihre mitgeführten Sachen durchsuchen darf,[7] mit einer durch ein Gericht bestätigten Weisung, eine Kontrolle zu ermöglichen, legt nahe, dass eine Begrenzung/Kontrolle der Kommunikationsmittel der unter Führungsaussicht stehenden Person nicht von vornherein ausgeschlossen sein dürfte. Immerhin hat sich die betroffene Person gerichtlich festgestellt als *„gefährlich"* erwiesen, denn sonst wäre sie ja nicht unter Führungsaufsicht gestellt worden. Darüber hinaus sei auf die Tatsache verwiesen, dass im Rahmen der Führungsaufsicht sogar – sicherlich am Einzelfall orientiert – grundsätzlich auch so schwerwiegende Eingriffe wie die elektronische Überwachung des Aufenthaltsortes mittels einer elektronischen Fußfessel im Rahmen der Führungsaufsicht erlaubt sind.[8]

Fakt ist, dass es sich bei der Kontrolle von E-Mails und Dateien um Eingriffe in das Fernmeldegeheimnis gemäß Art. 10 GG handelt.[9] Eingriffe in Art. 10 GG unterliegen den Schranken des Art. 10 Abs. 2 GG, also einem Gesetzesvorbehalt. Eine entsprechende gesetzliche Eingriffsgrundlage stellt z.B. § 100a StPO, Telekommunikationsüberwachung, dar. Neu lässt § 100a StPO eine Telekommunikationsüberwachung auch zur Aufklärung von Straftaten gemäß §§ 184b, 184c Abs. 2 StGB zu.[10]

Wenn denn bereits zum Zwecke der Aufklärung dieser Taten mit Richtervorbehalt ein heimlicher Eingriff in das Fernmeldegeheimnis der Betroffenen möglich ist, dann sollte dies erst recht zum Zweck der Verhütung dieser Taten nach richterlich festgestellter Wiederholungsgefahr und richterlich verfügter Führungsaufsicht möglich sein. Immerhin genügt für eine Anordnung nach § 100a StPO bereits ein Tatverdacht in Bezug auf eine entsprechend schwere Straftat, was in der Gewichtigkeit der Verdachtsmomente deutlich unterhalb von hinreichendem und dringendem Tatverdacht und damit unter einer Wahrscheinlichkeit von 50% für eine spätere Verurteilung rangiert.[11] Die demgegenüber für die Anordnung der Führungsaufsicht (§ 68 StGB) anzustellende Gefahrenprognose verlangt, dass bei dem Täter eher damit zu rechnen ist, dass er neue Straftaten begeht, als dass

## REZENSION

**Artkämper/Jakobs, Polizeibeamte als Zeugen vor Gericht. 3. Auflage 2022**

Polizeibeamte sind, wie andere Bürger auch, in die allgemeinen Zeugenpflichten eingebunden. Zudem treten sie vermehrt als Sachverständige im Strafverfahren auf. In beiden Funktionen tragen sie eine maßgebliche Verantwortung für den Ausgang des Verfahrens.
Allerdings kann das Verhältnis von Polizeibeamten zu Staatsanwaltschaft, Gericht und Verteidigung von Missverständnissen geprägt sein, die aus unterschiedlichen Aufgaben und Funktionen herrühren. In dem vorliegenden Buch gehen die erfahrenen Autoren, differenziert nach Zeugen und Sachverständigen, auf mögliche Problemkonstellationen ein und vermitteln das erforderliche Wissen für Polizeibeamte, um vor Gericht die notwendige Handlungssicherheit zu erlangen. Gleichzeitig wollen sie das Verantwortungsbewusstsein der Beamten für ihre anspruchsvollen Aufgaben in einem rechtsstaatlichen und fairen Strafprozess schärfen. Der „Fair-trial-Grundsatz" ist ein auf verfassungsrechtlicher Ebene angesiedelter Grundsatz des Verfahrensrechts, durch das BVerfG in ständiger Rechtsprechung bestätigt worden und darf niemals zur Disposition stehen.

Die Autoren, Staatsanwalt als Gruppenleiter a.D. Dr. Heiko Artkämper und Oberstaatsanwältin Carola Jakobs waren bzw. sind bei der Staatsanwaltschaft Dortmund tätig und einer breiten Fachöffentlichkeit aus zahlreichen Publikationen bekannt. Sie stehen für eine fundierte Auseinandersetzung mit der Thematik auf hohem Niveau.
Die vorliegende Neuauflage wurde grundlegend überarbeitet und ergänzt. Dabei wurden auch die pandemiebedingten Beschränkungen des Gerichtsalltags mit unmittelbaren Auswirkungen auf polizeiliche Zeugen und Sachverständige berücksichtigt. Zahlreiche Anmerkungen und ein umfangreiches Literaturverzeichnis ermöglichen die vertiefende Auseinandersetzung mit der Thematik.
In der Gesamtschau handelt es sich um ein sehr empfehlenswertes Fachbuch, das für Praktiker, Lehrende und Studierende gleichermaßen gut geeignet ist.

Hartmut Brenneisen, Preetz/Worms

| | |
|---|---|
| **Autoren:** | **Heiko Artkämper, Carola Jakobs** |
| **Titel:** | **Polizeibeamte als Zeugen vor Gericht** |
| **Auflage:** | **3. Auflage 2022** |
| **Format:** | **288 Seiten, DIN A5, Broschur** |
| **Preis:** | **26,90 Euro** |
| **ISBN:** | **978-3-8011-0909-7** |
| **Verlag** | **Verlag Deutsche Polizeiliteratur GmbH** |

solche ausbleiben werden, was einer Gefahr von über 50% entspricht.[12] Hinzu käme, dass, durch die vorherige Ankündigung entsprechender Maßnahmen in Form der gerichtlich verfügten Weisung, der Eingriff sogar milder als eine heimlich durchgeführte Überwachung der Telekommunikation ausfiele.

Die Verfasser kommen daher zu dem Ergebnis, dass eine Begrenzung oder Kontrolle der Kommunikationsmittel von unter Führungsaufsicht stehenden Personen zulässig ist. Allerdings dürfte eine Begrenzung aus dem Grund, dass Kommunikationsmittel wie das Mobiltelefon zum einen auch versteckt oder bei dritten Personen deponiert werden können und zum anderen in Notfällen zum Herbeiholen von Hilfe erforderlich sein könnten, eher nicht zielführend erscheinen.

Aber die Weisung, dass die unter Aufsicht stehenden Personen unangekündigte stichprobenhafte Kontrollen durch Polizeibeamte, wie auch immer technisch durchgeführt, zu ermöglichen haben, dürfte durchaus ausreichen, diese von der Begehung weiterer Straftaten abzuhalten oder aber eben einen Rückfall zu beweisen und daraus die entsprechenden Konsequenzen zu ziehen.

## 4 Schluss

Nach den Nachbesserungen zur Verbesserung des Schutzes von Kindern vor sexualisierter Gewalt hat sich vieles getan. Dabei gilt es noch einige der neuen Regelungen mit ihren Möglichkeiten weiter auszuloten und ohne unnötige Verzögerungen anzuwenden – so wie auch zukünftig die Führungsaufsicht nach Straftaten gemäß § 184b StGB.

## Anmerkungen

1 Rainer Becker ist Polizeidirektor und Hochschuldozent a.D. sowie Ehrenvorsitzender der Deutschen Kinderhilfe – Die ständige Kindervertretung e.V.; Prof. Dr. Mirko Faber lehrt Eingriffsrecht und Strafrecht am Fachbereich Polizei der Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes Mecklenburg-Vorpommern.
2 Gesetz zur Bekämpfung sexualisierter Gewalt gegen Kinder vom 16. Juni 2021, BGBl. I 2021, S. 1810–1815.
3 So ist für die Jahre 2016 bis 2021 ein enormer Anstieg in Bezug auf die Anzahl der polizeilich erfassten Fälle gemäß § 184b StGB von 5.687 (2016) auf 39.171 (2021) zu verzeichnen, vgl. https://de.statista.com/statistik/daten/studie/1110942/umfrage/polizeilich-erfasste-faelle-im-zusammenhang-mit-kinderpornographie/.
4 Braasch, M., in: Dölling/Duttge/Rössner: StGB, 5. Auflage 2022, § 68, Rn. 2.
5 Heuchemer, M., in: BeckOK, 53. Ed. 1.5.2022, § 68a, Rn. 4.
6 Groß, K.-H./Ruderich, D., in: MüKoStGB, 4. Auflage 2020, § 68a, Rn. 7–8.
7 Exemplarisch für die Zulässigkeit: §§ 29 Abs. 1, S. 2, 53 Abs. 1 Nr. 3, 57 Abs. 1 Nr. 4 SOG M-V.
8 § 86b Abs. 1 Nr. 12 StGB.
9 Das Fernmeldegeheimnis dient dem Schutz der unkörperlichen Übermittlung von Informationen an individualisierte Empfänger mit Hilfe des Telekommunikationsverkehrs, vgl. BVerfGE 115, 166 (182); 124, 43 (54). Einen Eingriff in das Fernmeldegeheimnis stellt jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt dar, vgl. BVerfGE 85, 386 (398); 100, 313 (366); 110, 33 (52 f.); 125, 260 (310).
10 § 100a Abs. 1 i.V.m. Abs. 2 Nr. 1 lit. g).
11 Graf, J.-P., in: BeckOK StPO, 43. Ed. 1.4.2022, § 100a, Rn. 106.
12 Groß, K.-H./Ruderich, D., in: MüKoStGB, 4. Auflage 2020, § 68, Rn. 8.

# Cyberkriminalität und Risiken in der „digitalen Sphäre“: Aktuelle und zukünftige Bedrohungslagen sowie tragfähige Präventionsmaßnahmen

Von Dr. Viktoria Schäfer und Dr. Yvonne Zimmermann, Montabaur[1]

## 1 Inhalte und Kontext des Beitrags

Der vorliegende Beitrag befasst sich mit dem Thema Cyberkriminalität und geeigneten Präventionsstrategien. Im Hinblick auf die Prävention werden in Unternehmen und anderen Organisationen mittlerweile entsprechende Schulungen von Mitarbeitern entwickelt und gezielte Weiterbildungsangebote umgesetzt. Solche Maßnahmen bilden einen wesentlichen inhaltlichen Gesichtspunkt des Beitrags, der insbesondere an Schwerpunktthemen der Ausgabe 2/2022 der Zeitschrift Die Kriminalpolizei anknüpft. In dieser Ausgabe wurden Herausforderungen der Cyberkriminologie ausführlich erläutert. Handlungsleitend ist demnach die Erkenntnis, dass bei

der Digitalisierung nicht primär an die Nutzung technischer Möglichkeiten und Geräte gedacht werden sollte, sondern an die *„Etablierung eines globalen digitalen Raumes – besser vermutlich einer globalen digitalen Sphäre – der grenzfreien Interaktion und Kommunikation zwischen Menschen auf der ganzen Welt und aus jedem Kulturkreis“*.[2] Die Folgerung, dass die Komplexität dieser digitalen Sphäre mit den sich hierin stellenden Deliktsmöglichkeiten der Entwicklung einer zukunftstragenden Polizeistrategie bedarf, ist vollauf nachvollziehbar. Der für eine solche Polizeistrategie relevante Präventionsgedanke wurde in der oben genannten Ausgabe auch in einem Fachartikel zur Sensibilisierung für Gefahren im Netz und zur Bekämpfung der verschiedenen Formen der Computerkriminalität unter besonderer Berücksichtigung der Schutzbelange von Kindern und Jugendlichen vertieft.[3] Erläutert wurden in weiteren Fachartikeln ferner Entwicklungen, Begehungsformen sowie Präventionserfordernisse und strafrechtliche Anforderungen im Deliktfeld *„Identitätsdiebstahl und -missbrauch im Internet“*.[4]

## 2 Präventionsorientierung möglichst früh vollziehen

Die Notwendigkeit der Präventionsorientierung in der digitalen Sphäre wurde unter dem forensischen und strafrechtlichen Blickwinkel in den angeführten Fachartikeln ausdrücklich hervorgehoben. Faktisch ist (leider) davon auszugehen, dass die Ausprägung und Deliktsrelevanz der verschiedenen Facetten der Cyberkriminalität auch zukünftig zunehmen werden. In Forschung und Praxis herrscht Konsens dahingehend, dass man solch einer problematischen Entwicklung durch eine möglichst früh, also bereits in der Schule erfolgende Verankerung von Präventions- und Abwehrstrategien begegnen sollte. Ein aktuelles Beispiel dafür ist *„ChatScouts“*, ein Projekt des LKA Niedersachsen. Dieses in Kooperation mit den Regionalen Landesämtern für Schule und Bildung (RLSB) und der Zentralstelle Jugendsachen des Landeskriminalamtes (LKA) Niedersachsen entwickelte Projekt erfuhr überdies die Unterstützung der kriminologischen Forschungsstelle des LKA Niedersachsen und spezialisierter Kräfte der Polizei Niedersachsen. Als Präventionsangebot richtet es sich an Kinder und verfolgt unter anderem das Ziel, Themen wie Cybermobbing und Mediensicherheit altersgerecht aufzubereiten. Hierzu werden neben Informationen, Unterrichtsmaterialien sowie Empfehlungen für pädagogische und polizeiliche Fachkräfte altersentsprechende Videoinhalte für die Kinder bereitgestellt. In seiner Gesamtheit beinhaltet das Projekt über die für Kinder entwickelten Elemente hinaus auch Empfehlungen für pädagogische Fachkräfte sowie, begleitend zu den Präventionsangeboten der Polizei an Schulen, Maßnahmen zur Einbeziehung und Sensibilisierung der Elternschaft.[5]

## 3 Transfer der Präventionsausrichtung auf den Berufsalltag – Bedrohungslage für KRITIS

Das LKA-Projektbeispiel zeigt einen Weg, wie die möglichst frühzeitige Aufklärung über Risiken in der digitalen Sphäre und die Vermittlung eines verantwortungsvollen Umgangs mit digitalen Medien realisiert werden kann. Solch eine – sinnvollerweise kontinuierlich angelegte – Präventionsarbeit kann entscheidend dazu beitragen, dass die Bewusstseinsbildung für die genannten Risiken und die erforderliche Verantwortungsherausbildung auch über die weitere Lebensspanne erfolgen und dann im Erwachsenenalter bzw. bei der Berufsausübung in Organisationen, Unternehmen usw. wirksam werden. Letzteres Ziel ist umso wichtiger, da – neben den die Betroffenen oftmals psychisch schwer belastenden *„Individualattacken“* von Cyberkriminellen (wie etwa Identitätsdiebstahl im Internet, Cybermobbing oder Cyberstalking)[6] – die gegen Unternehmen, Behörden und andere öffentliche Einrichtungen ausgeübte Cyberkriminalität immer mehr zunimmt. Man spricht in diesem Zusammenhang auch von *„Big Game Hunting“*, also von Cyberattacken auf herausragende Wirtschaftsunternehmen sowie Einrichtungen der sog. Kritischen Infrastrukturen (KRITIS). KRITIS repräsentieren *„Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“*.[7] KRITIS finden sich insbesondere in Bereichen wie der Energie- und Wasserversorgung, der medizinischen Versorgung und des öffentlichen Verkehrs. Fakt ist, dass in jüngster Zeit KRITIS, zu denen neben der Versorgung der Bevölkerung mit wichtigen Leistungen auch Verwaltungen mit großen Mengen an gespeicherten persönlichen Daten gehören, immer stärker in den Fokus von Cyberkriminellen geraten. Laut Expertenmeinung hat sich diese Situation seit dem Einmarsch russischer Streitkräfte in die Ukraine verschärft: *„Gerade der Ukraine-Konflikt hat hier eine neue Komponente noch einmal in Erinnerung gerufen: Angriffe auf die Netzwerke öffentlicher Verwaltungen tragen dazu bei, einen Staat und eine Regierung massiv zu destabilisieren und das Vertrauen von Menschen in den Staat zu schwächen“*.[8]

## 4 Hybride Konfliktaustragung und Cyberattacken, Angriffsformen und Schäden

Tatsächlich hat der Krieg in der Ukraine noch einmal mit Nachdruck auf die Gefahr der sog. hybriden Kriegsführung aufmerksam gemacht, denn kriegerische Auseinandersetzungen und geopolitische Konflikte können sowohl physisch mit Waffen als auch auf digitalen Ebenen ausgetragen werden: *„Der Krieg zwischen Russland und der Ukraine erreicht durch die Anwendung der hybriden Kriegsführung eine neue Stufe der Bedrohung. Es werden nicht nur konventionelle, sondern zunehmend auch Cyberwaffen eingesetzt, um Regierungs-, Infrastruktur- und Energie- sowie private Netzwerke zu zerstören. In der Ukraine begann dieser ‚stille‘ Krieg bereits Stunden vor dem Einmarsch der russischen Truppen, um die Kommunikation zu erschweren bzw. zu unterbrechen. Darüber hinaus sollen dadurch Panik geschürt, Falschinformationen verbreitet und das Vertrauen sowie die Moral der Bürger zur Verteidigung untergraben […] werden“*.[9] Im Zuge solcher Entwicklungen rücken die Cybersicherheit und damit Anstrengungen zur Verteidigung eines Landes, seiner Wirtschaft, Infrastruktur und letztlich der gesamten Gesellschaft gegen externe Cyberangriffe nochmals stärker in den Mittelpunkt. Datenauswertungen auf Basis aktueller Untersuchungen des Instituts der Deutschen Wirtschaft (IW) belegen für den Zeitraum von 2011 bis zur Gegenwart, dass schwere Cyberattacken auf Ziele in Deutschland[10] in 28% solcher Fälle ihren Ursprung in Russland hatten. Chinesische und iranische Akteure waren gemäß den Daten für 12% und 8% der Fälle verantwortlich. Es gilt aber auch kritisch darauf hinzuweisen, dass für weitere 4% dieser Fälle ein Ursprung in den USA identifiziert werden konnte und sich 48% der schwerwiegenden Attacken seit 2011 nicht eindeutig einem Staat zuordnen ließen.[11]

Der Gesamtschaden durch Cyberangriffe ist sehr hoch. Bereits 2020, im Jahr des Ausbruchs der Corona-Pandemie, entstanden der deutschen Wirtschaft durch diese Angriffe,

Mobil- und Datenträgerforensik.

verbunden mit dem Diebstahl von Daten, Spionage sowie Sabotage, Schäden von schätzungsweise rund 224 Mrd. Euro[12] Der durch die Pandemie ausgelöste Digitalisierungsschub hat die digitale Gefährdungslage offenkundig verschärft. Im Rahmen dieses Digitalisierungsschubes haben auch die industrielle Vernetzung und Steuerung sowie das damit verknüpfte *„Internet of things“* (IOT) ausgeprägte Innovationsimpulse erfahren. Intelligente Steuerung macht Fertigungsprozesse effizienter, die sog. *„smarte Analytik“* trägt durch vorausschauende Wartung zur Verhinderung des Ausfalls von Anlagen bei und maschinelles Lernen in der Fertigungskontrolle hebt die Qualität von Waren und Produkten. Die entsprechenden Leistungen im Maschinenbau, der Automatisierungstechnik und im zugehörigen Software-Engineering sind beeindruckend, sollten jedoch nicht den kritischen Blick auf potenzielle Gefahrenquellen trüben, denn *„das Risiko von Cyberattacken [wird] im Zuge der Vernetzung kontinuierlich immer größer. Mit jeder weiteren Maschine, jedem neuen Sensor, jedem zusätzlichen Gerät, das via Intra- und Internet auswert- und erreichbar wird, wächst die Gefahr, dass diese industriellen Steuerungssysteme auch zum Ziel von Hackerattacken werden“*.[13] Experten sprechen diesbezüglich von *„OT-Attacken“* durch Cyberkriminelle oder im Auftrag von Fremdstaaten handelnden Hackern (OT steht für operationale Technik).

OT-Angriffe und die weiter vorn angesprochenen Attacken auf KRITIS weisen teils Überschneidungsbereiche auf, die destruktive OT-Stoßrichtung zielt allerdings auf Unternehmen unterschiedlicher Branchen und Größenordnungen, also auch auf sog. KMU (kleinere Firmen und Mittelständler). Die zielgerichteten OT-Angriffe erreichen noch nicht das Ausmaß herkömmlicher IT-Attacken, die schon längst ein *„digitales Trommelfeuer“* auf die Firewalls und Virenschutz-Programme von Unternehmen darstellen, werden aber nach Prognosen von Fachleuten drastisch zunehmen und bergen enorme Schädigungsrisiken. OT-Angriffe zielen auf computergesteuerte Produktions- und Steuerungsanlagen, auf entsprechende Produktionsmaschinen und Fertigungstechnik sowie auf die Hard- und Software, die Geräte, Anlagen und Prozesse in industriellen Umgebungen steuert bzw. überwacht. Die Schädigungsrisiken können sich auf Leib und Leben erstrecken*: „das Schadensrisiko reicht weit über den bloßen Stillstand von IT-Systemen hinaus: Denn OT-Attacken können von reinen Maschinenstörungen und Fehlfunktionen bis hin zur kompletten mechanischen Zerstörung der Technik führen. Dass dabei, etwa beim Bersten von Druckkesseln oder Explosionen in chemischen Anlagen nach einer Fehlsteuerung der Produktion, auch Menschenleben gefährdet werden können, verleiht OT-Attacken eine ganz neue Qualität: Auf einmal drohen nicht nur finanzielle Verluste, sondern der Tod“*.[14]

## 5 Handlungsperspektiven: Cyberattacken abwehren, Risiken in der digitalen Sphäre neutralisieren, wirksame Präventionsmaßnahmen durchsetzen

Die entscheidende Zukunftsfrage lautet: Wie lassen sich die zuvor beschriebenen Cyberangriffe abwehren, wie kann dafür gesorgt werden, dass die aus solchen Angriffen resultierenden Schädigungen – die die Wirtschaft, öffentliche Einrichtungen und letztlich das gesamte Gemeinwesen betreffen – unterbunden werden? Auf der Ebene öffentlicher Einrichtungen muss zunächst konstatiert werden, dass insbesondere kleinere Kommunen in Deutschland im Hinblick auf Risiken in der digitalen Sphäre oftmals nicht ausreichend geschützt sind. Der Nachholbedarf ist beträchtlich. Nach Expertenhinweisen müssten, um solche Schwachstellen zu beheben, alle staatlichen Stellen – ob es sich nun um eine Landesbehörde, Kreisverwaltung oder Kommune handelt – mehr Investitionen in die IT-Sicherheit und den Datenschutz vornehmen.[15] Die Notwendigkeit dieser Schritte wird heutzutage von den Entscheidungsträgern in Behörden, Verwaltung und Politik nahezu ausnahmslos eingeräumt. Die Entwicklung von passgenauen Sicherheitsmodellen für komplette IT-Lebenszyklen einschließlich Analyse, Planung, Implementierung und Überwachung sowie die Sicherung der KRITIS im Einklang mit den gesetzlichen Vorgaben und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) schreitet folgerichtig voran, um die erheblichen Rückstände früherer Zeiten aufzuholen. Die entsprechenden Maßnahmen umfassen auch spezielle Modellierungen unterschiedlicher Risikoszenarien, sog. Vulnerabilitäts- und Penetrationstests (System- und Anwendungs-Checks auf Schwachstellen und mögliche Einfallstore für Hacker) sowie die Konzeption, Realisierung und Kontrolle der stetig dominanter werdenden Cloud-Verlagerungen.[16] Die im Juli 2022 vom Bundesinnenministerium vorgestellte Cybersicherheitsagenda unterstreicht die grundsätzliche Dringlichkeit derartiger und kontinuierlich auszubauender Maßnahmen. Kernelemente der Cybersicherheitsagenda sind eine neu organisierte Cybersicherheitsarchitektur mit einer führenden Rolle des Bundes, erweiterte Befugnisse für die Sicherheitsbehörden, um Cyberattacken abwehren zu können, die konsequente Bekämpfung und strafrechtliche Ahndung von Cyberkriminalität, aber auch die Stärkung der deutschen Cybersicherheitsforschung zur Erhöhung der sog. Cyber-Resilienz.[17]

Technischer Nachholbedarf in der IT-Sicherheit findet sich mithin auch in zahlreichen privatwirtschaftlichen Unternehmen. Eine besondere Vulnerabilität vieler Produktionsanlagen rührt daher, dass die Technik zum Teil bereits Jahrzehnte alt ist: *„Gerade in der Industrie sind Investitionszyklen von 30 bis 40 Jahren keine Seltenheit. Damit stammen Maschinen und Steuertechnik vielfach noch aus Zeiten, in denen die Vernetzung der Anlagen übers Internet oder gar die Auswertung der Betriebszustände mithilfe intelligenter Analysesoftware noch völlig irrelevant waren. Weil die Technik meist allenfalls intern vernetzt und damit gegen externe Zugriffe geschützt war, spielten mögliche Hackerbedrohungen jahrzehntelang keine Rolle. In Zeiten der allumfassenden Digitalisierung der Produktion, einschließlich der angejahrten Altsysteme, rächt sich das jetzt“*.[18] Es ist durchaus irritierend, dass Deutschland bei der digitalen Sicherheit internationalen Standards *„hinterherhinkt“*, obwohl es hinsichtlich der weltweiten Handelsbeziehungen in den zurückliegenden Jahren stets einen der vordersten Ränge einnehmen konnte.[19]

Die aufgeworfene Zukunftsfrage nach der wirksamen Unterbindung von Cyberattacken und deren gesamtwirtschaftlichen und gesellschaftlichen Schäden lässt sich also nicht nur für öffentliche Einrichtungen, sondern ebenso auf Seiten von Unternehmen in Deutschland im Sinne einer durchgreifenden

sicherheitstechnischen Optimierung beantworten. Eine entscheidende Rolle kommt dabei den Entscheidungsträgern und Führungskräften sowie der Organisationsentwicklung in den Unternehmen zu. Auf dieser personellen und organisatorischen Ebene *„hapert“* es allerdings nach wie vor. Das notwendige Gefahrenbewusstsein scheint oftmals nur rudimentär ausgeprägt zu sein. Nach aktuellen empirischen Erhebungen *„fehlt offenbar die nötige Sensibilität für den Schutz der Technik: Nicht einmal jedes fünfte Unternehmen hat […] bisher ein eigenes Cybersicherheitsbudget für den Schutz der OT-Systeme“*[20] – solch ein Erhebungsbefund sollte aufrütteln, da ja namentlich bei Industrieunternehmen die Zuverlässigkeit von digital eingebundenen Steuerungssystemen für die Betriebssicherheit und damit auch für den wirtschaftlichen Erfolg von essenzieller Bedeutung sind. Hinweise zum Gefahrenbewusstsein und zur Risikosensibilität machen deutlich, wie wichtig der Faktor Mensch bei dem Ringen um Cybersicherheit bzw. bei der wirksamen Abwehr derartiger, in Unternehmen und anderen Organisationen unentwegt erfolgenden Angriffe ist. Menschliches Fehlverhalten kann die technischen Potenziale einer noch so guten Cyberabwehr unterminieren und leider geschieht dies tatsächlich immer wieder. So weisen Studiendaten darauf hin, dass annähernd jeder zweite kritische Cybersicherheits-Vorfall oder -Hack das Resultat von Unaufmerksamkeit oder nicht ausreichender Schulung von Mitarbeitern war.[21] Es ist davon auszugehen, dass Mitarbeiter in Unternehmen und Organisationen oftmals nicht wirklich realisieren, dass Cyberbedrohungen sehr ernst zu nehmen sind, dass derartige Attacken gravierende Konsequenzen auf innerbetriebliche/-organisatorische Abläufe haben und letztlich den eigenen Arbeitsplatz gefährden können.

Mithin ist es nicht sinnvoll, primär eine Defizitperspektive einzunehmen, Menschen also vorrangig als *„Sicherheitslücke“* zu betrachten. Vielmehr sollte der Mensch als aktiver *„Abwehrschirm“* und *„Sicherheitsfaktor“* gegen Cyberattacken erkannt werden. Damit Menschen diese Rolle einnehmen können, bedarf es in Unternehmen, Organisationen und Institutionen gezielter Aus- und Weiterbildung sowie einer geeigneten Aktivierung der Risikoerkenntnisfähigkeit von Mitarbeitern. Der Auf- und Ausbau eines entsprechenden Problem- und Sicherheitsbewusstseins im Verbund mit regelmäßigen Schulungen sind *„wichtige präventive Maßnahmen um den ‚Sicherheits-Faktor Mensch‘ zu stärken. Relevante Gefährdungen müssen bekannt sein und die Erwartungshaltung hinsichtlich der Informationssicherheit in dem Unternehmen oder der Institution sollte klar kommuniziert werden. So wird die Grundlage für einen sensiblen Umgang mit Daten und IT-Informationssicherheit gelegt“*.[22] Man spricht in diesem Zusammenhang auch von *„Awareness“* als elementarer Sicherheitsmaßnahme. Awareness beinhaltet, dass zunächst das Problembewusstsein für Cybersicherheit erlangt werden muss, um darauf aufbauend die erforderlichen Verhaltensänderungen für die digitale Ebene umsetzen zu können.[23]

Sowohl Einzelfirmen und -organisationen als auch übergeordnete Institutionen und Verbände sind gefordert, ihre Mitarbeiter im Hinblick auf diese Awareness und konkrete Handlungskompetenzen zu schulen und kontinuierlich weiter zu qualifizieren. Im Bereich der Finanzwirtschaft, namentlich bei Banken, die für die Aktivitäten von Cyberkriminellen ein häufiger gewähltes Ziel darstellen, werden entsprechende Maßgaben umgesetzt. Die sich immer wieder ändernden Bedrohungslagen und Begehungsformen der Cyberkriminalität machen eine entsprechend flexible Anpassung bzw. Neuentwicklung von Schulungs- und Weiterbildungsprogrammen erforderlich. In der genossenschaftlichen Qualifizierung und Weiterbildung werden diese Herausforderungen aktiv angegangen, um hinsichtlich IT/Digitalisierung eine stetig aktualisierte und damit belastbare Wissensbasis sowie die notwendigen Handlungskompetenzen auf der Entscheiderebene, bei Fachkräften und anderen Mitarbeitern zu gewährleisten. Qualifizierungsmaßnahmen richten sich hier sowohl an die Mitarbeiter von Genossenschaftsbanken als auch genossenschaftlich verankerten Organisationen weiterer Branchen und zielen insbesondere auf ein tragfähiges Informationssicherheits- und Risikomanagement ab, das im Regelbetrieb Cybergefahren identifizieren und wirksam neutralisieren kann. Dabei wird auch die Vermittlung von strukturellen Grundlagenkenntnissen zur digitalen Transformation sowie von entsprechenden Handlungskompetenzen (Digital Leadership, Personal- und Organisationsentwicklung) angestrebt.

Bildrechte: Davide Oliveira.

## Anmerkungen

1 Viktoria Schäfer ist Master of Science und wurde an der Steinbeis-Hochschule Berlin promoviert. Sie ist als Vorstandsvorsitzende und wissenschaftliche Leiterin des genossenschaftlichen Forschungsinstituts ADG Scientific-Center für Research and Cooperation mit Sitz in Montabaur tätig. Yvonne Zimmermann ist Dipl.-Bankbetriebswirtin (ADG), Master of Leadership and Organisational Development und wurde an der Universität Hohenheim promoviert. Sie übernahm 2016 den Vorstandsvorsitz der Akademie Deutscher Genossenschaften (ADG) in Montabaur.

2 Rüdiger, Thomas-Gabriel (2022): Herausforderungen der Cyberkriminologie. Die Kriminalpolizei, Ausgabe 2/2022, S. 13-18.

3 Kemper, Klaus (2022): Computerprävention. Sensibilisierung für Gefahren im Netz. Die Kriminalpolizei, Ausgabe 2/2022, S. 11-13.

4 Berthel, Ralph (2022): Identitätsdiebstahl und -missbrauch im Internet. Aktuelle Entwicklungen und Herausforderungen. Die Kriminalpolizei, Ausgabe 2/2022, S. 4-7 sowie Schiemann, Anja (2022): Strafbarkeit des Identitätsdiebstahls durch Phishing, Pharming und Spoofing. Die Kriminalpolizei, Ausgabe 2/2022, S. 7-10.

5 Landeskriminalamt Niedersachsen (2022): ChatScouts – Gemeinsam gegen Cybermobbing. Presseinformation vom 29.6.2022, https://www.lka.polizei-nds.de/a/presse/pressemeldungen/chatscouts-gemeinsam-gegen-cybermobbing-116254.html.

6 Siehe zur Ausprägung und zu Folgen entsprechender Delikte Huber, Edith (2015): Cybercrime gegen Privatpersonen, in: Guzy, Nathalie, Birkel, Christoph & Mischkowitz, Robert (Hrsg.): Ziele, Nutzen und Forschungsstand. Viktimisierungsbefragungen in Deutschland, Bd. 1. Wiesbaden, BKA, S 393-420.

7 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2022): Was sind Kritische Infrastrukturen und warum sind sie so wichtig? KRITIS-Definition der Bundesressorts, Stand Juli 2022, https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html.

8 Berghoff, Tim (2022): Wiedergegebene Expertenaussagen von Tim Berghoff (G Data, Security Manager), in: Künstler, Diana: Cyber Security – Kommunen im Visier. funkschau Business Netzwerk ITK, Beitrag vom 30.6.2022, https://www.funkschau.de/sicherheit-datenschutz/kommunen-im-visier.195608.html (2 Seiten).

9 Krüger, Janine (2022): Die hybride Bedrohung – Cyberkriege und Cybersicherheit. Effecten Spiegel, Ausgabe 11, S. 4.

10 Angriffe auf deutsche Regierungsbehörden, Verteidigungs- und High-Tech-Unternehmen mit einem Schaden von umgerechnet mehr als 1 Mio. USD (Stand Februar 2022, Datenquelle gemäß der folgenden Anmerkung).

11 IW-Daten und Statista-Grafik (2022): Im Visier russischer Hacker – Anteil der bedeutenden Cyberangriffe auf Deutschland und die Ukraine nach Herkunft seit 2011 (in %). Effecten Spiegel, Ausgabe 11, S. 13.

12 Daten gemäß vorgenannter Anmerkung.

13 Kuhn, Thomas (2022): Cyberangriffe gegen Maschinen – Wenn die Smart Factory zur tödlichen Gefahr wird. Wirtschaftswoche, 31.5.2022, https://www.wiwo.de/technologie/digitale-welt/cyberangriffe-gegen-maschinen-wenn-die-smart-factory-zur-toedlichen-gefahr-wird/28380028.html (2 Seiten).

14 Wiedergegeben bei Kuhn (2022), siehe Anmerkung zuvor.

15 Wiedergegebene Fachmeinungen im Beitrag von Künstler (siehe Anm. weiter oben).

16 Ein kompakter Praxis-Leitfaden für Vulnerabilitäts-/Penetrationstest (IT-Sicherheit) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist abrufbar unter

17 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html.

18 Bundesministerium des Innern und für Heimat (2022): Bundesinnenministerin stellt ihre Cybersicherheitsagenda vor. Nancy Faeser: *„Bedrohungslage im Cyberraum wächst jeden Tag“*. Pressemitteilung vom 12.7.2022, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html.

19 Kuhn (2022), siehe Anmerkung weiter vorn.

20 Hinter den USA und Singapur fand sich Deutschland nach jüngeren Daten bereits auf Platz 3 der weltweit registrierten Cyberangriffe auf Unternehmen und Institutionen. Im Jahre 2021 war schon jedes fünfte Unternehmen in Deutschland von mindestens einem Ransomware-Angriff (Schadprogramme insbesondere in Form von Erpressungs- bzw. Verschlüsselungstrojanern) betroffen, wobei 43% dieser Angriffe beträchtliche

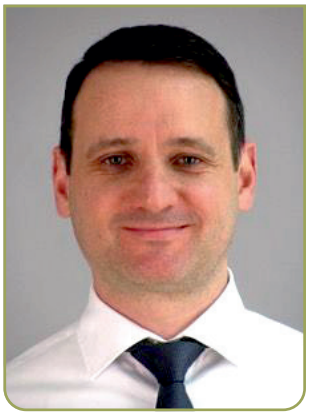
Auswirkungen auf den Betrieb hatten. Datenquelle: US-Analysehaus 451 Research, redakt. Wiedergabe in ‚boerse online‘, Ausgabe 21/2022, S. 34 (*„Unternehmen werden zunehmend Opfer von Hackern“*).

21 Kuhn (2022), siehe Anmerkung weiter vorn (unter Bezugnahme auf Erhebungsdaten des Beratungsunternehmens Lünendonk & Hossenfelder sowie der Wirtschaftsprüfungsgesellschaft KPMG u.a. aus dem produzierenden Sektor).

22 Gemäß Kaspersky-Daten von 5.000 Unternehmen weltweit (*„in 46% of cybersecurity incidents in the last year, careless/ uniformed staff have contributed to the attack“*). Quelle: The Human factor in IT security: How employees are making businesses vulnerable from within, https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

23 Cyber-Sicherheitsempfehlungen gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI): *„Faktor Mensch“*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/faktor-mensch_node.html.

24 Cyber-Sicherheitsempfehlungen gemäß Bundesamt für Sicherheit in der Informationstechnik (BSI): *„Faktor Mensch – Awareness“*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html.



# Virtualisierung und Meinungsbildung im Rechtsextremismus

Von RA Marcel Auber, Ludwigsburg[1]

## 1 Einleitung

Das Internet hat das Leben der Menschen nachhaltig verändert. Bedenkt man, in wie vielen Bereichen sich unser Verhalten durch die Virtualisierung und die hierfür genutzten Konsumgeräte gewandelt hat, kann man die Aussage von Wissenschaftlern, die Erfindung des Internets sei nach dem Buchdruck die bahnbrechendste Erfindung überhaupt, gut nachvollziehen. Wie nahezu alle Entwicklungen bringt das Internet neben positiven Auswirkungen auch negative Begleiterscheinungen mit sich. So haben neben den Pionieren der sog. Tech-Brache auch die Extremisten der Welt verstanden, das Netz für ihre Zwecke zu instrumentalisieren. Diese Tatsache stellt sowohl die Branche selbst, die Nutzer und zu guter Letzt auch die Sicherheitsbehörden vor enorme Herausforderungen. *„Die Virtualisierung hat den Rechtsextremismus geradezu revolutioniert“*, so ist es dem Abschnitt *„Virtualisierung des Rechtsextremismus bzw. Rechtsterrorismus“* im Jahresbericht 2020 des Landesamtes für Verfassungsschutz Baden-Württemberg zu entnehmen. Die Autoren begründen ihre Annahme mit der Aussage, dass es vor der Digitalisierung nahezu unmöglich gewesen sei, als Einzelperson im Sinne einer rechtsextremistischen Ideologie zu agieren, ohne zuvor mit einer entsprechenden Partei, Organisation oder sonstigen Gruppierung in Kontakt getreten zu sein.[2]

## 2 Verbreitung von Ideologien durch die Virtualisierung

Diese Annahme ist sicherlich zutreffend, letztlich jedoch nur ein Teilaspekt dieser Revolution, da die Virtualisierung einen exponentiellen Faktor an Möglichkeiten bietet, Ideologien zu verbreiten, neue Anhänger zu generieren oder das eigene Personenpotential zu bestärken. Gewiss ist dies kein Alleinstellungsmerkmal des Rechtsextremismus. Denken wir bspw. an die menschenverachtende Propaganda, die der sog. Islamische Staat äußerst professionell anfertigte und über die verschiedensten Plattformen in die Welt streute. Oder die sog. INCEL-Bewegung, die ihre misogynen Botschaften über das Netz verbreitet. Gerade die Entstehung dieser Bewegung, deren Nähe zum Rechtsextremismus nicht mehr geleugnet werden kann,[3] wäre ohne das Internet undenkbar gewesen. Dennoch soll sich dieser Artikel auf den Phänomenbereich des Rechtsextremismus beschränken und einige Aspekte in diesem Kontext beleuchten.

## 3 Nutzung des Internets durch die rechtsextremistische Szene

Die Nutzung des Internets stellt keineswegs eine neue Errungenschaft innerhalb der rechtsextremistischen Szene dar, bereits in den frühen 1990er-Jahren betrieben Rechtsextremisten das Thule-Netz,[4] um Texte und Musik zu teilen. Da dieses zunächst auf der Grundlage eines Mailbox-System operierte, war es nur für versierte Computernutzer zugänglich und konnte dadurch keine große Reichweite generieren. Heute liefern digitale Plattformen wie die *„Sozialen Netzwerke“*, *„Imageboards“*[5] oder *„Messangerdienste“* attraktive Plattformen, die für jedermann zugänglich und leicht zu bedienen sind. Nicht zuletzt die *„Sozialen Netzwerke“* sorgen durch ihre Algorithmen zusätzlich für eine schnelle Verbreitung der durch Rechtsextremisten erstellten Schlagzeilen. Viele dieser Plattformen sind Bestandteile von Technologieunternehmen, deren Wert sich zum Großteil dadurch bemisst, wie lange sich die einzelnen Nutzer auf den jeweiligen Webseiten aufhalten. Je länger die Verweildauer, desto mehr Daten können über die Nutzer gesammelt werden. Je mehr Daten in die entsprechenden Datenbanken fließen, desto gezielter können die Unternehmen Werbemaßnahmen einsetzen. Bedenkt man, dass bspw. Facebook im Jahr 2020 einen Umsatz von 85,9 Milliarden Dollar und einen Marktwert von 800 Milliarden Dollar erzielte[6], ohne ein haptisches Produkt herzustellen, ist es leicht vorstellbar, wie gut die gesammelten Daten den monetären Interessen der Betreiber entgegenkommen.

## 4 Implementierung von Algorithmen

Um die Nutzer möglichst lange auf ihren Webseiten zu halten, wurden Algorithmen implementiert, die sich verschiedene

Erkenntnisse der Psychologie und Soziologie zunutze machen. Bei den Algorithmen handelt es sich um streng gehütete Geheimnisse der jeweiligen Unternehmen. Dennoch konnten durch verschiedene Forschungsprojekte Anhaltspunkte für deren Funktionsweise *„entschlüsselt"* werden.[7] Der Nutzen der Algorithmen offenbart sich bereits auf den Startseiten der jeweiligen Plattformen, auf denen den Konsumenten Nachrichten angezeigt werden. Vermeintlich handelt es sich um solche, die sich am ehesten mit den Interessen der Nutzer decken. Tatsächlich werden aber die Nachrichten präsentiert, die im Sinne einer langen Verweildauer nützlich für die jeweiligen Betreiber sind – ähnlich den Schlagzeilen, die sich auf der ersten Seite einer Zeitung befinden und den Leser zum Kauf der Zeitung animieren sollen. Der Vorwurf, die Unternehmen würden durch den Einsatz der Algorithmen die Verbreitung extremistischer Inhalte unterstützen, darf aus meiner Sicht daher nicht erhoben werden. Wie jedes andere Unternehmen, versuchen die Tech-Giganten den größtmöglichen Gewinn zu erzielen. Nicht nur Rechtsextremisten, auch andere politische Akteure oder Unternehmen machen sich die Algorithmen zunutze. Hierfür wurden verschiedene Prozesse entwickelt, die genutzt werden können, um Meldungen schnell und mit größtmöglicher Reichweite zu verbreiten.

Mit dem *„Clickbaiting"* und *„Click and Share"* möchte ich auf zwei dieser Prozesse kurz eingehen, die nach meiner Auffassung von rechten bis rechtsextremistischen Meinungsmachern kombiniert werden.

Um höhere Nutzerzahlen zu generieren und so die Verbreitung von Nachrichten weiter zu beschleunigen, wird durch eine reißerische Meldung, Überschrift oder Bildmaterial, die Neugierde des Betrachters geweckt, ohne diese ausreichend zu befriedigen. Dieser wird dadurch verleitet, die Meldung anzuklicken, um seine Neugierde auf der verlinkten Website zu stillen *(„Clickbaiting")*. Durch auf den Websites implementierte Buttons kann die Nachricht dann auf dem eigenen Profil geteilt werden – *„Click and Share"*. Von dieser Möglichkeit machen auch seriöse Medien Gebrauch von der *„Augsburger Allgemeinen"* bis *zur „taz"*.

Durch die Faszination des *„Click and Share"* wird der Nutzer zeitgleich auch zum Reproduzenten der entsprechenden Nachricht. Fraglich bleibt hierbei, ob sich dieser Reproduzent zuvor ausreichend mit dem Text und dem ursprünglichen Verfasser auseinandergesetzt und somit den Inhalt validiert hat. Beispiele aus der jüngeren Vergangenheit deuten darauf hin, dass dies nicht immer der Fall ist.

Als Beispiel möchte ich hier einen Vorfall anführen, der sich 2019 in einem Düsseldorfer Freibad ereignet hat. Das auflagengrößte deutsche Boulevardblatt berichtete von tumultartigen Auseinandersetzungen, die sich zwischen der Polizei und 60 Flüchtlingen aus dem nordafrikanischen Raum ereignet haben sollen.[8] Wie das ARD-Magazin Monitor wenig später berichtete, blieben nach deren Recherchen nicht viele der Anschuldigungen übrig. Dennoch hatte die Nachricht immense Auswirkungen auf die öffentliche Meinung. Nicht nur Politiker der AfD, die von *„kriegsähnlichen"* Zuständen sprachen, auch ein Vertreter des Bundesministeriums des Innern (BMI) ließ es sich nicht nehmen, im Rahmen eines Interviews, das im Zusammenhang mit dem Vorfall geführt wurde, ausländerrechtliche Konsequenzen anzudeuten, bevor die Ermittlungen zum Vorfall aus polizeilicher Sicht abgeschlossen waren. Auch wenn das Geschehen nach Abschluss der Ermittlungen relativiert werden musste, blieben die Schlagzeilen von *„kriegsähnlichen Zuständen"* in einem deutschen Freibad, ausgelöst durch nordafrikanische Flüchtlinge, im Gedächtnis und wurden zuvor hunderttausendfach im Netz geteilt.

Angehörige der rechtsradikalen Szene.

## 5 Subjektive Wahrnehmung objektiver Gegebenheiten

Sicherlich gab es bereits vor der Virtualisierung Artikel oder Beiträge, die Menschen derart berührten, dass diese sich berufen fühlten, ihre Meinung in Form eines Leserbriefs an die Herausgeber oder Autoren kund zu tun, um so eine breitere Öffentlichkeit an ihren Gedanken teilhaben zu lassen. Dieser analogen Vorgehensweise war, zumindest bis zu einem gewissen Maße, eine besonnene Auseinandersetzung mit dem Text und der eigenen Erwiderung immanent. Zudem spielte der Faktor Zeit eine große Rolle. Hatte man seine Gedanken formuliert und zu Papier gebracht, musste dieses auch noch an den Empfänger gesendet werden. Früher bedeutete dies, einen Brief zum Empfänger zu befördern oder mittels Fax-Gerät an die Redaktion zu versenden. Durch die auf den Plattformen integrierten Kommentarfunktionen wird die impulsive Reaktion auf eine Nachricht geradezu provoziert – zumindest erheblich erleichtert und somit ein „emotionaler Effekt" genutzt.

Gezielt nutzen rechtsextremistische Agitatoren die soziologische Annahme, dass der Mensch nicht auf der Grundlage objektiver Gegebenheiten handelt, sondern danach, wie er diese subjektiv wahrnimmt. Die Akteure versuchen daher, emotionsgeladene Nachrichten zu verbreiten, die beim Leser assoziativ empfundene Ausnahmesituationen suggerieren. Als Beispiel kann hier die Mär von *„kinderquälenden Angehörigen einer Elite"* herangezogen werden, die als Grundlage der *„QAnon"*-Bewegung dient. Welchen Menschen lassen die Gedanken an Kinder, die in dunklen Kellern gefangen gehalten und gequält werden, kalt? Diesen Effekt scheinen sich auch Politiker bestimmter Parteien zunutze zu machen. Neben einem vulgären Vokabular, das seit dem Einzug der AfD im Deutschen Bundestag Einzug gehalten hat *(„Alimentierte Messermänner", „Kopftuchmädchen und andere Taugenichtse"*[9]), bedienen sich rechtsextremistische Stimmungsmacher seit Jahren derselben Argumente, um sich gegen Flüchtlinge zu echauffieren. Dazu zählt insbesondere die Argumentation, Flüchtlinge seien kriminell und würden sich lediglich wegen wirtschaftlicher Interessen auf den Weg in die Bundesrepublik machen.

Tatsächlich stammten 2020 68% der weltweit registrierten Flüchtlinge aus lediglich fünf Ländern, nämlich Afghanistan, Syrien, Venezuela, Südsudan und Myanmar.[10] Für die Bundesrepublik ergibt sich 2020 folgende Rangfolge: Syrien, Afghanistan, Irak, Türkei und Nigeria.[11] Dass Flüchtlinge krimineller sind als die hier geborene Bevölkerung, mag auf den ersten Blick den Tatsachen entsprechen. Von den 1.863.118 Tatverdächtigen die in der Polizeilichen Kriminal-Statistik (PKS) 2020 erfasst wurden,

waren 557.688 als *„nichtdeutsche Tatverdächtige"* klassifiziert worden.[12] Immerhin nahezu ein Drittel. Dennoch muss diese Zahl relativiert werden. Zu diesen nichtdeutschen Tatverdächtigen zählen auch Bürger, die hier seit mehreren Generationen leben, jedoch nicht im Besitz der deutschen Staatsangehörigkeit sind. De facto somit Teil der deutschen Bevölkerung. Zudem handelt es sich bei 73,5% der Asylsuchenden um Menschen, die das 30. Lebensjahr noch nicht vollendet hatten. 64% waren männlich.[13] Eigenschaften von Personen, die in der PKS seit jeher, unabhängig von der Staatszugehörigkeit, überproportional vertreten sind. Nichtsdestotrotz dienen diese Zahlen den rechtsextremistischen Meinungsmachern dazu, eine große Verunsicherung in der Bevölkerung hervorzurufen. Und es ist anzunehmen, dass genau darin deren Motivation liegt.

## 6 Mainstream oder alternative Medien

Um ihre Anhänger zu mobilisieren oder neue Anhänger zu gewinnen, versuchen rechte und rechtsextremistische Influencer Ausnahmesituationen zu suggerieren, die den Nachrichtenkonsumenten zu der Ansicht bringen sollen, er selbst oder die gesamte Bevölkerung befänden sich in einer Extremsituation. Durch diese Vorgehensweise werden die Emotionen des Lesers derart beeinflusst, dass sich dessen Wahrnehmung ändert und etwaige Zweifel in den Hintergrund gedrängt werden. Auch wenn sich die Wissenschaft noch nicht auf eine gemeinsame Definition für *„Emotionen"* einigen konnte, besteht doch kein Zweifel daran, dass eine Emotion aus mehreren Komponenten besteht, die wiederum Einfluss auf die Wahrnehmung nehmen.[14]

Um letzte Zweifel auszuräumen, bedienen sich die Agitatoren einer Analogie, die sie der 1999 erschienenen Film-Reihe *„The Matrix"* entnommen haben, um damit ihre Anhänger gegen differenziert lautende Nachrichten zu immunisieren. Der Trick ist so simpel wie wirkungsvoll. In der Filmreihe muss sich der Protagonist *„Neo"* entscheiden, ob er eine blaue Tablette einnehmen möchte, um weiterhin in seiner gewohnten Welt zu leben, oder ob er die rote Tablette einnimmt, um die Wahrheit über die Matrix zu erfahren. Besonders häufig ist diese Argumentation in der Welt der Verschwörungstheoretiker anzutreffen. Durch das Argument, die Anhänger der jeweiligen Theorie seien *„Redpilled"*, hätten also die Wahrheit erkannt, werden alle Medienformate, die eine (soweit möglich) objektive Berichterstattung anbieten, zur *„Lügenpresse"* deklariert und mit dem vermeintlichen Makel des *„Mainstream"* belegt. Sobald die Anhänger dieses Argument verinnerlicht haben, informieren sie sich fortan nur noch bei den *„alternativen Medien"*. Diese finden ihre Verbreitung nicht nur über das Internet. Als Beispiel möchte ich hier das *„Compact Magazin"* nennen, auf dessen Titelseite Bill Gates als *„Impf-Diktator"* bezeichnet[15] oder Putin als Freund der Deutschen stilisiert wird, der „günstiges Gas anbietet" und uns die *„Hand zur Freundschaft"* reicht.[16] Ergänzt wird die *„alternative Informationsgewinnung"* durch die unzähligen Kanäle auf Plattformen wie *„Telegram"* oder Gruppen auf anderen *„Sozialen Netzwerken"*.

Durch die vermeintliche Tatsache des *„Redpillings"* können sich die Menschen nicht mehr bei den *„Mainstream-Medien"* informieren, da die dort angebotenen Informationen nicht mit denen, der selbst gewählten *„alternativen Medien"*, übereinstimmen. Diese geistigen Widersprüche werden in der Psychologie als kognitive Dissonanz bezeichnet. Es muss davon ausgegangen werden, dass sich Rechtsextremisten diese bewusst zunutze machen. Wir alle haben im Umgang mit solchen kognitiven Dissonanzen bereits eigene Strategien entwickelt, die in der psychologischen Forschung als Dissonanzreduktionen bezeichnet werden. Auch hierfür möchte ich zur Erklärung zwei Beispiele aufführen, die wir alle kennen. Ein Beispiel wäre die Strategie, das eigene Handeln zu rechtfertigen. *„Natürlich wollte man im neuen Jahr mehr für das Klima tun, der Flug ins ferne Urlaubsziel muss trotzdem sein, denn die Menschen dort leben ja schließlich vom Tourismus und sind auf diesen angewiesen."* Oder die Strategie der Vermeidung. Informiert man sich nicht mehr bei den *„Mainstream-Medien"*, muss man sich auch nicht mit den widersprüchlichen Argumenten auseinandersetzen. Doch gerade diese kognitive Auseinandersetzung wäre die Lösung, die zum großen Teil unstimmigen Argumente der Verschwörungstheoretiker zu entlarven. Der politische Diskurs, der Austausch von Argumenten und schließlich die Kompromissfindung stellen wichtige Elemente unserer Demokratie dar. Stützt man seine Bezugsquellen für Informationen nur noch auf *„alternative Medien"*, entfernt man sich von diesen demokratischen Werten hin zu denen einer Autokratie.

## 7 Zum Abschluss

Ich habe den Versuch unternommen, einige Aspekte der Virtualisierung im Kontext des (Rechts-)Extremismus darzustellen und deren Komplexität aufzuzeigen. So facettenreich dieser Themenkomplex ist, so facettenreich muss auch die Antwort unserer Demokratie auf dieses Phänomen sein. Nach meiner Ansicht bedarf es hier eines interdisziplinären Ansatzes, der nicht ausschließlich von den Sicherheitsbehörden bedient werden kann. Angefangen von den Tech-Konzernen selbst bis zu jedem einzelnen Mitglied unserer Gesellschaft sind hier alle Akteure gefordert, die Entwicklung der Virtualisierung in die richtigen Bahnen zu lenken, um diese Revolution zu etwas durchweg Positivem auszubauen.

Bildrechte: ProPK.

## Anmerkungen

1 Der Autor ist als Regierungsamtmann beim Landesamt für Verfassungsschutz Baden-Württemberg tätig. Der Inhalt des Beitrages stellt seine persönliche Meinung dar.
2 Vgl. Verfassungsschutzbericht für Baden-Württemberg 2020, S. 165.
3 Vgl. *„Frauenhassende Online Subkulturen, Ideologien – Strategien - Handlungsempfehlungen"* der Amadeu Antonio Stiftung.
4 Vgl. bspw.: http://www.diss-duisburg.de/2012/10/thule-netz/.
5 Eine Art digitale Tauschbörse für Bilder und Texte.
6 Vgl. Inside Facebook, Sheera Frenkel und Cecilia Kang, S. 13.
7 Vgl. beispielsweise: https://netzpolitik.org/2019/facebooks-algorithmus-formt-unser-leben-dieser-hacker-will-herausfinden-wie/ abgerufen am 8.4.2022, 17:01 Uhr.
8 Vgl. https://www1.wdr.de/daserste/monitor/videos/video-aufruhr-im-freibad-vom-jugendstreich-zum-terrorakt-100.html.
9 Vgl. Rede im Bundestag von Alice Weidel am 16.5.2018 im Rahmen der Debatte um den Etatentwurf 2018.
10 Vgl. https://www.uno-fluechtlingshilfe.de/informieren/faktencheck, abgerufen am 7.4.2022, 09:24 Uhr.
11 Vgl. https://www.bamf.de/SharedDocs/Anlagen/DE/Statistik/BundesamtinZahlen/bundesamt-in-zahlen-2020.pdf;jsessionid=0D8BE7EBA962D1D887CFA50A30CAE200.intranet262?__blob=publicationFile&v=5 abgerufen am 8.4.2022, 07:18 Uhr.
12 Vgl. Bundeslagebild Kriminalität im Kontext von Zuwanderung 2020, Bundeskriminalamt.
13 Vgl. ebenda.
14 Vgl. Editorial zur Themenausgabe: *„Emotionen erleben und begreifen – Emotionspsychologie im Alltag"* von Julia Kozlik und Andrea Paulus (https://de.in-mind.org/article/editorial-zur-themenausgabe-emotionen-erleben-und-begreifen-emotionspsychologie-im-alltag?gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X3kiAsZjXUU4GJox4nJpHMHJ-WG5VRxE9QvT1mdOSkdI5UB45ntTb0oaArKdEALw_wcB).
15 Siehe Compact-Magazin, Ausgabe 6/2020.
16 Vgl. https://www.kopp-verlag.de/a/compact-spezial-nr.-33%3A-feindbild-russland?ws_tp1=kw&ref=googlemc&subref=pool/shopping&gclid=EAIaIQobChMI9brk7umD9wIVCIKDBx2t6QYcEAQYAiABEgLZgPD_BwE, abgerufen am 8.4.2022, 08:26 Uhr.

# Strafrechtliche Rechtsprechungsübersicht

Von EPHK & Ass. jur. Dirk Weingarten, Wiesbaden

*Wir bieten Ihnen einen Überblick über strafrechtliche Entscheidungen, welche überwiegend – jedoch nicht ausschließlich – für die kriminalpolizeiliche Arbeit von Bedeutung sind. Im Anschluss an eine Kurzdarstellung ist das Aktenzeichen zitiert, so dass eine Recherche möglich ist*

## I Materielles Strafrecht

**§ 132a Abs. 1 Nr. 4 StGB – Mißbrauch von Titeln, Berufsbezeichnungen und Abzeichen; hier: Tragen inländischer Uniform, Amtskleidung oder Amtsabzeichen mit der Aufschrift „Pozilei".** Der 43-jährige Angeklagte (A) befuhr zur Mittagszeit eine Straße mit seinem Pedelec. Hierbei trug er unter anderem eine dunkelblaue Hose und eine neonfarbene Jacke mit dunkelblauen Elementen, silberfarbenen Reflektorstreifen und der Aufschrift *„POZILEI"* in großen, grau-silberfarbenen Druckbuchstaben. Er hielt an einer Kreuzung neben einem Auto an, klopfte gegen die Seitenscheibe der Fahrerin und äußerte seinen Unmut über deren vorangegangene Fahrweise. Dabei gab er sich nicht als Polizeibeamter aus, so dass ihm Amtsanmaßung nicht zur Last gelegt wurde.

Die Vorinstanz (LG) wertete das Verhalten als unbefugtes Tragen von Uniformen, für das es nach dem Gesetz bereits ausreicht, wenn eine zum Verwechseln ähnliche Uniform getragen wird. Eine ausreichende Ähnlichkeit zu einer Polizeiuniform bejahte das LG aufgrund des Gesamteindrucks in der konkreten Situation und des Aufdrucks *„POZILEI"*. Die Beschriftung mit diesem tatsächlich nicht existierenden Wort werde bei flüchtiger Betrachtung als *„POLIZEI"* gelesen, da gegenüber diesem tatsächlich existierenden Wort lediglich zwei Buchstaben vertauscht seien. Genau hierauf ziele der *„Buchstabensalat"* auch ab, so das LG. Dem steht das Tragen einer dunklen Hose oder Jeans nicht entgegen, wenn das gesamte Erscheinungsbild einen objektiven, nicht besonders sachkundigen und nicht genau prüfenden Beobachter zu der Annahme führe, dass es sich um eine Polizeiuniform handelt. Auch sei es unerheblich, dass die Zeugen hier letztlich doch bemerkten, keinen Polizeibeamten vor sich zu haben. Denn die Vorschrift solle schon vor der bloßen Gefahr von Verwechslungen schützen. (OLG Hamm, Beschl. v. 9.6.2022 – 4 RVs 62/2)

**§ 201 Abs. 1 Nr. 1 StGB – Verletzung der Vertraulichkeit des Wortes; hier: Nicht öffentlich gesprochenes Wort; Personalienfeststellung durch die Polizei.** Um eine gültige Coronabekämpfungsverordnung durchzusetzen und den Hinweisen auf Straftaten nachzugehen, kontrollierte die Polizei Personen. Während die Polizeibeamten die Personalien anwesender Personen feststellten, filmte die Angeklagte (A) den Polizeieinsatz mit ihrem Smartphone. Sie beschränkte sich hierbei darauf, den Boden zu filmen und insbesondere eine Tonaufnahme des Einsatzes zu fertigen. Über einen Zeitraum von 39:07 Minuten wurden jedoch von ihr sämtliche Gespräche aufgezeichnet, die im Rahmen der Personenkontrolle stattfanden. Trotz mehrfacher Aufforderung der Polizei, das Video zu löschen und die Aufnahme zu stoppen, filmte die A weiter und folgte den Polizeibeamten dabei. Sie erklärte hierbei mehrfach, keine Portraitaufnahmen zu machen. Die Sicherstellung des Handys wurde angeordnet und durchgesetzt.

Wird von der Personalienfeststellung durch Polizeibeamte anlässlich der Kontrolle einer Personenansammlung eine Audioaufnahme gefertigt, liegt die Annahme des Anfangsverdachts für ein gem. § 201 Abs. 1 Nr. 1 StGB strafbares Vergehen der Verletzung der Vertraulichkeit des Wortes nahe. (OLG Zweibrücken, Beschl. v. 30.6.2022 – 1 OLG 2 Ss 62/21)

## II Prozessuales Strafrecht

**§ 100a Abs. 1 S. 1 StPO – Telekommunikationsüberwachung; hier: WhatsApp-Überwachung; Umfang.** Eine allgemeine richterliche Anordnung zur Überwachung und Aufzeichnung der über einen Mobilfunkanschluss abgewickelten (*„herkömmlichen"*) Telekommunikation umfasst die spezifische WhatsApp-Überwachung (mittels einer internetbasierten Anwendung) nicht. Erforderlich ist vielmehr eine richterliche Entscheidung bei jedem Einsatz dieser operativen Maßnahme am Einzelfall. Das Gericht hat sich mit der Verhältnismäßigkeit dieser spezifischen Überwachungsmaßnahme auseinanderzusetzen.

Auch der Nachrichtenaustausch über internetbasierte Chat- und Messenger-Dienste ist Telekommunikation i.S.d. § 100a Abs. 1 S. 1 StPO. Grundsätzlich werden auch die gespeicherten Nachrichteninhalte und Daten erfasst, die bereits vor Erlass einer entsprechenden Anordnung versandt oder empfangen wurden. (BGH, Beschl. v. 9.7.2020 – 2 BGs 468/20)

**§ 110 StPO – Durchsicht von Papieren und elektronischen Speichermedien; hier: Anwesenheitsrecht (der Verteidigung).** Eine Durchsuchung des Arbeitsplatzes des Beschuldigten (B) wurde angeordnet. Die Durchsuchung fand statt, wobei unter anderem Daten vom Server und dem Arbeitsplatz des B gesichert und zur Durchsicht an die Amtsstelle mitgenommen wurden. Die erste Durchsicht der sichergestellten Daten erfolgte in Anwesenheit des Verfahrensbevollmächtigten des B. Zeitlich später teilte die Staatsanwaltschaft dem Rechtsanwalt mit, dass eine weitere Teilnahme an der Durchsicht insbesondere aus verfahrensökonomischen Gründen nicht mehr zugelassen werde.

Der Rechtsbeistand eines von einer Durchsuchung Betroffenen hat i.d.R. ein Anwesenheitsrecht bei der Durchsicht der vorläufig sichergestellten Datenträger, wenn ein Großteil der sichergestellten Daten für das Ermittlungsverfahren nicht von

Relevanz ist und es zu Differenzen zwischen der Steuerfahndung und dem Rechtsbeistand des Betroffenen über die Art und Weise sowie den Umfang der Durchsicht gekommen ist. Hat der B ein gewichtiges Interesse daran, dass sein Rechtsanwalt der Durchsicht beiwohnen darf, sind damit einhergehende gewisse zeitliche Einschränkungen und erforderlich werdende organisatorische Maßnahmen im Rahmen der Sichtung durch die Strafverfolgungsbehörden hinzunehmen. (LG Kiel, Beschl. v. 18.6.2021 – 3 Qs 14/21)

**§ 110 StPO – Durchsicht von Papieren und elektronischen Speichermedien; hier: Akteneinsichtsrecht der Verteidigung.** Der Angeklagte (A) soll als Betriebsleiter einer Firma, welche im Wesentlichen im Bereich der Briefkonsolidierung, also der Abholung und Sortierung von Briefen im Vorfeld der Weiterbeförderung tätig ist, ein betrügerisches System errichtet haben. Im Rahmen von zahlreichen Durchsuchungen erfolgte die Sicherstellung zahlreicher Datenträger bzw. teilweise die Sicherung derselben, wobei eine Datenmenge von ca. 12 TB gesichert wurde, was in Dokumentenseiten gerechnet in etwa dem Inhalt von 15.600 gefüllten Aktenschränken entspricht.

Die Durchsicht beschlagnahmter Papiere bzw. elektronischer Speichermedien ist gem. § 110 Abs. 1 StPO Aufgabe der Staatsanwaltschaft und auf deren Anordnung ihrer Ermittlungspersonen, nicht der Verteidigung. Zu Beweisstücken i.S.d. § 147 Abs. 1 StPO werden im Rahmen der Durchsuchung vorläufig sichergestellte Datenträger bzw. Schriftstücke erst, wenn die Durchsicht gem. § 110 Abs. 1 StPO abgeschlossen und eine Beschlagnahmeanordnung ergangen ist. Ein Besichtigungsrecht der Verteidigung entsteht erst nach erfolgter Durchsicht und entsprechender Beschlagnahme.

Damit korrespondiert die Verpflichtung der Ermittlungsbehörden, die Auswertung vorläufig sichergestellter Schriftstücke und Daten im Hinblick auf den Verhältnismäßigkeitsgrundsatz und Rechte eventuell Dritter zügig vorzunehmen, um abhängig von der Menge des sichergestellten Materials und der Aufwändigkeit der Auswertung in angemessenere Zeit zu entscheiden, was als potentiell beweiserheblich dem Gericht zur Beschlagnahme vorgelegt werden und was an den Beschuldigten oder Dritte herausgegeben werden soll. Die Ressorts der Polizei- und Justizverwaltung sind insoweit gehalten, die erforderlichen personellen und technischen Ressourcen zur Verfügung zu stellen, die eine Bewältigung entsprechender Datenmengen gegebenenfalls auch mittels entsprechender Software und unter Hinzuziehung externen Sachverstands ermöglichen. Durch die zügige Auswertung soll insbesondere verhindert werden, dass nicht noch während bereits laufender Hauptverhandlung zuvor nicht ausgewertete Beweismittel aus dem sichergestellten Datenbestand nachgeschoben werden, welche den übrigen Beteiligten noch unbekannt sind. Ein mit der Durchsicht umfangreicher Datenbestände verbundener erhöhter Auswertungsaufwand rechtfertigt keine andere Vorgehensweise.

Ergänzend wurde im Beschluss angemerkt, dass trotz der Streichung der Regelung eines Anwesenheitsrechts des Inhabers der durchzusehenden Papiere und Daten in § 110 Abs. 3 StPO a. F. (Gesetz zur Modernisierung der Justiz 2004), es im Einzelfall von Verfassungs wegen geboten und insbesondere auch zweckdienlich sein kann, den Inhaber der sichergestellten Daten in die Prüfung der Verfahrenserheblichkeit einzubeziehen. Gerade hinsichtlich umfangreicher Datenmengen können konkrete, nachvollziehbare und überprüfbare Angaben vor allem Nichtverdächtiger zur Datenstruktur und zur Relevanz der jeweiligen Daten deren materielle Zuordnung vereinfachen und den Umfang der sicherzustellenden Daten reduzieren. (OLG Koblenz, Beschl. v. 30.3.2021 – 5 Ws 16/21)

**§ 110 StPO – Durchsicht von Papieren und elektronischen Speichermedien; hier: Modalitäten inhaltlicher Durchsicht.** Der Beschuldigte (B) wird verdächtigt, sich im Irak der Vereinigung *„Islamischer Staat“* als Mitglied angeschlossen zu haben und dort für den IS tätig gewesen zu sein. Auf der Basis eines Durchsuchungsbeschlusses wurden die Wohnräume des B durch Beamte eines LKA durchsucht. Dabei wurden zwei Mobiltelefone, ein Laptop sowie ein USB-Stick aufgefunden. Diese Speichermedien wurden gem. § 110 Abs. 1 StPO zur Durchsicht vorläufig sichergestellt und zur polizeilichen Auswertung mitgenommen.

Das sichergestellte Mobiltelefon durfte als elektronisches Speichermedium, dessen Durchsicht auf Beweisrelevanz im Rahmen der Wohnungsdurchsuchung vor Ort nicht möglich war, zur Auswertung mitgenommen und hierfür einstweilen sichergestellt werden. Da die Durchsicht des Mobiltelefons noch Teil der Durchsuchung ist, ist ihre (weitere) Zulässigkeit allerdings davon abhängig, dass die rechtlichen Voraussetzungen für eine Wohnungsdurchsuchung gem. § 102 StPO nach wie vor gegeben sind. Im Rahmen einer gerichtlichen Entscheidung nach § 110 Abs. 1 StPO i.V.m. § 98 Abs. 2 S. 2 StPO analog hat der nach § 98 Abs. 2 S. 3 StPO zuständige Richter allein darüber zu befinden, ob zum Entscheidungszeitpunkt die vorläufige Sicherstellung des betreffenden Gegenstandes für eine (weitere) Durchsicht zum Zwecke des Auffindens von Beweismitteln rechtmäßig und insbesondere noch verhältnismäßig ist. Eine eigenständige prognostische Bewertung des erforderlichen und verhältnismäßigen sachlichen und zeitlichen Umfangs noch ausstehender beziehungsweise möglicher weiterer Auswertungen ist ihm versagt. Die Entscheidung, in welchem Umfang eine inhaltliche Durchsicht potentieller Beweismittel nach § 110 StPO notwendig ist, wie sie im Einzelnen zu gestalten und wann sie zu beenden ist, obliegt vielmehr dem Ermessen der Staatsanwaltschaft. Die Rechtskontrolle durch den Ermittlungsrichter beschränkt sich deshalb darauf, ob die Staatsanwaltschaft im Entscheidungszeitpunkt die Grenzen des ihr zukommenden Ermittlungsermessens überschritten hat. Jedwede gerichtliche Entscheidung über einen Zeitpunkt, bis zu dem die Durchsicht eines vorläufig sichergestellten Gegenstandes abgeschlossen sein muss, enthielte notwendigerweise eigene Wertungen des Ermittlungsrichters hinsichtlich des Umfangs der in der Sache gebotenen Ermittlungen und griffe daher in den Ermessenspielraum der Staatsanwaltschaft ein. (BGH, Beschl. v. 20.5.2021 – StB 21/21)

**§ 261 StPO – Grundsatz der freien richterlichen Beweiswürdigung; hier: Unverwertbarkeit polizeirechtswidriger Videoaufnahmen.** Die Polizei führte während eines Fußballspiels de facto anlassunabhängig – und damit von der landesrechtlichen Eingriffsnorm des Polizeirechts nicht gedeckt – mehr oder weniger durchgängig Videoaufzeichnungen eines Fanblocks durch. Auf den allermeisten Videosequenzen ist legales Fanverhalten zu sehen. Lediglich in einer kurzen Sequenz hört man strafbare Beleidigungen.

Videoaufnahmen, die unter vorsätzlichem oder zumindest grob fahrlässigem Verstoß gegen polizeirechtliche Ermächtigungsgrundlagen von der Polizei aufgenommen werden, sind jedenfalls bei Tatvorwürfen aus dem Bereich der Kleinkriminalität (hier: Beleidigung) im Strafverfahren unverwertbar. (LG Köln, Beschl. v. 1.4.2021 – 157 Ns 8/20)

# Aktuelles aus dem Netz

Von EKHK Christian Zwick, Ludwigshafen

## Best of Cybercrime: Die verrücktesten Hackerangriffe

Es gibt auch Fälle von Kompromittierungen, die alles andere als konventionell ablaufen, wie die folgenden Beispiele zeigen. […] Im Jahr 2019 kam es in England zum ersten bekannten KI-basierten Vishing-Angriff: Die Angreifer benutzten kommerzielle KI Sprachsoftware, um die Stimme des deutschen Chefs eines britischen Energieversorgers zu imitieren. Mit Hilfe der Software riefen sie beim englischen CEO des Unternehmens an und überzeugten ihn davon, 243.000 Dollar an einen Lieferanten in Ungarn zu überweisen. Mehr: https://www.computerwoche.de/a/die-verruecktesten-hackerangriffe,3549494, Meldung vom 24.9.2022.

## Open Source: OpenAI veröffentlicht automatisches Spracherkennungssystem Whisper

OpenAI hat ein neues automatisches Spracherkennungssystem (automatic speech recognition system, ASR) namens Whisper bekannt gegeben. […] Whisper steht in fünf verschiedenen Modellgrößen auf GitHub zur Verfügung. Die Trainings-Parameter reichen von 39 Millionen bis über 1,5 Milliarden. Für das kleinste Modell sind etwa 1 GByte VRAM vonnöten, das größte braucht etwa 10 GByte. Bis auf die größte Version können die Modelle ausschließlich mit Englisch umgehen. Mehr: https://www.heise.de/news/Open-Source-OpenAI-veroeffentlicht-automatisches-Spracherkennungssystem-Whisper-7273104.html, Meldung vom 22.09.2022.

## Was ist ein Netzwerk-Switch?

Er nimmt […] Datenpakete derjenigen Geräte auf, die an seine physischen Ports angeschlossen sind und sendet diese dann weiter – und zwar ausschließlich an die adressierten Zielgeräte. […] Während Geräte lokal über Switches verbunden sind, stehen Netzwerke untereinander durch Router in Verbindung. Natürlich gibt es auch einige Router mit Switch-Funktionalitäten. Das naheliegendste Beispiel hierfür ist der heimische WLAN-Router, der zusätzlich zu seiner Breitbandverbindung (per WAN) über Ethernet-Ports verfügt, an die man seinen Computer, Fernseher, Drucker oder die Spielekonsole anschließen kann. Mehr: https://www.computerwoche.de/a/was-ist-ein-netzwerk-switch, Meldung vom 9.10.2022.

## BSI bestätigt Sicherheitseigenschaften von iPhone und iPad

Das BSI konnte aus diesem Prüfungsergebnis eine Freigabe der handelsüblichen iPhones und iPads für den staatlichen Einsatz durch die Behörden des Bundes ableiten. Dies betrifft auch die Verarbeitung von Verschlusssachen der Kategorie „Nur für den Dienstgebrauch“ (VS-NfD). Dazu sind Vorgaben des BSI hinsichtlich des Nutzerverhaltens, der sicheren Anbindung an Infrastrukturen durch ein Virtual Private Network (VPN) und der Verwendung eines Mobile Device Management Systems (MDM) einzuhalten. Mehr: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/221005_Apple_Sicherheitsfunktionen.html, Meldung vom 5.10.2022.

## Datenschutzrechtliche Schranken für die private Videoüberwachung

Private Überwachungskameras sind allgegenwärtig. Ihr Einsatz kollidiert allerdings oft mit dem Datenschutz. […] Ausgenommen ist die Überwachung von privaten Bereichen, die nicht öffentlich zugänglich sind. […] Allerdings wird diese Schwelle schnell gedankenlos überschritten, etwa bei der „Überwachung“ des öffentlichen Verkehrsraums mit Auto- oder Fahrrad-Dashcams – hier werden immer die Rechte Dritter tangiert. Mehr: https://www.heise.de/hintergrund/Datenschutzrechtliche-Schranken-fuer-die-private-Videoueberwachung-7238200.html, Meldung vom 7.9.2022.

## Bedingter Schutz: Android und iOS hebeln VPN teilweise aus

Ein VPN (Virtual Private Network) dient dazu, den Datenverkehr beispielsweise vor Netzbetreibern oder den Betreibern eines öffentlichen Netzwerks zu verbergen. Sowohl Apple als auch Google senden allerdings Sicherheitsforschern zufolge trotz aktiviertem VPN bestimmte Daten nicht über den VPN-Tunnel. Mehr: https://www.netzwelt.de/news/208997-bedingter-schutz-android-ios-hebeln-vpn-teilweise.html, Meldung vom 14.10.2022.

## Login-Versuche mit gestohlenen Zugangsdaten

Vor allem „Credential Stuffing“ ist eine beliebte Form des Cyberangriffs. Dabei nutzen Kriminelle gestohlene Anmeldedaten – meist die Kombinationen von Benutzernamen und Passwörtern –, um sich illegal Zugang zu Benutzerkonten zu verschaffen. […] Häufig haben sie leichtes Spiel und nutzen die Angewohnheit von Verbraucherinnen und Verbrauchern aus, dasselbe Passwort für mehrere Accounts zu nutzen […] Zu Beginn des Jahres 2022 wurden laut des State of Secure Identity Reports 113 Millionen Versuche zur Umgehung von MFA (Multi-Faktor-Authentifizierung) unternommen – mehr als jemals zuvor. Mehr: https://www.zdnet.de/88404011/login-versuche-mit-gestohlenen-zugangsdaten, Meldung vom 10.10.2022.