DIE KRIMINALPOLIZEI

Zeitschrift der Gewerkschaft der Polizei

Ausgabe 2/2022

Baden-Württemberg

Bundespolizei

Bundeskriminalamt

Niedersachsen

Saarland

Freistaat Sachsen

Sachsen-Anhalt

Identitätsdiebstahl und -missbrauch im Internet

Herausforderungen der Cyberkriminologie

Jahrhundert-Katastrophe im Ahrtal

www.kriminalpolizei.de

Editorial

Liebe Leserinnen, liebe Leser,

in der Ausgabe 2/2022 unserer Fachzeitschrift „Die Kriminalpolizei“ widmen wir uns zunächst dem Themenfeld „Identitätsdiebstahl und -missbrauch im Internet“.

Kaum eine Entwicklung hat unsere Gesellschaft in den letzten Jahrzehnten so nachhaltig verändert wie die Digitalisierung. Damit gewinnt aber auch das Tatmittel „Internet“ in nahezu allen Deliktsbereichen zunehmend an Bedeutung. Im „Bundeslagebild 2020 – Cybercrime“ wird durch das Bundeskriminalamt auf eine deutliche Steigerung der in diesem Kontext erfassten Straftaten um 7,9% hingewiesen. Es wird herausgestellt, dass der Fokus von Cyberkriminellen vermehrt im Bereich „Big Game Hunting“ liegt, sie häufig global vernetzt sind, zunehmend professioneller agieren und die auf finanziellen Profit ausgerichtete Underground Economy als kriminelle Parallelwirtschaft besorgniserregend wächst. Die Anzahl der DDoS-Angriffe steigt an und Ransomware zählt zu den primären Bedrohungen für öffentliche Einrichtungen und Wirtschaftsunternehmen. Erfolgreiche Attacken können hier drastische Folgen nach sich ziehen und dies gilt nicht allein für die finanzielle Dimension. Unübersehbar sind in diesem Zusammenhang auch die Einflüsse der anhaltenden Corona-Pandemie als Beschleunigungsfaktoren, da die Gesellschaft vermehrt auf digitale Angebote zurückgreift. Streaming- und Messenger-Dienste verzeichnen ebenso einen starken Anstieg der Nutzerzahlen wie die zahlreichen Online-Shops. Für Kriminelle geht damit naturgemäß eine erhöhte Bandbreite an Tatgelegenheiten einher, die sie für ihre Zwecke ausnutzen können. Seit wenigen Tagen liegt nun bereits das „Bundeslagebild 2021 – Cybercrime“ vor, das über die Homepage des Bundeskriminalamtes abrufbar ist und weitergehende Erkenntnisse enthält. Unter anderem wird eine erneute Steigerung erfasster Cyberstraftaten um über 12% bei Schäden in Milliardenhöhe und einer sinkenden Aufklärungsquote festgestellt.

Auf dieser Grundlage setzt sich der Leitende Kriminaldirektor a.D., Hochschullehrer, Redakteur und Fachautor **Ralph Berthel** einführend mit den aktuellen Entwicklungen und Herausforderungen zum Identitätsdiebstahl und -missbrauch im Internet auseinander. Neben der Erläuterung verschiedener Fachtermini stellt er ausgewählte Erkenntnisse zur Lage und zum Gefahrenpotenzial von Cyberangriffen einschließlich der damit verbundenen Ängste dar und geht auf Herausforderungen und Konsequenzen ein. In diesem Rahmen nimmt Ralph Berthel auch auf die Ergebnisse einer durch das Landeskriminalamt und die Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege Mecklenburg-Vorpommern gemeinsam mit der Universität Greifswald durchgeführten Dunkelfelduntersuchung Bezug. Im Ergebnis fordert er eine deutlich verstärkte Internetpräsenz der Polizeien des Bundes und der Länder, die inzwischen auch auf den verschiedenen politischen Ebenen weitgehend anerkannt worden ist.

Prof. Dr. Anja Schiemann erläutert die Strafbarkeit des Identitätsdiebstahls hinsichtlich der Datenbeschaffung, Datenverwendung sowie Anwerbung von Finanzkurieren und geht in diesem Zusammenhang auf die Begehungsformen des sog. Phishing, Pharming und IP-Spoofing ein. Nach Darlegung der Lehrstuhlinhaberin für Strafrecht und Strafprozessrecht an der Universität zu Köln sowie zugleich Gastprofessorin an der Deutschen Hochschule der Polizei in Münster bietet das geltende Strafrecht ausreichenden Schutz gegen die Formen und Unterformen des Identitätsdiebstahls, wenngleich der Gesetzgeber stets neuere Tatmodalitäten im Blick haben müsse. Dadurch könne mit einer Nachjustierung der strafrechtlichen Vorschriften jederzeit angemessen auf kriminelles Verhalten reagiert werden.

Da Cybercrime auch künftig weiter an Relevanz gewinnen dürfte, ist eine besondere Sensibilisierung für die Gefahren im digitalen Raum geboten. Der ehemalige Leiter des Kriminalkommissariats für Kriminalprävention und Opferschutz beim Polizeipräsidium Duisburg und Erste Kriminalhauptkommissar a.D. **Klaus Kemper** geht auf mögliche präventive Ansätze zur Bekämpfung der verschiedenen Formen der Computerkriminalität und dabei unter anderem auch auf die besonders schutzbedürftige Gruppe der Kinder und Jugendlichen ein.

Die Herausforderungen der Cyberkriminologie werden durch **Dr. Thomas-Gabriel Rüdiger** thematisiert. Der Akademische Oberrat und Leiter des Instituts für Cyberkriminologie der Hochschule der Polizei des Landes Brandenburg hält eine überzeugende digitale Polizeistrategie für dringend geboten. Er begründet dies mit einer Überforderung der Kapazitäten der Sicherheitsbehörden gerade bei kinderpornographischen Inhalten und spricht von einem „eigenständigen polizeilichen Einsatzraum“, der ständig an Bedeutung gewinnt.

Weitere Fachbeiträge beschäftigen sich mit der Jahrhundert-Katastrophe im Ahrtal aus Sicht der betroffenen Polizeidirektion Mayen, den sehr repressiv ausgerichteten Ahndungsbestimmungen des neuen VersG NRW, der RAF-Propaganda zwischen Wahn und Wirklichkeit sowie praktischen Aspekten der Kriminalprävention. Mit diesen Themen setzen sich unter anderem **Thorsten Runkel, Dr. Harald Bergsdorf, Rudi Heimann** und **Dr. Jürgen Fritzsche** auseinander.

Eine strafrechtliche Rechtsprechungsübersicht, Aktuelles aus dem Netz, eine Buchbesprechung und gewerkschaftspolitische Nachrichten runden unsere Zeitschrift schließlich wie gewohnt ab.

Liebe Leserinnen und Leser, wir wünschen Ihnen eine anregende Lektüre und freuen uns auf Ihre Rückmeldungen.

Für das Redaktionsteam

Ihr

Hartmut Brenneisen

Foto: H. Immel/GdP.

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,
HWR Berlin

Erster Kriminalhauptkommissar a. D. Peter Trapp,
CDU 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 Sachsen-Anhalt

Landespolizeidirektor Karl-Albert Grewe,
Ministerium für Inneres und Sport des Landes Sachsen-Anhalt

Landespolizeidirektor a. D. Rolf-Peter Wachholz

Schleswig-Holstein

Ministerialdirigent a. D. Jörg Muhlack

Landespolizeidirektor Michael Wilksen,
Landespolizeiamt

Leitender Kriminaldirektor Rainer Bretsch,
MILIG des Landes Schleswig-Holstein

Polizeidirektor Frank Ritter,
Polizeidirektion Itzehoe

Leitender Polizeidirektor Ralph Garschke,
Landespolizeiamt

Kriminaldirektor Michael Raasch,
Polizeidirektion Flensburg

Thüringen

Präsident Jens Kehr,
Landeskriminalamt Thüringen

Editorial 1

Identitätsdiebstahl und -missbrauch im Internet 4
Von LKD a.D. Ralph Berthel, Frankenberg/Sa.

Strafbarkeit des Identitätsdiebstahls durch Phishing, Pharming und Spoofing 7
Von Prof. Dr. Anja Schiemann, Köln/Münster

Computerprävention – Sensibilisierung für Gefahren im Netz 11
Von EKHK a.D. Klaus Kemper, Duisburg

Herausforderungen der Cyberkriminologie 13
Von Dr. Thomas-Gabriel Rüdiger, Oranienburg

Jahrhundert-Katastrophe im Ahrtal – „Hölle und Himmel am selben Fleck“ 18
Von KD Thorsten Runkel, Mayen

Die Ahndungsbestimmungen im VersG NRW 23
Von Hartmut Brenneisen, Preetz/Worms

Die Propaganda der RAF zwischen Wahn und Wirklichkeit 1970-1998 26
Von Dr. Harald Bergsdorf, Dümpelfeld

„Geh´ mit (k)einem Fremden mit...!“ – Kriminalprävention in der Praxis (Teil 2) 30
Von Rudi Heimann und Dr. Jürgen Fritzsche, Selters/Luxemburg

Strafrechtliche Rechtsprechungsübersicht 33
Von EPHK & Ass. jur. Dirk Weingarten, Wiesbaden

Aktuelles aus dem Netz 35
Von EKHK Christian Zwick, Ludwigshafen

Resolution der Gewerkschaft der Polizei (GdP) zu den Polizistenmorden von Ulmet 36
Bundesvorstand der Gewerkschaft der Polizei

Buchrezension 10

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:
Oliver Malchow, 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**

Identitätsdiebstahl und -missbrauch im Internet – aktuelle Entwicklungen und Herausforderungen

Von LKD a.D. Ralph Berthel, Frankenberg/Sa.[1]

Betrügen, also das Vorspiegeln falscher oder das Entstellen bzw. Unterdrücken wahrer Tatsachen mit dem Ziel, einen Irrtum zu erregen oder aufrechtzuerhalten, um sich rechtswidrig Vermögensvorteile zu verschaffen, zählt neben dem Diebstahl fraglos zu den ältesten Delikten, die die Kriminalgeschichte kennt. Zu den aktuellen Begehungsweisen beider Tatbestände gehören auch der Diebstahl und die betrügerische Nutzung von Daten, die die Identität einer Person charakterisieren. Identität (Abstraktum, also ein etwas nicht Gegenständliches bezeichnendes Hauptwort, zu lateinisch īdem – svw. *„derselbe"*) soll hier als die Gesamtheit der Eigenschaften, die kennzeichnend für ein Individuum sind, Verwendung finden.[2] Handeln nach *„Treu und Glauben"*, also redliches, anständiges und verlässliches Agieren von Menschen wie auch Institutionen stellt sowohl im realen als auch im digitalen Alltag eine maßgebliche Voraussetzung für ein funktionsfähiges Gemeinwesen im Allgemeinen und für erfolgreiche Interaktionen im Rechtsverkehr im Besonderen dar.

Mit der Verlagerung großer Teile menschlicher Interaktionen in den digitalen Raum erlangen einerseits die Sicherheit von digitalen Identitäten und anderseits der rechtswidrige Zugriff auf diese sowie deren missbräuchliche Nutzung eine zunehmende Bedeutung. Für Täter stellen sie Tatgelegenheiten, für potentielle Opfer Bedrohungen und für Sicherheitsakteure eine der aktuellsten und größten Herausforderungen bei der Verbrechensbekämpfung und -prävention dar.[3]

1 Identität, Diebstahl und Missbrauch von Identitätsdaten im Internet – einige Begriffe

Klassische, analoge Identitätsprüfungsverfahren beruhen auf einem Dokument mit hoher Fälschungssicherheit, das von einer vertrauenswürdigen Instanz, wie im Falle des Personalausweises durch die zuständige Personalausweisbehörde, herausgegeben wird.

Die eineindeutige Identifikation handelnder Personen oder Institutionen stellt eine hochaktuelle Herausforderung für alle Akteure im digitalen Raum dar. Immer mehr Lebensbereiche werden digitalisiert. Damit sind auch immer mehr Daten und Informationen[4] über Personen, Institutionen und Prozesse im Netz verfügbar. Beispiele für die Identifizierung im Netz finden sich etwa beim Online-Banking oder jüngst bei digitalen Impfzertifikaten. Zuverlässige digitale Identitäten sind Garanten für Absender und Empfänger zugleich, dass sie die sind, die sie vorgeben, zu sein. Das trifft sowohl für Menschen als auch Maschinen zu.

In einer Vielzahl von Fallgestaltungen bilden Identifizierungen die Voraussetzung für Zugriffsrechte, Transaktionsmöglichkeiten oder Verwaltungsbefugnisse von Daten und Informationen. Eine Vielzahl derartiger Fallkonstellationen bieten auch Ansätze für Missbrauch und mithin kriminalistisch relevantes Handeln.

Aus der Perspektive der Informationssicherheit kennzeichnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Begriff ***„Identität"*** wie folgt:

„Unter einer Identität wird im Kontext der Informationssicherheit die Menge von Merkmalen verstanden, die die Echtheit einer Person oder Sache nachweist. Die Identität einer Person oder Sache kann sowohl durch ein einziges Merkmal oder aber durch die Kombination diverser Merkmale bestimmt werden. Im Internet wird auf die Identität einer Person meist aus Identifikations- und Authentisierungsdaten geschlossen wie zum Beispiel aus der Kombination von Benutzername und Passwort."[5] Dabei ist der Begriff „digitale Identität" nicht scharf konturiert. *„Im Prinzip erzeugen wir mit jeder Registrierung bei einem Online-Dienst eine neue digitale Identität."*[6] Digitale Identitäten beziehen sich dabei sowohl auf digitale Identitätsnachweise von natürlichen als auch juristischen Personen.

Als **Identitätsdiebstahl** kennzeichnet das BSI *die „rechtswidrige Aneignung solcher Daten"*. Wird zudem die Identität nach dem Diebstahl unautorisiert für eigene oder fremde Zwecke verwendet, wird dies als **Identitätsmissbrauch** bezeichnet.[7] Aus viktimologischer Sicht können sich kriminalistisch relevante Zugriffe auf bzw. missbräuchliche Nutzungen von digitalen Identitäten also sowohl auf Privatpersonen als auch Institutionen bzw. Unternehmen als Opfer beziehen.

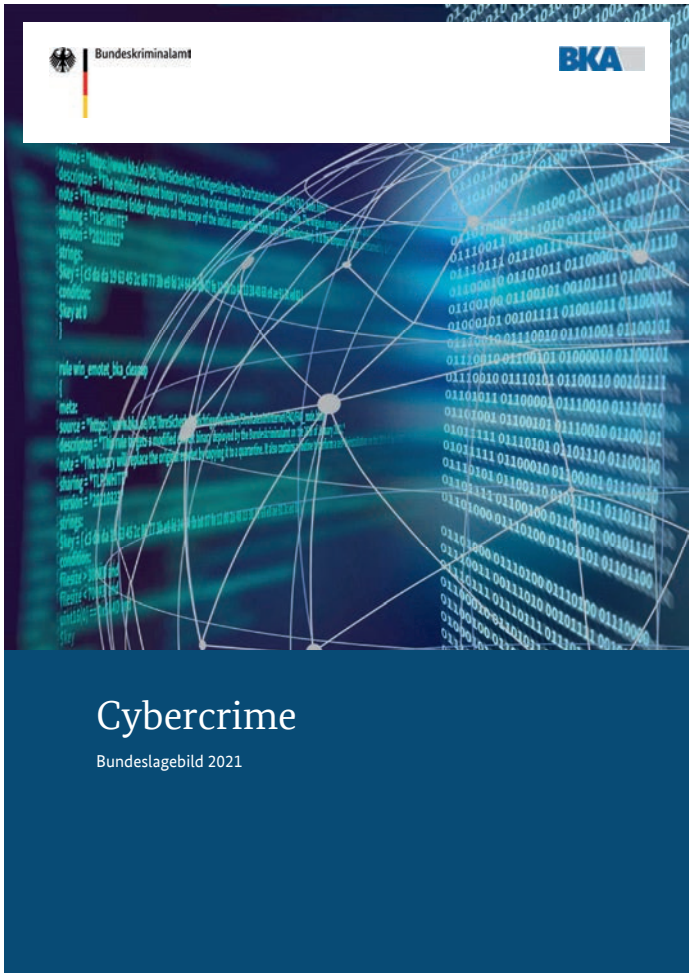
Im Zusammenhang mit der kriminalistischen Betrachtung von Identitätsdiebstahl- und -missbrauch ist gelegentlich von **kompromittierten Accounts** die Rede.[8] Dabei handelt es sich um *„ein System oder einen Datensatz, die als kompromittiert betrachtet werden können, wenn der Eigentümer des Systems, einer Datenbank oder eines Datensatzes keine Kontrolle mehr über die korrekte Funktionsweise und deren Sicherheit hat."*[9] Beim **Social Engineering** (eigentlich *„angewandte Sozialwissenschaft bzw. „soziale Manipulation"*, also soziale Beeinflussung, um bestimmte Reaktionen hervorzurufen) werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, insbesondere durch Täuschung über die Identität und die Absicht des Täters. So geben sich Täter z.B. als Techniker oder als Mitarbeiter eines Unternehmens wie etwa PayPal, Facebook oder eines Telekommunikationsunternehmens aus, um Opfer zur Preisgabe von Anmelde- oder Kontoinformationen oder zum Besuch von präparierten Webseiten zu verleiten.[10]

In den Fällen, in denen Hacker vorgeben, jemand zu sein, der einer Person oder einem Netzwerk bekannt ist, um auf

vertrauliche Informationen zugreifen zu können, wird von **Spoofing** gesprochen. Das BSI charakterisiert diese Begehungsweise als "*Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel dieser Handlungen besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben*".[11] Zu ergänzen ist diese Definition um die Zielsetzung, Benutzer zu Handlungen zu bewegen, die dem Hacker zugutekommen, etwa indem er auf vertrauliche Daten zugreifen kann und/oder dem Benutzer Schaden zufügen. Eine typische Begehungsweise ist das **Mail-Spoofing**, bei dem die Täter darauf abzielen, dass persönliche Daten preisgegeben oder Finanztransaktionen durchgeführt werden. Die E-Mails, mit denen diese Angriffe gestartet werden, stammen scheinbar von vertrauenswürdigen Absendern wie Kunden, Kollegen oder Vorgesetzten. Darüber hinaus enthalten Spoof-E-Mails manchmal Anhänge, die beim Öffnen Malware wie etwa Trojaner oder Viren installieren. Eine weitere Begehungsweise stellt das **IP-Spoofing** dar. *„Während sich Betrüger beim Mail-Spoofing auf einzelne Benutzer konzentrieren, ist IP-Spoofing in erster Linie auf Netzwerke ausgerichtet. Beim IP-Spoofing versucht ein Angreifer, durch das Senden von Nachrichten von einer gefälschten oder „gespooften" IP-Adresse unbefugten Zugang zu einem System zu erlangen."*[12]

*„Spoofing im großen Stil wird als **Phishing** bezeichnet. Bei einem Phishing-Angriff legen Cyberkriminelle zahllose „Köder" in Form gefälschter E-Mails, die an das E-Mail-Layout bekannter Unternehmen wie Amazon, DHL, eBay oder Postbank erinnern. … Sobald der Empfänger auf einen Link klickt, aktiviert er dadurch eine von vielen potenziellen Gefahren. … Cyberkriminelle können im Rahmen einer Phishing-Attacke ganz unterschiedliche Tools einsetzen. Ransomware ist ein direkter Angriff auf das Gerät des Empfängers. Keylogger und viele Trojaner dagegen stellen eher eine schleichende Gefahr dar: Sie überwachen die Aktionen des Nutzers und greifen Informationen zur Identität des Opfers ab, etwa persönliche oder finanzielle Daten, die für zukünftige Betrügereien verwendet werden können."*[13] Mit Phishing-Mails verfolgen Täter das Ziel, gutgläubige Nutzer dazu zu bewegen, auf einen *„verseuchten"* Link zu klicken.

Beim sog. **Pharming** werden Opfer hingegen auf eine völlig falsche Website umgeleitet. Pharmer nutzen üblicherweise Schwachstellen in der DNS-Serversoftware aus. DNS-Server (Domain Name Service) lösen Internetnamen in numerische IP-Adressen auf. Cyberkriminelle leiten ihre Opfer auf gefälschte Websites um. Diese sind den Originalen täuschend ähnlich sind. Die Opfer ahnen oft nicht einmal etwas von der Manipulation. Gegenüber dem Phishing hängt der Erfolg der Täuschungshandlung hier nicht davon ab, dass das Opfer auf einen falschen Link hereinfällt und ihn anklickt.[14]



In diesem Aufsatz bezieht sich der Autor auf das Bundeslagebild Cybercrime 2020. Das Lagebild für das Jahr 2021 lag zum Zeitpunkt des Redaktionsschlusses noch nicht vor, ist aber mittlerweile erschienen und über die Homepage des Bundeskriminalamtes abrufbar.

2 Zur Lage und zum Gefahrenpotenzial – ausgewählte Erkenntnisse

Während die in der Polizeilichen Kriminalstatistik (PKS) für 2020 erfassten Fallzahlen insgesamt eine rückläufige Tendenz gegenüber dem Vorjahr aufweisen (5.310.621 in 2020 gegenüber 5.436.401 im Jahr 2019; das entspricht einem Rückgang um 2,3%), weisen die Cybercrimedelikte eine deutliche Steigerung auf. Für 2020 wurden rund 108.000 Delikte der Cybercrime im engeren Sinne (CCieS)[15] registriert, was eine Steigerung von +7,9% im Vergleich zu den 2019 erfassten Fällen bedeutet. Während im gesamtgesellschaftlichen Maßstab davon auszugehen ist, dass sich zunehmend mehr Lebensbereiche in den digitalen Raum verlagern oder zumindest auch in diesem stattfinden, ist das Wissen um deliktisches Handeln im Cyberraum eher schlecht ausgeprägt. Das BKA geht im Bereich Cybercrime von einem *„überdurchschnittlich"* großen Dunkelfeld aus. Das führt das BKA u.a. auf folgende Deliktsspezifika zurück:

- Die Opfer erkennen ihre Betroffenheit nicht (z.B. bei Diebstahl ihrer Identität bei einem Online-Shop). Die von ihnen eingesetzten technischen Geräte werden unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht (z.B. bei Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen).
- Straftaten werden durch die Betroffenen oftmals nicht angezeigt, insbesondere dann, wenn noch kein finanzieller Schaden entstanden ist (z.B. bloßer Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z.B. Versicherung) reguliert wird.
- Geschädigte, insbesondere Wirtschaftsunternehmen, zeigen erkannte Straftaten nicht an, um u.a. die Reputation als *„sicherer und zuverlässiger Partner"* im Kundenkreis nicht zu verlieren.[16]

Es erscheint nachvollziehbar, dass der mit ca. 2% in der PKS abgebildete Anteil der CCieS an der Gesamtkriminalität nur einen Bruchteil dessen darstellen dürfte, was an kriminalistisch relevantem Handeln im Cyberraum tatsächlich stattfindet.

Im Bundeslagebild Cybercrime für 2020 werden digitale Identitäten als *„beliebte Handelsware"* bezeichnet.[17] Unter Verweis auf *„HaveIBeenPwnd"*[18] bzw. das Hasso-Plattner-Institut werden dort rund 10 Mrd. bzw. 12 Mrd. identifizierte kompromittierte Accounts angeführt. Letztgenanntes Institut rechnet mit

1.635.908 geleakten Accounts pro Tag. Jeder gestohlene Datensatz könne wiederum als Ausgangspunkt für weitere kriminelle Handlungen genutzt werden, so das BKA.

Als klassisch für das rechtswidrige Erlangen digitaler Identitäten werden im Lagebild Spam-Mail-Kampagnen und professionelle Phishing-Mails mit maliziösen, also bösartigen, Office-Anhängen genannt. Der Spamversand erfolge über zuvor kompromittierte oder aber kommerziell angemietete Serverkapazitäten sowie über von Angreifern gestohlene legitime E-Mail-Accounts. Ein weiterer Modus Oprandi sei das aggressive Eindringen in ein System via Brute-Force-Angriff, also um den Versuch, ein Passwort oder einen Benutzernamen zu knacken oder eine verborgene Webseite oder den Schlüssel zu finden. Dabei nutzten Täter mangelhaft geschützte Remote-Desktop-Protokolle (RDP). Über diese würden wiederum Schadprogramme oder missbräuchlich eingesetzte Pentesting-Tools[19] eingeschleust, betont das BKA. In der Folge würden Daten ausgespäht und an die Täter weitergeleitet.

2.1 Cyberangriffe auf die Wirtschaft und öffentliche Einrichtungen

Mit dem Begriff **Big Game Hunting** (eigentlich: Großwildjagd) werden Cyberangriffe auf herausragende Wirtschaftsunternehmen, Einrichtungen, Organisationen bzw. Unternehmen im Bereich der KRITIS[20] bezeichnet.

Das BKA konstatierte für das Jahr 2020, in dem vor allem dem Gesundheitswesen und der öffentlichen Verwaltung eine besondere Bedeutung zukam, eine Intensivierung des *„Big Game Hunting“*. Als Beispiel nannte das Amt den im Dezember 2020 bekanntgewordenen Netzwerkeinbruch bei dem US-amerikanischen Technologie-Unternehmens *„SolarWinds“*, durch den über die unternehmensseitigen Aktualisierungen der Software *„Orion“*[21] persistent, also dauerhaft und schwer abbaubare Zugriffe auf die IT-Netzwerke von Kunden möglich waren. Weltweit waren über 18.000 Systeme betroffen, darunter KRITIS und Behörden. Die Kompromittierung von *„Orion“* gilt als einer der bisher größten und schwerwiegendsten Cyberangriffe der Kriminalgeschichte.[22]

2.2 Diebstahl digitaler Identitäten – Neuer Modus Operandi im Bereich Mobile Payment

Für das Jahr 2020 vermeldete das BKA erstmals Betrugshandlungen im Zusammenhang mit Mobile Payment. Bargeldlose Bezahlungen mittels Kreditkarten sollen durch die Nutzung sog. Token, also einer Hardwarekomponente zur Identifizierung und Authentifizierung von Benutzern, eigentlich effektiver und sicherer werden. Gleichwohl ist es Tätern über Phishing und Social Engineering gelungen, an für das Online-Banking notwendige Daten zu gelangen und im weiteren Verlauf der Tathandlungen sog. One Time Passwords, die z.B. für den Implementierungsprozess (Enrolement) von Kreditkartennummern in Apple Pay und Google Pay erforderlich sind, zu aktivieren und anschließend betrügerisch einzusetzen. Die Täter nutzten in der Folge die Bezahlfunktion von Smartphones an POS-Terminals vor Ort bei unterschiedlichen Vertragsunternehmen mittels Near Field Communication[23] zur betrügerischen Erlangung von Waren.[24]

2.3 Angst vor Identitätsdiebstahl und -missbrauch ist groß

Laut einer 2019 veröffentlichten Studie des Cyber-Sicherheitsanbieters F-Secure machen sich neun von zehn Verbrauchern zumindest grundsätzlich Sorgen darüber, dass ihr Bankkonto gehackt werden könnte, um ihr Geld zu stehlen (89%), sie Opfer von Online-Shopping-Betrug werden könnten (87%) oder jemand mithilfe ihrer Identität eine Straftat begeht (87%).[25]

Mittlerweile ist auch die Sorge bei Unternehmen, etwa im Bereich E-Commerce, groß, dass man Opfer von *„Identitätsbetrug“* werden könnte. Begriffe wie ***„Cyber Security Awareness“*** oder ***„Phishing Awareness“*** (Awareness svw. Problembewusstsein) etwa zum Schutz vor Passwortdiebstahl mittels Phishing-Mails erleben Hochkonjunktur.[26]

3 Konsequenzen/Herausforderungen

Identitätsdiebstahl und -missbrauch im Internet als Bestandteil der Computerkriminalität verunsichern einerseits Nutzer des Internets oder digitaler Anwendungen, verursachen bei Privatpersonen wie Unternehmen z.T. erhebliche Schäden und stellen für die Sicherheitsakteure eine zunehmende Herausforderung dar. Folgt man der von Balschmiter bereits 2017 entwickelten These, dass ein Teil des Hellfeldes klassischer Kriminalitätsformen offensichtlich in das Dunkelfeld moderner Computerkriminalitätsdelikte übergegangen ist,[27] sind die Positivinterpretationen des Rückganges der Fallzahlen in der Polizeilichen Kriminalstatik[28] jedenfalls kritisch zu hinterfragen. Zwar ist der Anteil der Cybercrimedelikte (Computerkriminalität – PKS-Summenschlüssel 897000) an der Gesamtkriminalität in den vergangenen Jahren leicht gestiegen (2018: rd. 2% [110.475 Fälle]; 2020: rd. 2,46% [130.611 Fälle]), eine signifikante Erhellung des Dunkelfeldes ist damit jedoch keinesfalls verbunden. Und auch ein tatsächliches Widerspiegeln der Verlagerung großer Teile des gesellschaftlichen Lebens in die digitale Welt als gesellschaftliche Realität ist daraus nicht abzuleiten. Da weder eine echte Erhellung des Cybercrime-Dunkelfeldes erfolgte und auch die Ressourcen der Sicherheitsbehörden in diesem Deliktsbereich offenbar nicht in dem Maße wie die Verlagerung gesellschaftlichen Lebens in die digitale Welt stattfand, verstärkt wurden, existiert hier erheblicher Handlungsbedarf. Es ist daher Rüdiger zuzustimmen, der bereits 2019 im Rahmen der BKA-Herbsttagung eine deutlich verstärkte Internetpräsenz der deutschen Polizeien forderte und zudem ein Nachdenken über die Einführung des Opportunitätsprinzips bei derartigen Delikten anregte.[29]

Anmerkungen

1 Der Autor studierte Rechtswissenschaften an der Humboldt-Universität zu Berlin. Berufliche Stationen waren u.a.: Leitung verschiedener Kripo-Dienststellen, Kriminalistik-Dozent an der damaligen Polizei-Führungsakademie in Münster-Hiltrup (2001-2005), Leitung der Hochschule der Sächsischen Polizei (FH) in Rothenburg/O.L. (2005-2013) und die Leitung der Abteilung Auswertung und Ermittlungen im Landeskriminalamt Sachsen (2015-2019) sowie die Vertretung der Polizei Sachsen in den Kommissionen Wirtschaftskriminalität und Organisierte Kriminalität der AG Kripo. Der Autor ist Dozent im Masterstudiengang *„Kriminologie, Kriminalistik und Polizeiwissenschaft“* an der Ruhr-Universität Bochum und im Masterstudiengang *„Öffentliche Verwaltung – Polizeimanagement“* an der Deutschen Hochschule der Polizei sowie im Masterstudiengang *„Kriminalistik“* an der Hochschule der Polizei des Landes Brandenburg. Er ist Gründungsmitglied der Deutschen Gesellschaft für Kriminalistik e.V. Erreichbarkeit: ralph-berthel@web.de.

2 Es wird dabei nicht verkannt, dass der Begriff *„Identität"* in unterschiedlichen Wissenschaftsgebieten auch unterschiedlich definiert wird. Aus psychologischer und pädagogischer Sicht spielt etwa die Identitätsbildung nach Erikson, die in erster Linie die psychosoziale Entwicklung des Menschen betrachtet, eine wichtige Rolle. In verschiedenen Definitionen des Begriffs Identität werden Eigenschaften von Identitäten neben natürlichen Personen auch Entitäten, Gegenständen oder Objekten zugeordnet. Aus juristischer Sicht liefert die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr Anhaltspunkte zur Beschreibung dessen, was mit der Identifizierung von Menschen und damit auch deren Identität verbunden werden kann. Dort heißt es in Art 2 a): „Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind".

3 Alle im Text verwendeten Internetadressen wurden letztmalig am 19.9.2021 aufgerufen.

4 Der Begriff *„Daten"* wird hier für gesammelte einfache, isolierte Fakten, die einer Interpretation bedürfen, verwendet. Informationen sind hingegen bewertete, d.h. bereits interpretierte Daten, die für den Nutzer für die Lösung einer spezifischen Aufgabenstellung hilfreich sind. (Berthel, Ralph, Lapp, Matthias, Kriminalstrategie, 2017, S. 74).

5 BSI, Die Lage der IT-Sicherheit in Deutschland 2020, S. 18.

6 Pollmann, Malte, Ostler, Ulrike, Was ist digitale Identität und ist sie sicher? Datencenter Insider, 25.08.2021, https://www.datacenter-insider.de/was-ist-digitale-identitaet-und-ist-sie-sicher-a-1050665/.

7 BSI, 2020, S. 18.

8 Vgl. u.a. BKA, Cybercrime, Bundeslagebild 2020, 2021, S. 12.

9 Reuter, Caroline, Was bedeutet kompromittiertes Konto? 1.9.2021, https://alleantworten.de/was-bedeutet-kompromittiertes-konto.

10 BSI, Social Engineering – der Mensch als Schwachstelle, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html.

11 BSI, Glossar der Cyber-Sicherheit, https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Informationen-und-weiterfuehrende-Angebote/Glossar-der-Cyber-Sicherheit/Functions/glossar.html?cms_lv2=132814.

12 Vgl. Kaspersky, Was ist Spoofing? https://www.kaspersky.de/resource-center/definitions/ip-and-email-spoofing.

13 Avira, Spoofing, Phishing, Pharming: drei Methoden des Identitätsdiebstahls im Internet, 12.4.2018, https://www.avira.com/de/blog/avira-identity-scanner-schutz-vor-identitaetsdiebstahl.

14 Ebd.

15 Das BKA definiert Cybercrime im engeren Sinne als Straftaten, die sich gegen das Internet, informationstechnische Systeme oder deren Daten richten. BKA, 2021, S. 42.

16 BKA, 2021, S. 9.

17 BKA, 2021, S. 12.

18 Bei *„Have I Been Pwned"* (HIBP), dt. *„Wurde ich erwischt? Wurde ich gehackt?"* handelt es sich um die Website des unabhängigen Sicherheitsforschers Troy Hunt, der ermittelt, ob eine E-Mail-Adresse in einem öffentlich gewordenen Hack auftaucht.

19 Penetrationstests prüfen die Vulnerabilität von IT-Systemen gegenüber Angriffen. Sie sind grundlegender Bestandteil von IT-Sicherheits- und Schwachstellenanalysen.

20 KRITIS (Kritische Infrastrukturen) sind 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. (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundesamt für Sicherheit in der Informationstechnik, Kritische Infrastrukturen, Definition und Übersicht, (https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html).

21 *„Orion"* ist eine IT-Management und -Monitoring-Software, die weltweit eingesetzt wird.

22 Ausführlich vgl. BKA, 2021, S. 29f.

23 Bei Near Field Communication (NFC), also Nahfeldkommunikation, handelt es sich um einen Übertragungsstandard zum kontaktlosen Austausch von Daten zwischen zwei Geräten in einer Entfernung von 10 bis 20 cm. Die Geschwindigkeit ist dabei auf 424 Kilobits pro Sekunde beschränkt. Beide Geräte können sowohl Daten senden als auch empfangen (https://www.netzwelt.de/nfc/index.html).

24 Ausführlich vgl.: BKA, 2021, S. 17.

25 F-Secure, *„Identity Protection Consumer (B2C)", Ist* Identitätsdiebstahl das Cyber-Verbrechen, das wir am meisten fürchten? Eine Verbraucherumfrage zu den Themen *„Identitätsdiebstahl und Cyber-Kriminalität"*. https://www.f-secure.com/de/press/p/neue-studie-bestaetigt-die-angst-vieler-internetnutzer-vor-identitaetsdiebstahl.

26 Vgl. z.B. BSI, Awareness, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html.

27 Balschmiter, Peter, et al. Landeskriminalamt Mecklenburg-Vorpommern, Fachhochschule für öffentliche Verwaltung, Polizei und Rechtspflege des Landes MV, Ernst-Moritz-Arndt Universität Greifswald, Erste Untersuchung zum Dunkelfeld der Kriminalität in Mecklenburg-Vorpommern. Abschlussbericht, 2017, S. 54.

28 Bundesministerium des Innern, für Bau und Heimat, Kriminalstatistik 2020: Straftaten auf niedrigstem Stand seit 1993, Pressemitteilung, 15.4.2021.

29 Berthel, Ralph, Ausgrenzung, Hass und Gewalt – Herausforderungen für den Rechtsstaat und die Sicherheitsbehörden - Mit einem Bericht zur 65. Herbsttagung des Bundeskriminalamtes, DIE POLIZEI, 2020, S. 107.

Strafbarkeit des Identitätsdiebstahls durch Phishing, Pharming und Spoofing

Von Prof. Dr. Anja Schiemann, Köln/Münster[1]

1 Einleitung

Die bekannteste Form des Identitätsdiebstahls ist das sog. Phishing, das Fischen nach Onlinezugangsdaten.[2] In rechtlicher Hinsicht muss nach vier Stufen differenziert werden. Im ersten Schritt geht es um die Erlangung der relevanten Zugangsdaten und TANs für das Online-Banking. Hierzu locken die Täter vornehmlich Bankkunden durch massenhaft versendete E-Mails auf imitierte Webseites, um sie zur Preisgabe von nutzbaren Daten zu bewegen. Im zweiten Schritt werden, soweit dies erforderlich ist, die so erlangten Daten verändert, bevor sie im dritten Schritt vom Täter zur Durchführung der Transaktion missbraucht werden. Im vierten Schritt werden zur Abwicklung des Geldtransfers sog. Finanzmanager oder Finanzagenten eingesetzt, die das erlangte Geld entgegennehmen und gegen Provision ins Ausland transferieren.[3] Die ersten beiden Schritte sind im Hinblick auf den Identitätsdiebstahl sowie die Datenveränderung relevant. Dagegen soll der vierte Schritt und die Frage nach der Strafbarkeit des Finanzagenten im Rahmen dieses Aufsatzes ausgespart werden, da dies nicht unmittelbar mit dem Phishingvorgang in Verbindung steht.[4]

Soweit in der ersten Phase die Nutzer statt mit einer E-Mail unmittelbar durch Manipulationen an Domain-Name-Servern (DNS) auf gefälschte Web-Seiten umgeleitet werden,

spricht man vom sog. Pharming. Das Pharming kommt also ohne die Spam-E-Mail mit dem darin befindlichen Hyperlink aus. Durch die Malware wird vielmehr nicht die Original-Banking-Webseite, sondern die vom Täter manipulierte Webseite aufgerufen.[5]

Beim IP-Spoofing werden falsche IP-Nummern verwendet, um dem angegriffenen Rechner oder System eine falsche Identität vorzutäuschen. Hierbei werden bspw. die IP-Adressen in den Datenpaketen verändert, die an den Eingangs-Port eines Netz-Routers übertragen werden.[6] Insofern sind IP-Spoofing und Pharming stark verwandte Phänomene.

2 Strafbarkeit

2.1 Strafbarkeit hinsichtlich der Datenverschaffung

2.1.1 Nicht in Betracht kommende Straftatbestände

Das Phishing der sensiblen Daten selbst erfüllt nur sehr wenige Straftatbestände. Insbesondere die Straftatbestände Betrug, Computerbetrug oder das Ausspähen oder Abfangen von Daten werden nicht verwirklicht. Warum? Der Straftatbestand des Betrugs gem. § 263 StGB setzt voraus, dass das getäuschte Opfer irrtumsbedingt eine Verfügung über sein Vermögen trifft und sich dadurch selbst schädigt. Die Herausgabe der persönlichen Zugangsdaten als solche wirkt aber nicht unmittelbar vermögensmindernd, sondern schafft vielmehr die Voraussetzungen dafür, dass der Täter durch eine weitere Handlung auf das Konto des Opfers zugreift und erst dadurch einen Vermögensschaden herbeiführt.[7] Auch ein versuchter Computerbetrug wurde vom KG verneint. Denn ein unmittelbares Ansetzen zur Verwirklichung des Straftatbestands i.S.d. § 22 StGB läge erst dann vor, wenn der Täter die erlangten Daten auch verwendet. Dagegen stelle die Einrichtung von Zielkonten, eine fingierte polizeiliche Anmeldung und das Abfangen von Kontounterlagen noch keinen versuchten Computerbetrug dar.[8]

Eine Strafbarkeit in Form der Vorbereitung eines Computerbetrugs gem. § 263a Abs. 3 StGB wird ebenfalls in der Regel nicht verwirklicht, weil hierzu ein Computerprogramm gegeben sein muss, dessen Zweck auf die Begehung einer Tat nach Abs. 1 gerichtet ist.[9] Das Verfassen einer sog. Phishing-E-Mail ist aber keine solche Vorbereitungshandlung, weil als Programm nur eine Befehlsfolge an einen Computer bezeichnet werden kann, die selbsttätig abläuft und ein eigenes Arbeitsergebnis produziert. Auch soweit mit entsprechender Intention eine Internet-Seite erstellt wird, die als Programm gewertet werden kann, fehlt es am erforderlichen Unmittelbarkeitszusammenhang, da nicht dieses Programm, sondern erst die darüber erlangten Daten für den späteren Computerbetrug verwendet werden.[10] Auch sofern seit Inkrafttreten des 61. StrÄndG v. 10.3.2021[11] am 18.3.2021 gem. Nr. 2 Passwörter oder sonstige Sicherungscodes als Tatobjekte erfasst werden, kommt eine Strafbarkeit nicht in Betracht.[12]

Auch der Straftatbestand des Ausspähens von Daten gem. § 202a StGB ist nicht einschlägig. Aufgrund der weiten Auslegung des Datenbegriffs können PIN und TAN als Kontozugangs- und Transaktionsinformationen zwar hierunter subsumiert werden.[13] Allerdings veranlasst der Täter das Opfer selbst dazu, die fraglichen Daten an seinen Rechner zu übersenden. Insofern muss der Täter keine Sicherung gegen den unberechtigten Zugang überwinden, vielmehr sind die Daten für ihn bestimmt.[14]

Strafbar gem. § 202a StGB ist dagegen das IP-Spoofing. Denn soweit das Opfer die vorgespiegelte Adresse für vertrauenswürdig hält, gibt es den Zugang zu seinem Netzwerk und damit zu den dort vorhandenen Daten frei. Da hier mit dem Netzwerk-Rechner Daten ausgetauscht werden und zusätzlich die Adresse eines weiteren Rechners benutzt wird, werden Geheimhaltungs- und Sicherungsmaßnahmen des Verfügungsberechtigten ausschaltet.[15] Einschränkend ist aber erforderlich, dass ein Zugangsschutz überwunden wurde.[16]

Der Straftatbestand des Abfangens von Daten gem. § 202b StGB ist in keiner Konstellation erfüllt. Voraussetzung ist nämlich, dass der Täter Daten aus einer nichtöffentlichen Datenübermittlung oder einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage abfängt. Hierfür müsste sich der Täter in die Datenübermittlung zwischen Bankkunden und Bank schalten. Dies ist aber beim Versenden von Phishing-E-Mails und dem Aufbau von Phishing-Websites ersichtlich nicht der Fall, weil die Datenübermittlung von Anfang an nur zwischen Täter und Opfer stattfindet.[17]

Ebenfalls nicht verwirklicht sind die Straftatbestände der Datenveränderung gem. § 303a Abs. 1 StGB und der Computersabotage gem. § 303b Abs. 1 StGB. Weder verursachen Phishing-Mails oder Phishing-Websites ein Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von nach § 303a StGB geschützten Daten, noch liegt eine Störung der Datenverarbeitung i.S.v. § 303b Abs. 1 StGB vor.

2.1.2 Fälschung beweiserheblicher Daten

Zentrale Vorschrift, um dem ersten Schritt des Phishings, nämlich der Datenbeschaffung, strafrechtlich zu begegnen, ist § 269 Abs. 1 StGB. Allerdings sollte die *„Schlagkraft“* dieser Vorschrift nicht überschätzt werden.[18] Die Prüfung der Strafbarkeit nach § 269 StGB erfordert eine *„urkundengerechte“* Umsetzung der Datenverarbeitungsvorgänge.[19] Daher gelten für die Bestimmung des Ausstellerbegriffs und der Echtheit die Regeln zur Urkundenechtheit analog.[20]

Der wirkliche oder scheinbare Aussteller einer Erklärung per E-Mail kann also auch aus der E-Mail-Adresse oder einem Firmenlogo des Absenders hervorgehen. Deshalb ist eine sog. Phishing-Mail, mit der unter falscher Absenderangabe, z.B. einer Bank, persönliche Daten und sensible Informationen abgefragt werden, eine unechte Datenurkunde. Denn hier werden rechtlich erhebliche Gedankenerklärungen unter falscher Identität gemacht, so dass über den wahren erkennbaren Aussteller getäuscht wird.[21]

Auch die Einrichtung einer Homepage mit falschen Angaben zur Identität des Betreibers (Pharming) ist nach § 269 StGB strafbar, wenn diese scheinbar eine rechtserhebliche Erklärung der wahrheitswidrig genannten Person enthält. Hierfür ist weder die Verwendung einer gefälschten elektronischen Signatur, noch der Einsatz einer gefälschten IP-Adresse erforderlich. Denn die rechtserhebliche Erklärung wird in erster Linie durch den Text verkörpert, an dem sich das Täuschungsopfer im Rechtsverkehr orientiert.[22]

Auch bei IP-Spoofing ist eine Strafbarkeit nach § 269 StGB gegeben. Denn beim echten IP-Spoofing werden falsche IP-Nummern verwendet, um eine falsche Identität vorzuspiegeln. Insofern werden falsche Absenderkennungen verschickt.[23] Durch das Verändern der Daten wird eine echte Urkunde verfälscht.[24] Doch auch beim unechten IP-Spoofing[25] ist § 269 StGB in Form des Gebrauchs gespeicherter oder veränderter Daten verwirklicht.[26]

2.1.3 Weitere Vorschriften

Für eine Strafbarkeit in Betracht kommen darüber hinaus auch weniger bekannte Vorschriften aus dem Nebenstrafrecht. Soweit Elemente des Corporate Designs einer Bank oder ähnlicher benutzter Adressaten markenrechtlich oder urheberrechtlich geschützt sind, verwirklicht der Täter durch die Benutzung von Logos, geschäftlichen Bezeichnungen und ähnlichem die Straftatbestände der §§ 143 Abs. 1, 143a Abs. 1 MarkenG sowie der §§ 106 ff. UrhG.[27]

Daneben ist eine Strafbarkeit in Form der unzulässigen Datenverarbeitung personenbezogener Daten gem. Art. 84 Abs. 1 DSGVO i.V.m. § 42 Abs. 2 Nr. 1 BDSG denkbar, da PIN und TAN zweifellos personenbezogene Daten nach Art. 4 Nr. 1 DSGVO darstellen. Die für die Datenverarbeitung erforderliche Einwilligung oder ein gesetzlicher Erlaubnistatbestand sind nicht gegeben, so dass die Datenverarbeitung unzulässig ist. Wird vorsätzlich und mit Bereicherungsabsicht gehandelt, ist der Straftatbestand erfüllt.[28]

2.2 Strafbarkeit hinsichtlich der Datenverwendung

Der zweite Schritt des Phishings, nämlich die Nutzung der erlangten Zugangsdaten für eine Onlineüberweisung zulasten des Kontos des Getäuschten, erfüllt dann mehr Straftatbestände als der erste Schritt. Zunächst steht eine Strafbarkeit gem. § 202a StGB im Raum. Mit PIN und TAN verschafft sich der Täter Zugang zu den Konto- oder Depotinformationen des Opfers, die eigentlich ausschließlich für den Kontoinhaber bestimmt und durch die vorgeschaltete Abfrage der Zugangsdaten besonders gesichert sind. Da es dem Täter gerade um die Erlangung der Informationen geht, handelt er auch vorsätzlich.[29]

§ 202b StGB ist dagegen auch im Rahmen der Datenverwendung nicht verwirklicht, da es auch hier zu keinem Datenaustausch zwischen dem Bankkunden und der Bank kommt.

Verwirklicht ist dagegen der Straftatbestand des Computerbetrugs in der Tatalternative des unbefugten Verwendens von Daten gem. § 263a Abs. 1 Var. 3 StGB. Durch die betrugsspezifische Auslegung des Tatbestandsmerkmals der unbefugten Datenverwendung, wird eine täuschungsäquivalente Handlung des Phishers vorausgesetzt. Der Täter gibt gegenüber der Bank vor, der berechtigte Bankkunde zu sein. Auch wenn die Preisgabe von PIN und TAN durch das Opfer bewusst erfolgte, so erstreckt sich dies jedoch nicht auf die zweckfremde Nutzung der Daten, so dass die Datenverwendung durch den Täter unbefugt ist. Indem der Phisher die Passwörter beim kontoführenden Institut einsetzt und sich ins System einloggt, beeinflusst er zudem das Ergebnis eines automatisierten Datenverarbeitungsvorgangs. Dieser Datenverarbeitungsvorgang wirkt sich unmittelbar vermögensmindernd aus, da hierfür die Freigabe eines vermögensrelevanten Zugangs ausreicht. Durch die Überweisung des Geldbetrags durch den Täter auf das Zielkonto tritt ein Vermögensschaden ein.[30] Auch die Bereicherungsabsicht ist gegeben, da es dem Täter, auch wenn er das Geld zunächst auf ein Konto eines Finanzkuriers transferiert, darum geht, sich selbst zu bereichern. Hat man wegen der Stoffgleichheit aufgrund der Tatsache, dass in den Fällen, in denen ein Finanzkurier beteiligt ist, zunächst eine Bereicherung beim Finanzkurier eintritt, Zweifel, so ist zu bedenken, dass es ausreicht, wenn der rechtswidrige Vermögensvorteil für einen Dritten erlangt werden soll.[31]

Auch der Straftatbestand der Fälschung beweiserheblicher Daten ist gegeben. Der Phisher stellt durch die Eingabe der Zugangsdaten des Opfers auf der Bankwebsite und die Tätigung einer Onlineüberweisung einen Datensatz her, den die Bank speichert. Erklärungsinhalt ist der Überweisungsauftrag. Durch die Verwendung von PIN und TAN erklärt der Täter, Verfügungsberechtigter über das Konto zu sein. Damit werden beweiserhebliche Daten so gespeichert, dass bei ihrer Wahrnehmung eine unechte Urkunde vorliegen würde. Da der Täter infolge des automatisierten Vorgangs keinen Menschen im Rechtsverkehr täuscht, muss ein Rückgriff auf § 270 StGB erfolgen, nach dem die fälschliche Beeinflussung einer Datenverarbeitung der Täuschung im Rechtsverkehr gleichsteht.[32]

2.3 Strafbarkeit hinsichtlich des Anwerbens eines Finanzkuriers

Dagegen ist das reine Anwerben eines Finanzkuriers durch den Phisher nicht strafbar. In Betracht käme allein eine Strafbarkeit wegen Betrugs gem. § 263 StGB. Die Spam-Mail des Täters stellt dabei zweifellos eine Täuschungshandlung dar, weil die beschriebene Aufgabe des Kuriers eine andere ist, als seine tatsächlich vorgesehene Rolle. Der Finanzkurier geht nämlich davon aus, eine legale Arbeitsleistung zu erbringen. Sieht man mit der herrschenden Meinung Arbeitsleistungen generell als Bestandteil des rechtlich geschützten Vermögens an, so ist auch eine irrtumsbedingte Vermögensverfügung in Form der vom Finanzkurier erbrachten Dienstleistung gegeben.[33] Auch ein Vermögensschaden kann bejaht werden, da der Finanzagent der Bank des Kontoinhabers gegenüber bereicherungsrechtlichen Haftungsansprüchen ausgesetzt ist. Letztlich scheitert eine Betrugsstrafbarkeit jedoch an der fehlenden Stoffgleichheit. Nach dem Gesichtspunkt der Stoffgleichheit muss sich die Bereicherungsabsicht des Täters auf einen Vorteil beziehen, der unmittelbar aus dem Vermögen des Opfers stammt.[34] Der Bereicherungsanspruch der Bank führt aber zu einem Schaden des Finanzkuriers und beruht daher nicht auf der Überweisung und insofern nicht auf einer Verfügung des Täters.[35]

3 Fazit

Der Phishingtäter erfüllt durch sein Verhalten einen bunten Strauß von Straftatbeständen, wobei zwischen den Handlungen der Datenbeschaffung und anschließenden Datenverwendung differenziert werden muss. Bereits durch die Datenbeschaffung durch das Verschicken der Phishing-E-Mail oder das Erstellen der Phishing-Webseite macht er sich nach § 269 StGB strafbar. Sofern die Variante des IP-Spoofing gegeben ist, wird ggf. noch § 202a StGB verwirklicht. Darüber hinaus verwirklicht der Phishing-, Pharming- oder Spoofing-Täter im Nebenstrafrecht die Strafnormen der §§ 143, 143a MarkenG sowie §§ 106 ff. UrhG, sofern er markenrechtlich oder urheberrechtlich geschützte Kennzeichen oder Bezeichnungen verwendet. Auch eine Strafbarkeit nach datenschutzrechtlichen Vorschriften steht im Raum.

Durch die anschließende Datenverwendung verwirklicht der Phisher § 202a StGB, indem er sich durch die abgefischten Daten Zugang zu den Kontoinformationen des Opfers verschafft. Durch die Verwendung der Daten im Rahmen der Onlineüberweisung ist darüber hinaus eine Strafbarkeit gemäß § 263a und §§ 269, 270 StGB gegeben.

Diese kurze rechtliche Würdigung macht deutlich, dass das geltende Strafrecht ausreichend Schutz gegen das Phishing

und seine Sonderformen insgesamt bietet. Dennoch sollte der Gesetzgeber auch neuere Formen und Tatmodalitäten stets im Blick haben, um hier mit einer Nachjustierung der strafrechtlichen Vorschriften angemessen auf die fortschreitende Digitalisierung auch kriminellen Verhaltens reagieren zu können.

Anmerkungen

1 Die Verfasserin war bis Ende März 2022 Leiterin des Fachgebiets Strafrecht, Strafprozessrecht und Kriminalpolitik an der Deutschen Hochschule der Polizei (DHPol) in Münster. Zum 1. April 2022 ist die Universitätsprofessorin auf den Lehrstuhl für Strafrecht und Strafprozessrecht an der Universität zu Köln gewechselt. Der DHPol bleibt sie über eine Gastprofessur verbunden.
2 So Bär, in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl. (2017), § 269 Rn. 15.
3 Vgl. Bär, in: Graf/Jäger/Wittig, § 263a Rn. 27; Sanli, ZWH 2018, 205.
4 Vgl. hierzu ausführlich Sanli, ZWH 2018, 205 (211 f.); Seidl/Fuchs, HRRS 2010, 85 (90 f.).
5 S. Borges, NJW 2005, 3313 (3314); Popp, MMR 2006, 84.
6 S. Weidemann, in: BeckOK-StGB, Computerkriminalität, 51. Ed. (1.11.2021), Rn. 8; Metz, JR 2019, 492 (498 f.).
7 Vgl. ausf. Popp, MMR 2006, 84 (85 f.); Popp, NJW 2004, 3517 (3518); Sanli, ZWH 2018, 205 (208).
8 So KG, MMR 2012, 845.
9 S. Fischer, StGB, 68. Aufl. (2021), § 263a Rn. 30.
10 Vgl. hierzu Mühlbauer, in: MK-StGB, Bd. 5, 3. Aufl. (2019), § 263a Rn. 115; Sanli, ZWH 2018, 205 (209); Waßmer, in: Leitner/Rosenau, Wirtschafts- und Steuerstrafrecht, 1. Aufl. (2017), § 263a Rn. 108.
11 BGBl. 2021 I, 333.
12 Nach Auffassung des Gesetzgebers sollten hierdurch primär Skimming-Fälle erfasst werden, vgl. BT-Drs. 19/25631, S. 23.
13 So Stuckenberg, ZStW 118 (2006), 878 (884); Goerckenjahn, wistra 2009, 47 (52); zweifelnd Popp, MMR 2006, 84 (85).
14 S. Popp, MMR 2006, 84 (85); Fischer, § 202a Rn. 9a; Kargl, in: NK-StGB, 5. Aufl. (2017), § 202a Rn. 10.
15 So Graf, in: MK-StGB, Bd. 4, 4. Aufl. (2021), § 202a Rn. 92.
16 S. Böken, in: Kipker, Cybersecurity, 1. Auf. (2020), Kap. 15 Rn. 76; Graf, in: MK-StGB, § 202a Rn. 92.
17 Hierzu Sanli, ZWH 2018, 205 (208); Bär, in: Wabnitz/Janovsky/Schmitt, Hdb. Wirtschafts- und Steuerstrafrecht, 5. Aufl. (2020), Kap. 15 Rn. 88.
18 So Popp, MMR 2006, 84 (85).
19 Fischer, § 269 Rn. 3.
20 Vgl. Heger, in: Lackner/Kühl, StGB, 29. Aufl. (2018), § 269 Rn. 2; ausf. Buggisch, NJW 2004, 3519 (3520 f.).
21 Vgl. Bär, in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl. (2017), § 269 Rn. 15; Erb, in: MK-StGB, Bd. 5, 3. Aufl. (2019), § 269 Rn. 33; Stuckenberg, ZStW 118 (2006), 878 (890).
22 S. Erb, in: MK-StGB, § 269 Rn. 34; Sanli, ZWH 2018, 205 (209).
23 Vgl. Rinker, MMR 2002, 663.
24 S. Rinker, MMR 2002, 663 (664); Marberth-Kubicki, Computer- und Internetstrafrecht, 2. Aufl. (2020), Rn. 178.
25 Hier wird vom Hacker der Rechner eines Dritten benutzt, um davon gezielt Datenpakete an den Dritten zu schicken. Die Daten stammen also von dem Rechner, der als Absender bezeichnet wird. Allerdings bleib der Hacker anonym und das Opfer hält den infiltrierten Computer für den Absender bzw. Angreifer, vgl. Rinker, MMR 2002, 663.
26 Ausf. Rinker, MMR 2002, 663 (664); Marberth-Kubicki, Rn. 111.
27 S. Sanli, ZWH 2018, 205 (210); Ingerl/Rohnke, Markengesetz, 3. Aufl. (2010), § 143 Rn. 10; ausf. Beck/Dornis, CR 2007, 642; Marberth-Kubicki, Rn. 73; Seidl/Fuchs, HRRS 2010, 85 (87 f.).
28 S. Sanli, ZWH 2018, 205 (210); zur alten Rechtslage Heghmanns, wistra 2007, 167.
29 Vgl. Seidl/Fuchs, HRRS 2010, 85 (88); Sanli, ZWH 2018, 205 (210); a.A. Graf, NStZ 2007, 129 (131).
30 Wo genau dieser Vermögensschaden eintritt, kann im Einzelfall problematisch sein und richtet sich nach § 675u und § 675v BGB und soll hier nicht weiter vertieft werden. Ausf. hierzu aber Seidl/Fuchs, HRRS 2010, 85 (89).
31 Vgl. Fischer, § 263 Rn. 186; zu den Fallkonstellationen Sanli, ZWH 2018, 205 (209).
32 So auch Sanli, ZWH 2018, 205 (210); Seidl/Fuchs, HRRS 2010, 85 (89); Stuckenberg, ZStZ 118 (2006), 878 (906).
33 Diese Auffassung ist aber durchaus umstritten, s. dazu ausf. Heinrich, GA 1997, 24; Saliger, in: Matt/Renzikowski, StGB, 2. Aufl. (2020), § 263 Rn. 169.
34 Vgl. Fischer, § 263 Rn. 187; Lackner/Kühl, § 263 Rn. 59.
35 Insg. hierzu Sanli, ZWH 2018, 205 (211); Seidl/Fuchs, HRRS 2010, 85 (90); Goeckenjan, wistra 2008, 128 (132 f.).

REZENSION

Peters/Janz, Handbuch Versammlungsrecht. 2. Auflage 2021

Mit der Föderalismusreform I ist die Auseinandersetzung mit der Thematik des Versammlungsrechts deutlich komplexer geworden. Unterschiedliche sicherheitspolitische Ansätze der nunmehr zuständigen Ländergesetzgeber haben zu einer uneinheitlichen, fragmentierten und wenig übersichtlichen Rechtslage geführt. Ein problematischer Flickenteppich ist entstanden, der gerade bei länderübergreifenden Polizeieinsätzen erkennbar Probleme bereitet. Wertvolle Hilfestellungen bieten in diesem Zusammenhang die Rechtsprechung sowie das einschlägige Schrifttum an.

Zu der Orientierung gebenden Fachliteratur gehört das von Dr. Wilfried Peters und Prof. Dr. Norbert Janz herausgegebene Handbuch Versammlungsrecht, das nach sechs Jahren nunmehr in der 2. Auflage erschienen ist.

Das anspruchsvolle Werk enthält ausführliche Erläuterungen zu den Entwicklungslinien der bedeutenden Versammlungsfreiheit, zu verfassungsrechtlichen Fragestellungen, zu internationalen und europäischen Gewährleistungen, zur bundes- und landesgesetzlichen Ausgestaltung des Versammlungsrechts, zu bereichsspezifischen Pflichten und Verboten, zu Inhalt und Grenzen hoheitlicher Eingriffsbefugnisse, zum gerichtlichen Rechtsschutz sowie zum Versammlungsstrafrecht. In diesem Rahmen wird auch zu den Auswirkungen der andauernden Corona-Pandemie einschließlich der vorliegenden Entscheidungen zur Durchführung und Auflösung von Versammlungen Stellung bezogen. Die Bearbeitung der einzelnen Kapitel ist durch namhafte Autoren aus Wissenschaft und Praxis erfolgt.

Sehr zielführend ist die Beiziehung und Ausweisung vieler bedeutsamer Quellen aus Rechtsprechung und Literatur, die eine vertiefende Auseinandersetzung mit der jeweiligen Problemstellung ermöglicht. Eher kritisch ist hingegen die nicht durchgehend überzeugende Gliederung in die Kapitel A bis I zu bewerten, die zu überflüssigen Überschneidungen führt, so dass eine Kommentierung aus einem Guss nicht immer gegeben ist.

In der Gesamtschau handelt es sich dennoch um ein empfehlenswertes Werk, das nicht nur die ausgewiesene Zielgruppe anspricht, sondern durchaus auch für den Polizeivollzugsdienst von Bedeutung ist.

Hartmut Brenneisen, Preetz/Worms

Herausgeber:	**Wilfried Peters, Norbert Janz**
Titel:	**Handbuch Versammlungsrecht**
Auflage:	**2. Auflage 2021**
Format:	**515 Seiten, 24,5 x 16,5 cm, Hardcover**
Preis:	**119,00 Euro**
ISBN:	**978-3-406-77035-7**
Verlag:	**Verlag C. H. Beck oHG**

Computerprävention – Sensibilisierung für Gefahren im Netz

Von EKHK a.D. Klaus Kemper, Duisburg[1]

1 Allgemeines

Ende der 1990er-Jahre setzte sich in der deutschen Polizei die Einsicht durch, dass es dringend geboten sei, neben der Strafverfolgung auch der Kriminalprävention in Form eigener Organisationseinheiten einen höheren Stellenwert einzuräumen. Neben den bereits seit Jahrzehnten durchgeführten sicherheitstechnischen Hinweisen zur Vermeidung von Einbruchsdiebstählen wurde in diesen Dienststellen nun auch verstärkt auf die Verhaltensprävention im Zusammenhang mit den Bereichen Rauschgift-, Gewalt- und Jugendkriminalität sowie Sexual- und Betrugsdelikte gesetzt. Nachdem um die Jahrtausendwende Computer sowie das Internet praktisch für jeden Bürger verfügbar geworden waren, dauerte es nicht lange, bis die ersten Anwender auch die sich ihnen bietenden Möglichkeiten dieser technischen Errungenschaften nutzten, um mit ihnen Straftaten zu begehen. Diese mittels Anwendung der Informations- und Kommunikationstechnik, kurz IuK, durchgeführten Delikte werden unter dem Oberbegriff *„Computerkriminalität"* oder auch *„Cybercrime"* zusammengefasst und haben in den letzten zwei Jahrzehnten einen enormen Aufschwung erlebt. Laut der Polizeilichen Kriminalstatistik des BKA für das Jahr 2020 wurden in diesem Zeitraum 130.611 Fälle bekannt, was einen Anstieg von 7.605 Fällen bzw. ein Plus von 6,2% bedeutet.[2] Da sich diese Entwicklung verhältnismäßig frühzeitig abzeichnete, wurden die bekannt gewordenen Modi Operandi auch recht zügig in das Portefeuille der kriminalpolizeilichen Vorbeugungsmaßnahmen aufgenommen und die Sachrate *„Computerprävention"* geschaffen.

2 Persönliche Daten

Die persönlichen Daten jedes einzelnen Menschen können für andere Privatpersonen, Institutionen oder Firmen für ihre eigenen Zwecke von großem Interesse sein. Sie geben nicht nur Aufschluss über Namen, Geburtsort und -datum sowie Wohnanschrift, sondern ermöglichen Interessierten auch einen Blick auf Vorlieben, Kaufgewohnheiten oder Bewegungsbilder. Um dies zu vermeiden, sind die Persönlichkeitsrechte in der Bundesrepublik seit Jahren durch entsprechende Datenschutzgesetze und -verordnungen, z.B. das Bundesdatenschutzgesetz (BDSG), geschützt. Während in der gesamten Europäischen Union entsprechende rechtliche Bestimmungen gelten, hat in den USA nach den terroristischen Anschlägen im Jahr 2001 der sog. *„Patriot Act"* die diesbezüglichen Rechte der Bürger in bestimmten Situationen eingeschränkt.

3 Erschleichen von Daten und deren Missbrauch

Wie bereits angesprochen, aber auch detailliert in den vorangegangenen Beiträgen der Fachzeitschrift *„Die Kriminalpolizei"* dargelegt, hat der Missbrauch persönlicher Daten in den letzten Jahren stark zugenommen. Dabei ist zunächst festzuhalten, dass natürlich gegen deren freiwillige Preisgabe durch den Bürger nichts einzuwenden ist. Dazu ist aber die ausdrückliche Einwilligung erforderlich. Im Gegensatz zu Deutschland nehmen es viele andere Länder mit dem Datenschutz weniger genau, dort hat sich mittlerweile ein regelrechter Markt für diese *„Ware"* gebildet. Hintergrund ist u.a. das Interesse der Werbeindustrie, auf diese Weise an Personenprofile zu gelangen. Diese helfen dann dabei, die Bürger per Internet oder auf andere Art mit auf sie zugeschnittener Werbung zu konfrontieren. Ist dieses Vorgehen für die Betroffenen eher lästig, so sind andere (strafbare) Handlungen im Zusammenhang mit persönlichen Daten oft auch mit finanziellem Schaden verbunden. Dabei wurde diesbezüglich auch schon vor dem *„Computer-Zeitalter"* auf Möglichkeiten der Telekommunikation zugegriffen. So köderten Straftäter per Telefon arglose, häufig betagte Bürger mit angeblich bei Gewinnspielen für sie ausgelosten Preisen, ihre persönlichen Daten preiszugeben. Mit gezielt gestellten Formulierungen, die zwangsläufig ein zustimmendes *„ja"* beim Angerufenen hervorlockten, wurde diesen dann, ohne dass sie es wussten, z.B. ein Zeitschriften-Abonnement *„untergejubelt"*. Exemplarisch sei hier auch noch der *„Enkeltrick"* erwähnt, bei dem der Anrufer zunächst durch geschickte Fragen an persönliche Daten aus dem familiären Umfeld eines kontaktierten Senioren gelangt. Mit diesen wird dann die Notlage eines Enkels oder anderen Verwandten vorgetäuscht und der Senior zum Abheben einer bestimmten Geldsumme bewegt, die dann einem Boten des vermeintlich in Not geratenen Familienmitglieds übergeben werden soll. Mit dem Einzug des Computers in den Alltag der Bürger wurde die Palette der damit verbundenen kriminellen Möglichkeiten erheblich erweitert, wobei diese zum Großteil im Zusammenhang mit bekannten Straftatbeständen, wie z.B. dem Betrug, stehen. Die Aufgabe der Sachrate Computerprävention besteht darin, die Öffentlichkeit über die entsprechenden Modi Operandi zu informieren und Möglichkeiten aufzuzeigen, wie man vermeidet, Opfer derartiger Delikte zu werden. Im Folgenden sind einige der gängigen Arten von Malware ebenso aufgeführt wie Hinweise, sie als solche zu erkennen.

3.1 Spyware

3.1.1 Phishing

Grundsätzlich ist die Datenweitergabe durch Dritte nicht strafbar, sofern die Einwilligung dazu vorliegt. Strafbar ist sie allerdings, wenn sie ohne eine solche durchgeführt wird, um damit dann Aktionen durchzuführen, durch die der eigentliche Eigentümer geschädigt wird. Im Zusammenhang mit den Möglichkeiten des Internets ist nicht einmal ein wie auch immer gearteter direkter Kontakt

zwischen den Parteien vonnöten. Es bedarf lediglich der geschickten Täuschung, die den eigentlichen Nutzer, meist per E-Mail, zur Herausgabe seiner Daten, bevorzugt z.B. seiner Kontonummer oder ähnlicher sensibler Informationen, veranlasst. Dazu bedient der Täter sich oft angeblich seriöser Einrichtungen, wie z.B. Geldinstituten oder Telefonanbietern, die aufgrund sich ergebender Notwendigkeiten um die Übersendung der benötigten Angaben bitten. Im Erfolgsfall wird den Opfern dann in der Regel ein finanzieller Schaden zugefügt, da nun auf deren Konto zugegriffen werden kann. Diese Praxis wird als *„Phishing"* bezeichnet, einem dem englischen *„fishing"* (fischen) nachempfundenen Begriff. Die Gefahr, Geschädigter einer solchen Cyber-Attacke zu werden, reduziert sich erheblich, wenn der angeschriebene User die folgenden Hinweise beherzigt:

- Auch wenn die im Anschreiben niedergelegte E-Mail-Adresse aufgrund früherer Kommunikationen bekannt scheint, sollte sie noch einmal eingehend geprüft werden. Hintergrund ist die Tatsache, dass sich verschiedene Buchstaben in den möglichen Computerschriften verwechseln lassen. Als Beispiel seien hier der Kleinbuchstabe l (Calibri) und der Großbuchstabe I (Arial) genannt. Darüber hinaus sind auch die Null und der Großbuchstabe O schnell zu verwechseln.
- Zip-Dateien werden generell nicht im Zusammenhang mit Zahlungsaufforderungen verschickt.
- Meist wird der Adressat nicht direkt angesprochen, sondern mit den allgemeinen Floskeln *„sehr geehrter Kunde"* oder *„sehr geehrte Damen und Herren"*, eine Praxis, die in echten Schreiben in der Regel nicht verwendet wird.
- Die E-Mails beinhalten oft Grammatikfehler oder fragliche Redewendungen, was darauf hinweisen kann, dass sie mit Hilfe eines Übersetzungsprogramms erstellt worden sind. Derartige Formulierungsprobleme finden sich niemals in tatsächlichen Benachrichtigungen von Kreditinstituten oder seriösen Firmen.
- Enthält das eingegangene Schreiben den Hinweis auf eine gewisse zeitliche Dringlichkeit der erbetenen oder gar geforderten Maßnahme, besteht der Verdacht einer Phishing-Mail.
- Eine weitere Möglichkeit, sich über die Echtheit des Anschreibens rückzuversichern, besteht im Vergleich der angeblichen E-Mail-Adresse des Absenders mit dessen tatsächlicher elektronischer Erreichbarkeit.
- Auch der Griff zum Telefon zwecks fernmündlicher Rücksprache mit einem Sachbearbeiter bringt Klarheit, inwieweit die Benachrichtigung der Wahrheit entspricht.
- Bei Bewerbungen auf Ausschreibungen ist es ratsam, in den zu übersendenden Unterlagen zunächst keine Kontodaten oder Kopien von Personalpapieren mitzuschicken. Das kann auch zu einem späteren Zeitpunkt erfolgen, wenn die Seriosität des Gegenübers feststeht.

3.1.2 Spear-Phishing

Beim *„Spear-Phishing"* handelt es sich um eine Abwandlung des Phishing, bei dem bestimmte Personengruppen, z.B. Studierende einer Universität, gezielt von einem angeblich ortsansässigen Geldinstitut angeschrieben werden. Die Wahrscheinlichkeit, dabei tatsächliche Kunden zu erreichen, liegt so höher als bei wahllos auf den Weg gebrachten E-Mails. Entsprechend wünschenswert ist ein flächendeckender Hinweis der jeweiligen Einrichtung an ihre Mitglieder auf die Gefahr, Opfer dieses kriminellen Ausspähversuches zu werden. Neben der Beherzigung vorgenannter Hinweise bietet auch darauf ausgerichtete Hardware nachhaltigen Schutz gegen derartige und ähnlich gelagerte Phishing-Angriffe. Exemplarisch sei hier noch das *„Pharming"* genannt, bei dem die DNS-Anfragen von Webbrowsern, z.B. durch DNS-Spoofing, so manipuliert werden, dass der User auf gefälschte Websites umgelenkt wird. Darüber hinaus können die Bürger sich natürlich auch bei den Fachberatern der Kriminalpolizeilichen Präventionsdienststellen informieren.

3.2 Ransomware

Wurden bei den bisherigen Betrachtungen Straftaten in den Vordergrund gestellt, die durch Erschleichen persönlicher Daten des Bürgers mittels Internet diesen finanziell schädigen, soll auch auf eine andere, *„Ransomware"* genannte Art der Malware eingegangen werden. Dabei gelingt es dem Kriminellen, den User dazu zu bewegen, eine bestimmte infizierte Seite zu öffnen, durch die dann ein Schadstoffprogramm bei ihm aufgespielt wird. Dies kann durch gezielte Täuschung, versehentlich oder auch aus Neugier geschehen. Danach ist ein Zugriff auf das Gerät in der Regel nicht mehr möglich. Erst nach Zahlung eines Lösegelds werden die Daten wieder freigegeben. Da, insbesondere auf dem wirtschaftlichen Sektor, im Falle eines Verlustes von Geschäftsdaten oder anderer wichtiger Informationen schwere finanzielle Einbußen die Folge sein können, wird dringend geraten, sich entsprechende Antivirenprogramme auf den Computer aufzuspielen.

4 Kinder und Jugendliche im Netz

Die meisten der Kinder und Jugendlichen in der heutigen Zeit sind wie selbstverständlich mit dem Computer und den sich damit ergebenden Möglichkeiten aufgewachsen. Natürlich ist es den jeweiligen Erziehungsberechtigten überlassen, inwieweit sie die Zugriffe ihrer Sprösslinge auf dieses Medium dulden bzw. beschränken. Es ist eine erfreuliche Tatsache, dass die mit dem Thema Computerprävention befassten Polizeibeamten immer wieder in Lehrerkonferenzen oder Elternversammlungen, aber auch zu Thementagen eingeladen werden, um dort die Möglichkeiten der dort anwesenden Personengruppen, ihre eigenen oder die ihnen anvertrauten jungen Menschen vor den möglichen Gefahren des Internets zu bewahren, darzulegen. Dabei ist die Erklärung der jeweiligen Modi Operandi von nicht unerheblicher Bedeutung. Nachfolgend soll kurz auf die häufigsten Delikte im Zusammenhang mit Minderjährigen eingegangen werden:

4.1 Soziale Netzwerke

Viele Kinder und Jugendliche haben Freude daran, sog. Soziale Netzwerke zu nutzen und sich in ihnen mit Gleichaltrigen über für diese Altersgruppen typische Themen auszutauschen. Dabei werden oft auch persönliche Daten preisgegeben sowie Bilder verschickt. Dies geschieht meist arglos und ohne daran zu denken, dass grundsätzlich auch die Gefahr besteht, dass andere, dem Absender unbekannte Personen, über welche Wege auch immer, an diese Angaben oder Fotografien gelangen und diese dann eventuell missbräuchlich verwenden können. Das kann später möglicherweise zu Unannehmlichkeiten für den betroffenen Minderjährigen führen, die er niemals in Erwägung gezogen hat. Aus diesem Grund, aber auch im Zusammenhang mit noch weiter aufgeführten Gefahren im Netz, wird Eltern, Lehrkräften sowie anderen Vertrauenspersonen der Kinder und Jugendlichen geraten, ihre Schutzbefohlenen auf solche Aktivitäten hinzuweisen und sie davon zu überzeugen, dass sie stets als vertrauensvolle Gesprächspartner zur Verfügung stehen. Im oben genannten Fall ist es z.B. wichtig, den jungen Menschen klar zu machen, dass sie möglichst wenig von sich preisgeben und sichere Passwörter wählen sollen, aber

auch, dass sie selbst, etwa durch das Verwenden von Lichtbildern Anderer, im Sinne des Urheber- und Persönlichkeitsrechts in einen strafbaren Bereich geraten können.

4.2 Cybermobbing und -grooming

Im Zusammenhang mit den unter 4.1 aufgeführten Fakten muss auch auf die Phänomene Cybermobbing und -grooming hingewiesen werden. Im ersten Fall werden junge Menschen, meist anonym, mittels in sozialen Netzwerken veröffentlichten Beschimpfungen, anderer Unflätigkeiten oder ungünstigen Fotos verunglimpft, was für diese Person oft zu schweren psychischen Belastungen bis hin zu weiteren Folgen wie Depression oder gar Suizidgedanken führen kann. Beim Cybergrooming wiederum versuchen Erwachsene, Kontakt zu Kindern oder Jugendlichen aufzubauen mit dem Ziel, ihre Opfer letztlich persönlich zu treffen, sie möglicherweise zu sexuellen Handlungen zu bewegen. Dies kann, selbst wenn es beim Versuch bleibt, beim Betroffenen zu schweren seelischen Schäden führen. Selbstverständlich gelten auch hier die im vorhergegangenen Unterpunkt benannten Verhaltenshinweise, verbunden mit dem sofortigen Abbruch der Chats sowie einer Strafanzeige.

4.3 „Abzocke" im Internet

Auch im Internet sind Betrüger unterwegs, die versuchen, User um ihr Geld zu bringen. Dabei lassen sich oft auch surfende Minderjährige dazu verleiten, auf verlockende Angebote hereinzufallen. Exemplarisch sei hier die scheinbar kostenlose Teilnahme an Gewinnspielen genannt, bei der sich hinterher herausstellt, dass dies keineswegs so ist. Hat der junge Mensch sich als volljährig ausgegeben und die AGB anerkannt, flattert dann eine Rechnung ist Haus, die meist so spät kommt, dass auch das Widerrufsrecht abgelaufen ist. Ebenso mit Vorsicht zu genießen sind besonders verlockende Verkaufsangebote, gerade wenn deren Lieferung gegen Vorkasse erfolgen soll. Oft geht die Ware danach beim Käufer niemals ein. Bezüglich dieser Betrugsmaschen sollte den jungen Menschen verdeutlicht werden, dass solche Angebote immer mit der gebotenen Skepsis zu betrachten sind und nie per Vorkasse bezahlt werden sollten, wobei auch Nachforschungen in Diskussionsforen häufig weitere Klarheit bezüglich der Seriosität des Verkäufers bringen können.

Über die angesprochenen Themen hält neben den polizeilichen Beratungsstellen auch das überörtliche ProPK (Programm Polizeiliche Kriminalprävention) unter dem Titel *„Klicks-Momente"* Informationsmaterial für interessierte Bürger bereit.[3]

Anmerkungen

1 Der Autor war als EKHK Leiter der Kriminalkommissariats für Kriminalprävention und Opferschutz (KK KP/O) beim Polizeipräsidium Duisburg.
2 PKS BKA für 2020, S. 22.
3 www.polizei-beratung.de/gefahren-im-internet.

Herausforderungen der Cyberkriminologie

Von Dr. Thomas-Gabriel Rüdiger, Oranienburg*

1 Digitaler Transformationsprozess

Kaum eine Entwicklung in den letzten Jahrzehnten hat vermutlich solch ein Potential grundlegende gesellschaftliche Transformationsprozesse auszulösen wie die allgegenwertige Digitalisierung. Dabei nur von Digitalisierung im Sinne einer Nutzung technischer Möglichkeiten und Geräte auszugehen, geht hierbei nicht weit genug. Vielmehr umfasst die Digitalisierung auch 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. Diese Kommunikation und Interaktion findet gegenwärtig vor allem über sog. Soziale Medien statt, diese stellen dabei eine Art Metabegriff für unterschiedlichste Formen von Programmen dar. Am ehesten kann man sich hierunter onlinebasierte Programme vorstellen, die eine Vernetzung und Kommunikation zwischen den Nutzern zu lassen. Diese Definition erfasst dann sowohl die klassische Vorstellung Sozialer Netzwerke wie Facebook, Instagram, TikTok oder Twitter, geht über Messenger wie Whatsapp, Telegram oder Kik und reicht bis zu dem hier klar dazu zählenden Bereich der Onlinespiele (Bayerl und Rüdiger 2017, 921 ff). Diese Medien sind schon lange kein Randphänomen mehr, sondern Menschen halten sich in diesen genauso selbstverständlich auf wie im öffentlichen Straßenverkehr.

2 Mediennutzung in Deutschland

Knapp 94% aller Deutschen ab 14 Jahren sollen in irgendeiner Form in diesem digitalen Raum unterwegs sein. Bei den 14- bis

49-jährigen sollen es 100% sein, bei den bis 69-jährigen 95% und bei den über 77-jährigen noch immer 77% (Krupp und Bellut 2021, S. 6). Täglich nutzen sogar 76% der Deutschen ab 14 Jahren das Internet, was in etwa 54 Millionen Menschen entspricht (Beisch und Koch 2021, S. 488). Bei der Internetnutzung spielen auch in Deutschland die Sozialen Medien eine wichtige Rolle, diese werden von 59% der Bevölkerung ab 14 Jahren genutzt. Allein WhatsApp wird von 70% der Bevölkerung täglich genutzt. Bei der Nutzung Sozialer Medien zeichnet sich zudem eine gewisse Alterskluft ab, so nutzen in der Alterskategorie der 14- bis 29-jährigen 66% täglich Soziale Medien, bei den 50- bis 69-jährigen hingegen nur 17%. Als verbreitetes klassisches Soziales Medium, hat Instagram, das von 18% der Befragten täglich genutzt wird, mittlerweile Facebook abgelöst, dass nur von 15% am Tag noch angesteuert wird. Trotz der medialen Präsenz von Twitter nutzen es nur 2% der Befragten, genauso viele wie Twitch, eine Plattform auf der primär Gamingsessions gestreamt werden (Beisch und Koch 2021, S. 498). Alleine die 14- bis 29-jährigen nutzen Onlinemedien mittlerweile 269 Minuten also fast 5 Stunden am Tag (Beisch und Koch 2021, S. 491). Dabei ist diese Entwicklung nicht nur auf Jugendliche und Erwachsene beschränkt. Bereits im Jahr 2014 nutzten 25% der Kinder von 6 bis 7 Jahren zumindest selten das Internet. Mittlerweile sind es in dieser Alterskategorie 34%, bei den 8- bis 9-jährigen sind es sogar 60% und bei den 12- bis 13-jährigen kann mit 97% von einer Vollabdeckung gesprochen werden. Im Durchschnitt nutzen 82% der Kinder unter 14 Jahren mehrmals das Internet in der Woche (Feierabend et al. 2020, S. 37). Auch in diesen Altersstufen ist WhatsApp das wichtigste Soziale Medium und wird von 53% der Kinder täglich und 68% zumindest mehrmals in der Woche genutzt. Weitere 59% nutzen Youtube, 20% Instagram und Snapchat (Feierabend et al. 2020, S. 39). Nach der *„Mediensuchtstudie 2020"* der DAK ist die Nutzungszeit Sozialer Medien bei Minderjährigen um 66% von 115 auf 192 Minuten täglich angestiegen (Bodanowitz und Scharf 2020, S. 10). Es erscheint daher nicht unrealistisch anzunehmen, dass viele Menschen über alle Altersgrenzen hinweg spätestens im Rahmen der Corona-Einschränkungen täglich mehr Zeit in der digitalen Sphäre verbringen als im gesamten physischen Straßenverkehr.

3 Cyberkriminologische Betrachtung eines globalen digitalen Raums

Ein Grundgedanke der Kriminalwissenschaft ist, dass Kriminalität und normenabweichendes Verhalten immer aus einer Interaktion und Kommunikation zwischen Menschen entsteht. Das gleiche gilt im Umkehrschluss auch für die Normengenese und Formen der Normendurchsetzung. Eine Gemeinschaft einigt sich durch unterschiedliche Prozesse auf gemeinsame Verhaltensweisen und darauf, dass diese dann bei Bruch der Regeln auch durchgesetzt und geahndet werden oder im Falle von einer Neubetrachtung zu Legalisierungen führen. Hierfür braucht es einerseits das Verständnis, dass man sich als eine Gemeinschaft definiert und damit die Regeln akzeptiert. Andererseits müssen die Gruppenmitglieder zumindest rudimentär wissen welchen Regeln sie konkret unterliegen. Eine Thematik die sich auch im sog. Bestimmtheitsgebot als Ausformung des Art. 20 Abs. 3 GG widerspiegelt. Ein hierzu notwendiges und gleichzeitig naheliegendes Grundkonstrukt ist es, dass ein Mensch weiß in welchem Land er sich aufhält und welchen Regeln er damit auch unterliegt. Dies wird faktisch auch dadurch gewährleistet, dass ein Mensch – je nach Konstellation – physische Landesgrenzen überqueren muss und dadurch ahnt, dass er neuen Regeln unterliegt. Auch die Kriminalwissenschaft hat hierbei die leichte Tendenz, die Betrachtung von Kriminalität auf das jeweilige nationale Verständnis von unterschiedlichen Deliktsformen auszurichten.

Das Konzept, dass Menschen wissen sie befinden sich physisch an einem Ort und unterliegen dessen Gesetzen, findet aber seine Grenze im digitalen Raum. Denn das Kennzeichen vor allem von Sozialen Medien, Onlinegames und Co. ist gerade die Schaffung einer prinzipiell globalen und grenzfreien Vernetzungs- und Kommunikationssphäre. Diese Globalität des digitalen Raums kennt aber im Gegenzug keine sichtbaren virtuellen Landesgrenzen in sozialen Medien und im Internet im Allgemeinen, die man überschreiten könnte. Dies bedeutet faktisch auch, dass die moralischen und damit auch rechtlichen Vorstellungen unterschiedlichster Länder in derselben Sphäre aufeinandertreffen. Genauer die Menschen, die durch diese Vorstellungen geprägt wurden, nun aber ihre eigenen Vorstellungen in diesem Raum transportieren, ohne das klar definiert ist, wer welchem Recht in welchem Moment eigentlich unterliegt. Was in dem einen Land in den Sozialen Medien strafbar sein könnte, könnte in dem anderen Land, vielleicht überhaupt nicht gesetzlich geahndet werden.

Als ein Beispiel was damit gemeint ist könnte eventuell die Einordnung sog. *„Posingbilder"*, also Abbildungen von unnatürlichen Köperhaltungen von Kindern in teils bekleideten oder unbekleideten Zustand, als kinderpornographische Inhalte herangezogen werden. Hierunter können beispielsweise entsprechende Inhalte von Kindern in Unterwäsche fallen. Spätestens seit der Reform des § 184b StGB im Jahr 2014/2015 sind solche Abbildungen in § 184b Abs. 1 Nr. 1 StGB als strafbar einzuordnen. Für einige immer wieder überraschend sind kinder- oder auch jugendpornographische Inhalte nicht nur auf das Darknet beschränkt. Nach einer Analyse im Rahmen des Projekts Arachnid des Canadian Centre for Child Protection (CSAM) waren 97% der festgestellten Missbrauchsabbildungen im Clearweb abgelegt und nicht im Darknet (CSAM 2021, S. 2). In letzter Zeit wird immer klarer, dass Missbrauchsabbildungen auch in Sozialen Medien zu finden und über Messenger geteilt werden. In den USA können Missbrauchsabbildungen, auf die Nutzer stoßen, über die Meldefunktion *„CyberTipline"* des National Center for Mising & Exploited Children (NCMEC) gemeldet werden, die nach einer Prüfung die Informationen an Sicherheitsbehörden auch in Deutschland weitermelden. Im Jahr 2020 gab es hierüber etwa 22 Millionen Meldungen, etwa 100.000 davon entfielen auf Deutschland (NCMEC 2021b). Von diesen 22 Millionen Meldungen betrafen knapp 90% die Social Media Programme von Meta (früher Facebook), also Facebook, Instagram und WhatsApp. Die Problematik von Missbrauchsabbildungen in Sozialen

Medien greift daher auch die polizeiliche Prävention durch entsprechende Kampagnen auf (ProPK 2021).

Hier schließt sich nun der gedankliche Kreis. Es gibt nämlich keine weltweit absolut gültige Definition von kinderpornographischen Inhalten. Das bedeutet, dass beispielhaft ein Nutzer auf einer Social Media Plattform ein problematisches Bild eines Kindes sehen könnte, dass in Deutschland z.B. als Posingbild qualifiziert wird, aber in dem Land in dem der Nutzer das hochgeladen hat, vielleicht gar keine strafrechtliche Relevanz hat. Dadurch kann theoretisch die Situation eintreten, dass Nutzer aus dem einen Land sich fragen, warum offenbar andere völlig unproblematische aus ihrer Sicht strafbare Handlungen posten können. Wessen strafrechtliche Wertevorstellung sollen dann in Sozialen Medien eigentlich greifen?

4 Ein globales digitales Strafrecht?

Faktisch bräuchte ein globaler digitaler Raum auch ein gemeinsames globales Strafrecht, dass eine weitestgehend akzeptierte Wertevorstellung umfasst. Die Forderung eines globalen Strafrechts für den digitalen Raum ist dabei nicht neu, auch wenn es offenbar nicht mehr sehr präsent ist. Bereits im Jahr 2000 hat der damalige deutsche Innenminister Schily im Rahmen von Angriffen durch den Email Wurm *„ILOVEYOU"* ein globales Strafrecht für das Internet gefordert und schon zu dem Zeitpunkt betont, dass das Internet kein rechtsfreier Raum sei (Kuri 2000). Erst jüngst hat sich die mangelnde Durchsetzungsmöglichkeiten eines nationalen Staates auf den global agierenden Messenger *„Telegram"* mit Sitz in Dubai gezeigt (Hoven 2021). Dieser reagiert schlicht nicht auf Anfragen des deutschen Staates im Zusammenhang mit der Bekämpfung von Hasskriminalität bzw. der Erfassung als Soziales Netzwerk nach dem Netzwerkdurchsetzungsgesetz (NetzDG) und zeigt sich auch nicht sehr kooperativ in der Zusammenarbeit mit deutschen Sicherheitsbehörden (Metzger 2021). Dies zeigt auch im Umkehrschluss auf, dass die Durchsetzung nationaler Regeln doch stark auf ein *„good will"* der beteiligten Firmen angewiesen ist, wenn das aber nicht vorhanden ist wird es schwierig. Gleichzeitig nutzen aber bereits 2019 etwa 8 Millionen Deutsche auch Telegram (Mehner 2021). Dabei werden die Telegram Nutzer hier auch mit problematischen Inhalten konfrontiert, sehen gleichzeitig aber, dass gerade die Sicherheitsbehörden offenbar kaum in der Lage sind hier Regeln durchzusetzen. Während die Menschen also physisch in dem einen Land sind und eigentlich wissen, dass sie dessen Regeln unterliegen, sind sie im virtuellen gleichzeitig in einer eigenständigen Sphäre unterwegs, in welcher der Staat wesentlich geringere Durchsetzungsmöglichkeit hat oder die vorhandenen nur selten anwendet.

5 Normalität digitaler Delikte?

Neben einer Vielzahl an Auswirkungen dieser Globalität auf die gefühlte und tatsächliche Strafverfolgungswahrscheinlichkeit im digitalen Raum, soll hier ein besonderer Punkt angesprochen werden. Die nur geringe Durchsetzung von nationalen Regeln, wird jedem Nutzer vermutlich nicht selten bei seiner täglichen Internetnutzung präsentiert. Bereits ein Blick in den Spamordner, konfrontiert viele Nutzer tagtäglich mit versuchten Betrugsdelikten in Form von Phishing-Emails. Eine Erhebung von Statista im Auftrag der Internet-Sicherheitsfirma GData ergab, dass 31% der Internetnutzer angaben, bereits Opfer von einer Phishing-Email geworden zu sein (GData 2021). Eine Studie der Bitkom ergab, dass sich die Anzahl der Nutzer, die noch nie Erfahrungen mit Kriminalität im Netz gemacht haben, seit 2018 von damals noch 40% auf nur noch 21% im Jahr 2021 fast halbiert hat (Bitkom 2021). Nach derselben Studie stieg zudem die Konfrontation mit digitaler Hasskriminalität an. Gaben 2020 nur 6% der Nutzer an damit selbst Erfahrung gemacht zu haben, waren es 2021 bereits 14% (Bitkom 2021). Besonders bedenklich sind in diesem Zusammenhang auch die Ergebnisse der JIM-Studie 2021, nach der 58% der befragten Minderjährigen von 12 bis 19 Jahren in einem Monat mit Hassbotschaften und 56% mit *„extremen politischen Ansichten"* konfrontiert wurden (Feierabend et al. 2021, S. 62). Gleiches gilt auch für den Bereich der sexuellen Übergriffe, denen sich Minderjährige im Netz ausgesetzt sehen. Hier sticht vor allem Cybergrooming, also die onlinebasierte Anbahnung oder Intensivierung eines sexuellen Kindesmissbrauchs, hervor (Bruhn et al. 2021, S. 120; Rüdiger 2020). Eine repräsentative Studie der Landesanstalt für Medien NRW kommt für das Jahr 2021 zu dem Ergebnis, dass knapp jeder vierte befragte Minderjährige onlinebasierte Kontaktanbahnungen durch Erwachsene mit dem Ziel eines Treffens erlebt hat. Konkret berichteten 9% der 8- bis 9-jährigen, 14% der 10- bis 12-jährigen und 25% der 13- bis 15-jährigen sowie knapp 40% der 16- bis 18-jährigen von solchen Kontaktanbahnungen (Nennstiel und Isenberg 2021). Ähnlich viele Minderjährige haben auch erlebt, dass Erwachsene ihnen im Netz im Austausch für Bilder von ihnen beispielhaft virtuelle Items in Onlinespielen verspochen haben (Nennstiel und Isenberg 2021, S. 20). Auch wenn juristisch Cybergrooming unter § 176a Abs. 1 Nr. 3 und § 176b Abs. 1 StGB nur Kinder als Betroffene erfasst, sind dies aber Zahlen, die sich bereits länger in unterschiedlichen Studien mit ähnlichen Konfrontationshöhen widerspiegeln und es deutet viel auf eine erlebte Normalität dieser Übergriffe im Netz hin (Rüdiger 2020). Man kann es auch anders formulieren, bereits seit einiger Zeit werden Minderjährige und damit mittlerweile auch junge Erwachsene zumindest teilsozialisiert in einem digitalen Raum, der offenbar geprägt ist von diesem Erleben der Konfrontation mit Kriminalität und Normenbrüchen. Sie sind quasi mit einer Art Unrechtskultur im digitalen Raum aufgewachsen (Rüdiger 2019). Was dies eigentlich für Auswirkungen auf diese Generationen hatte und hat, ist bisher überraschenderweise weitestgehend unerforscht.

6 Hat die digitale Kriminalitätstransparenz Auswirkungen auf das Sicherheitsgefühl der Menschen?

All diese Deliktsformen haben zumindest eine Besonderheit sie machen Kriminalität im Netz für die Nutzer transparent und zeigen gleichzeitig, dass offenbar viele TäterInnen keine allzu große Angst vor einer Strafverfolgung haben müssen, sonst würden sie ja vermutlich nicht mit so viele Delikten stetig konfrontiert werden. Kriminalität im Netz wird also in einer Form für die Nutzer wahrnehmbar, wie sie es aus dem physischen Raum in dieser Omnipräsenz nicht kennen. Das Ergebnis hiervon ist offenbar das Gefühl, dass der Rechtsstaat im Netz weitestgehend versagt. Im Rahmen der bereits zitierten Bitkom Studie stieg der Anteil derjenigen die mehr Angst vor Kriminalität im Netz, als vor solcher im analogen Raum haben, von 39% im Jahr 2020 auf 48% im Jahr 2021 (Bitkom 2021). Man könnte es vermutlich auch anders formulieren, die Frage, ob Menschen Kriminalitätsfurcht haben, scheint immer mehr von ihrem Onlineerleben beeinflusst zu werden. Demgemäß glauben auch

nur 6%, dass *„Internetkriminalität in der öffentlichen Debatte übertrieben dargestellt"* werde (Bitkom 2021).

Vielleicht ist diese Situation auch eine der Erklärungen dafür, warum seit Jahren eine Diskrepanz zwischen polizeilich registrierten Anzeigen (die an die Staatsanwaltschaft abgegeben werden) (PKS) und dem Sicherheitsgefühl der Menschen in Deutschland besteht (vgl. hierzu u.a. Bruhn et al. 2021). Nach einer Studie der Konrad Adenauer Stiftung gehen Ende 2021 52% der dort Befragten davon aus, dass Kriminalität in Deutschland in den letzten fünf Jahren etwas (36%) bis stark (26%) zugenommen hat (Konrad Adenauer Stiftung 2021). Teilweise scheint in der Innenpolitik ein Art Unverständnis zu herrschen, warum die Leute eigentlich eine so *„falsche Wahrnehmung"* von Kriminalität haben, wenn diese doch vermeintlich zurückgeht.

Tatsächlich verzeichnet die PKS seit dem Jahr 2015 einen kontinuierlichen Rückgang von 6.330.649 Fällen auf 5.310.621 Fälle im Jahr 2020, was einer Verminderung von etwas über 16% der angezeigten Handlungen entspricht (BMI 2021b). Diese ist insofern überraschend, da im selben Zeitraum die Bevölkerungszahl Deutschlands mit etwa 83,1 Millionen Einwohnern im Jahr 2021 stetig angestiegen ist und mittlerweile einen Höchststand erreicht hat (Statistisches Bundesamt 2021). Dieser Deliktsrückgang gilt jedoch nicht für Delikte im Zusammenhang mit dem Tatmittel Internet.

Bereits im ersten Halbjahr 2021 sollen so viele kinderpornographische Delikte bei der Polizei zur Kenntnis gekommen sein wie die gesamte Polizeiliche Kriminalstatistik (PKS) 2020 zu registrieren hatte (Welle 2021). Dabei hatte die PKS 2020 mit 18.761 Fällen bereits einen signifikanten Anstieg, um knapp 55% im Verhältnis zu 2019 mit 12.262 Fällen, zu verzeichnen (BMI 2021b). Sollte sich diese Entwicklung tatsächlich bewahrheiten, würden sich die Fallzahlen in der PKS 2022 bei etwa 40.000 Fällen einpegeln. Noch im Jahr 2015 lagen die Fallzahlen bei lediglich 5.687, dies würde, wenn es so eintritt, also einen Anstieg von etwa 600% seit dem bedeuten. Entsprechend warnt der Präsident des Bundeskriminalamt auch davor, dass *„die deutliche Zunahme solcher Fälle die Polizei zunehmend an Kapazitätsgrenzen bringen (wird) … "* (Welle 2021). Dabei muss davon ausgegangen werden, dass diese Entwicklung vornehmlich durch internetbasierte Modi Operandi getragen wird. Von den 18.761 Fällen in der PKS 2020 wurden 12.516 über das Tatmittel Internet begangen, auch der Anstieg der internetbasierten Delikte entspricht 56% und ähnelt damit dem Anstieg der Gesamtzahlen in diesem Bereich (BMI 2021a). Dieser Anstieg ist sicherlich auch auf die oben beschriebenen automatischen Meldungen über die Cybertipline von NCMEC zurückzuführen (NCMEC 2021a).

7 Braucht es im Netz eine nutzerfreundliche Anzeigemöglichkeit?

Zumindest teilweise kann der Rückgang der PKS Fallzahlen in den letzten Jahren offenbar damit erklärt werden, dass die Menschen im analogen öffentlichen Raum immer weniger Zeit verbringen. Damit sinkt auch das Risiko, dass hier Kriminalität, bspw. Straßenkriminalität, begangen werden kann. Faktisch auch weil potentielle TäterInnen und Opfer weniger Möglichkeiten haben aufeinanderzutreffen. Parallel verbringen die Menschen aber immer mehr Zeit im digitalen Raum und werden hier einerseits mit Kriminalität konfrontiert und es bieten sich ihnen andererseits auch Möglichkeiten zu einfachen Tatbegehungen, dank einer niedrigen Tatbegehungsschwelle. Ein Grundproblem hierbei ist, dass die sog. Dunkelzifferrelation, also das Verhältnis zwischen einem Delikt im Hell- und Dunkelfeld, wesentlich ungünstiger ist als bei klassischen analogen Delikten (Rüdiger 2021). Das Ergebnis ist, dass das Hellfeld analoger Delikte sinkt, das Dunkelfeld digitaler Delikte aber im Gegenzug nur minimal aufgehellt wird. Diese Situation aufzubrechen, würde eine Erhöhung der Anzeigewahrscheinlichkeit erfordern. Dies kann entweder dadurch geschehen, dass den Nutzern verdeutlicht wird, wann es sich um Straftaten handelt und dass sich eine Anzeige auch lohnt. Dies könnte beispielhaft mit niederschwelligen Anzeigemöglichkeiten im Netz ermöglicht werden. So ist es wenig verständlich, warum in einem globalen digitalen Raum jedes Bundesland eine eigene Internet- oder Onlinewache unterhalten muss, anstatt eine Art Single Point of Contact Möglichkeit für Anzeigen über digitale Wege anzubieten. Auch kann hinterfragt werden, ob die Anzeigemöglichkeit über diese virtuellen Wachen *„nutzerfreundlich"* gestaltet oder doch eher kompliziert vom Mechanismus her sind. So fehlt es faktisch an einer Art rund um die Uhr besetzten virtuellen Anzeigeraum, bei dem auch Onlinenutzer direkt mit Polizeiangehörigen per Chat kommunizieren können. Also ähnlich wie es auf den meisten Polizeiwachen ja möglich ist. Auch existieren keine sich speziell an die Bedürfnisse von Kindern ausgerichtete Kontaktmöglichkeiten im digitalen Raum zur Polizei. Beispielhaft eine Kinderonlinewache, die rund um die Uhr mit Fachpersonal aus verschiedenen Bereichen besetzt ist und eine Chatmöglichkeit für Kindern gerade in Zeiten von Homeschooling bietet. Selbst viele offizielle polizeiliche Social Media Accounts beispielhaft auf Instagram, die für eine Kontaktaufnahme durch Nutzer aber vor allem Minderjährige in Frage kämen, beinhalten in ihren Profilen den Hinweis *„keine Anzeigen"* (@Polizeiberlin 2021), *„keine Anzeigenerstattung & DM"* [gemeint ist Kontaktmöglichkeit über *„direct messenger"*] (@bremenpolizei 2021), oder gleich den Hinweis *„Nachrichten werden nicht gelesen!"* (@polizeisachsen 2021). Hintergrund dieser Hinweise und einer offenbar vorhandenen Form von Kommunikationsunlust der Sicherheitsbehörden im digitalen Raum ist vermutlich eine gewisse Skepsis vor einer Überforderung mit der Sichtung von Anfragen und den damit einhergehenden Personalbedarf, ausgelöst auch aus der weitestgehenden absoluten Gültigkeit des Legalitätsprinzips.

Welche Außenwirkung dies aber z.B. auf Minderjährige haben könnte, die gerade in ihrer digitalen Lebenssphäre Hilfe suchen, wurde noch nicht hinterfragt. Im Rahmen der oben bereits zitierten Studie zu Cybergrooming wurde auch herausgearbeitet, dass lediglich 9,6% der betroffenen Minderjährigen das Verhalten bei der Polizei zur Anzeige bringen würde (Nennstiel und Isenberg 2021, S. 34). Umso wichtiger wäre es, die Kommunikationsschwelle mit der Polizei und damit auch die Möglichkeit der Anzeigenerstattung allgemein im Netz niedrig zu halten, oder anders ausgedrückt nutzerfreundlich.

Eine weitere Möglichkeit wäre, dass die Polizei selbst im Netz aktive zufällige Präsenz zeigt, also auf eine Art virtuelle Streife geht und dabei die dort selbst festgestellten Straftaten zur Anzeige bringt. Teilweise finden solche Maßnahmen im Sinne der sog. *„anlassunabhängigen Internetrecherche"* zumindest punktuell, wenn auch verdeckt, statt (LKA NRW 2021). Eine belastbare Aussage über die Anzahl von deutschen Polizeiangehörigen, die in dieser Form im Netz dienstlich auf Streife gehen ist für die letzten Jahre nicht eruierbar, es lässt sich aber vermuten, dass diese nicht allzu hoch sein dürfte. Schilderungen deuten zudem daraufhin, dass wenn sie durchgeführt werden, solche Streifen nicht als Hauptaufgabe gesehen werden, sondern offenbar nur als eine Art *„Nebenbei"*. Im Kontext einer TV-Dokumentation zu den Auswirkungen

der Aufstufung des § 184b StGB zu einem Verbrechenstatbestand, äußerten Kriminalbeamte, dass sie vor allem durch die Zunahme an kinderpornographischen Medien gar nicht mehr in der Lage sind gegen das Phänomen Cybergrooming aktiv selbst vorzugehen: *„Dazu haben wir keine Zeit. Das bearbeiten wir im Zweifel erst, wenn tatsächlich schon etwas passiert ist"* (NDR 2021). Ein proaktives Vorgehen über sog. polizeiliche Scheinkindoperationen – wenn sich also Polizisten im Netz als Kinder ausgeben, um TäterInnen zu überführen (Rüdiger 2020) – um die Taten im Vorfeld zu verhindern, findet demnach weitestgehend gar nicht statt. Im übertragenen Sinne bedeutet es, dass der Fensterwurf nicht verhindert wird, sondern nur die Scherben aufgekehrt werden. Konkret vorzuwerfen ist dies nicht, scheint es doch ein Symptom eines strukturellen Problems der Adaption der Mechanismen des digitalen Raums durch die Sicherheitsbehörden zu sein.

8 Es braucht eine echte digitale Polizeistrategie

In Kombination mit der Warnung des BKA-Präsidenten vor einer Überforderung der Kapazitäten der Sicherheitsbehörden bei kinderpornographischen Inhalten, den hohen Fallzahlen bei digitalen Delikten im Allgemeinen und Schilderungen wie in dem vorhergehenden Beispiel entsteht das Bild, dass die Sicherheitsbehörden gegenwärtig nur gering aktiv sein können, um selbst Straftaten aufzudecken und in der Folge dann auch verfolgen zu müssen. Denn je mehr die Sicherheitsbehörden investieren würden, umso mehr Anzeigen würde es – auch ganz in Anlehnung nach dem Lüchow-Dannenberg Syndrom – geben. Eine Situation die innenpolitisch auch ausgehalten werden müsste. Dazu kommt, dass die bisherigen Formen von Präsenz bei virtuellen Streifen für die Nutzer weitestgehend nicht erkennbar sind, die generalpräventive Wirkung, die beispielsweise durch Uniformen und Streifenwagen im Straßenverkehr entstehen, können so offenbar gar nicht erst im digitalen Raum greifen. Ohne diese Wirkung aber, könnten die Sicherheitsbehörden vermutlich noch so viel Personal im Netz einsetzen, ohne einen allzu großen Effekt zu haben. Denn dieser Raum besteht ja nicht nur aus deutschen Nutzern, sondern faktisch aus den weltweiten Internetnutzern. Dies zeigt sich gegenwärtig offenbar bei der digitalen Hasskriminalität, bei der sich trotz aller polizeilichen und kriminalpolitischen Maßnahmen die Situation, wie die dargestellte Studienlage zeigt, noch weiter verschlechtert hat.

Im digitalen Raum scheint eine Situation eingetreten zu sein, nach der Kriminalität so sichtbar wird, dass das von Popitz beschriebene Prinzip der *„Präventivwirkung des Nichtwissens"*, nach der das Vorhandensein eines Dunkelfelds einen normenstabilisierenden Faktor einnimmt, durchbrochen zu sein scheint (Rüdiger 2021). Das bedeutet, dass sich die Sicherheitsbehörden grundlegenden auch strukturellen Herausforderungen stellen müssen. Welche Aufgabe können sie wie in einem globalen digitalen Raum mit weltweiten Internetnutzern wahrnehmen, in dem Kriminalität für die Menschen transparent und wahrnehmbar wird, und gleichzeitig die Mechanismen der Normenkontrolle (noch) kein Gegengewicht bilden. Hier gibt es keine einfachen Antworten nach dem Motto, ich bilde mal X *„Cybercops"* aus oder engagiere einige ExpertInnen. Wenn die Sicherheitsbehörden ihre Funktion als Normenkontrolle im Netz nicht vollends an große digitale Plattformen wie Meta verlieren wollen, dann braucht es jetzt die Entwicklung einer echten zukunftstragenden Polizeistrategie für einen digitalen Raum, die sich als Teil einer grundlegenden kriminalpolitischen, eventuell sogar globalen Neuausrichtung sieht. Diese Strategie darf dann auch nicht davor zurückscheuen, Fragen wie die Relevanz einer auf örtlicher Zuständigkeit basierenden polizeilichen Gefahrenabwehr im digitalen Raum, die absolute Gültigkeit des Legalitätsprinzips vor dem Hintergrund der Masse der digitalen Delikte und der damit erschwerten Schwerpunktsetzung, oder auch die nach der Sinnhaftigkeit einer föderativen Polizeistruktur in diesem Raum, zu stellen.

Seit etwa 10 Jahren war diese Entwicklung absehbar (Denef und Rüdiger 2013), es sollte nicht ein weiteres Jahrzehnt dauern bis man erkennt, dass es sich nicht einfach nur um *„neue"* Kriminalitätsphänomene, sondern um einen gänzlich eigenständigen polizeilichen Einsatzraum handelt, der in einer Wechselwirkung mit dem analogen steht, aber dennoch auch etwas eigenständiges ist. Wenn es schon nicht bei den vergangenen Generationen geglückt ist, sollten doch zukünftige Generationen davor bewahrt werden, in einer Art anomischen digitalen Raum teilsozialisiert zu werden. Das erfordert eine Kraftanstrengung, die es aber wert sein wird.

Bildrechte: Landespolizeiamt Schleswig-Holstein.

Literaturverzeichnis

@bremenpolizei (2021): Instagram Account. Online verfügbar unter https://www.instagram.com/bremenpolizei/, zuletzt aktualisiert am 22.12.2021, zuletzt geprüft am 22.12.2021.

@Polizeiberlin (2021): Instagram Account. Online verfügbar unter https://www.instagram.com/polizeiberlin/, zuletzt aktualisiert am 22.12.2021, zuletzt geprüft am 22.12.2021.

@polizeisachsen (2021): Instagram Account. Online verfügbar unter https://www.instagram.com/polizeisachsen/, zuletzt aktualisiert am 22.12.2021, zuletzt geprüft am 22.12.2021.

Bayerl, P. Saskia; Rüdiger, Thomas-Gabriel (2017): Die polizeiliche Nutzung sozialer Medien in Deutschland: Die Polizei im digitalen Neuland. In: Jürgen Stierle, Dieter Wehe und Helmut Siller (Hg.): Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft - Polizeipraxis. Wiesbaden: Springer Gabler (SpringerLink Bücher), S. 919–943.

Beisch, Natalie; Koch, Wolfgang (2021): 25 Jahre ARD/ZDF-Onlinestudie: Aktuelle Aspekte der Internetnutzung in Deutschland. In: Media Perspektiven (10/2021), S. 486–503.

Bitkom (2021): Acht von zehn Personen werden Opfer von Internetkriminalität. In: Bitkom e.V., 2021. Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/IT-und-Cybersicherheit-2021, zuletzt geprüft am 20.12.2021.

BMI (2021a): Polizeiliche Kriminalstatistik 2020. Grundtabelle 05 - Tatschlüssel 143200. Online verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/BundFalltabellen/bundfalltabellen.html?nn=145506.

BMI (2021b): Polizeiliche Kriminalstatistik 2020. Zeitreihe 01 - Tatschlüssel 143200. Online verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2020/PKSTabellen/Zeitreihen/zeitreihen_node.html.

Bodanowitz, Jörg; SCharf, Rüdiger (2020): Mediensucht 2020. Gaming und Social Media in Zeiten von Corona. DAK Forschung. Online verfügbar unter https://www.dak.de/dak/gesundheit/dak-studie-gaming-social-media-und-corona-2295548.html#/.

Bruhn, Heike; Church, Daniel; Rau, Matthias; Vogeler, Lena; Wilms, Yvonne (2021): Dritter Periodischer Sicherheitsbericht. Hg. v. Bundesminsiterium des Inneren, für Bau und Heimat und Bundesministerium der Justiz und für Verbraucherschutz. Online verfügbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PeriodischerSicherheitsbericht/periodischersicherheitsbericht_node.html.

CSAM (2021): PROJECT ARACHNID: ONLINE AVAILABILITY OF CHILD SEXUAL ABUSE MATERIAL. An analysis of CSAM and harmful-abusive content linked to certain electronic service providers. Online verfügbar unter https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/.

Denef, Sebastian; Rüdiger, Thomas-Gabriel (2013): Soziale Medien – Muss sich die Polizei neu ausrichten? In: Deutsche Polizei 11/2013, S. 4–12.

Feierabend, Sabine; Rathgeb, Thomas; Kheredmand, Hediye; Glöckler, Stephan (2020): KIM 2020. Kindheit, Internet, Medien - Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland. Online verfügbar unter https://www.mpfs.de/studien/kim-studie/2020/.

Feierabend, Sabine; Rathgeb, Thomas; Kheredmand, Hediye; Glöckler, Stephan (2021): JIM-Studie 2021. Jugend, Information, Medien. Online verfügbar unter https://www.mpfs.de/studien/jim-studie/2021/.

GData (2021): Cybersicherheit – Zahl der Woche: Jede dritte Familie ist bereits einer Phishing-Mail zum Opfer gefallen. Online verfügbar unter https://www.gdata.de/news/2021/12/37171-cybersicherheit-jede-dritte-familie-ist-bereits-einer-phishing-mail-zum-opfer-gefallen, zuletzt aktualisiert am 20.12.2021, zuletzt geprüft am 20.12.2021.

Hoven, Elisa (2021): „Reagiert Telegram wie bisher nicht auf die deutschen Behörden, sind die derzeit möglichen juristischen Wege erschöpft". Online verfügbar unter https://

nachrichten.idw-online.de/2021/12/16/reagiert-telegram-wie-bisher-nicht-auf-die-deutschen-behoerden-sind-die-derzeit-moeglichen-juristischen-wege-erschoepft/, zuletzt aktualisiert am 16.12.2021, zuletzt geprüft am 16.12.2021.

Konrad Adenauer Stiftung (2021): Wenn es Nacht wird in Deutschland. Ergebnisse einer repräsentativen Umfrage zu Kriminalitätsangst und der Akzeptanz von Maßnahmen gegen Kriminalität.

Krupp, Manfred; Bellut, Thomas (2021): ARD/ZDF-Onlinestudie 2021. Kompakte Präsentation. ARD ZDF. Online verfügbar unter https://www.ard-zdf-onlinestudie.de/files/2021/ARD_ZDF_Onlinestudie_2021_Publikationscharts_final.pdf.

Kuri, Jürgen (2000): Bundesregierung: Globales Strafrecht gegen Internet-Kriminalität. In: heise online, 10.05.2000. Online verfügbar unter https://www.heise.de/newsticker/meldung/Bundesregierung-Globales-Strafrecht-gegen-Internet-Kriminalitaet-20444.html, zuletzt geprüft am 16.12.2021.

LKA NRW (2021): Schriftliche Anhörung von Sachverständigen durch die Kommission zur Wahrnehmung der Belange der Kinder des Ausschusses für Familie, Kinder und Jugend des Landtags Nordrhein-Westfalen „Polizei und Justiz". Stellungnahme 17/4176. Online verfügbar unter https://polit-x.de/de/documents/6074495/bundeslander/nordrhein-westfalen/landtag/ausschusse/stellungnahme-2021-08-25-polizei-und-justiz-schriftliche-anhorung-der-kommission-zur-wahrnehmung-der-belange-der-kinder-des-ausschusses-fur-familie-kinder-und-jugend.

Metzger, Nils (2021): Zwischen Extremismus und Geschäftsinteresse. In: Digitales, 16.01.2021. Online verfügbar unter https://www.zdf.de/nachrichten/digitales/telegram-wachstum-extremismus-werbung-100.html, zuletzt geprüft am 16.12.2021.

NCMEC (2021a): 2020 Reports by Electronic Service Providers (ESP).

NCMEC (2021b): Reports by Country. Online verfügbar unter https://www.missingkids.org/gethelpnow/cybertipline, zuletzt aktualisiert am 02.12.2021, zuletzt geprüft am 16.12.2021.

NDR (2021): Sexuelle Gewalt gegen Kinder - wo bleibt die Hilfe? Online verfügbar unter https://www.ndr.de/fernsehen/sendungen/45_min/Sexuelle-Gewalt-gegen-Kinder-wo-bleibt-die-Hilfe,sendung1204448.html.

Nennstiel, Sabrine; Isenberg, Meike (2021): Kinder und Jugendliche als Opfer von Cybergrooming. Zentrale Ergebnisse der 1. Befragungswelle 2021. Hg. v. Landesanstalt für Medien NRW. Online verfügbar unter https://www.medienanstalt-nrw.de/presse/pressemitteilungen-2021/2021/dezember/repraesentative-zahlen-zur-erfahrung-von-kindern-zwischen-8-und-18-jahren-mit-sexualisierter-ansprache-im-netz.html?fbclid=IwAR24lBWi-Z9dZjPJksJ0tV257tFtN13zbz4EKUUpN4IcMBadd6NrBgDD8Cc.

ProPK (2021): Kampagne gegen die Verbreitung von Kinderpornografie. Polizeiliche Kriminalprävention der Länder und des Bundes. Online verfügbar unter https://www.polizei-beratung.de/themen-und-tipps/sexualdelikte/kinderpornografie/die-kampagne/, zuletzt aktualisiert am 16.12.2021, zuletzt geprüft am 16.12.2021.

Rüdiger, Thomas-Gabriel (2019): Haben wir eine Unrechtskultur im digitalen Raum? In: Kriminalistik (01/2019), S. 37–43.

Rüdiger, Thomas-Gabriel (2020): Die onlinebasierte Anbahnung des sexuellen Missbrauchs eines Kindes: Verlag für Polizeiwissenschaft.

Rüdiger, Thomas-Gabriel (2021): Digitale Kriminalitätstransparenz. Von der Durchbrechung der „Präventivwirkung des Nichtwissens". In: Kriminalistik (2/2021), S. 72–78.

Statistisches Bundesamt (2021): Bevölkerung nach Nationalität und Geschlecht (Quartalszahlen). Online verfügbar unter https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/Tabellen/liste-zensus-geschlecht-staatsangehoerigkeit.html;jsessionid=FA2E4D117DF817E8C8305732F61D8851.live711, zuletzt aktualisiert am 07.07.2021, zuletzt geprüft am 11.11.2021.

Welle, Deutsche (2021): BKA: Kinderpornografie massiv gestiegen | DW | 07.11.2021. Deutsche Welle (www.dw.com). Online verfügbar unter https://www.dw.com/de/bka-kinderpornografie-massiv-gestiegen/a-59747468?maca=de-Twitter-sharing, zuletzt aktualisiert am 10.11.2021, zuletzt geprüft am 10.11.2021.

Anmerkungen

* Dr. iur. Thomas-Gabriel Rüdiger M.A. ist Akademischer Oberrat und Leiter des Instituts für Cyberkriminologie an der Hochschule der Polizei des Landes Brandenburg.

Aufgrund des Redaktionsschlusses des Artikels finden nur die Fallzahlen bis zur PKS 2020 Berücksichtigung.

Jahrhundert-Katastrophe im Ahrtal – „Hölle und Himmel am selben Fleck"

Von KD Thorsten Runkel, Mayen

1 Vorwort

Die Flutkatastrophe vom 14./15. Juli 2021 im Ahrtal löste europaweit große Betroffenheit aus. Ein Ereignis, mit dessen Ausmaß man nicht gerechnet hätte und das binnen Stunden das Leben einer ganzen Region verändert hat. Im Katastrophengebiet wurden auch Dienststellen der Polizeidirektion Mayen beschädigt, gar teilweise zerstört. Mehr als 40 Kolleginnen und Kollegen waren und sind unmittelbar, teils persönlich verhängnisvoll betroffen. Nicht nur die Polizei, auch die Menschen unserer vertrauten und verbundenen kommunalen Familie sind ebenso hart getroffen. Diese Schicksale haben sich nicht nur auf die Handlungsfähigkeiten ausgewirkt, sondern uns insbesondere vor Augen geführt, wie anfällig oder auch zerbrechlich unser Glück ist und der Wohlstand, den wir genießen.

In einem bisher noch nie dagewesenen Polizeieinsatz wurden innerhalb kürzester Zeit viele weitreichende Entscheidungen zum Wohle der Betroffenen notwendig. Entscheidungen für die es in der Ausnahmesituation auf allen Ebenen und in allen Phasen keine Blaupausen gab, an denen wir uns hätten orientieren können. Entscheidungen, die zügig, pragmatisch und zugleich mit großer Umsicht und Sorgfalt getroffen werden mussten.

„Die Kriminalpolizei" bat darum, einen Einblick in die Geschehnisse aus Sicht der betroffenen Polizeidirektion zu gewähren. Als Leiter der Polizeidirektion Mayen bin ich in der Alltagsorganisation (AAO) für das Ahrtal zuständig und komme der Bitte gerne nach. Die Erstmaßnahmen trafen die Menschen unserer Dienststellen vor Ort. Mit Fortgang der fürchterlichen Ereignisse übernahm ich gemäß Planentscheid die Führung des Einsatzabschnitts „Ereignisort" in der eingerichteten Besonderen Aufbauorganisation (BAO) „Ahr" unter der Führung von Polizeivizepräsident Jürgen Süs. Nach stufenweiser Rückführung endete die BAO nach 175 Tagen offiziell. Der Alltag kehrte damit bis heute weder für die Bevölkerung noch für die Kolleginnen und Kollegen vor Ort zurück. Die dargestellten Ereignisse und Aufgaben können vor dem Hintergrund des – zumindest regional gesehen – apokalyptischen Ausmaßes und der daraus folgenden Komplexität der Gesamtlage selbstverständlich stets nur zu kurz greifen – das ist zwangsläufig und dessen bin ich mir bewusst.

Foto: Verklausung – ohne Schwemmgut berechneten die Fachleute einen ca. 2 Meter geringeren Pegelstand.

2 Polizeidirektion Mayen

Die Polizeidirektion Mayen ist mit 1.728 Quadratkilometern die flächenmäßig größte von vier regionalen Direktionen des Polizeipräsidiums Koblenz. Ihr nachgeordnet sind die Polizeiinspektionen (PI) Mayen und Cochem sowie die drei besonders von der Flut betroffenen Dienststellen Adenau, Bad Neuenahr-Ahrweiler und Remagen, die unmittelbar an das ebenfalls von der Flutkatastrophe heimgesuchte Nordrhein-Westfalen (NRW) grenzen.

Auch in der AAO ist die PD Mayen eine Einsatzdirektion, in deren Zuständigkeitsgebiet der Nürburgring mit seiner Vielzahl von Veranstaltungen fällt. Festivals wie Rock am Ring, Truck Grand Prix und 24h-Rennen erstrecken sich über mehrere Tage und die Besucherzahlen gehen über Tage verteilt teils über die Gesamtzahl von 100.000 täglich hinaus. Das Festival Rock am Ring wurde 2015 und 2016 von Unwetterlagen heimgesucht. Aufgrund einer Terrorverdachtslage 2017 war eine Räumung des Festivalgeländes notwendig. Bereits in der Vergangenheit wurde die PD Mayen so bei der Bewältigung großer Lagen geprüft und durfte Erfahrungen sammeln. Die waren bei der Bewältigung dieses Einsatzes hilfreich und sind daher der besonderen Erwähnung wert.

3 Das Ahrtal

Die Strukturen sind ländlich geprägt. Als Weinanbaugebiet, attraktive Tourismusregion und auch geschätzter Altersruhesitz über die Grenzen von Rheinland-Pfalz bekannt. Die Bevölkerung entlang der Ahr verteilt sich größtenteils auf kleinere Ortschaften, man kennt sich und die Anonymität einer Großstadt ist hier fremd. Die größte Stadt ist Bad Neuenahr-Ahrweiler, die mit ihren ca. 27.000 Einwohnern den mondänen Charakter einer Kurstadt mit Spielbank genoss. Eine wirklich lebens- und liebenswerte Region auf Erden, die zumindest für den Augenblick ihre Identität verloren hat.

Das Flüsschen Ahr entspringt in der Gemeinde Blankenheim (NRW), durchfließt teils wild romantisch das zerklüftete mittlere Ahrtal, dann im weiteren Verlauf entlang parkähnlichen Anlagen die Stadt Bad Neuenahr-Ahrweiler und mündet schließlich nach einer Länge von ca. 85 Kilometer bei Sinzig in den Rhein.

Das Ahrtal wurde bereits in der Vergangenheit mehrfach von Hochwasserereignissen heimgesucht. Im Jahr 1804 starben dabei 64 und im Jahr 1910 57 Menschen. Frühwarnsysteme und Wetterprognosen waren zu der damaligen Zeit wenig verbreitet. Im Jahr 2016 kam es zu einem weiteren „Jahrhunderthochwasser“ mit einem Pegelstand von 3,69 Meter, bei dem glücklicherweise keine Menschen zu Tode kamen. Die mit einem Tsunami zu vergleichende Flutkatastrophe im Jahr 2021 stellt aber alle bisherigen Hochwasserereignisse in den Schatten. Insbesondere die Frage der Vorhersehbarkeit beschäftigt die Menschen bis heute.

4 Wie konnte das Wasser eine solch zerstörerische Kraft entfalten?

Das Tiefdruckgebiet „Bernd“ zog im Juli 2021 über weite Teile Deutschlands. Von Mittwoch, dem 14. Juli auf Donnerstag, dem 15. Juli 2021 fielen innerhalb von 24 Stunden mehr als 100 Liter Regen pro Quadratmeter und verwandelte die Ahr zu einem reißenden Fluss. Durch das Mittelgebirgsgelände wurden die Wassermassen kanalisiert, was zu schnell ansteigenden Pegelständen führte und die verheerenden Zerstörungen zur Folge hatte. 134 Menschen starben, zwei Personen werden weiterhin vermisst, 766 wurden verletzt und etliche Menschen verloren ihre gesamte Existenz. Die Unbändigkeit der Wassermassen zeigt der Blick auf die Pegelstände beispielhaft in der Ortslage Altenahr. Üblicherweise liegt der Pegel dort bei einer niedrigen Tiefe von 0,75 Meter. An dem Abend der Flut stieg er innerhalb kürzester Zeit zunächst auf 5,75 Meter und erreichte schließlich seinen Höchststand bei ca. 7,00 Metern - zwei Stockwerke eines Wohnhauses.

Nach Auskunft von Fachleuten führte, neben der unglücklichen Witterungssituation und der Bodenbeschaffenheit, besonders das Schwemmgut zur Eskalation der Situation. Hauptsächlich an den Brücken kam es zu Verklausungen und staute das Wasser zu der enormen Höhe an. Die meisten der im Ahrtal befindlichen Brücken gaben irgendwann nach, wurden zerstört und sogar gänzlich weggespült.

5 Situation unserer be- und getroffenen Polizeidienststellen

Die Funktionsfähigkeit der zuständigen Polizeidienststellen Adenau, Bad Neuenahr-Ahrweiler und Remagen war in den ersten Tagen nach der Flut massiv eingeschränkt und teilweise gar nicht mehr gegeben. Die Polizeiinspektion Adenau zog bereits in der ersten Einsatzphase in ein Polizeigebäude um, das für die geplanten Großeinsatzlagen am Nürburgring glücklicherweise ausgerüstet vorgehalten wird. Am stärksten war die Dienststelle in Bad Neuenahr-Ahrweiler betroffen. Dort wurden die Haustechnik, der Serverraum, die Gewahrsamszellen und die Umkleideräume der Kolleginnen und Kollegen geflutet und dadurch auch wichtige Führungs- und Einsatzmittel, Uniformteile sowie private Gegenstände vollständig zerstört; der Inhalt der Asservatenkammer teilweise weggespült. Die Wassermassen drangen mit einer solchen Wucht ein, dass die im Gebäude befindliche Luft hörbar und spürbar nach oben über das Dach aus dem Gebäude gedrückt wurde. Man kann von Glück sprechen, dass die Gewahrsamszellen zu diesem Zeitpunkt nicht belegt waren. Ein Retten der Menschen wäre nicht mehr möglich gewesen. In den ersten Tagen war das Dienstgebäude noch notdürftig besetzt, musste später aber geräumt werden.

Die in Bad Neuenahr-Ahrweiler ansässige Bundesakademie für Bevölkerungsschutz und Zivilschutz (BABZ) half unbürokratisch und ermöglichte die Weiterführung des Dienstbetriebes in ihrer Liegenschaft. Die PI Remagen war nicht unmittelbar von dem Hochwasser betroffen, jedoch schränkten die umfangreichen technischen Ausfälle im Ahrtal auch deren Funktionsfähigkeit deutlich ein. In der Flutnacht brachen Festnetz, Mobilfunk, EDV-Systeme und der Digitalfunk teilweise komplett zusammen. Die Verständigung zwischen den Dienststellen und den eingesetzten Kräften war anfangs nur sehr eingeschränkt oder gar nicht möglich. Am 14. und 15. Juli 2021 waren im Zusammenhang mit der Flut insgesamt 1.759 Notrufe zu verzeichnen. Ohne den Ausfall von Festnetz und Mobilfunk wäre das Aufkommen sicherlich noch deutlich größer gewesen. Die Notruf- und Amtsleitungen wurden zur benachbarten Polizeiinspektion

Mayen und zur Führungszentrale in das Oberzentrum nach Koblenz geroutet.

Durch umsichtiges Handeln waren zwar keine Streifenwagen als Totalverluste zu beklagen, jedoch kam es aufgrund der enormen Müllansammlungen auf den Straßen fortwährend zu einer Vielzahl von beschädigten Reifen, die immer wieder zu Ausfällen des Einsatzmittels führten.

Bis heute sind die Renovierungsarbeiten an dem Gebäude der PI Bad Neuenahr-Ahrweiler nicht abgeschlossen. Trotz der großen Hilfe der BABZ befinden sich die Mitarbeiterinnen und Mitarbeiter nach rund neun Monaten noch immer in einer schwierigen Situation.

5.1 AAO – die ersten Stunden

Die Kolleginnen und Kollegen traten am 14. Juli 2021 regulär ihren Dienst an und ahnten nicht, was auf sie zukommen würde. Mit dem Fortgang der Katastrophe baute sich die Dramatik des Einsatzes schnell auf. Es zeichnete sich in der Folge deutlich ab, dass alles bisher Dagewesene übertroffen wurde und über die Grenzen einer Polizeidirektion oder eines Präsidiums hinausging. In den ersten Stunden waren die Kräfte des Wechselschichtdienstes auf sich alleine gestellt. Sie wurden konfrontiert mit Verzweiflung, Hilflosigkeit und Panik. Anrufer meldeten, dass gerade die Ehefrau im Keller ertrunken sei oder sich eine ganze Familie nach dem Heraustreten der Dachziegel von innen auf das Dach des Hauses gerettet hat, das jeden Moment einzustürzen droht. Durch das Zusammenbrechen des Funk- und Telefonnetzes konnten Notrufe nicht zurückverfolgt werden. Zu eingeschlossenen Anwohnern, die um Hilfe riefen, war der Weg abgeschnitten. Häuser wurden samt Menschen weggeschwemmt. Gerade die Kräfte des Nachtdienstes mussten sich mit dieser Machtlosigkeit und auch der eigenen Hilflosigkeit der nicht enden wollenden Katastrophe stellen. Sie waren auch großer Gefahr ausgesetzt, mussten sich teils selbst retten. Die Einsatzsteuerung war ob der technischen Ausfälle nur sehr eingeschränkt möglich.

5.2 BAO – EA Ereignisort

In der polizeitaktischen Bewertung und Kommunikation ist man geneigt in der Kategorie eines zentralen Ereignisortes zu denken. Es handelte es sich hier aber um einen Einsatzraum, der sich über eine Distanz von mehr als 50 Kilometern erstreckte. Es waren über 30 Ortschaften und rund 130.000 Einwohner betroffen. Teilweise unterschied sich das Schadensausmaß erheblich, ebenso die individuellen Zugangsmöglichkeiten zu Hilfen. Die Betrachtung von der Außenperspektive erfolgte gerade in der Anfangszeit oft wenig differenziert und dadurch manchmal verkürzt. Der Übergang von AAO zur BAO: Ein Einsatzgrundsatz ist, die „chaotische Phase“ nach einem Schadenseintritt möglichst kurz zu halten. Ohne jeglichen Vorwurf - aufgrund der Übermacht der Ereignisse - zog sich dieser Übergang tatsächlich über Tage hin. Im Laufe des 175 Tage dauernden Einsatzes war die Struktur der BAO natürlich den Erfordernissen immer wieder anzupassen. Dies betraf selbstverständlich auch den EA Ereignisort. Naturgemäß ein zentraler Einsatzabschnitt, in dem es kaum Maßnahmen des Gesamteinsatzes gab, die dort nicht ihren Ursprung fanden, endeten und auch außerhalb polizeioriginärer Zuständigkeiten getroffen wurden.

Nachfolgend werden ausgewählte Aspekte des EA Ereignisort dargestellt.

UA Absuche / UA Hilfe

Der wesentliche Unterabschnitt (UA) im Einsatzabschnitt der PD Mayen war in den ersten vier Tagen der UA „Absuche“.

Gemäß Vorgabe des Gesamtpolizeiführers sollte das Schadensgebiet selbstverständlich gründlich und schnell abgesucht sein. Eine Herausforderung, bei der nachfolgendes Stufenkonzept zur Anwendung kam:

1) Lebende finden und retten
2) Leichen suchen und bergen
3) Gefahrenquellen identifizieren
4) Herausragende Wertgegenstände feststellen und sichern

Die Fläche des abzusuchenden Gebietes war so groß, dass darüber hinaus eine weitergehende örtliche Priorisierung notwendig wurde. Nach Überflügen im Polizeihubschrauber unter Begleitung eines ortskundigen Polizeibeamten wurde die Region kartiert und schließlich in 15 Sektoren aufgeteilt. Offenkundig besonders stark betroffene und vor allem bewohnte Gebiete waren vorzuziehen. Dort waren am ehesten noch Überlebende zu vermuten. Zur Vermeidung „blinder Flecken“ oder von Doppelabsuchen bei den zeitkritischen lebensrettenden Maßnahmen kam der Dokumentation dabei eine besondere Bedeutung zu. In Auftragstaktik hat die eingegliederte Bereitschaftspolizei des Polizeipräsidiums Einsatz, Logistik und Technik dieses Konzept sodann unter eigener Führung selbständig umgesetzt.

Begleitet durch Ortskräfte konzentrierte sich die Absuche auf die angeschwemmten Fahrzeuge sowie Wohnwagen und Ortslagen. Im weiteren Verlauf dann auch auf Bereiche außerhalb der Bebauung. Da einige Ortschaften durch die Zerstörungen über den Landweg nicht erreicht werden konnten, war eine Luftverlastung der Kräfte notwendig. Die Dokumentation der Suchfortschritte erfolgte fortlaufend im Einsatzprotokollsystem (EPSweb). Am Abend des 18. Juli 2021 konnte die Absuche der priorisierten Regionen abgeschlossen werden und die Einsatzkräfte begaben sich am Folgetag in die nachrangig priorisierten Bereiche. Wohnhäuser und sonstige Gebäude, bei denen nach Hinweisen auch nur die Vermutung auf einen Leichenfund bestand, wurden aufgesucht, vollgelaufene Keller abgepumpt und abgesuchte Sektoren dokumentiert. Eine vermisste Frau war Tage später in Rotterdam (Niederlande) tot angelandet. Neben der persönlichen Dramatik verdeutlicht dies die Schwierigkeit den abzusuchenden Bereich einzugrenzen.

Ab dem 20. Juli 2021 änderte sich die Lagebeurteilung. Die Struktur und der Auftrag waren anzupassen. Der Unterabschnitt wurde von „Absuche“ in „Hilfe“ umbenannt und blieb unter der Führung der Bereitschaftspolizei. Die Bevölkerung im Ahrtal hatte nach dem Erlebten und dem nach der Katastrophe in weiten Teilen eingetretenen zivilisatorischen Ausnahmezustand ein deutlich erhöhtes Sicherheitsbedürfnis, weshalb die Stärkung des subjektiven Sicherheitsgefühls im Zentrum der polizeilichen Maßnahmen des nunmehr umbenannten EA

Foto: Helfen Hand in Hand.

Foto: Bewässerung zur Reduzierung der Staubbelastung.

„Absperrung / Verkehr / Ereignisort" stand. Durch offene und flächendeckende Präsenz im Katastrophengebiet, Gewährleistung einer ständigen Ansprechbarkeit sowie Hilfe bei Aufräumarbeiten bestanden unmittelbare Kontakte zu den Bürgerinnen und Bürgern im Ahrtal. Der Polizeiführer BAO „Ahr" hatte die Polizei den Menschen zugewandt und helfend eingestellt, die Befehlsstelle des EA Ereignisortes nahm die Verantwortung an und die Einsatzkräfte vor Ort lebten die Bürgerpolizei in einer noch nicht dagewesenen mitmenschlichen Art und Weise.

Die Gesamt-BAO war hinreichend elastisch und die Struktur folgte der Strategie. Zur Gewährleistung der Ansprechbarkeit der Polizei war zeitweise der gesonderte EA „Anlaufstellen" eingerichtet, die aufwachsende Aufgabe der Bürgernähe dort weitergehender konzeptioniert und umgesetzt worden. Später erfolgte die Rückführung in den EA Ereignisort unter Fortentwicklung dieser Konzepte.

Der UA „Hilfe" hatte sich aus mehreren Hundertschaften der Bereitschaftspolizeien aus dem gesamten Bundesgebiet aber auch von Studierenden der Hochschule der Polizei Rheinland-Pfalz sowie der Bundeswehr personalisiert. Einen Unterabschnitt, den es in den Planentscheiden bisher nicht gab, der jedoch das von außen erkennbare Gesicht einer der Bevölkerung zugewandten Polizei verkörperte. Neben der Wahrnehmung klassischer örtlicher Polizeiarbeit erfolgte die unkonventionelle und unbürokratische Hilfe für die Bürgerinnen und Bürger – bis hin später zur Unterstützung bei den amtlichen Beantragungsverfahren für Fluthilfen. Dies alles führte zwischen Menschen im Ahrtal und den Polizisten zu einer Verbundenheit, die teils bis heute persönlich fortbesteht.

Im Zusammenhang mit der polizeilichen Hilfe ist der Einsatz der Wasserwerfer noch einmal besonders hervorzuheben. Unter der Leitung der Technischen Einsatzeinheit (TEE) der Polizei Rheinland-Pfalz waren mit Unterstützung der Bundespolizei bis zum 20. Oktober 2021 täglich bis zu drei Wasserwerfer im Einsatz und Teil des gesamten Versorgungskonzeptes. Zu den vorrangingen Aufgaben gehörten der Transport von Brauchwasser für Wassertanks und Duschcontainer, Reinigung von Straßen und Gerätschaften, Bewässerung von Straßen und Beregnung beim Abriss von Gebäuden zur Reduzierung der enormen Staubbelastung. Die Abgabemengen betrugen zwischen 80.000 und 180.000 Liter Wasser täglich. Durch die vielfältigen Einsatzmöglichkeiten hat die Bevölkerung den Einsatzwert der Wasserwerfer als sehr positiv wahrgenommen und ihn als „Partner" schätzen gelernt. Diese geschlossene Einheit verließ mit als letzte den Einsatzraum.

UA Verkehr

Gewährleistung eines ungehinderten Einsatzes der BOS / Freihalten der Not- und Rettungswege. Dies ist einer der originären Aufgaben der Polizei in größeren Gefahren- und Schadenslagen.

Das Verkehrsnetz im Ahrtal war in großen Teilen kriegsähnlich zerstört oder stark beschädigt. Straßen waren unterspült oder gänzlich weggebrochen, Brücken überwiegend Opfer der Flut und damit die Verbindung zum anderen Ufer gekappt. Geröllmassen und Schutt versperrten wichtige Zufahrtswege. Viele Ortschaften waren zunächst nicht über Land erreichbar und mussten aus der Luft versorgt werden. Selbst die international bedeutsame Bundesautobahn 61 wurde so stark beschädigt, dass sie im Bereich Autobahnkreuz Meckenheim über Monate teilweise gesperrt werden musste. Die Erstellung eines belastbaren Lagebildes zur Verkehrslage und zum Zustand der Verkehrsinfrastruktur war in den ersten Tagen nahezu unmöglich. Vorhandenes Kartenmaterial entsprach nicht dem IST-Zustand. Die Aufklärung zur Verkehrslage erfolgte vorwiegend durch die Polizeihubschrauberstaffel. Aber nur aus der Luft konnte die Standsicherheit und Befahrbarkeit der Verkehrswege nicht bewertet werden.

Die verbliebenen befahrbaren Straßen wurden von Hilfeleistenden, BOS-Fahrzeugen und Anwohnern dementsprechend stark belastet. Von Anfang an ergab sich über die Landesgrenzen hinaus eine Welle der Hilfsbereitschaft. Das führte zu einer enormen Anreise von Fluthelfern aus dem gesamten Bundesgebiet, die das bereits geschwächte Verkehrsnetz teilweise zum Erliegen brachte. Die technische Einsatzleitung hat nach Abstimmung mit der Polizei Allgemeinverfügungen zum Individualverkehr erlassen, Durchlassstellen und dauerhafte Kontrollpunkte an relevanten Stellen eingerichtet sowie überörtliche Einbahnstraßen ausgewiesen und beschildert. Die Synchronisation mit dem privat eingerichteten Helfershuttle erfolgte erst später. Die Umsetzung der vorgenannten Maßnahmen mit der zügigen provisorischen Instandsetzung wichtiger Verkehrswege führten erst im weiteren Verlauf zu einer Entspannung der Verkehrslage. In vielen Einzeldiskussionen mit betroffenen Menschen an den „Checkpoints" war die Durchsetzung von Durchfahrtsverboten teils sehr konfliktträchtig, aber alternativlos.

6 Müllbeseitigung / gesundheitsgefährdende Stoffe

Schon nach wenigen Tagen ergaben sich Seuchengefahren und Gefahren durch gefährliche Stoffe. Friedhöfe waren durch die Flut freigelegt sowie Leichen und Gebeine weggespült. Tierkadaver verbargen sich unter den riesigen Müllmassen und große Mengen Heizöl aus den aufgebrochenen Öltanks sowie Fäkalschlamm aus den zerstörten Kläranlagen verteilten sich unaufhaltsam. Um Seuchen entgegenzuwirken aber auch den Verkehrsraum freizumachen war es notwendig, in einer Art Befreiungsschlag mit hunderten von Lastkraftwagen den besonders gesundheitsgefährlichen Müll abzutransportieren. Rund 300.000 Tonnen teils kontaminierten Sperrmülls, so viel wie in 40 Jahren. In einer konzertierten Aktion waren hierzu am 25. und 26. Juli 2021 unterstützend weitreichende Verkehrsmaßnahmen notwendig. In nur einer Nacht haben die Kräfte der Befehlsstelle zwei Ringstraßen mit Einbahnregelung auf einer Gesamtlänge von 58 Kilometern konzeptioniert und vorbereitet. Die Umsetzung erfolgte durch Kräfte des Frühdienstes. Auf jedem Verkehrsabschnitt galt es dabei zu gewährleisten, dass auch aus keiner noch so kleinen Seitenstraße oder Waldweg ein Verkehrsteilnehmer gefährlich entgegen der rettenden Einbahnstraße einfährt. Beispielhaft für vieles in diesem Einsatz: Hand in Hand - von der zu erkennenden Gefahr, einer Idee zur Abwehr, über die Planung, die Organisation und Versorgung der Kräfte bis hin zur taktischen Umsetzung vor Ort. Beeindruckend war dabei das arbeitsteilige und nahtlose geschlossene Vorgehen auch in Zusammenarbeit mit den unterstützenden Kräften des Bundes und

den anderen Bundesländern. Dies zeigte sich in der Zusammenarbeit der Ministerien beim nationalen Kräftemanagement, des Führungsstabes, der Befehlsstellen, der Verbindungsbeamten, den Kräftesammelstellen, der Abteilung Polizeiverwaltung und insbesondere der Motivation, Leidenschaft und dem Pragmatismus der vor Ort eingesetzten Kolleginnen und Kollegen. Alle hatten länderübergreifend eine „geteilte Vorstellung" von dem was zu tun ist, auch mentales Modell („shared mental model") genannt, über die Art und Weise wie der polizeiliche Einsatz zu erledigen ist. Nur beispielhaft, aber beeindruckend! Unstreitig war diese Verkehrsmaßnahme nur eine von vielen schwierigen Aktionen im Gesamteinsatz und natürlich lief sie ob der Umstände auch nicht bis ins Detail reibungslos. Sie war aber im Ergebnis erfolgreich und das zählt am Ende.

Die Gefahrenquellen waren insgesamt vielschichtig. Weitere ergaben sich durch offenliegende Strom- oder abgerissene Gasleitungen. So berichtete eine Kollegin aus einem benachbarten Einsatzabschnitt, die mit der Leichenbergung aus einem Behindertenheim betraut war, dass sie gerade in hüfthohem Wasser stand, als sie durch einen Feuerwehrmann darauf aufmerksam gemacht wurde, dass just die zuvor ausgefallene Elektrizität in dem Gebäude nun wieder funktioniere. Viele Bomben und Munition aus dem 2. Weltkrieg (Anmerkung: Die Ahrtalbahn war Nachschublinie auch für die Kämpfe rund um die Brücke von Remagen), Gas- und Öltanks, legale und illegale Waffen aus Privatbesitz aber auch Geldautomaten bis hin zu Jetons aus der zerstörten Spielbank wurden von der Flut kilometerweit verteilt. Die Wasserversorgung und die Kanalisation waren in manchen Bereichen komplett zerstört. Eine mobile Kläranlage, die in internationalen Krisengebieten eingesetzt wird, wurde in der Ortslage Mayschoß aufgebaut und war auch wegen der darin verbauten wertvollen Hochleistungspumpen gefahrenabwehrend als kritische Infrastruktur einzustufen.

7 Veranstaltungen / Besuche von Schutzpersonen

Eine weitere Herausforderung stellten die Besuche von Amtsträgern / Schutzpersonen sowie Veranstaltungen rund um die Flutkatastrophe dar. Neben den regelmäßigen Besuchen von Landespolitikern waren insbesondere die Besuche eingestufter Vertreter aus der Bundespolitik polizeilich zu begleiten. Auch wenn zu diesen Anlässen seiner Zeit die BAO „Ahr" um den Einsatzabschnitt „Besuche" bzw. „Veranstaltung" erweitert und damit verstärkt wurde, blieben der Schnelllebigkeit der Entwicklungen geschuldet dennoch deutliche Überhänge für den EA Ereignisort. Bis heute besuchen hochrangige Politiker das Ahrtal. So galt es zuletzt am 29. März 2022 die Sicherheit von Bundeskanzler Scholz, Bundesinnenministerin Faeser, Ministerpräsidentin Dreyer und Innenminister Lewentz in Ahrbrück durch die PD Mayen zu gewährleisten. Diese Besuche waren wichtig, um den politischen Raum über die Schwere der Katastrophe und die Notwendigkeit von großen Hilfen zu informieren.

Mit zeitlichem Abstand trat leider ein fast zu erwartendes Problem auf – Katastrophentourismus. Meist durch Auswärtige, häufig durch Motorradfahrer, die die tief getroffene Region fragwürdig als Ausflugsziel in ihre Freizeitgestaltung aufgenommen haben. Mal auch in guter Absicht, manchmal vielleicht bestenfalls gesehen nur naiv. Aus Sicht der Gefahrenabwehr jedenfalls kritisch erwähnenswert waren die in der Weihnachtszeit aufkommenden Traktor-Sternfahrten. Hunderte von geschmückten landwirtschaftlichen Fahrzeugen nutzten das belastete enge Ahrtal und damit gleichzeitig auch den Verkehrsraum für Rettungsahrzeuge. Symbolisch hätten weniger Traktoren auch gereicht. Zum Glück ist aus polizeilicher Sicht nichts passiert!

8 Zukunftskonferenzen und Einwohnerversammlungen

Der vollständige Wiederaufbau des zerstörten Gebiets entlang der Ahr wird voraussichtlich noch Jahre dauern. Frühzeitig wurde begonnen in Einwohnerversammlungen die Bürgerinnen und Bürger über den Wiederaufbau zu informieren. An den Einwohnerversammlungen nahmen die Landesbeauftragte für den Wiederaufbau, Sonderbeauftragte der Landesregierung, behördlich verantwortliche Stellen sowie zahlreiche Expertinnen und Experten teil. Über 200 Beteiligte aus Behörden, Unternehmen, Kommunen, Hilfsorganisationen und Kammern berieten und informierten bei Zukunftskonferenzen über das weitere Vorgehen. Auch die Polizei begleitet den Wiederaufbau und unterstützt die zuständige Verwaltung unbürokratisch dort, wo es möglich ist.

9 Rückführung der BAO in eine verstärkte AAO

Am 27.08.2021 ging die Gesamteinsatzleitung wieder vollständig an die Polizeidirektion Mayen über. Für die Wiederherstellung des Sicherheitsgefühls der Bevölkerung im Ahrtal hatte das PP Koblenz die mehrstufige „Rahmenkonzeption des PP Koblenz zur Stärkung des Sicherheitsgefühls in der Bevölkerung und Begleitung des Wiederaufbaus im Ahrtal nach der Flutkatastrophe" erstellt. Zunächst wurde die Aufrechterhaltung der Einsatzstruktur ermöglicht; später der Kräfteansatz sukzessive und angemessen reduziert. Die sichtbare polizeiliche Präsenz wird ab Mitte des Jahres 2022 nach einer personellen Sonderzuweisung wieder in den AAO-Dienststellen in Remagen, Adenau und insbesondere Bad Neuenahr-Ahrweiler gewährleistet.

In Umsetzung des Rahmenkonzeptes lauten die Leitlinien der Polizeidirektion Mayen:

- Die Stabilisierung und Stärkung des Sicherheitsgefühls der Bevölkerung haben oberste Priorität.
- Die Polizei zeigt sich gesprächs- und kommunikationsbereit. Einsatzkräfte treten jederzeit bürgerfreundlich und mit anlassbezogenem Ermessen bei hoher Einschreitschwelle auf. Gegen erkannte Straftäter / Störer ist frühzeitig und konsequent, bei niedriger Einschreitschwelle, unter Anwendung aller rechtlichen Möglichkeiten, vorzugehen.
- Die Polizei unterstützt im Rahmen ihrer Zuständigkeit den Wiederaufbau unbürokratisch. Sie arbeitet eng mit den zuständigen Behörden und sonstigen anerkannten Organisationen zusammen.

10 Anstöße

Nach einem Vortrag vor Führungskräften wurde die Frage nach einem möglichen Erfolgsrezept reduziert auf eine Kernaussage aufgeworfen. Diese Frage überfordert. Reflektierend könnte man vielleicht sagen: Handlungsspielräume ausnutzen, handeln, mit Auftragstaktik führen, den gut ausgebildeten Kolleginnen und Kollegen vertrauen und Verantwortung übernehmen.

„Wer jetzt noch nicht verstanden hat was wir an unserer Polizei haben, dem ist nicht mehr zu helfen!"

(Staatsminister Lewentz, Veranstaltung anlässlich der offiziellen Beendigung der BAO Ahr im PP Koblenz, 10.2.2022)

„Wir haben hier an der Ahr mit einem Schlag den Himmel und die Hölle an einem Fleck gehabt. Die Hölle: Das Wasser kam. Der Himmel war, dass sich ein Kern frei gelegt hat in unserer Gesellschaft, der für mich immer verloren geglaubt war …: Das ist dieser Zusammenhalt, diese Solidarität, diese Nächstenliebe. Das ist einfach eine Sache, die gibt einem Hoffnung, das macht einem Mut."

(Thomas Pütz, Staatsakt aus Anlass der Trauerfeierlichkeit am Nürburgring, 01.9.2021)

11 Hinweis

Bis heute befasst sich der Parlamentarische Untersuchungsausschuss (PUA) mit der Flutkatastrophe und strafrechtliche Ermittlungen sind anhängig. Es handelt sich mithin um laufende Verfahren.

Datenübersicht:	
Tote	134
Vermisste	2
Einsatzraum	ca. 50 Kilometer
Pegelstand normal	0,75 Meter
Pegel Höchststand	7 Meter
betroffene Einwohner (RLP)	130.000
betroffene Ortschaften (RLP)	31
Wiederaufbaukosten	15.000.000.000 €
BAO	175 Tage
Einsatzkräfte	36923
Einsatzstunden	408708

Die Ahndungsbestimmungen im VersG NRW – Abkehr von einem liberalen Verständnis der Versammlungsfreiheit?

Von Hartmut Brenneisen, Preetz/Worms[1]

Am 15.12.2021 ist das Versammlungsgesetz des Landes Nordrhein-Westfalen (VersG NRW) verabschiedet worden.[2] Dies stellt grundsätzlich eine schlüssige Konsequenz aus der Föderalismusreform I dar, durch die das Versammlungsrecht im Jahr 2006 aus der konkurrierenden Gesetzgebungskompetenz des Bundes entlassen wurde.[3] Fraglich ist allerdings, ob damit auch ein inhaltlich überzeugendes, praktikables und den Anforderungen des Art. 8 GG gerecht werdendes Normengefüge geschaffen wurde.[4] Insbesondere die sehr restriktiven und zum Teil unabgestimmten Ahndungsbestimmungen lassen Zweifel aufkommen.

1 Grundlegung

Die Versammlungsfreiheit aus Art. 8 GG gehört zu den unentbehrlichen Funktionselementen eines demokratischen Gemeinwesens. Sie stellt ein Stück demokratischer Offenheit und eine wichtige Ventilfunktion speziell für Unzufriedene dar. Der hoheitliche Umgang mit ihr bedarf eines besonderen Maßes an Sensibilität, da häufig verschiedene Interessen austariert werden müssen.[5] Dies ist bereits dem *„Brokdorf-Beschluss"* des BVerfG[6] zu entnehmen, der berechtigt als *„Lehrbuch des Versammlungsrechts"* und *„Magna Charta der Versammlungsfreiheit"* bezeichnet wird,[7] und gilt auch in schwierigen Zeiten, wie der aktuellen Corona-Pandemie.[8] Problematisch ist die fehlende Bestimmtheit des versammlungsrechtlichen Normengefüges, die auch nach der Föderalismusreform I fortbesteht. Von der neuen Gesetzgebungskompetenz haben bisher nur die Länder Bayern, Berlin, teilweise Brandenburg, Niedersachsen, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und nunmehr auch Nordrhein-Westfalen Gebrauch gemacht – und dies trotz vorliegender Musterschriften[9] in sehr unterschiedlicher Form. Eine wünschenswerte Angleichung ist nicht festzustellen.[10] Daneben gelten gemäß Art. 125a Abs. 1 GG in allen Ländern, in denen die bundesrechtlichen Regelungen nicht ersetzt wurden, diese auf unbestimmte Zeit und mit allen bekannten Mängeln fort, so dass der bestehende Zustand andauern dürfte. Die Neufassung eines bereichsspezifischen Landesgesetzes hat dabei durchgehend die Freiheit, Unabhängigkeit und Mündigkeit des selbstbewussten Bürgers in den Blick zu nehmen. Zweifellos erforderliche hoheitliche Befugnisse sind stets mit der Zielstellung einer rechtsstaatlich klaren Begrenzung zu formulieren.

2 Gesetzgebungsverfahren

Dem Koalitionsvertrag für die Legislaturperiode 2017 bis 2022 folgend hat die Landesregierung NRW am 21.1.2021 den

Gesetzentwurf zur Einführung eines nordrhein-westfälischen Versammlungsgesetzes und zur Änderung weiterer Vorschriften eingebracht (VersGEinfG NRW).[11] Zuvor war bereits am 3.11.2020 die Fraktion der SPD mit dem Entwurf eines Versammlungsfreiheitsgesetzes für das Land Nordrhein-Westfalen initiativ geworden (VersFG NRW).[12] Beide Vorlagen enthalten – trotz deutlicher Unterschiede in der Ausrichtung – überzeugende Ansätze und stellen Verbesserungen zum geltenden Rechtszustand dar. Dabei ist die Vorlage der Landesregierung eher restriktiv gefasst und stellt die Sanktionierung von Rechtsverstößen als bedeutsames Instrument im Versammlungsgeschehen besonders heraus. Ahndungsnormen werden als wichtiges Mittel bezeichnet, um *„jedenfalls nachträglich die Verbindlichkeit der Verwaltungsakte und sonstigen behördlichen Ge- und Verbote zu verdeutlichen"*. Zugleich wird es als *„eher fernliegende und nicht zustimmungsfähige Einschätzung" betrachtet, „dass die sanktionsbewehrte Einforderung der Beachtung des geltenden Rechts in einem Rechtsstaat eine Art Einschüchterungswirkung auslösen könnte"*.[13] Inhaltlich weicht der Entwurf deutlich von den zuletzt verabschiedeten freiheitsbetonenden Landesgesetzen in Schleswig-Holstein (VersFG SH) und Berlin (VersFG BE) ab. In dem SPD-Entwurf wird hingegen in enger Anlehnung an den MEVersG, das VersFG SH und das VersFG BE die Interpretation als *„Grundrechtsgewährleistungsrecht"* verfolgt und Versammlungen ein ausgesprochen freiheitlicher Rahmen zuerkannt.[14] Nach Anhörungsverfahren[15] und Ausschussberatungen[16] erfolgte am 15.12.2021 mit der Zweiten Lesung im nordrhein-westfälischen Landtag die Ablehnung der SPD-Vorlage, während der Entwurf der Landesregierung in der Fassung der Beschlüsse des Innenausschusses[17] mit den Stimmen von CDU und FDP angenommen wurde.[18] Das Gesetz wurde am 17.12.2021 verkündet, trat am Folgetag in Kraft und ist damit seit dem 18.12.2021 in NRW geltendes Recht.

3 Regelungen mit Licht und Schatten

Das verabschiedete Gesetz ist ein Normengefüge mit Licht und Schatten. Überzeugend sind beispielsweise der konkret definierte Regelungsbereich einschließlich der Wirksamkeit bei nichtöffentlichen Versammlungen (§ 2 VersG), die Verpflichtung zur kooperativen Zusammenarbeit (§ 3 VersG), die Stärkung der Versammlungsleitung (§§ 5, 6 VersG), eine eingefügte Transferklausel in das allgemeine Polizeirecht (§ 9 VersG), die Regelung der Anzeigepflicht unter Berücksichtigung von Eil- und Spontanversammlungen (§ 10 VersG), Teile der auf Vorschlag des Innenausschusses nachgebesserten zentralen Befugnis für Beschränkungen, Verbot und Auflösung bei Versammlungen unter freiem Himmel (§ 13 VersG),[19] die Berücksichtigung von öffentlichen Verkehrsflächen in Privateigentum (§ 21) sowie eine Berichts- und Evaluierungsklausel als rechtsstaatliche Sicherung (§ 34 VersG).[20] Erkennbare Schwächen liegen hingegen insbesondere in der widersprüchlichen und nicht verfassungsrechtlichen Standards entsprechenden Begrenzung des zeitlichen Anwendungsbereichs (§ 9 Abs. 4 VersG),[21] einer fehlenden Regelung über die Anwesenheit und Legitimation von Polizeikräften bei Versammlungen unter freiem Himmel,[22] in systematisch unglücklich verankerten Ermächtigungen für Gefährderansprachen (§ 14 Abs. 1 VersG) und Meldeauflagen (§ 14 Abs. 2 VersG) sowie den lückenhaften Datenerhebungsnormen (§§ 16, 26 VersG).[23]

4 Ahndungsbestimmungen mit Einschüchterungspotenzial

Sehr kritisch sind die restriktiv ausgerichteten und teilweise unabgestimmten Strafrechtsnormen (§ 27 VersG) zu bewerten, die obrigkeitsstaatlicher Tradition entsprechen, mit denen entgegen der Gesetzesbegründung[24] deutliches Einschüchterungspotenzial verbunden ist und die der Polizei im Lichte des Legalitätsprinzips[25] zudem nur wenig Handlungsspielraum eröffnen. Damit wird aber zugleich die überragende Bedeutung der Versammlungsfreiheit verkannt und der repressive Teil des Gesetzes zu stark betont. An dieser Bewertung ändert auch der Hinweis auf die grundsätzliche Zuständigkeit des Gesetzgebers für die Festlegung von Ahndungsvorschriften nichts.[26] Zu bemängeln sind die im Gegensatz zu den Entkriminalisierungstendenzen im MEVersG, NVersG, VersFG SH und VersFG BE stehende Ausweisung zahlreicher Verhaltensweisen als kriminelles Unrecht sowie systematische Unstimmigkeiten, die trotz einiger Nachbesserungen im Gesetzgebungsverfahren[27] nach wie vor unübersehbar sind. Der Charakter eines *„Grundrechtsgewährleistungsrechts"* geht damit weitgehend verloren. Im Einzelnen sind folgende Regelungen kritisch zu beurteilen:

4.1 Überhöhung von Ordnungsvorschriften

Die Durchführung einer öffentlichen Versammlung unter freiem Himmel ohne Anzeige i.S.d. § 10 VersG ist für Veranstalter und Leiter in § 27 Abs. 1 VersG als Straftat ausgewiesen und mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht worden. Damit folgt der Gesetzgeber der überkommen Regelung des § 26 Nr. 2 BVersG und weicht deutlich von den meisten vorliegenden Landesgesetzen ab.[28] Die gleiche Strafandrohung gilt zudem für die vorgenannten Adressaten bei Durchführung bzw. Fortsetzung einer vollziehbar verbotenen oder polizeilich aufgelösten bzw. unterbrochenen Versammlung unter freiem Himmel.[29] Sofern bei der Durchführung einer öffentlichen Versammlung unter freiem Himmel durch den Leiter wesentlich von den Veranstalterangaben in der Anzeige[30] abgewichen oder Beschränkungen nach § 13 Abs. 1 VersG nicht nachgekommen wird, ist gem. § 27 Abs. 2 VersG eine Freiheitsstrafe bis zu sechs Monaten oder eine Geldstrafe bis zu 180 Tagessätzen vorgesehen.[31] Damit wird die Missachtung von Ordnungsvorschriften aber deutlich überhöht und ohne Not zu einer Kriminalisierung von Veranstaltern und Leitern beigetragen. Eine Ahndung als Ordnungswidrigkeit würde dem Gewicht der Zuwiderhandlungen entsprechen und vollkommen ausreichen.[32]

4.2 Vermummungsverbot

Kritikwürdig ist zudem die überkommene Ausweisung des Vermummungsverbots als kriminelles Unrecht mit einer Strafandrohung von bis zu zwei Jahren oder Geldstrafe. Die Entwurfsbegründung,[33] dass entsprechende Zuwiderhandlungen in *„besonders eklatanter Weise"* gegen die Grundrechtsverbürgungen des Art. 8 GG verstoßen, kann nicht überzeugen und wird den unterschiedlichen Fallkonstellationen nur unzureichend gerecht. Zunächst korrespondiert die Verbotsnorm des § 17 Abs. 1 Nr. 1 VersG nur bedingt mit den Ahndungsbestimmungen des § 27 Abs. 7 Satz 1 VersG (Straftat) und im Falle des bloßen Mitführens des § 28 Abs. 1 Nr. 7 VersG (Ordnungswidrigkeit). Während die verbotene Handlung *„bei oder im Zusammenhang"* mit einer öffentlichen Versammlung oder einer sonstigen öffentlichen Veranstaltung unter freiem Himmel und damit in allen verfassungsrechtlich geschützten Phasen[34] erfolgen kann, setzt die Ahndung nur in der Hauptphase und auf dem Weg zu derartigen Versammlungen oder Veranstaltungen ein. In Übereinstimmung mit § 9 Abs. 4 VersG[35] kommt eine Sanktion in der Nachphase damit nicht in Betracht. Zudem verzichtet der Gesetzgeber auf die etablierte Rechtsfigur der *„Verwaltungsakzessorietät"*[36] und

lässt die *„rechtsstaatliche Funktion des Verwaltungsakts"* weitgehend unbeachtet.[37] Etwas anderes gilt nur bei dem Ordnungswidrigkeitentatbestand des § 28 Abs. 1 Nr. 6 VersG, der u.a. bei Zuwiderhandlungen gegen auf § 17 Abs. 2 VersG basierenden Anordnungen Wirkung entfaltet. Nur schwer aufzulösende Wertungswidersprüche sind die Folge. Schließlich ist die Erweiterung des Vermummungsverbots auf sonstige öffentliche Veranstaltungen unter freiem Himmel in der Tradition des Bundesrechts fragwürdig und als *„systemwidrig"* abzulehnen.[38]

4.3 Schutzausrüstungsverbot

Die Ausführungen zum Vermummungsverbot gelten im Wesentlichen auch für das Schutzausrüstungsverbot gem. § 17 Abs. 1 Nr. 2 i.V.m. § 27 Abs. 7 Satz 2 VersG. Positiv wirkt allerdings die Abkehr vom umstrittenen Terminus der *„Schutzwaffe"*.[39] Es wird zudem nicht mehr zwischen Gegenständen im technischen und nichttechnischen Sinne differenziert und neben der Eignung ist stets ein erkennbarer Wille erforderlich, Vollstreckungsmaßnahmen eines Trägers von Hoheitsbefugnissen abzuwehren.[40] Aber auch in diesem Kontext liegen systematische Unstimmigkeiten zwischen Verbots- und Ahndungsbestimmung sowie zur Begrenzung durch § 9 Abs. 4 VersG und zum Verhältnis zwischen § 27 Abs. 7 Satz 2 und § 28 Abs. 1 Nr. 6 VersG vor. Zudem wird auch hier auf die Implementierung der generell geltenden und Klarheit schaffenden *„Verwaltungsakzessorietät"* verzichtet und eine systemwidrige Erweiterung auf sonstige öffentliche Veranstaltungen unter freiem Himmel vorgenommen. Mögliche Regelungslücken[41] bei Fußballspielen, Volksfesten, Konzerten und anderen Veranstaltungen können dabei nicht überzeugend angeführt werden, da durchaus schlüssige Ersatzlösungen möglich sind.[42]

4.4 Gewalt- und Einschüchterungsverbot

Mit § 18 VersG ist ein Gewalt- und Einschüchterungsverbot geschaffen worden, das im Gesetzentwurf zunächst als *„Militanzverbot"* bezeichnet wurde.[43] Die Verbotsnorm weicht deutlich von allen bisher bestehenden Regelungen ab,[44] gilt für öffentliche Versammlungen und für sonstige öffentliche Veranstaltungen unter freiem Himmel, richtet sich grundsätzlich an Veranstalter, Leiter und Teilnehmer und ist gem. § 27 Abs. 8 VersG als kriminelles Unrecht mit einer Strafandrohung von bis zu zwei Jahren oder Geldstrafe ausgewiesen worden.[45] Diese Strafandrohung gilt allerdings nur für Personen, die durch ihr *„eigenes äußeres Erscheinungsbild"* zu der Vermittlung von Gewaltbereitschaft und zur einschüchternden Wirkung beitragen und zudem auch nur bei Versammlungen i.S.d. § 2 Abs. 3 VersG. Bei sonstigen öffentlichen Veranstaltungen unter freiem Himmel kommt allein ein Rückgriff auf den Ordnungswidrigkeitentatbestand des § 28 Abs. 1 Nr. 6 VersG in Betracht, sofern gegen Anordnungen zur Durchsetzung des Verbots nach § 18 Abs. 2 VersG verstoßen wird.

4.5 Waffenverbot

Unzureichend ausgestaltet ist schließlich auch das mit den verfassungsunmittelbaren Gewährleistungsschranken der Friedlichkeit und Waffenlosigkeit aus Art. 8 Abs. 1 GG korrespondierende und damit besonders bedeutsame Waffenverbot.[46] Während die verbotene Handlung gem. § 8 Abs. 1 VersG *„bei Versammlungen oder auf dem Weg zu oder von Versammlungen"* erfolgen kann und auch die Ahndungsbestimmung des § 27 Abs. 5 im Gegensatz zur § 27 Abs. 7 VersG die verfassungsrechtlich geschützte Vor-, Haupt- oder Nachphase erfasst, soll das Gesetz gem. § 9 Abs. 4 VersG in der dort definierten Nachphase keine Wirkung mehr entfalten. Die beabsichtigte *„legislativ-deklaratorische"* Abrundung des speziellen Anwendungsbereichs des Gesetzes führt damit gerade nicht zu der angestrebten *„Rechtssicherheit in der Verwaltungspraxis"*.[47] Zudem fehlt eine wünschenswerte Subsidiaritätsklausel,[48] so dass es zu einem vermeidbaren Wertungswiderspruch zwischen der durch Art. 3 Abs. 1 Nr. 1 EGStGB dirigierten Strafandrohung des VersG (Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe) und der aus § 52 Abs. 3 Nr. 9 WaffG (Freiheitsstrafe bis zu drei Jahren oder Geldstrafe) kommt.

5 Befund

Die Entwicklung und Verabschiedung eines bereichsspezifischen Gesetzes für das Versammlungswesen war grundsätzlich ein richtiger und zukunftsweisender Schritt für das Land NRW. Im Ergebnis ist das Normengefüge jedoch deutlich restriktiver gefasst, als der vorliegende MEVersG sowie die Regelungen in Schleswig-Holstein und Berlin, aber auch in Bayern und Niedersachsen. In Teilen bewegt es sich auf einer Ebene mit dem überkommenen Bundesrecht sowie den unzureichenden Normen in Sachsen und Sachsen-Anhalt.[49] Dabei ist das BVersG bei den parlamentarischen Beratungen zuvor berechtigt als *„in die Jahre gekommen"* bezeichnet worden.[50] Deutliche Kritik ist insbesondere hinsichtlich der Ahndungsbestimmungen angezeigt, die Einschüchterungspotenzial enthalten, nur schwer mit dem freiheitlichen Grundgedanken des Art. 8 GG zu vereinbaren sind und damit eine Abkehr vom liberalen Verständnis der Versammlungsfreiheit bedeuten. Hinzu kommen von mangelnder Sorgfalt zeugende systematische Unstimmigkeiten bei der Ausgestaltung des Normengefüges. Eine handlungsleitende Wirkung wird damit gerade nicht erreicht, so dass unweigerlich Probleme für Grundrechtsträger und Polizei entstehen dürften. Letztlich steht das VersG NRW auch für eine weitere *„Zersplitterung"* des bereichsspezifischen Rechts[51] und damit eine versammlungsrechtliche *„Kleinstaaterei"*,[52] der auch nicht durch Hinweise auf zulässige *„politische Akzente"* und Wesensmerkmale des *„(Sicherheits-)Föderalismus"* schlüssig begegnet werden kann.[53]

Anmerkungen

1 Hartmut Brenneisen ist Professor, Ltd. Regierungsdirektor u. Polizeidirektor a.D. Er ist heute als Redakteur, Gutachter, Lehrbeauftragter sowie Herausgeber u. Autor von Fachpublikationen tätig. Dieser Beitrag baut auf einem Aufsatz des Autors in der DP 4/2022 auf.
2 GV. 2022, S. 1.
3 BGBl. 2006 I, S. 2034.
4 Bejahung durch Pietsch, KriPoZ 2022, S. 36 sowie die Regierungskoalition in NRW, PlPr 17/155, S. 61 (Katzidis), S. 65 (Lürbke) u. S. 70 (Reul).
5 Zur Bedeutung der Versammlungsfreiheit vgl. nur Höfling, in: Sachs, 2021, Grundgesetz, Kommentar, 9. Aufl., Art. 8, Rn. 8; Ernst, in: Kämmerer/Kotzur, 2021, Grundgesetz, Kommentar, 7. Aufl., Art. 8, Rn. 12; Jarass, in: Jarass/Kment, 2020, Grundgesetz, Kommentar, 16. Aufl., Art. 8, Rn. 1; Schneider, in: Epping/Hillgruber, 2020, Grundgesetz, Kommentar, 3. Aufl., Art. 8, Rn. 1.
6 BVerfGE 69, 315 (*„Brokdorf"*).
7 Wiefelspütz, DÖV 2001, S. 21; ders., DÖV 2000, S. 281.
8 Vgl. Hong, in: Peters/Janz, 2021, Handbuch Versammlungsrecht, 2. Aufl., B, Rn. 78b ff.; Brenneisen/Wilksen/Staack/Martins, 2020, Versammlungsrecht, 5. Aufl., S. 181.
9 Vgl. insbesondere Enders/Hoffmann-Riem/Kniesel/Poscher/Schulze-Fielitz, 2010, Musterentwurf eines Versammlungsgesetzes; siehe dazu Pahl/Tölle, in: Peters/Janz, 2021, a.a.O., E, Rn. 4.
10 Pahl/Tölle, in: Peters/Janz, 2021, a.a.O., E, Rn. 115; Lembke, in: Breitbach/Deiseroth, 2020, Versammlungsrecht, 2. Aufl., S. 936; Brenneisen, Die Kriminalpolizei 1/2020, S. 28.
11 Drs. 17/12423.
12 Drs. 17/11673.

13 Drs. 17/12423, S. 84, 86, 87; dazu Brenneisen, DP 4/2022, S. 30.
14 Drs. 17/11673, S. 2; zum *„Grundrechtsgewährleistungsrecht"* vgl. Knape/Brenneisen, 2021, Versammlungsfreiheitsgesetz Berlin, § 3, Rn. 6; Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 308; dies., 2016, Versammlungsfreiheitsgesetz für das Land Schleswig-Holstein, **§ 3,** Rn. 2; Enders/Hoffmann-Riem/Kniesel/Poscher/Schulze-Fielitz, 2010, a.a.O., S. 2; kritisch dazu Pietsch, KriPoZ 2022, S. 36.
15 APr 17/1406; vgl. insbesondere die Stellungnahmen 17/3778 (Gusy), 17/3805 (Brenneisen), 17/3812 (Ullrich), 17/3815 (von Coelln), 17/3834 (Arzt), 17/3851 (Schwarz) u. 17/3858 (Thiel).
16 Die Gesetzentwürfe wurden vom Plenum zur federführenden Beratung an den Innenausschuss sowie zur Mitberatung an den Hauptausschuss u. den Rechtsausschuss überwiesen; vgl. PlPr 17/114, S. 124.
17 Drs. 17/15915-neu.
18 PlPr 17/155, S. 73.
19 Drs. 17/15915-neu (so ist das Rechtsgut der *„öffentlichen Ordnung"* überzeugend ersatzlos gestrichen worden; verfassungsrechtlich problematisch ist hingegen ein generelles Verbot von Versammlungen auf Bundesautobahnen).
20 Brenneisen, DP 4/2022, S. 30.
21 Kritik auch durch Pietsch, KriPoZ 2022, S. 36.
22 Vgl. dazu Tölle, Die Polizei 2022, S. 119; Brenneisen, DP 4/2022, S. 30.
23 Brenneisen, DP 4/2022, S. 30.
24 Drs. 17/12423, S. 84.
25 Vgl. Köhler, in: Meyer-Goßner/Schmitt, 2021, Strafprozessordnung, 64. Aufl., § 163, Rn. 1; Griesbaum, in: Hannich, 2019, Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl., § 163, Rn. 1.
26 Drs. 17/12423, S. 84.
27 Drs. 17/15915-neu.
28 Für Verwaltungsunrecht § 28 Abs. 1 Nr. 1 MEVersG, Art. 21 Abs. 1 Nr. 7 BayVersG, § 28 Abs. 1 Nr. 2 VersammlG LSA, § 21 Abs. 1 Nr. 4 NVersG, § 24 Abs. 1 Nr. 1 VersFG SH u. § 27 Abs. 1 Nr. 1 VersFG BE; vgl. dazu Schott/Ullrich, in: Ullrich/von Coelln/Heusch, 2021, Handbuch Versammlungsrecht, Rn. 324; Peters, in: Peters/Janz, 2021, a.a.O., F, Rn. 29; Elzermann/Schwier, 2019, Sächsisches Versammlungsgesetz, 2. Aufl., § 28, Rn. 4; Brenneisen/Martins, Die Polizei 2018, S. 330.
29 Für Verwaltungsunrecht § 28 Abs. 1 Nr. 8 MEVersG, § 24 Abs. 1 Nr. 5 VersFG SH u. § 27 Abs. 1 Nr. 4 VersFG BE.
30 Redaktionell fehlerhaft ist in § 27 Abs. 2 VersG noch von einer *„Anmeldung"* die Rede.
31 Bei abweichender Durchführung für Verwaltungsunrecht § 28 Abs. 1 Nr. 5 MEVersG, § 21 Abs. 1 Nr. 7 NVersG, § 24 Abs. 1 Nr. 4 VersFG SH u. § 27 Abs. 1 Nr. 1 VersFG BE; bei einer Missachtung von Beschränkungen für Verwaltungsunrecht § 28 Abs. 1 Nr. 6 MEVersG, § 21 Abs. 1 Nr. 10 NVersG, § 24 Abs. 1 Nr. 5 VersFG SH u. § 27 Abs. 1 Nr. 4 VersFG BE.
32 So auch Brinsa, in: Breitbach/Deiseroth, 2020, a.a.O., S. 1018, 1025.
33 Drs. 17/12423, S. 86.
34 Vgl. dazu Knape/Brenneisen, 2021, a.a.O., § 19, Rn. 15; Brenneisen/Wilksen/Staack/Martins, 2016, a.a.O., § 17, Rn. 8; siehe auch Lembke, in: Breitbach/Deiseroth, 2020, a.a.O., S. 1619; Kniesel/Poscher, in: Bäcker/Denninger/Graulich, 2021, Handbuch des Polizeirechts, 7. Aufl., J, Rn. 86; Kniesel, in: Kniesel/Braun/Keller, 2019, Versammlungsgesetze, 18. Aufl., I, Rn. 194.
35 Brenneisen, DP 4/2022, S. 30; Pietsch, KriPoZ 2022, S. 36.
36 Für Verwaltungsunrecht u. zusätzliche Verwaltungsakzessorietät § 28 Abs. 1 Nr. 7 MEVersG, § 24 Abs. 1 Nr. 7 VersFG SH; für kriminelles Unrecht u. Verwaltungsakzessorietät § 20 Abs. 2 Nr. 4, 5 NVersG, § 26 Abs. 2 Nr. 3 VersFG BE; vgl. dazu Knape/Brenneisen, 2021, a.a.O., § 19, Rn. 23; Brenneisen/Wilksen/Staack/Martins, 2016, a.a.O., § 17, Rn. 18; Miller, in: Wefelmeier/Miller, 2020, Niedersächsisches Versammlungsgesetz, 2. Aufl., § 20, Rn. 11.
37 BVerfGE 122, 342; vgl. dazu Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 262.
38 Kniesel, in: Kniesel/Braun/Keller, 2019, a.a.O., II, § 17a, Rn. 4; vgl. auch Lembke, in: Breitbach/Deiseroth, 2020, a.a.O., S. 912; Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 250; dies., 2016, a.a.O., § 17, Rn. 29; Brenneisen/Wilksen, Die Kriminalpolizei 4/2018, S. 20; Brenneisen/Martins, Die Polizei 2016, S. 258.
39 Brenneisen/Wilksen, Die Kriminalpolizei 4/2018, S. 20; Brenneisen/Martins, Die Polizei 2016, S. 258; dies., Kriminalistik 2015, S. 318.
40 Vergleichbar auch § 17 Abs. 1 Nr. 2 MEVersG, § 9 Abs. 1 NVersG, § 17 Abs. 1 Nr. 2 VersFG SH u. § 19 Abs. 1 Nr. 2 VersFG BE; siehe dazu Knape/Brenneisen, 2021, a.a.O., § 19, Rn. 16; Brenneisen/Wilksen/Staack/Martins, 2016, a.a.O., § 17, Rn. 9.
41 Vgl. dazu LG Stendal v. 4.4.2014, Az. 503 Qs 1/14-juris; vorgehend AG Burg v. 27.1.2014, Az. 22a Ds 303 Js 14896/13-juris.
42 Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 250; nicht überzeugend hingegen Bewertung der GeneralStA Berlin v. 8.12.2021, Az. 4030-419-4.
43 Drs. 17/12423.
44 Vgl. §§ 18, 28 Abs. 1 Nr. 7 MEVersG, §§ 3, 28 BVersG, Art. 7, 21 Abs. 1 Nr. 2 BayVersG, §§ 3 Abs. 3, 21 Abs. 1 Nr. 1 NVersG, §§ 3, 29 SächsVersG, §§ 3, 27 VersammlG LSA, §§ 8 Abs. 2, 24 Abs. 1 Nr. 7 VersFG SH u. §§ 9 Abs. 2, 27 Abs. 1 Nr. 6 VersFG BE; dazu Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 242.
45 Für Verwaltungsunrecht Art. 21 Abs. 1 Nr. 2 BayVersG; Für Verwaltungsunrecht u. zusätzliche Verwaltungsakzessorietät § 28 Abs. 1 Nr. 7 MEVersG, § 21 Abs. 1 Nr. 1 NVersG, § 24 Abs. 1 Nr. 7 VersFG SH u. § 27 Abs. 1 Nr. 6 VersFG BE.
46 Zum verfassungsrechtlichen Waffenverbot vgl. Höfling, in: Sachs, 2021, a.a.O., Art. 8, Rn. 38; Ernst, in: Kämmerer/Kotzur, 2021, a.a.O., Art. 8, Rn. 62; Jarass, in: Jarass/Kment, 2020, a.a.O., Art. 8, Rn. 9.
47 Drs. 17/12423, S. 62; zur Kritik an dieser Bestimmung Brenneisen, DP 4/2022, S. 30; Pietsch, KriPoZ 2022, S. 36.
48 Als Vorbild kommen hier § 20 Abs. 1 Nr. 1 NVersG, § 23 Abs. 2 VersFG SH u. § 26 Abs. 2 Nr. 1 VersFG BE in Betracht; vgl. dazu Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 233; Brenneisen, Kriminalistik 2018, S. 34.
49 Zu den *„Mängeln des Sächsischen Versammlungsgesetzes"* vgl. z.B. Schwier, 2017, Zum aktuellen Stand des Versammlungsrechts, S. 195 ff.; vgl. zum SächsVersG u. VersammlG LSA auch Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 60-62.
50 PlPr 17/114, S. 131 (Reul); PlPr 17/155, S. 61 (Katzidis), S. 65 (Lürbke) u. S. 70 (Reul).
51 Pahl/Tölle, in: Peters/Janz, 2021, a.a.O., E, Rn. 115; Kniesel/Poscher, in: Bäcker/Denninger/Graulich, 2021, a.a.O., J, Rn. 22; Wapler, in: Breitbach/Deiseroth, 2020, a.a.O., S. 1161; Brenneisen/Wilksen/Staack/Martins, 2020, a.a.O., S. 593; Brenneisen, Die Kriminalpolizei 1/2020, S. 28; Schieder, NVwZ 2013, S. 1325.
52 Enders, in: Dürig-Friedl/Enders, 2016, Versammlungsrecht, Einl., Rn. 16.
53 So aber wohl Pietsch, KriPoZ 2022, S. 36 (u.a. unter Hinweis auf Frommel, NK 2020, S. 123).

Die Propaganda der RAF zwischen Wahn und Wirklichkeit 1970-1998

– Täter als Opfer und Opfer als Täter

Von Dr. Harald Bergsdorf, Dümpelfeld*

1 Einleitung

Am 14. Mai 1970 befreiten Gudrun Ensslin, Ulrike Meinhof und weitere RAF-Kader den inhaftierten Andreas Baader während eines Freigangs in einer Bibliothek. Hierbei verletzten sie einen Angestellten schwer. Die Tat gilt als Gründungsdatum der RAF. 50 Jahre danach und über 20 Jahre nach ihrer Selbstauflösung am 20. April 1998 beschäftigt die *„Rote Armee Fraktion"* (RAF) weiterhin Teile der bundesdeutschen Öffentlichkeit. Gerade Jahrestage liefern Anlässe, sich mit der RAF zu befassen, deren Mordserie bis heute partiell unaufgeklärt ist, darunter die Attentate auf Ernst Zimmermann 1985, Karl Heinz Beckurts und seinen

Fahrer Eckhard Groppler 1986, Gerold von Braunmühl 1986, Alfred Herrhausen 1989 und Detlev Karsten Rohwedder 1991.

Einige Filmemacher, Journalisten, Publizisten und Wissenschaftler zieht die mörderische RAF-Geschichte bis heute sogar in ihren Bann. Das Abtauchen einer kleinen Gruppe junger Leute in den Untergrund, ihr terroristischer *„Kampf"* gegen die westdeutsche Wohlstandsgesellschaft und ihre offenkundige Bereitschaft, nach dem Motto *„Sieg oder Tod"* sowohl zu morden als auch selbst zu sterben, verströmen immer noch eine *„morbide Faszination"* (Petra Terhoeven). Das umso mehr, weil die meisten RAF-Terroristen, insbesondere RAF-Führungspersonen, nicht als abgehängte Außenseiter geboren und aufgewachsen waren, sondern oft aus gehobenen, religiös und bildungsbürgerlich geprägten Milieus stammten. Aus den sozialen Souterrains der Gesellschaft kam lediglich eine Minderheit in der RAF, darunter Petra Schelm, Verena Becker und Peter-Jürgen Boock.

Inzwischen sind zahlreiche Gesamtdarstellungen über die RAF erschienen. Zugleich mangelt es weiterhin an Spezialstudien zum Beispiel über die Rolle der RAF-Anwälte, die sich mehrheitlich als *„Genossen"* der Täter verstanden. Ebenso fehlt es an biographischen Untersuchungen über Führungsfiguren der sogenannten 2. und 3. RAF-Generation wie vor allem Brigitte Mohnhaupt und Birgit Hogefeld – beide liefern Beispiele für die fast durchgängige Dominanz von Frauen in RAF-Führungspositionen, wohingegen Männer als Täter in der allgemeinen Kriminalität deutlich überrepräsentiert sind. Ein weiteres Desiderat besteht nicht nur in Studien über prominente und vor allem nicht-prominente RAF-Opfer und ihre Hinterbliebenen, sondern auch in Analysen der RAF-Propaganda, die einen wesentlichen Beitrag zum fast dreißigjährigen Überleben der Terrorgruppierung leistete. Die RAF betrieb eben auch eine Kommunikationsstrategie, um durch Propaganda eine Diskurs- und Deutungshoheit über die eigenen Verbrechen zu erlangen. Letztlich wollte die RAF sowohl Schrecken erzeugen als auch durch Propaganda größere gesellschaftliche Gruppen für ihre revolutionären Ziele gewinnen und mobilisieren.

2 Selbstviktimisierung

Zu den zentralen Kennzeichen der RAF-Propaganda gehörte es, auf Basis ihrer *„Antifaschismus"*-Doktrin eine Täter-Opfer-Umkehr zu betreiben, das heißt: RAF-Täter zu viktimisieren und RAF-Opfer zu entmenschlichen bzw. zu animalisieren – u.a. als *„Kapitalisten-, Bullen- und Nazischweine"*. Im Kern präsentierte die RAF die Opfer ihrer Mordanschläge als die angeblich wirklichen Täter. Um ihre Morde als *„Gegengewalt"* und *„Notwehr"* zu legitimieren, hatte sie bereits in ihrem *„Konzept Stadtguerilla"* von 1971 proklamiert: *„Stadtguerilla heißt, sich von der Gewalt des Systems nicht demoralisieren zu lassen"*. Später befand sie in ihrer Auflösungserklärung 1998: *„Wir haben gewalttätige Verhältnisse mit der Gewalt der Revolte beantwortet"*.

Schon die Tötung des Studenten Benno Ohnesorg am 2. Juni 1967 durch den Schusswaffeneinsatz des Polizisten Karl-Heinz Kurras hatten spätere RAF-Gründer genutzt, um zum gewalttätigen Kampf gegen die Bundesrepublik zu mobilisieren. Hierbei hatten sie sich durchaus nicht nur auf Fiktionen, sondern partiell auch auf Fakten gestützt. Denn zum einen hatte Kurras den unbewaffneten Studenten, der als Pazifist galt und in einer evangelischen Studentengemeinde aktiv war, von hinten erschossen. Zum anderen hatte der wegen fahrlässiger Tötung angeklagte Täter vor Gericht sogar einen Freispruch wegen schuldausschließender Notwehr (*„putativer Notwehr"*) errungen, weil er irrigerweise hatte glaubhaft machen können, sich durch den unbewaffneten Studenten mit einem Messer angegriffen gefühlt zu haben. Nicht nur spätere RAF-Gründer empörte damals sowohl die Tötung des Unbewaffneten als auch der Freispruch des Täters.

Später nutzte die RAF die Tötung Ohnesorgs und den Freispruch Kurras für ihre pauschale Propaganda gegen den *„faschistischen Repressionsstaat"* und zur Legitimation ihrer Morde – dass der später als MfS-Zuträger enttarnte Todesschütze Kurras sein Opfer Ohnesorg im Auftrag der SED ermordet hat, lässt sich bislang nicht belegen, würde aber wenig verwundern. Gudrun Ensslin hatte bereits kurz nach der Tötung Ohnesorgs durch Kurras appelliert: *„Dieser faschistische Staat ist darauf aus, uns alle zu töten. Das ist die Generation von Auschwitz! Wir müssen Widerstand leisten. Gewalt kann nur mit Gewalt beantwortet werden."* Die *„Bewegung 2. Juni"*, später unter Übernahme einer stattlichen Mitgift teilweise in der RAF aufgegangen, instrumentalisierte das Datum der Tötung Ohnesorgs bereits in ihrer Selbstbezeichnung, um ihren Terror als *„Gegengewalt"* zu legitimieren.

Im Kampf gegen den angeblich strukturell gewalttätigen *„Kapitalismus"* hatte Ulrike Meinhof bereits im Juni 1970 den Einsatz von Schusswaffen gegen Polizeibeamte als Vertreter des *„faschistischen Repressionsstaates"* propagiert, der in seiner realen Ausrichtung weit entfernt vom NS-Unrechtsstaat war (und ist). Das gilt (und galt) auch nach dem parlamentarischen Beschluss der Notstands- und der Antiterrorgesetze, die aus RAF-Sicht eine Neuauflage von NS-Gesetzen bedeuteten, womit die RAF die Hitler-Diktatur verharmloste. In ihrem *„Schießbefehl"* hatte die RAF-Propagandachefin appelliert: *„Wir sagen natürlich, die Bullen sind Schweine, wir sagen, der Typ in Uniform ist ein Schwein, kein Mensch, und so haben wir uns mit ihm auseinanderzusetzen. D.h. wir haben nicht mit ihm zu reden…und natürlich kann geschossen werden!"* Denn Aufgabe der *„Bullen"*, denen sie das Menschsein abspricht, sei es, die *„Verbrechen des Systems zu schützen"*.

Tatsächlich war die Mehrzahl der RAF-Mitglieder bei ihrer Verhaftung mit geladenen und entsicherten Pistolen bewaffnet, um sich einen Fluchtweg frei zu schießen. Das gilt u.a. für Brigitte Mohnhaupt und Adelheid Schulz bei ihrer Festnahme 1982 am RAF-Zentraldepot nahe Heusenstamm und für Christian Klar – äußerlich stark verändert und als Jogger getarnt – bei seiner Festnahme ebenfalls 1982 durch ein Großaufgebot an Spezialkräften, die dem Topterroristen erfolgreich eine Falle gestellt hatten, am RAF-Depot *„Daphne"* bei Aumühle im Sachsenwald. Bei (versuchten) Verhaftungen töteten RAF-Kader mehrfach vor allem geringer besoldete Polizeibeamte, u.a. Norbert Schmidt 1971 und Michael Newrzella 1993, oder verletzten sie schwer. Immer wieder gebrauchten RAF-Täter bei ihren Anschlägen auch Schrapnellmunition, um besonders schwere Verletzungen zu verursachen. Nach Meinhofs *„Schießbefehl"* starben auch mehrere RAF-Mitglieder, darunter Petra Schelm 1971, die auf jene Polizisten geschossen hatte, die sie daraufhin in Notwehr töteten. Um sich als Opfer des angeblich strukturell gewalttätigen *„Kapitalismus"* zu stilisieren, überschrieb die RAF ihre Tatbekennungen (*„Kommandoerklärungen"*) nach ihren Mordanschlägen üblicherweise mit den Namen von in Haft u.a. durch Selbsttötung gestorbenen oder bei Polizeieinsätzen getöteten RAF-Mitgliedern. Damit betrieb sie eine Art von Opferkult – zuletzt in ihrer Auflösungserklärung 1998.

Einen Höhepunkt erreichte die RAF-Propaganda gegen den *„faschistischen Repressionsstaat"* und gegen die *„kapitalistische Klassenjustiz"* 1972 nach der Verhaftung fast der gesamten Spitze der sog. 1. RAF-Generation. Die 2. RAF-Generation mutierte daraufhin – und nicht erst 1977 – beinahe zu einer RAF-Gefangenen-Freipressungsvereinigung. Hierzu agitierte die RAF in enger Kooperation mit ihren Anwälten zum einen mit dem Propagandabegriff der *„Isolationsfolter"* (*„Vernichtungshaft"*) und agierte zum anderen in Justizvollzugsanstalten mit *„kollektiven Hungerstreiks"*, um den Kampf gegen das

„Schweinesystem" aus der Haft heraus fortzusetzen. Insbesondere *„Isolationsfolter"* und *„Vernichtungshaft"* belegten aus RAF-Sicht die schleichende Entwicklung des bundesdeutschen *„Kapitalismus"* zum *„Faschismus"*.

Zwar lebten RAF-Gefangene – wie Ulrike Meinhof in einem abgelegenen Teil der Justizvollzugsanstalt Köln-Ossendorf – phasenweise unter harten Haftbedingungen, die u.a. dazu dienten, bewaffnete Befreiungsversuche, wie sie die RAF durchaus propagiert hatte, und Selbsttötungen von Gefangenen zu erschweren. Kritiker monierten damals, die Zelle Meinhofs sei rund um die Uhr beleuchtet. Darüber hinaus dürfe sie im *„toten Trakt"* nur selten Besuch empfangen und das ausschließlich unter polizeilicher Überwachung. Letztlich leide sie unter sozialer Isolation und sowohl akustischem als auch visuellem Reizentzug (*„sensorische Deprivation"*). Meinhof scheute sich damals freilich nicht, das eigene Schicksal in Ossendorf mit den Mordfabriken in Auschwitz beinahe gleichzusetzen. Fast zeitgleich hatte sie den palästinensischen Mordanschlag auf israelische Sportler in München, mit dem auch sie freigepresst werden sollte, noch als *„antifaschistische"* und antiimperialistische Großtat der *„Menschlichkeit"* heroisiert.

Doch gerade in Stuttgart-Stammheim profitierte die RAF-Spitze von besonders generösen Haftumständen. In Stammheim brach der Strafvollzug unter dem Druck der damals breiten RAF-Sympathisantenszene mit zwei traditionellen Grundsätzen: Zum einen dem Prinzip, Männer und Frauen getrennt unterzubringen und zum anderen der Regel, Beschuldigte eines Verfahrens ebenfalls getrennt unterzubringen, um Absprachen zu erschweren. Dadurch verbrachten die privilegierten Häftlinge täglich mehrere Stunden miteinander im *„Umschluss"*. Obendrein empfingen sie häufig Besuch, genossen eine besondere Verpflegung und erhielten Sportgeräte – nicht zuletzt, um ihre Haft- und Verhandlungsfähigkeit im RAF-Prozess zu sichern. Beachtlich war neben Fernseh- und Radiogeräten auch die Literatur in den Haftzellen der RAF-Täter, darunter nicht nur Werke von Marx – als dem geistigen Urvater des gewaltsamen *„Antikapitalismus"* –, Lenin und Mao, sondern auch *„Guerilla"*-Literatur u.a. über moderne Sprengtechniken und polizeiliche Fachliteratur u.a. über Fahndungsmethoden.

Das alles vernebelten die *„politischen Gefangenen"* der RAF, die entgegen ihrer Propaganda nicht wegen ihrer politischen Überzeugungen, sondern wegen des dringenden Verdachts schwerster Straftaten inhaftiert waren. Obendrein erreichten die RAF und ihre Anwälte – nach der Selbsttötung Ulrike Meinhofs 1976 nach schweren Auseinandersetzungen in der RAF-Spitze – die Verlegung Brigitte Mohnhaupts nach Stammheim. Damit wollten die zuständigen Politiker der RAF-Propaganda über die Haftbedingungen entgegenwirken. In Stammheim nutzten Baader und Ensslin die Zeit bis zur Haftentlassung Mohnhaupts im Februar 1977 freilich, um mit ihr die Mordanschläge der Folgezeit zu planen. Unter massivem Druck der *„Stammheimer"* auf ihre Genossen im Untergrund forcierte die sogenannte 2. RAF-Generation um Mohnhaupt 1977 ihre Versuche, die inhaftierte RAF-Spitze nach dem Vorbild der Lorenz-Entführung freizupressen.

Die faktenferne RAF-Agitation gegen die *„Isolationsfolter"* förderten u.a. zahlreiche RAF-Anwälte und Intellektuelle wie Jean-Paul Sartre und Heinrich Böll, die sich frühzeitig an RAF-Desinformationskampagnen beteiligt hatten, indem sie die damalige Bundesrepublik in die Nähe des *„Dritten Reiches"* rückten. Im Kern ging es der RAF freilich weniger darum, Haftbedingungen zu verbessern. Vielmehr zielte sie darauf, RAF-Täter zu Opfern zu stilisieren, um die wirklichen Opfer herabzuwürdigen und als die wahren Täter darzustellen. Zustimmend hatte sie in ihrem programmatischen Text *„dem Volke dienen"* schon 1972 die Mao-Parole zitiert, wonach Bedeutung und Lebensrecht von Opfern *„fortschrittlichen"* Terrors letztlich weniger wögen als *„Schwanenflaum"* und getötete bzw. verstorbene Mitglieder der *„Guerilla des Volkes"*, also Täter, in ihrem Wert mehr Gewicht aufbrächten als ein *„Berg"*.

Als weiteres Druckmittel der RAF gegen den *„faschistischen Repressionsstaat"* fungierten *„kollektive"* Hungerstreiks. Gerade auch dadurch versuchte die RAF-Spitze, Täter als Opfer zu präsentieren. Hierbei kalkulierte die RAF-Spitze um Ensslin und Baader, die ihre Hungerstreiks immer wieder heimlich unterbrachen, frühzeitig mit Todesopfern unter ihren Gesinnungsgenossen, um den öffentlichen Druck auf die Politik zu erhöhen. Wörtlich hieß es dazu in einem Zellenzirkular von 1973: *„Wir brauchen eine leiche…eine leiche und wir haben was in der Hand"*. Daher forderten Ensslin und Baader von ihren Mitstreitern in den Hungerstreiks immer wieder, weiter an Körpergewicht zu verlieren.

Später, im November 1974, starb Holger Meins in der Justizvollzugsanstalt Wittlich/Mosel trotz Zwangsernährung an den Folgen des Hungerstreiks – nach seinem Tod bemängelten Kritiker medizinische Versäumnisse bei der ärztlichen Betreuung des Inhaftierten im Hungerstreik. Das wirkmächtige Bild seines Leichnams erinnerte Birgit Hogefeld an NS-Opfer in Auschwitz. Einen Tag nach dem Tod von Meins, den die RAF und ihre Anwälte zur Rekrutierung neuer Mitglieder gebrauchten, ermordete die *„Bewegung 2. Juni"* den Präsidenten des Berliner Kammergerichtes, Günter von Drenkmann, der mit Terroristen-Prozessen nie befasst war, aber aus RAF-Sicht zur verhassten *„Klassenjustiz"* gehörte. In ihren Bekennerschreiben versuchten die Täter, mit denen die RAF eine konfliktuelle Komplizenschaft verband, den Mord mit den Worten *„wer gewalt sät, wird gewalt ernten"* zu rechtfertigen.

Nach dem Tod von Meins demonstrierten jeweils mehrere tausend Personen in mehreren Städten der Bundesrepublik gegen den demokratischen Rechtsstaat, der am Tod des Mitglieds der RAF-Kommandoebene mitschuldig sei. Gerade auch den Tod und das Foto des Leichnams von Holger Meins nutzte die RAF für ihren propagandistischen Kampf mit Worten und Bildern gegen den *„faschistischen Repressionsstaat"*, der das Mitglied der RAF-Kommandoebene ermordet habe. Ähnlich agitierte die RAF nach der Selbsttötung Ulrike Meinhofs im Mai 1976 und den Suiziden Andreas Baaders, Gudrun Ensslins und Jan-Karl Raspes im Oktober 1977 nach dem Scheitern mehrerer Versuche der sogenannten 2. RAF-Generation und ihrer palästinensischen Komplizen, durch Entführungen und Morde die inhaftierte Spitze der sog. 1. RAF-Generation freizupressen. Den Tod durch Selbsttötung in der *„Stammheimer Todesnacht"* 1977 bestätigen später gerichtsmedizinische Gutachter aus dem In- und Ausland. Anhaltspunkte für schuldhaftes Verhalten Dritter verneinte die zuständige Staatsanwaltschaft damals. Mit ihren als *„faschistische"* Morde präsentierten Selbsttötungen wollten Ensslin, Baader und Raspe dem *„System"* offenbar einen letzten schweren Schlag versetzen und der RAF einen letzten Dienst erweisen – aus RAF-Sicht hatte der *„kapitalistische"* Staat die Gefangenen entweder direkt ermordet oder ihren Tod durch *„Repression"* zumindest indirekt verursacht. Nach der *„Stammheimer Todesnacht"* rekrutierte die RAF für sich weiteren Nachwuchs.

Letztlich versuchte die RAF durchgängig, die eigenen Verbrechen durch Verweis auf den *„gewalttätigen Kapitalismus"* zu legitimieren. So heißt es in ihrer Auflösungserklärung ausgerechnet vom 20. April 1998, die RAF-Opfer so gut wie komplett ausblendet, RAF-Täter weiter heroisiert und RAF-Verbrechen erneut rechtfertigt: *„Wir stehen zu unserer Geschichte…Wir sind froh, Teil dieses Versuchs gewesen zu sein…Das Ende des Projektes zeigt, dass wir auf diesem Weg nicht durchkommen konnten.*

Aber es spricht nicht gegen die Notwendigkeit und Legitimation der Revolte…Denn der tatsächliche Terror besteht im Normalzustand des ökonomischen Systems". Bezeichnenderweise erinnert die RAF in ihrer Auflösungserklärung mit Schleyer nur an ein einziges RAF-Opfer, um ihn nochmals ausschließlich als Täter darzustellen, ohne – natürlich – an sein Engagement in der rechtsstaatlichen Demokratie zu erinnern, der es aus RAF-Sicht vollständig an Legitimität fehlte. Als ihren letztlich einzigen Fehler konzediert die RAF in ihrer Auflösungserklärung lediglich, sie habe es versäumt, über und neben ihr als mordender *„Fraktion"* eine politische Partei aufzubauen, um den *„terroristischen Kapitalismus"* wirkungsvoller mit Attentaten und Agitation zu bekämpfen.

In typischer RAF-Diktion hatte Bernhard Rössner, einer der Täter des RAF-Anschlags auf die deutsche Botschaft 1975 in Stockholm, bereits 1994 über sein Verhältnis zu RAF-Opfern und ihren Hinterbliebenen erklärt, er empfinde weder Reue noch Bedauern über RAF-Morde. Denn *„Krieg ist Krieg und vorbei ist vorbei"*. Als wahre Opfer sehe er ohnehin eher die Armen und Vernachlässigten des *„Kapitalismus"*. Damit befolgte Rössner wie fast alle anderen RAF-Mitglieder die RAF-Devise, keine Reue und kein Bedauern gegenüber RAF-Opfern zu zeigen.

3 Fazit

Im Ergebnis haben Terror und Propaganda der RAF die Bundesrepublik zwar erschüttert, aber in ihrer Substanz und Existenz nie gefährdet. Die Morde und anderen Gewalttaten der RAF bedeuteten primär eine ernste Herausforderung für die öffentliche Sicherheit der rechtsstaatlichen Demokratie. Nie war die freiheitlich-demokratische Grundordnung selbst durch die RAF wirklich gefährdet. Vielmehr erwies sich die rechtsstaatliche Demokratie als wehrhaft. Zu keiner Zeit gelang es der gesellschaftlich und politisch weitgehend und zunehmend isolierten RAF, durch Terror und Propaganda mehr als nur kleine und laute, später schrumpfende Minderheit an Sympathisanten hinter sich zu scharen, bei denen die RAF-Agitation zumindest phasenweise auf fruchtbare Felder fiel. Das Ziel der RAF, die Akzeptanz der rechtsstaatlichen Demokratie in der Bevölkerung zu verringern und den eigenen Rückhalt unter den Bundesbürgern zu erhöhen, scheitere fast vollständig. Letztlich wandte sich die übergroße Mehrheit der Befragten gegen die RAF, darunter die überwältigende Mehrheit der Arbeiter, Arbeitslosen und Randgruppen, für deren Ideale und Interessen die RAF einst zu kämpfen vorgegeben hatte.

Die weitgehende und zunehmende Isolierung der RAF in der Bevölkerung gründete inhaltlich erstens auf der wachsenden Selbstbezogenheit der Terrorgruppierung, deren sog. 2. Generation fast ausschließlich auf die Befreiung der eigenen Genossen aus der Haft zielte. Eine andere Ursache für ihren fortschreitenden Niedergang bestand zweitens in der außerordentlichen Brutalität der RAF, die weder vor der Tötung junger Polizisten zurückschreckte noch vor der besonders perfiden Ermordung des jungen US-Soldaten Edward Pimental per Genickschuss, dessen Hinrichtung 1985 – weit nach Ende des Vietnamkrieges – durch Mitglieder der sog. 3. RAF-Generation selbst in Teilen des RAF-Sympathisantenumfeldes eher aus strategischen als moralischen Gründen auf Kritik stieß und auch RAF-Apologeten an SS-Methoden erinnerte. Erst viel später nannte Birgit Hogefeld die Ermordung des jungen Soldaten *„zutiefst unmenschlich"* und erkannte zwischen NS- und RAF-Methoden gar einige Parallelen. Bereits 1977 war die RAF als Auftraggeberin (mit-) verantwortlich für die Entführung einer Lufthansa-Maschine mit vielen normalen Urlaubern, darunter Kinder, an Bord und die Ermordung des Flugkapitäns Jürgen Schumann durch palästinensische Terroristen, die damit letztlich vergeblich versuchten, die Stammheimer Häftlinge freizupressen. Gerade auch damit stieß die RAF auf besonders hohe Ablehnung in der Bevölkerung. Trotz ihrer Versuche, nach 1977 wieder stärker Anschluss an linksextremistische Milieus zu finden, wuchs die Isolierung der RAF. Im Ergebnis avancierte die RAF nie zu einer Avantgarde einer Front aller *„fortschrittlichen Kräfte"* gegen den *„faschistischen Kapitalismus"*.

Drittens basierte die weitgehende Isolierung der RAF sowohl auf der grundsätzlich breiten Unterstützung der rechtsstaatlichen Demokratie und Sozialen Marktwirtschaft in der bundesdeutschen Bevölkerung als auch dem konkreten Handeln der verantwortlichen Politiker bei der Terrorbekämpfung. Wie stark die große Mehrheit der Wahlberechtigten damals die demokratischen und staatstragenden Parteien CDU/CSU, SPD und FDP und damit auch die rechtsstaatliche Demokratie selbst unterstützte, unterstreichen unter anderem ihre Zweitstimmenanteile bei den Bundestagswahlen 1976 und 1980 von insgesamt je über 95%. Dieses Ergebnis deutet auf eine grundsätzlich hohe Zustimmung zur Politik der wichtigsten Parteien, die damals gerade auch mit Terrorbekämpfung befasst waren.

Die maßgeblichen Parteien des Verfassungsbogens reagierten aus Sicht der großen Bevölkerungsmehrheit insgesamt gleichermaßen hart und besonnen auf die Bedrohung durch die RAF. Einerseits zeigten Regierung und Opposition gerade während der Schleyer-Entführung 1977 Härte, um den Erpressern – anders als während der Lorenz-Entführung 1975 durch die *„Bewegung 2. Juni"* – nicht nachzugeben. Das zentrale Ziel bestand darin, an potentielle Nachahmer ein klares Signal der Konsequenz auszusenden. Das auch deshalb, weil zwei durch die Lorenz-Entführung freigepresste Terroristen danach ihren terroristischen Kampf in der RAF fortgesetzt hatten.

Dass der demokratische Rechtsstaat gegenüber weitgehend reuigen RAF-Mördern andererseits, wenn sie Kooperationsbereitschaft zeigen, auch zur Milde fähig ist, belegt der Fall des Werner Lotze, der trotz eines vollendeten Mordes an einem Polizeibeamten bereits nach fünfeinhalb Jahren auf Bewährung aus der Haft freikam. Lotze profitierte von der Kronzeugenregelung, weil er über seine und Tatbeiträge anderer RAF-Täter substanziell ausgesagt hatte. Auch durch die Verkürzung langjähriger Haftstrafen – die sog. *„Kinkel-Initiative"* von 1992 durch den damaligen Bundesjustizminister Klaus Kinkel im Auftrag des seinerzeitigen Bundeskanzlers Helmut Kohl – bewies der demokratische Rechtsstaat eine Bereitschaft zur *„Versöhnung"*. Obendrein leistete er dadurch einen Beitrag, die RAF zu spalten und weiter zu schwächen, die durch das Ende der SED-Diktatur einen wichtigen Helfer verlor.

Auf andere Art besonnen hatte bereits 1977 der damalige Oberbürgermeister von Stuttgart Manfred Rommel, Sohn eines Generals der Wehrmacht, auf hasserfüllte Forderungen aus der Bevölkerung reagiert, Ensslin, Baader und Raspe nach der *„Stammheimer Todesnacht"* auf einer Müllhalde zu verscharren. Rommel widersprach dem deutlich. Der christdemokratische Politiker plädierte vielmehr und letztlich erfolgreich dafür, alle drei Terroristen in Stuttgart auf einem Friedhof zu bestatten, weil mit dem Tod jede Feindschaft aufhören müsse. Nebenbei erschwerte eine solche Haltung die RAF-Propaganda gegen den *„faschistischen Repressionsstaat"*.

Anmerkung

* Der Autor ist Politikwissenschaftler, Zeithistoriker und Buchautor mit den Schwerpunkten Parteien, Demokratie, Extremismus, Terrorismus und deutsche Geschichte seit 1870/71.

„Geh´ mit (k)einem Fremden mit...!“ – Kriminalprävention in der Praxis (Teil 2)

Von Rudi Heimann und Dr. Jürgen Fritzsche, Selters/Luxemburg[1]

2.1 Sally-Anne-Test

Eine Möglichkeit, um die Fähigkeit eines Kindes zu testen, ob es die Ansichten oder Perspektiven anderer Personen von den eigenen zu unterscheiden vermag, ist der Sally-Anne-Test.[2] Dabei wird dem Kind die kurze Geschichte von Sally und Anne erzählt – möglicherweise auch mit einem Puppenspiel visualisiert. Sally und Anne sind in einem Zimmer. Sally hat einen Korb und Anne eine Box. Sally nimmt eine Murmel und versteckt diese in ihrem Korb. Dann verlässt sie den Raum und geht spazieren. Während ihrer Abwesenheit nimmt Anne die Murmel aus Sallys Korb und legt sie in ihre eigene Box. Sally kehrt in den Raum zurück und dem Kind wird die Schlüsselfrage *„Wo wird Sally nach ihrer Murmel suchen?“* gestellt. Antwortet das Kind richtigerweise, dass Sally glaubt die Murmel sei noch immer in ihrem Korb, zeigt dies, dass das Kind versteht, dass Sally eigene Überzeugungen hat, die möglicherweise nicht der Wirklichkeit entsprechen. Antwortet das Kind, dass die Murmel in der Box sei, war es ihm nicht möglich, sich in die Perspektive von Sally hinein zu denken.

2.2 Weitere Hilfestellungen

Je vertrauter einem Kind die soziale Umgebung ist, desto wahrscheinlicher können Kinder über Ursache-Wirkungs-Verhältnisse reflektieren.[3] Die Flexibilität des Denkens führt dazu, dass sie mehrere Aspekte und damit mehrere Sichtweisen ein und derselben Situation betrachten können. Während jüngere Kinder noch die Angewohnheit aufweisen, bei einer Aufgabe zu verharren, zeigen Grundschulkinder die Fähigkeit, sich wechselnden Anforderungen anzupassen und darauf zu reagieren. Dies beinhaltet auch raschere und zielführendere Planungen eigener Handlungen. Je mehr soziale Vergleiche mit Gleichaltrigen wahrgenommen werden, desto differenzierter, umfassender und realistischer werden Selbsteinschätzungen vorgenommen. Die Schule fördert diese Tendenz und dies insbesondere dadurch, wenn die Leistungen durch Notengebung wiederholt miteinander verglichen werden. Die Kinder beginnen übergreifende Konzepte zu bilden *(„Ich kann gut schwimmen und schieße viele Tore – damit bin ich sportlich“)*. Neben der eigenen Einschätzung haben die Anerkennung und der Zuspruch von Erwachsenen und Gleichaltrigen einen Einfluss auf das Selbstwertgefühl. Selbst Kinder, die ihre Leistungen in sämtlichen Bereichen eher gering einschätzen, können bei entsprechender Unterstützung und Wertschätzung durch das soziale Umfeld ein hohes Selbstwertgefühl entwickeln, wenn ihnen der Eindruck vermittelt wird, dass sie so, wie sie sind, anerkannt werden. Im Gegenteil kann ein Kind, das zwar diese Anerkennung erfährt, jedoch ständig an seinen eigenen Leistungsansprüchen scheitert, ein geringes Selbstwertgefühl haben. Dieser Entwicklung kann entgegengewirkt werden, indem durch ein ausgewogenes Verhältnis von Erfolgs- und Misserfolgserlebnissen ein realistisches Selbstbild gefördert wird[4]. Bereits Kleinkinder streben danach, sich so viele Erfolgserlebnisse wie möglich zu verschaffen, weil sie dadurch ihre Autonomie stärken. Sie erleben und begreifen sich selbst immer mehr als Individuum und entwickeln eine erstaunliche Willensstärke, wenn es darum geht, ihre Ziele zu verfolgen. Eines der typischsten Beispiele für bestätigende Erfolgserlebnisse ist das Laufen lernen. Häufig finden die entmutigenden Versuche der Kleinkinder fernab von elterlichen Beobachtungen, und damit abseits von Lob, statt. Die Belohnung liegt in der erfolgreichen Bewältigung und erst in zweiter Instanz in der Anerkennung durch die Umgebung. Andererseits müssen Kinder und Jugendliche lernen, mit Misserfolgen umzugehen. Sie beobachten immer wieder, dass sie im Vergleich mit anderen an ihre Grenzen stoßen, weil sie bestimmte Dinge nicht so gut können wie andere. Dieses frustrierende Ereignis ist im Laufe des Heranwachsens unausweichlich und sollte durch die Eltern zugelassen werden. Kinder und Jugendliche müssen lernen, in solchen Situationen nicht an sich selbst zu zweifeln, sondern die Misserfolge entweder hinzunehmen oder sich dazu entschließen, aktiv zu werden, um doch noch Erfolg zu haben. Dies kann gelingen, indem sie beispielsweise um Hilfe bitten oder die Motivation aufbringen, zu üben und die eigenen Fähigkeiten zu trainieren und zu verbessern. Der Selbstwert wird zudem nicht nur von schweren, sondern auch durch regelmäßige leichte Körperstrafen negativ beeinflusst.[5] Diese Strafen bergen zudem die Risiken von:

- einer Eskalation der Gewalt in der Familie
- schweren psycho-sozialen Auffälligkeiten (Ängstlichkeit, Kontaktarmut, Drogensucht)
- anti-sozialen Verhaltensweisen (Aggressivität oder fehlende Empathie)
- Lernen von Gewalt zur Konfliktlösung (Kreislauf der Gewalt)
- höherer Kriminalitätsneigung der Kinder (insbesondere häufigere Gewaltdelikte)

Daher ist es wichtig, so früh als möglich wirksame Alternativen

zu nutzen oder Verhaltensweisen in die Erziehung einzubinden, die unabhängig von entwicklungspsychologischen Gesetzmäßigkeiten die Sicherheit von Kindern erhöhen. Und dies geschieht idealerweise mit einer Wirksamkeit, die über die Kinderzeit und das Jugendalter hinaus reicht.

3 Eine Alternative

Die oft gehörte Warnung vor Fremden hat seine in diesem Beitrag aufgezeigten Grenzen und kann bei vertiefender Betrachtung keinesfalls die Wirkung erzielen, die Eltern oder andere Erziehungsverantwortliche damit gerne erreichen würden. Interpretationsspielräume, Verständnisprobleme, Zielgruppenungenauigkeit, altersbedingte und damit entwicklungspsychologische Grenzen machen das Befolgen der Verhaltensmaßregel für Kinder unter Umständen unmöglich. Bei der hier vorgeschlagenen Alternative spielen Emotionen eine wichtige Rolle. Sie bestimmen über unsere gesamte Lebenszeit als Auslöser das menschliche Handeln und wirken auch bei kognitiven Entscheidungsprozessen in bedeutender Weise mit. Dabei ist unser Bestreben grundsätzlich, angenehme Emotionen zu erzielen und unangenehme Emotionen zu vermeiden oder wenn letztere vorhanden sind, diese zu reduzieren. Die Emotionen selbst treten ab bestimmten Zeitpunkten im Verlauf der Kindheit erstmalig auf und erfüllen in Bezug auf die Person selbst sowie die soziale Umgebung unterschiedliche Funktionen. Bedeutend ist hier die Emotion der Furcht, die etwa ab dem neunten Monat feststellbar ist. Dass ein Kind Gefahr wahrnimmt, ist die Grundvoraussetzung, um eine Gefahr zu identifizieren und die natürlichen Flucht- oder Angriffstendenzen zu auszulösen.

3.1 Auf die Intuition ist Verlass

In einer Gefahrensituation ist das ungute Gefühl einer der verlässlichsten Faktoren, der einen Menschen vor dieser Gefahr warnen könnte. Dieses ungute Gefühl kann mit den Begriffen Angst oder Furcht gleichgesetzt werden. Gerade Angst wird jedoch eher als negatives Gefühl gewertet, das unerwünscht ist. Es wird nicht selten in einem Atemzug mit Depression genannt. Ängste müssen *„überwunden“* oder Angststörungen *„beseitigt“* werden. Dabei gehört Angst zu unseren Grundgefühlen[6] und sichert unser Überleben. Sie gehört zu den Emotionen, die kulturübergreifend vorhanden sind, woraus sich auf eine angeborene Kompetenz[7] schließen lässt. Es ist zur Erhöhung der eigenen Sicherheit wichtig, ungute Gefühle zu beachten und damit die eigene Intuition ernst zu nehmen. Dabei geht es nicht darum, in ständiger Besorgnis zu leben, sondern gelassen auf die vorhandenen Instinkte zu vertrauen. Um diese Instinkte zu fördern und zu fordern, können mit Kindern frühzeitig Gespräche über Lebenssituationen und die darin auftretenden Gefühle geführt werden. Interessanterweise haben Eltern kaum ein Problem damit, ihrem Kind zu erklären, was denn passieren könnte, wenn es unvorsichtig ohne Kontrollmaßnahmen (Blicke nach links und rechts) über die Straße geht. Die gleichen Eltern sprechen mit ihren Kindern jedoch nicht darüber, welche konkreten Folgen es haben kann, wenn sich Kinder trotz unguter Gefühle, ohne Kontrollmechanismen einem Erwachsenen anvertrauen oder einen Weg weitergehen, auf dem in Sichtweite mehrere ältere Kinder *„herumlungern“*. Diese sicherheitsfördernden Gespräche sollten sich an Standardsituationen orientieren, es können Erlebnisse des Tages besprochen werden oder es werden dazu Bilder mit emotionaler Gesichtsmimik genutzt, die zahlreich im Internet zu finden sind. Die hier dargestellte Aufzählung (Gefühlsliste) sollte altersangemessen und individuell erweitert werden und kann als Diskussionsgrundlage unter den Erziehungsverantwortlichen, wie auch im Dialog mit den Kindern dienen. Emotionsbezogene Erziehungspraktiken wirken sich positiv auf die sozioemotionale Entwicklung des Kindes aus.[8]

3.2 Die Gefühlsliste

Gefühlsliste – Welche Gefühle gibt es und welches werde ich als Kind bei nachstehenden Beispielen wahrscheinlich entwickeln?	
Ein angeleinter, großer Hund kommt auf dich zugestürmt.	Angst, Furcht
Ein anderes Kind hat ein neues Spielzeug.	Neugier, Neid
Du beobachtest auf dem Heimweg von der Schule wie ein Kind geschubst wird.	…
Du beobachtest ein Kind, das nach seinen Eltern sucht.	…
Ein Mitschüler will von dir Geld, damit er dich nicht schlägt oder schubst.	…
Du siehst einen Jugendlichen an einer Bushaltestelle, wie er mit einem Messer an den Plastiksitzen schnitzt.	…
Deine Lehrerin sagt laut in der Klasse, dass du eine *„Fünf“* in der Arbeit geschrieben hast.	…
Deine Oma möchte dich küssen, obwohl du es nicht willst.	…

Vor diesem Hintergrund ist stets zu prüfen, ob wir Kindern *„Ängste ausreden“* sollten oder diese – und damit auch die sonstigen Gefühle – nicht einfach nur ernst nehmen und *„erwachsen“* damit umgehen sollten. Der Angst, dass ein *„Monster unter dem Bett liegt“* kann entweder damit begegnet werden, dass es die Eltern weg sprechen *(„Da ist kein Monster. Du brauchst keine Angst zu haben.“)* oder es kann ernst genommen werden *(„Du hast also Angst, das hätte ich auch, wenn dort ein Monster wäre. Lass uns mal gemeinsam mit der Taschenlampe nachschauen.“)*. Auf lange Sicht führt die erste Variante dazu, dass es letztlich die Erwachsenen sind, die Kindern aus einer wissenden und überlegenen Position heraus sagen, wie ihre Gefühle *„sein sollten“* – was ein Kind zu empfinden hat. Ein fataler Schritt, wenn dann irgendwann potentielle Gewalttäter das Gleiche tun. Völlig tabu sind daher auch Erziehungsmaßregeln, die damit begründet werden, dass man selbst *„erwachsen“* sei, wisse, was gut für das Kind ist und damit das Kind mehr oder weniger bedingungslos – auf Grund seines Kindseins – den Anweisungen zu folgen habe *(„Erwachsene haben immer Recht“, „Erwachsenen widerspricht man nicht“)*. Dabei sind die Erziehungsmaßregeln nicht immer so plump und offensichtlich ungeschickt formuliert. Ein ständiges *„Ich weiß, was richtig/gut für dich ist“*, erwähnt zwar nicht ausdrücklich das Erwachsensein. Das Kind spürt jedoch sehr wohl, dass hierdurch das Erwachsenen-Kind-Verhältnis betont wird. Es ist auch darüber nachzudenken, ob die Zurückhaltung mit eigenen Gefühlen, wie sie uns durch soziale Instanzen wie Schulen, Universitäten, Arbeitsstellen und die Gesellschaft im Allgemeinen auferlegt werden, so erstrebenswert ist. Diese regulativen Elemente unserer Kultur werden von Kindern im Verlauf der Vorschulzeit

übernommen und später in ihr sich entwickelndes Selbst transferiert.[9] Wenn das Kind die Gefahr über seine Gefühle wahrnimmt, stellt sich die Frage, was in der Praxis zu tun ist, um das Risiko zu minimieren: An wen kann sich das Kind wenden; auf wen kann sich das Kind unter allen Umständen verlassen – auch ohne akuten elterlichen Rat? Als Antwort auf diese Fragen kann eine sogenannte Positivliste dienen, mit der sich gerade auf die Vertrauenspersonen im Leben eines Kindes konzentriert wird.

3.3 Positivliste

Mit einer Positivliste[10] ist die Frage zu klären, mit wem ein Kind immer und unter allen Umständen mitgehen oder mitfahren darf. Auch gilt, dass die festgelegte Person in die Wohnung gelassen werden darf, wenn das Kind alleine zu Hause wäre. Sie umfasst damit alle Vertrauenspersonen, die nach der einheitlich gefundenen Meinung von Kind, Vater und Mutter (oder anderen Erziehungsverantwortlichen) jederzeit das Kind überall alleine abholen dürften oder wenn es alleine in der Wohnung ist, diesen die Tür öffnen darf. Um dem Kind die Aufgabe nicht zu leicht zu machen, sollte es zuerst Namen aufschreiben. Anschließend das eine Elternteil und schließlich, getrennt davon, das andere Elternteil. Kann das Kind noch nicht im erforderlichen Ausmaß lesen und schreiben, dienen Fotos als Hilfe. Sind die Eltern nicht derselben Meinung, ergeben sich daraus Gespräche, warum abweichende Sichtweisen bestehen. Das Kind lernt, dass sich die Erziehungsverantwortlichen sorgen und mit Rat und Tat bereitstehen. Ideen wie: *„Nach Absprache"* oder *„Ruf mich an"* funktionieren in stressbehafteten Situationen nicht, sind von weiteren Bedingungen wie der Möglichkeit zu telefonieren abhängig und sollten unbedingt vermieden werden. Bei der Erstellung dieser Listen ist zu berücksichtigen, dass neben den Eltern andere Erziehungsverantwortliche existieren, die für das Kind besonders wichtig sind. Sie sollte um Telefonnummern erweitert werden, damit, wenn einmal die bevorzugten Vertrauenspersonen nicht erreicht werden können, weitere Menschen auf der Liste zu finden sind, die als mögliche Helfer zur Verfügung stehen. Dabei sollen die Rufnummern auswendig präsent und nicht nur über eine Kurzwahl oder Kontaktliste abrufbar sein, da ansonsten ohne dieses Gerät die Nummern nicht vorhanden sind. Wir sind immer wieder verwundert, welche großen Zahlenkolonnen gerade von Kindern im Gedächtnis abgespeichert werden können. Ist die Liste erstellt, sollte sie regelmäßig – jedoch immer bei Veränderungen wie Umzug, Schulwechsel, Vereinseintritt oder -austritt oder verändertem Freundeskreis – aktualisiert werden. Hat eine Person auch nur ein *„Minus"*, sollte sie von der Liste genommen werden und die Frage nach deren Erreichbarkeit erübrigt sich. Die Anpassung der Liste ist damit ein weiterer regelhafter Anlass, mit seinen Kindern über das Thema zu sprechen und es damit im Bewusstsein zu halten. Was und warum ein Kind darf oder nicht, sollte im Kreis verantwortungsvoller Erziehungsberechtigter offen besprochen werden können – im Interesse der Sicherheit des Kindes.

Beispiel-Positivliste direkt nach der Erstellung

Kind	Mama	Papa	Telefonnummer
Mama	+	+	0175-1223456
Papa	+	+	…
Oma Eva	+	+	…
Opa Heinz	+	+	…
Onkel Lukas	+	–	----------
Tante Carmen	+	+	…
Papa von Viktoria	–	–	----------
Mama von Alexander	+	+	…
Sporttrainer	–	+	----------
Klassenlehrerin	+	+	…

Diese Liste ist dabei nur Teil einer Gesamtkonzeption, bei der alle Erziehungsverantwortlichen in passenden Dosierungen regelmäßig an dem Thema Vorbeugung vor Gewalt arbeiten. Durch begleitende Seminare oder Trainings mit Kindern lassen sich zwar wichtige Impulse setzen – doch so wenig, wie ein zweitägiges Dauertraining einmal im Jahr zum Erhalt oder Steigerung der körperlichen Fitness führt – so wichtig ist die beständige Beschäftigung mit dem Thema Sicherheit. Die Liste führt in der Praxis dazu, dass ein Kind sehr genau weiß, welchem erwachsenen Menschen es vertrauen und damit auch *„sich anvertrauen"* kann. Daraus können sich Vertrauensverhältnisse entwickeln, die auch über schwierige Zeiten der Pubertät und Adoleszenz hinweghelfen können. Und das überdies in Eltern-Kind-Themen, bei denen es gerade nicht um Sicherheit oder Umgang mit Gewalt geht.

Bildrechte: Autoren.

Anmerkungen

1 Rudi Heimann ist Polizeivizepräsident im PP Südhessen, Kommentator der PDV 100 VS-NfD und Ressortverantwortlicher für die Ausbildung von Gewaltschutztrainern im Deutschen Karate Verband e.V. (DKV); Dr. Jürgen Fritzsche ist technischer Direktor des luxemburgischen Karateverbandes, ehemaliger Bundeslehrwart und wissenschaftlicher Koordinator des DKV.

2 Wimmer, H. & Perner, J. (1983). Beliefs about beliefs: Representation and constraining function of wrong beliefs in young children's understanding of deception. Cognition, 13(1) 10-128.

3 Goswami, U. (2008). Cognitive development. The learning brain. New York: Psychology Press.

4 Heimann R. & Kullmann K. (2020). Verantwortliche der Erziehung. In R. Heimann & J. Fritzsche (Hrsg.). Gewaltprävention in Erziehung, Schule und Verein. (S. 128 f). Wiesbaden: Springer.

5 Bussmann, K.-D. (2001). RdJB 2001, 35. S. 52.

6 Schloss, J. (2009). Does evolution explain human nature? Totally, for a Martian. In Celebrating the bicentenary of the birth of Charles Darwin. Philadelphia: John Templeton Foundation.

7 Ekman, P. & Friesen, W. V. (1971). Constants across cultures in the face and emotion. Journal of Personality and Social Psychology, 17(2). 124-129.

8 Eisenberg, N., Fabes, R. A., Shepard, S. A., Guthrie, I. K., Murphy, B. C. & Reiser, M. (1999). Parental reactions to children's negative emotions: Longitudinal relations to quality of children's social functioning. Child Development, 70(2), 513-534.

9 Heimann R. (2021). Gewaltprävention. In R. Heimann & J. Fritzsche (Hrsg.). Gewalt- und Krisenprävention in Beruf und Alltag: Ursachen und Lösungen für Gewalt und Krisen. Wiesbaden: Springer.

10 Fritzsche J. (2020). Modellseminar. In R. Heimann & J. Fritzsche (Hrsg.). Gewaltprävention in Erziehung, Schule und Verein. (S. 261). Wiesbaden: Springer.

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

§ 223 StGB – Körperverletzung; hier: Schütteln eines Säuglings. Im Anschluss an eine Impfung war ein Säugling zuerst ruhig und schläfrig, begann aber später zu weinen und zu quengeln. Schließlich wurde der A hektisch. In Unkenntnis der möglichen Folgen packte er den Säugling im Bereich des Beckens und riss ihn nach oben, um ihn an seine Schulter zu drücken. Dadurch fiel dessen Kopf zuerst nach hinten und dann nach vorn gegen die Schulter des A. Dies verursachte ein *„Schütteltrauma"*. Das Schreien des Säuglings verstummte zunächst nicht; kurze Zeit später erschlaffte sein Körper. Er reagierte dann nur noch auf mechanische Reize mit schrillem Schreien und es stellten sich Krämpfe ein. Es wurden umfangreiche Verletzungen diagnostiziert.

Die Tatsache, dass ruckartige Bewegungen eines Säuglings ohne Abstützen des Kopfes zu einer schwerwiegenden gesundheitlichen Beeinträchtigung führen können, ist allgemein bekannt. Auch der für Fälle der Verursachung eines Schütteltraumas bei Säuglingen oder Kleinkindern typische affektive Erregungszustand führt im Allgemeinen nicht dazu, dass die Gefährlichkeit der Handlung nicht ins Bewusstsein des Täters dringt. Ob der A, wie festgestellt, nur einmal (durch Hochreißen), oder aber, wie angeklagt, mehrfach (im Sinne eines Schüttelns) gewaltsam auf den Säugling eingewirkt hat, rechtfertigt vor allem die Abgrenzung zwischen direktem und bedingtem Verletzungsvorsatz, aber nicht die generelle Verneinung eines für das Grunddelikt maßgeblichen Körperverletzungsvorsatzes. (BGH, Urt. v. 16.12.2020 – 2 StR 209/20)

§§ 240, 22, 23 StGB – Versuchte Nötigung; hier gegenüber einem Polizeibeamten. Der A parkte verkehrsordnungswidrig und entgegnete dem aufnehmenden Zeugen POK: *„Sie sind ja ein ganz schlauer Oberkommissar"*. Zudem äußerte er wahrheitswidrig den Leiter des zuständigen Abschnittes zu kennen und dass er *„von diesem hören werde"*. Er wollte damit den Zeugen einschüchtern und erreichen, dass dieser die Anzeige gegen ihn unterließ. Sein Ziel weiterverfolgend rief A auf der Wache des Abschnitts an und äußerte gegenüber dem Wachhabender, er solle auf seinen Kollegen einwirken. Schließlich schickte A dem POK eine SMS auf das Diensthandy sinngemäß mit folgendem Inhalt: Lieber POK, es wäre sehr freundlich, wenn Sie der Verhältnismäßigkeit bei der Aufnahme von VK-Owis an Radwegen eine Chance geben würden! Hierbei benutzte A bewusst die persönliche Anrede und die Telefonnummer des Diensthandys, mithin Interna, um den Anschein zu verstärken, dass er tatsächlich den Dienststellenleiter kannte. Dies gelang ihm auch, wobei letztlich nicht geklärt werden konnte, wie A an die dienstliche Telefonnummer des POK gelangen konnte. Da der POK sein berufliches Fortkommen trotz der behaupteten Bekanntschaft des A mit dem Dienststellenleiter nicht gefährdet sah, erstattete er die Anzeige.

Die Drohung mit einer *„gewöhnlichen"* Dienstaufsichtsbeschwerde ist kein empfindliches Übel im Sinne des § 240 StGB. Die zuvor beschriebenen, mithin erforderlichen Feststellungen sind für eine Verurteilung wegen versuchter Nötigung bei Drohung mit *„Konsequenzen von höherer Stelle"* gegenüber einem Polizeibeamten als zumindest notwendig zu erachten. (KG Berlin, Urt. v. 18.3.2021 – (3) 121 Ss 14/21 (10/21))

§ 244 Abs. 1 Nr. 3 StGB – Wohnungseinbruchdiebstahl; hier: Gemischt genutztes Anwesen. Der Begriff der Wohnung umfasst auch typischerweise dem Wohnen zuzuordnende Räume, wenn sie mit dem Wohnbereich unmittelbar verbunden sind, wie etwa Kellerräume eines Einfamilienhauses, nicht dagegen Geschäfts- oder Ladenlokale. Bricht der Täter bei einem gemischt genutzten Anwesen in einen ausschließlich zu betrieblichen Zwecken genutzten Raum ein und gelangt von dort ungehindert in den Wohnbereich des Tatopfers, um auch dort zu stehlen, kann darin nur dann ein Wohnungseinbruch gesehen werden, wenn der Geschäftsraum so in den Wohnbereich integriert ist, dass beide eine in sich geschlossene Einheit bilden.

Der Wortlaut des § 244 Abs.1 Nr. 3, Abs. 4 StGB verbietet nämlich eine Bestrafung wegen (Privat-)Wohnungseinbruchsdiebstahls, wenn der Täter bei gemischt genutzten Gebäuden zunächst in die Betriebsräumlichkeiten einbricht und von dort ungehindert in den Wohnbereich gelangt, um (auch) dort zu stehlen. (BGH, Beschl. v. 24.3.2021 – 6 StR 46/21)

§§ 281 Abs. 1 S. 1, 269 Abs. 1 StGB – Missbrauch von Ausweispapieren, Fälschung beweiserheblicher Daten. Der Begriff des Gebrauchens ist nach Auffassung des BGH in § 281 Abs. 1 S. 1 StGB wie in § 267 Abs. 1 StGB auszulegen. Auch durch Vorlage der Kopie oder durch elektronische Übersendung des Bildes eines echten Ausweises zur Identitätstäuschung kann ein Ausweispapier im Sinne von § 281 Abs. 1 S. 1 StGB zur Täuschung im Rechtsverkehr gebraucht werden. § 269 Abs. 1 StGB unterfallen nicht nur Veränderungen an einem bestehenden eBay-Konto, sondern auch die Einrichtung eines eBay-Kontos unter falschen Personalien. (BGH, Beschl. v. Beschl. v. 21.7.2020 – 5 StR 146/19)

II Prozessuales Strafrecht

§ 94 StPO – Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken; hier: Potenzielle

Beweisbedeutung. Ein Gegenstand hat potenzielle Beweisbedeutung, wenn in einer ex-ante-Sicht die nicht fernliegende Möglichkeit besteht, ihn im Verfahren zu Untersuchungszwecken in irgendeiner Weise zu verwenden. In welcher Weise der Gegenstand Beweisbedeutung haben kann, braucht zum Zeitpunkt der Sicherstellung noch nicht festzustehen.

Unter Verhältnismäßigkeitsgesichtspunkte kann es ausreichend sein, von den sichergestellten Gegenständen Lichtbilder zu verwenden, soweit eine kriminaltechnische Untersuchung der Gegenstände nicht erforderlich erscheint. (BGH, Beschl. v. 14.6.2018 - StB 13/18)

§ 110 Abs. 3 StPO – Durchsicht von Papieren und elektronischen Speichermedien; hier: Zugriff auf Internetseiten des Beschuldigten im Internet. Beim Beschuldigten (B) durchsuchte die Polizei wegen des Vorwurfs der Steuerhinterziehung. Das Handy des B wurde am Durchsuchungstag vor Ort mit dem UFED Physical Analyzer gesichert. Dabei werden unter anderem auch die auf dem Gerät gespeicherten Zugangsdaten zu Online- und Clouddiensten ausgelesen und in einem sogenannten Account-Package dem IT-Prüfer zur Verfügung gestellt. Dieses Package kann sodann mit einem anderen Tool, dem UFED Cloud Analyzer, eingelesen werden. In den nächsten Tagen bemerkte B, dass von einer fremden IP-Adresse auf seine Konten bei Facebook, Google und LinkedIn zugegriffen wurde. Wie sich herausstellte, versuchte der Cloud Analyzer, sich mit dem Internet zu verbinden und online mithilfe der Zugangsdaten weitere, online gespeicherte Daten abzurufen.

Das LG Koblenz sieht hierin eine zulässige Maßnahme in Form einer Online-Sichtung gem. § 110 Abs. 3 StPO und hält für den Zugriff auf die (wohl) im Ausland gespeicherten Daten kein Rechtshilfeersuchen für notwendig. (LG Koblenz, Beschl. v. 24.8.2021 – 4 Qs 59/21)

§ 119 StPO – Haftgrundbezogene Beschränkungen während der Untersuchungshaft; hier: Durchsuchung, Fesselung, Spuckschutz und Vermummung. Der vollziehbar ausreisepflichtig türkische Staatsangehörige (K) wurde aus der Untersuchungshaft heraus durch das SEK zur Gerichtsverhandlung (Verdacht des Fahrens ohne Fahrerlaubnis in elf Fällen in Tatmehrheit mit unerlaubtem Handeltreiben mit Betäubungsmitteln in nicht geringer Menge in drei Fällen) verbracht. Nach dem Ende der Verhandlung betraten zwei Beamte des SEK die Zelle des K, um den Rücktransport in die JVA vorzubereiten. Die Beamten trugen hierbei Sturmhauben. Die persönlichen Sachen K´s wurden untersucht und – in unbekleidetem Zustand – seine natürlichen Körperöffnungen, Achselhöhlen und Kniekehlen in Augenschein genommen. Ein Arzt war nicht anwesend. Dem K wurden Hand- und Fußfesseln angelegt, die mittels Feuerwehrgurt am Körper fixiert wurden. Die Beamten setzten ihm eine Spuckhaube und eine Schlafbrille auf. Zusätzlich wurde ihm ein Gehörschutz angelegt. Der K verhielt sich während dieser Maßnahme kooperativ.

Durchsuchungen, die mit einer Entkleidung verbunden sind, stellen sich als schwerwiegender Eingriff in die Intimsphäre und damit in das durch Art. 2 Abs.1 GG gewährleistete Persönlichkeitsrecht dar und berühren zudem die Menschenwürde (Art. 1 Abs. 1 GG). Das gilt in besonderem Maße, wenn sie mit der Nachschau im Bereich von normalerweise bedeckten Körperöffnungen verbunden sind. Derartige körperliche Durchsuchungen können durch die Erfordernisse der öffentlichen Sicherheit und Ordnung gerechtfertigt sein, sie dürfen aber nur in schonender Weise und nicht routinemäßig, unabhängig von den konkreten Umständen des Einzelfalles, durchgeführt werden. Vielmehr sind alle Umstände des Einzelfalles abzuwägen. (VG Braunschweig, Urt. v. 2.12.2020 – 5 A 65/20)

§ 158 StGB – Strafanzeige, Strafantrag; hier: Strafantrag bei einer *„Internet-Wache“* der Polizei. Ein über eine sog. Online-Wache gestellter Antrag erfüllt nicht das Schriftformerfordernis und ist unwirksam. Denn es würde die Schutzfunktion des Schriftformerfordernisses in § 158 Abs. 2 StPO aufgegeben, wenn ein *„nur online“* gestellten Strafantrag bei einer *„Internet-Wache“* der Polizei genügen würde. (AG Auerbach, Beschl. v. 26.1.2021 – 3 Cs 500 Js 24368/20)

§§ 163b Abs. 1, 163c StPO – Maßnahmen/Freiheitsentziehung zur Identitätsfeststellung; hier: Zuerst strafprozessuale und danach präventive Ausrichtung der Maßnahme. Am 9.2.2019 gegen 7:26 Uhr versuchte der B, gemeinsam mit weiteren Personen auf dem Gelände des Tagebaus G. einen Braunkohlebagger zu besetzen. Gegen 9:07 Uhr wurde die Gruppe zur Identitätsfeststellung nach §§ 163b Abs. 1, 163c StPO in Gewahrsam genommen. Eine Identifizierung des B war (zunächst) nicht möglich, da er sich weigerte, Angaben zu seiner Person zu machen, er keine Ausweispapiere bei sich führte und seine Fingerkuppen verklebt waren. Er lehnte es ab, die Fingerkuppen zur Abnahme von Fingerabdrücken mit dem Lösungsmittel Aceton reinigen zu lassen. Gegen 18:45 Uhr erfolgte am selben Tag die richterliche Anhörung. Sodann wurde eine Freiheitsentziehung des namentlich noch nicht bekannten B auf Grund des Polizeigesetzes des Landes Nordrhein-Westfalen (PolG NRW) zum Zweck der Feststellung seiner Identität für zulässig erklärt und die Fortdauer des Gewahrsams bis längstens 14.2.2019 12:00 Uhr angeordnet. Die Ingewahrsamnahme wurde damit begründet, dass es der Polizei ohne Feststellung der Identität des B nicht möglich wäre, ein Aufenthaltsverbot nach § 34 Abs. 2 PolG NRW auszusprechen. Bei unterlassener Identifizierung sei ein erneutes Eindringen in das Tagebaugebiet zu erwarten, was durch die Erteilung eines polizeilichen Aufenthaltsverbotes im Rahmen der Gefahrenabwehr verhindert werden solle. Nach Vorlage des Führerscheins durch dritte Personen konnte die Identität des B ermittelt werden und er wurde am 11.2.2019 um 12:45 Uhr aus dem polizeilichen Gewahrsam entlassen.

Zwar regeln §§ 163b und 163c StPO die Befugnis zur Identitätsfeststellung zum Zwecke der Strafverfolgung einschließlich damit verbundener Freiheitsentziehung abschließend, sodass insofern ein Rückgriff auf weiterreichende polizeiliche Ermächtigungen nicht möglich ist. Die polizeirechtlichen Ermächtigungsgrundlagen bleiben dagegen aber anwendbar, soweit präventive Zwecke außerhalb des Strafverfahrens verfolgt werden. So, dass eine zunächst nach StPO angeordnete Gewahrsamnahme anschließen auch auf gefahrenabwehrrechtliche Grundlagen gestützt werden kann, wenn dies eben solchen Zwecken dient. (BGH, Beschl. v. 17.12.2020 – 3 ZB 8/19)

III Sonstiges

Ein betrunkener Kraftfahrer wurde im Auto sitzend von der Polizei angetroffen und griff noch vor Ort im Zuge von Maßnahmen zur Feststellung der Alkoholkonzentration alsbald die Polizei tätlich an. Ein Strafbefehl wegen Wiederstandes wurde am 7.7.2020 rechtskräftig, ein Urteil wegen vorsätzlicher Trunkenheit im Verkehr erging am 23.7.2020.

Mit Beschluss vom 1.7.2021 (1 Rv 13 Ss 421/21) stellte das OLG Stuttgart per Beschluss fest, dass die Sanktionierung einer Trunkenheitsfahrt wegen des **Doppelverfolgungsverbotes** dann nicht möglich ist, wenn der tätliche Angriff auf Polizeibeamte bereits rechtskräftig abgeurteilt worden ist.

Aktuelles aus dem Netz

Von EKHK Christian Zwick, Ludwigshafen

NetzDG vom VG Köln gestoppt: Kommt die Neuauflage aus Brüssel?

Das VG Köln hat der Beschwerden von Facebook und Google gegen neue Regelungen des novellierten Netzwerkdurchsetzungsgesetzes (NetzDG) im Eilverfahren vorläufig stattgegeben. Die Meldepflicht nach § 3a NetzDG sei mit dem Herkunftslandprinzip der Richtlinie über den elektronischen Geschäftsverkehr (ECR) nicht vereinbar und daher unanwendbar. […] Der europäische Gesetzgeber hat in kurzer Abfolge eine Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte sowie Entwürfe für eine Verordnung zur Bekämpfung des sexuellen Missbrauchs von Kindern und ein Gesetz über digitale Dienste (Digital Services Act – DSA) auf den Weg gebracht. Der DSA ist bereits im Trilog-Verfahren und könnte noch bis Ostern 2022 beschlossen werden. Mehr: https://www.lto.de/recht/hintergruende/h/vg-koeln-stoppt-netzdg-loeschpflichten-hate-speech-regulierung-medien-facebook-google/, Meldung vom 8.3.2022.

Telefónica nimmt Mini-Funkzellen mit Open RAN in Betrieb

Die Mini-Zellen, die an Hausfassaden angebracht werden, ergänzen die bestehende Antenneninfrastruktur auf den Dächern. Sie sollen helfen, stark frequentierte Innenstadtbereiche mit vielen Anwendern besser mit 4G mit bis zu 100 MBit/s im Nahbereich zu versorgen. Mehr: https://www.com-magazin.de/news/mobilfunk/telefonica-nimmt-mini-funkzellen-open-ran-in-betrieb-2733101.html, Meldung vom 19.1.2022.

Krypto-Diebe erbeuten knapp eine Milliarde Dollar in nur 6 Monaten

Dezentralisierte Finanzprojekte (DeFi) haben im vergangenen halben Jahr erhebliche Verluste verzeichnet. […] In den von tradingplatforms.com erfassten Zeitraum fallen auch einige der größten Krypto-Raubüberfälle der jüngeren Geschichte. Der prominenteste und aktuellste ist der Wormhole-Hack, bei dem 320 Millionen Dollar erbeutet wurde. […] Diebstahl von Krypto-Assets tritt in vielen unterschiedlichen Formen auf. Am häufigsten sind jedoch Smart-Contract-Hacks, Phishing-Betrug und Flash-Loan-Angriffe. Mehr: https://www.it-finanzmagazin.de/krypto-diebe-erbeuten-knapp-eine-milliarde-dollar-in-nur-6-monaten-135285/, Meldung vom 16.2.2022.

Achtung, Handy hört mit: Smartphone-Apps als Wanze

Lauschen Smartphones permanent mit und geben Gesprächsinhalte dann an Facebook, Google & Co. weiter? […] Die BR-Experimente zeigen, dass es technisch durchaus möglich ist, dass Smartphone-Apps unter bestimmten Voraussetzungen Gespräche belauschen – und das sogar heimlich. Dass die Internetriesen tatsächlich davon Gebrauch machen, um passende Werbung auszuspielen, ist allerdings weiterhin nicht belegt. Mehr: https://www.heise.de/news/Achtung-Handy-hoert-mit-Smartphone-Apps-als-Wanze-6517559.html, Meldung vom 4.3.2022.

Open Source Intelligence - Die besten OSINT Tools

Hacker nutzen Open Source Intelligence, um Systeme zu kompromittieren. Sie können OSINT Tools nutzen, um herauszufinden, welche Ihrer Informationen offenliegen. […] Im Folgenden stellen wir Ihnen einige der besten Open Source Intelligence Tools sowie deren individuelle Stärken vor. Mehr: https://www.computerwoche.de/a/wie-viel-wissen-hacker-ueber-sie, Meldung vom 8.3.2022.

Hass im Internet: Software soll Fahndern bei Schnellerkennung helfen

Bedrohung von Amtsträgern, Verhöhnung von Gewaltopfern oder der pure Antisemitismus: Blanker Hass und Hetze auch mit strafrechtlicher Relevanz sind längst Alltag im Internet. In Hessen soll bei Ermittlern ab Mitte des Jahres die neue Software bei der schnelleren Einordnung der Relevanz gemeldeter Hasskommentare im Netz helfen und im Fall akuter Gefahr auch warnen. Mehr: https://www.heise.de/amp/hintergrund/Hass-im-Internet-Software-soll-Fahndern-bei-Schnellerkennung-helfen-6540532.html, Meldung vom 8.3.2022.

KI übersetzt alle Sprachen der Welt: Zuckerberg stellt neue Pläne für Metaverse vor

Meta-CEO Mark Zuckerberg offenbarte kürzlich seine neusten Pläne in Sachen Metaverse. Im Zentrum der Entwicklungen steht dabei die Künstliche Intelligenz (KI). Mit deren Hilfe will Zuckerberg die virtuelle Welt im Metaverse weiter ausbauen. Außerdem soll eine KI alle Sprachen der Welt in Echtzeit übersetzen. Mehr: https://www.basicthinking.de/blog/2022/02/24/neue-meta-plaene-ki/, Meldung vom 24.2.2022.

Resolution der Gewerkschaft der Polizei (GdP) zu den Polizistenmorden von Ulmet

Bundesvorstand der Gewerkschaft der Polizei

Nach den brutalen Morden an unserer 24-jährigen Kollegin Yasmin und unserem 29-jährigen Kollegen Alexander am 31. Januar 2022 im rheinland-pfälzischen Landkreis Kusel zeigt sich der Bundesvorstand der Gewerkschaft der Polizei (GdP) fassungslos und in tiefer Trauer. Der Albtraum einer jeden Polizistin, eines jeden Polizisten und eines jeden aus der gesamten Polizeifamilie hierzulande sei eingetreten, betonte das Gremium in einer Erklärung im Rahmen einer Bundesvorstandssitzung am 8. Februar 2022 vor dem Hintergrund der erschütternden Tat. Zuvor hatte der GdP-Bundesvorstand in einer Schweigeminute den beiden im Dienst ermordeten Kollegen gedacht.

Erst die schrecklichen Morde an den beiden Polizeibeamten im rheinland-pfälzischen Ulmet haben es offenbar vermocht, den Fokus der Gesellschaft, der Medien und der Politik auf die seit Jahren zunehmende Gewalt gegen Polizeibeamtinnen und Polizeibeamte zu lenken. Zudem wirft die Tat ein Schlaglicht auf Entwicklungen in unserem Rechtsstaat, die zu großer Besorgnis Anlass geben.

Seit rund zwei Jahrzehnten weist die GdP auf die Zunahme von Respektlosigkeiten, Diffamierungen sowie Angriffen und Gewaltattacken auf unsere Kolleginnen und Kollegen als Repräsentantinnen und Repräsentanten unseres demokratischen Staates hin. Dieser nicht zu tolerierenden Entwicklung darf nicht mit dem vermeintlichen Argument des polizeilichen Berufsrisikos entgegnet werden. Es darf nicht kleingeredet werden, dass Polizistinnen und Polizisten mit Hass- und Hetzaufrufen im Netz, vor allem in den sozialen Medien, belegt werden. Wir wollen nicht hinnehmen, dass solches inakzeptables Handeln zu unserem polizeilichen Berufsalltag gehören soll.

Um dieser Entwicklung wirksam zu entgegnen, fordert die GdP gesellschaftlichen Rückhalt für ihre Polizei. Diese sowie unser demokratischer Rechtsstaat benötigen mehr Wertschätzung, breite Anerkennung und Respekt. Polizeibeschäftigte geben tagtäglich 100 Prozent Einsatz. Nicht mehr fordern sie zurück.

Es kann nicht länger sein, dass eine Unkultur des ständigen Hinterfragens staatlichen und polizeilichen Tuns Fahrt aufnimmt. Es geht dabei nicht um die demokratische Kontrolle des Staates. Selbstverständlich ist es jeder und jedem überlassen, Maßnahmen juristisch überprüfen zu lassen. Es geht im besten Fall um Trotzigkeit vor dem Hintergrund fehlenden Wissens um das Funktionieren des Rechtsstaates. Es geht um das Ignorieren der Kompetenzen staatlicher Institutionen bis hin zu einer erklärten Feindschaft gegenüber der Demokratie und gegenüber denen, die sie bewahren. Die GdP fordert einen starken und selbstbewussten Staat, der diese Probleme offen benennt, transparent debattiert und zielgerichtete Lösungen auf den Weg bringt.

In Deutschland arbeitet eine Bürgerpolizei. Eine Polizei, die Teil der Gesellschaft ist, und es auch sein will. Dazu gehört es, die weitreichenden Rechte aller zu schützen, jedoch auch denen, die gegen Regeln verstoßen, Grenzen zu verdeutlichen. Unsere Kolleginnen und Kollegen sind rund um die Uhr im Einsatz, oft dort, wo sich Konflikte abspielen, Menschen zu Tätern und Opfern werden. Die Polizei blickt häufig in menschliche Abgründe und wird mit Not und Elend konfrontiert. Die Polizei ist weder eine Bedrohung noch eine Gefahr. Sie hilft und schützt! Wer anderen mit Polemik, Verleumdungen und falschen Behauptungen das Gegenteil eintrichtern will, handelt gegen unseren Staat.

Politische Entscheider müssen dringend sowohl die polizeilichen Erkenntnisse und Wahrnehmungen als auch die der Justiz, der Staatsanwaltschaften und Gerichte ernsthaft berücksichtigen und daraus ein realistisches Lagebild unserer Gesellschaft zeichnen. Weiter dem Motto zu folgen: *„Was ich nicht sehe, ist nicht da!“*, führt in die falsche Richtung. Die Dinge müssen auf den Tisch.

Die Gewerkschaft der Polizei (GdP) fordert einen Staat, der sich zu wehren weiß. Dazu benötigt er neben einer personell und sachlich stark ausgestatteten und aufgebauten Polizei auch Investitionen in die Justiz. Eine tiefgehende Debatte über den Zustand des Rechtsstaates ist unumgänglich.

Der GdP-Bundesvorstand kündigt an, mit dem nötigen emotionalen Abstand und nach Ende der Ermittlungen die Erkenntnisse der Polizistenmorde von Ulmet intensiv auszuwerten und nötige Schlussfolgerungen daraus, zu den politischen Entscheidern zu tragen.