Schriften zum Digitalwirtschaftsrecht
Studies on Digital Business Law

Lukas Staffler | Jakob Ebbinghaus [Hrsg.]

Perspektiven des Datenschutz- und Cybersicherheitsrechts

facultas DIKE

Nomos

Schriften zum Digitalwirtschaftsrecht
Studies on Digital Business Law

Herausgegeben von
Univ.-Prof. Dr. Simon Laimer, LL.M.
Prof. Dr. Anne-Christin Mittwoch
Univ.-Prof. Dr. Thomas Müller, LL.M.
Dr. Lukas Staffler, LL.M.

Band 4

Lukas Staffler | Jakob Ebbinghaus [Hrsg.]

Perspektiven des Datenschutz- und Cybersicherheitsrechts

facultas DIKE

Nomos

Die Herausgeber danken für die großzügige finanzielle Unterstützung bei der Realisierung dieses Werks, nämlich der Universitätsbibliothek Zürich und Humboldt Universität zu Berlin (Lehrstuhl Prof. Luis Greco).

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-3379-9
(Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, Print)
ISBN 978-3-7489-6342-4
(Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, ePDF)

ISBN 978-3-03891-871-4 (Dike Verlag, Zürich/St. Gallen)

ISBN 978-3-7089-2677-3 (facultas Verlag, Wien)

DOI: https://doi.org/10.5771/9783748963424

Onlineversion
Nomos eLibrary

Inhaltsverzeichnis

Professionelle Cyberkriminalität

Jakob Ebbinghaus, Lukas Staffler

1. Einleitung

„Cyberbedrohungen sind zu einem integralen Bestandteil der Bedrohungslandschaft in der Schweiz aber auch international geworden“[1] – so fasste der im November 2024 erschiene Lagebericht des Schweizerischen Bundesamts für Cybersicherheit (BACS) die gegenwärtigen Entwicklungen zur Cybersicherheit zusammen und berichtete zum ersten Halbjahr 2024 von nahezu einer Verdopplung der Meldungen zu sicherheitsrelevanten Vorfällen zur Vergleichsperiode im Vorjahr. Dies zeigt exemplarisch, dass Wirtschaft und Gesellschaft mit einem cyberkriminellen Phänomen konfrontiert wird, das nicht nur Unternehmen, sondern auch Privatpersonen und letztlich sogar staatliche Strukturen bedroht.[2]

Das Phänomen Cyberkriminalität ist dabei sehr dynamisch[3] und die bisherige Erfahrung legt nahe, dass es sich bei diesem Phänomen nicht einfach um die Begehung von Straftaten mit digitalen Mitteln in Anlehnung an analoge Kriminalität handelt. Vielmehr ist anzunehmen, dass es ein neuartiges, komplexes und zum Teil grundlegend andersartiges Kriminalitätsphänomen darstellt,[4] das die Mittel des nationalen (Straf-)Rechts in bisher nicht gekanntem Ausmaß herausfordert. Nach der hier vertretenen Auffassung handelt sich um eine neue Form der Wirtschaftskriminalität[5],

1 BACS, Cybersicherheit Lage in der Schweiz und international, Halbjahresbericht 2024/I vom 07.11.2024.

2 Instruktiv *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 151 ff.; etwa zum Ransomware-Angriff auf Costa Rica, vgl. Couretas Cyber Operations, 2024, S. 1.

3 Empfehlenswert *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, 41 ff. (insb. 79 ff., 98 ff.).

4 Exemplarisch *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., 2018, 185 ff.; zusammenfassend *Staffler*, ZWF 2025, 172 ff.

5 Dabei ist sogleich darauf hinzuweisen, dass Cybercrime nicht nur aus wirtschaftlicher Motivation, sondern auch aus politisch, ideologischer oder terroristischer Motivation begangen wird: *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 151. Wirtschaftskriminalität ist nicht legaldefiniert, als Orientierungspunkt kann

die allerdings mit den bisherigen Erfahrungen von kriminellen Machenschaften durch legale Unternehmen (wie etwa Untreue oder Betrug) nur noch wenig gemein hat. Vielmehr zeichnen sich diese Phänomene durch einen hohen Grad an Professionalisierung und Arbeitsteilung aus.[6] Es sind Strukturen, die in ihrer Dynamik und internationalen Verflechtung noch wenig erforscht sind. Gleichzeitig treffen die neuen Kriminalitätsphänomene auf Wirtschaft und Gesellschaft, die zwar eine hohe Affinität zur Digitalisierung aufweisen, aber noch nicht ausreichend für die damit verbundenen Risiken sensibilisiert sind.

Vor diesem Hintergrund besteht das Ziel dieses Beitrags darin, jüngere Entwicklungen aus dem Bereich Cybercrime dahingehend zu reflektieren, inwiefern klassische Straftatbestände wie der Tatbestand der kriminellen Vereinigung im deutschen Strafrecht diese noch erfassen kann. Es wird geprüft, ob die bestehenden rechtlichen und gesellschaftlichen Ansätze einer Anpassung bedürfen, um diesen Herausforderungen effektiv begegnen zu können.

2. Phänomenologie von Ransomware

Um die einleitend beschriebenen Tendenzen näher zu ergründen, wird im Folgenden Ransomware im Hinblick auf Struktur, Funktionsweise und gesellschaftlichen Auswirkungen analysiert. Ransomware entstammt der digitalen Sphäre, ist gegenwärtig überaus praxisrelevant und veranschaulicht exemplarisch, wie organisierte Cyberkriminalität nicht nur technologische Schwachstellen ausnutzt, sondern auch auf psychologische Manipulation und soziale Dynamiken setzen, um ihre Ziele zu erreichen. Zudem folgt das Phänomen einem sehr strukturierten, arbeitsteiligen Vorgehen und basiert auf der gezielten Ausnutzung menschlicher und technischer Anfälligkeiten.

---

§ 74c I 1 GVG herangezogen werden; eine anerkannte Definition existiert für das deutsche Strafrecht nicht (vgl. *Dannecker/Bülte* Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts und Steuerstrafrecht, 2025 § 1 Rn. 5), oftmals wird darauf abgestellt, dass die besonderen Umstände des Wirtschaftsverkehr ausgenutzt werden, wie der Missbrauch des für das Funktionieren der Wirtschaft erforderlichen Vertrauens. Ransomware-Angriffe werden für Gewöhnlich nicht hierunter gefasst, obwohl bei den Phishing Angriffen ein solcher Vertrauensmissbrauch, Ausnutzen von Gepflogenheiten im Geschäftsverkehr, typisch ist.

6 *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 142.

2.1. Begriff

Der Begriff „Ransomware" setzt sich aus den englischen Wörtern „*ransom*" (Lösegeld) und „*software*" zusammen. Die Wortbildung folgt einem in der Informationstechnologie üblichen Muster, bei dem der Wortteil „*-ware*" für verschiedene Arten von Software verwendet wird, wie beispielsweise bei „*malware*" (bösartige Software) oder „*adware*" (werbefinanzierte Software). Die Kombination dieser Begriffe zu „Ransomware" beschreibt somit eine Schadsoftware, die darauf abzielt, den Zugriff auf Daten oder Systeme zu blockieren, um vom Opfer Lösegeld zu erpressen.[7]

In den letzten Jahren gab es eine Reihe prominenter Ransomware-Angriffe, die die Aufmerksamkeit auf diese Art von Cybercrime und ihr Ausmaß gelenkt haben.[8] Exemplarisch ist der WannaCry-Angriff aus dem Jahr 2017 zu nennen, der weltweit hunderttausende Computersysteme in mehr als 150 Ländern betraf. WannaCry nutzte eine Schwachstelle im Windows-Betriebssystem aus, die ursprünglich von der NSA entdeckt und später von einer Hackergruppe veröffentlicht wurde. Der Angriff führte zu massiven Störungen in staatlichen Einrichtungen und privaten Unternehmen.[9] Ein anderes berühmtes Beispiel ist der Colonial Pipeline-Angriff im Jahr 2021, bei dem ein wichtiges Pipeline-Netzwerk in den USA lahmgelegt wurde, was zu erheblichen Treibstoffengpässen führte. Die Angreifer, die die Ransomware „DarkSide" verwendeten, erpressten ein Lösegeld in Millionenhöhe, das von den Behörden teilweise zurückverfolgt werden konnte.[10]

2.2. Funktionsweise

Die Funktionsweise von Ransomware basiert auf einer Kombination von Verschlüsselungstechnologien, Techniken zur sozialen Manipulation und Mechanismen zur finanziellen Erpressung. Die Bedrohung durch Ransomware besteht im Wesentlichen darin, dass Daten auf einem infizierten System verschlüsselt werden, so dass der betroffene Nutzer den Zugriff auf diese Daten oder das gesamte System verliert.

---

7 Statt vieler s. *Meyer/Biermann*, MMR 2022, 940.

8 Vgl. *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 3 f., 5.

9 *Dickmann*, Cyberversicherung, 2025, Rn. 59.

10 US DoJ Dep.Attorney General Monaco Comprehensive Cyber Review July 2022 S.2,10,11; *Dickmann*, Cyberversicherung, 2025, Rn. 64.

2.2.1. Infiltration

Zunächst wird Ransomware über verschiedene Methoden verbreitet, die sich je nach Zielgruppe und Technik unterscheiden.[11] Besonders häufig werden E-Mails als Angriffskanal genutzt, wobei die Angreifenden Phishing-Kampagnen einsetzen, um die Nutzer zur Interaktion mit der Schadsoftware zu verleiten. Diese E-Mails sind dann so gestaltet, dass sie von vertrauenswürdigen Absendern wie etwa Banken, Behörden oder bekannten Unternehmen zu stammen scheinen.

Im Kontext von Phishing kann zwischen klassischen Massenangriffen und zielgerichteteren Techniken unterschieden werden: Sogenanntes Spear Phishing zielt auf bestimmte Personen oder Organisationen ab und nutzt individuell angepasste Inhalte, z.B. auf Basis öffentlich zugänglicher Informationen aus sozialen Netzwerken oder Unternehmenswebseiten.[12] Im Gegensatz dazu verfolgt sog. Dynamite Phishing einen hybriden Ansatz: Es beginnt mit einer breit gestreuten, generischen E-Mail-Kampagne, die auf eine erste Reaktion abzielt. Reagieren, wie beabsichtigt, einzelne Nutzer darauf, wird der Angriff gezielt vertieft und personalisiert – eine Eskalation, die typischerweise die Auslieferung der eigentlichen Ransomware bezweckt.[13] Darüber hinaus können auch infizierte Webseiten[14] oder kompromittierte Werbeanzeigen als Verbreitungswege dienen, die Nutzerinnen und Nutzer beim Besuch der entsprechenden Seiten automatisch mit der Schadsoftware infizieren.

Ferner spielt das Ausnutzen von Sicherheitslücken in Betriebssystemen oder Software spielt eine wichtige Rolle. Häufig wird Ransomware über sog. Exploit-Kits verbreitet, die gezielt Schwachstellen, insb. sogenannte „*zero-day-exploits*",[15] in nicht aktualisierten Systemen ausnutzen.

---

11 *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 4 f.

12 *Bär* in Wabnitz/Janovsky/Schmitt (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, 6. Aufl. 2025, § 15 Rn. 32.

13 Heise Online, Dynamit-Phishing: Emotet perfektioniert seine Angriffe weiter, 12.4.2019, abrufbar unter https://www.heise.de/security/meldung/Dynamit-Phishing-Emotet-perfektioniert-seine-Angriffe-weiter-4398626.html (abgerufen am 06.04.2025).

14 Vgl. jüngst https://www.bleepingcomputer.com/news/security/fbi-warnings-are-true-fake-file-converters-do-push-malware/ (abgerufen am 23.03.2025): online PDF-Konverter als Einfallstor.

15 Wobei mit zero day Exploits nicht Schwachstellen gemeint sind, die noch nicht geschlossen sind, wie z.B. *Brodowski/Schmid/Scholzen/Zoller* NStZ 2023, 385, 386

2.2.2. Verschlüsselung

Sobald unbemerkter Zugriff auf das infizierte System möglich ist, beginnt die Ransomware (oder die Angreifer) damit, Dateistrukturen zu analysieren und gezielt Dateien auszuwählen, die verschlüsselt werden sollen. Erfahrungsgemäß werden häufig Dateien mit bestimmten Dateierweiterungen wie .docx, .jpg oder .xlsx bevorzugt, da diese in der Regel für den Benutzer von großer Bedeutung sind. Die Verschlüsselung selbst erfolgt mit oftmals selbstentwickelten kryptografischen Verfahren, die sicherstellen sollen, dass die verschlüsselten Daten ohne den richtigen Schlüssel nicht wiederhergestellt werden können.[16]

2.2.3. Lösegelderpressung

Nachdem die Ransomware ihre Aufgabe erfüllt hat, beginnt die Phase der Lösegeldforderung. In einer auffälligen Nachricht wird das Opfer darüber informiert, dass dessen Daten verschlüsselt wurden und die einzige Möglichkeit, sie wiederherzustellen, in der Zahlung eines Lösegelds besteht.[17] Diese Mitteilungen sind oft detailliert und enthalten Anweisungen, wie die Zahlung zu erfolgen hat. Bei gewissen Opfern erfolgt ein Kontakt oft zusätzlich auch über einen verschlüsselten Chatdienst, um weiter Druck auf das Opfer auszuüben.

Um bestmögliche Anonymität in der Zahlungsabwicklung zu gewährleisten, verlangen die Angreifer erfahrungsgemäß die Zahlung in Kryptowährungen wie Bitcoin oder Monero, da diese aufgrund ihres dezentralen Charakters schwerer nachzuverfolgen sind. Transaktionen von Kryptowährungen werden typischerweise auf einer Blockchain, einer Art öffentlich einsehbarem Register, eingetragen, sodass eine durchgeführte Transaktion grundsätzlich nicht rückgängig gemacht werden kann. Zwar ist eine anonyme Nutzung möglich,[18] allerdings können die einzelnen Transaktionen

---

meinen, sondern vielmehr den Schweregrad beschreibt: Schwachstellen, die so gefährlich sind, dass nur null Tage Zeit bleibt, um diese zu schließen.

16 Vgl. allgemein zur Kryptografie im Internet: https://www.quantamagazine.org/how-public-key-cryptography-really-works-20241115/ (abgerufen am 27.03.2025).

17 *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 11 f.

18 *Brenneis*, APuZ 2017, 29, 33 f.; wobei nach einem Hack durchaus auch eine Änderung möglich ist, vorausgesetzt genügend Inhaber stimmen dem „Fork", also der Änderung im Protokoll zu, vgl. https://www.heise.de/news/Nach-dem-DAO-Hack-Ethereum-glueckt-der-harte-Fork-3273618.html (27.3.25).

nachverfolgt werden (Blockchainanalysis), daher ist eine Identifizierung bei Auszahlung grundsätzlich möglich.[19]

Um genau diese Rückverfolgbarkeit zu erschweren, nutzen Täter bisweilen sogenannte Kryptowährungs-Mixer (auch *Tumbler* genannt).[20] Diese Dienste sammeln Transaktionen unterschiedlicher Nutzer, vermischen die ein- und ausgehenden Beträge über viele Zwischenkonten und senden schließlich den Zielbetrag an eine neue Adresse – in stark fragmentierter und kaum rekonstruierbarer Form. Durch dieses „Waschen" der Kette verschwimmt die Spur des Geldflusses. In Kombination mit länderübergreifenden Transfers – insbesondere, wenn die Täter in nicht-kooperative Staaten wie Russland oder China agieren – steht die Strafverfolgung daher vor erheblichen praktischen Herausforderungen.[21]

2.2.4. Zwischenfazit

Zusammenfassend lässt sich sagen, dass Ransomware-Angriffe einem klaren und strukturierten Ablauf folgen, der sich in mehrere Phasen unterteilen lässt.

- In der ersten Phase der Infiltration soll die Ransomware unbemerkt auf dem Zielsystem installiert werden. Dies geschieht entweder durch betrügerisches Verhalten – wie Phishing oder Social Engineering – oder durch technisches Eindringen – beispielsweise über Sicherheitslücken mittels Exploit Kits.
- In der zweiten Phase, in der die Angreifer bereits Zugriff auf das System haben, werden die Daten verschlüsselt. Sobald der Vorgang abgeschlossen ist, kann der Nutzer nicht mehr auf das System oder die Dateien zugreifen.
- Die dritte Phase umfasst oft die Lösegeldverhandlungen. Die Angreifer fordern das Opfer in einer expliziten Nachricht auf, ein Lösegeld zu zahlen, um die verschlüsselten Daten wieder freizugeben. Die Nachricht enthält oft detaillierte Anweisungen für die Zahlung, die meist in Kryptowährungen erfolgt, um eine Rückverfolgung zu erschweren.

19 https://www.newyorker.com/business/currency/how-a-young-couple-failed-to-launder-billions-of-dollars-in-stolen-bitcoin (abgerufen am 23.12.2022).

20 *Fromberger/Haffke/Zimmermann*, BKR 2019, 377, 178 f.; *Maume/Haffke*, in; Maume/Maute, Rechtshandbuch Kryptowerte, 2020, § 15 Rn. 27.

21 https://www.newyorker.com/business/currency/how-a-young-couple-failed-to-launder-billions-of-dollars-in-stolen-bitcoin (abgerufen am 23.12.2022).

Die Verhandlungen werden durch klare Fristen und Drohungen wie die vollständige Löschung der Daten, eine Veröffentlichung privater Daten im Darknet oder eine Erhöhung des Lösegelds bei nicht rechtzeitiger Zahlung verstärkt.[22]

2.3. Ransomware-as-a-Service (RaaS)

Die Struktur eines Ransomware-Angriffs macht deutlich, dass arbeitsteiliges Vorgehen möglich ist, das verschiedene Kompetenzen kombiniert. Ein erfolgreicher Angriff erfordert betrügerisches Verhalten, technisches Know-how und geschickte Verhandlungsstrategien bei der Lösegeldforderung. Diese Komplexität hat in den letzten Jahren die Entstehung eines kriminellen Ökosystems rund um Ransomware begünstigt. Im Schutz der Anonymität des sogenannten Darknets, erfahrungsgemäß aber auch auf Telegram, bieten spezialisierte Akteure und Dienstleister nahezu alle Aspekte eines Ransomware-Angriffs als modulare Dienstleistungen an – ein Modell, das unter dem Begriff „Ransomware as a Service" (kurz: RaaS) bekannt geworden ist.

2.3.1. Ransomware-Ökosystem

In diesem kriminellen Ökosystem haben mehrere Akteure unterschiedliche Rollen, sodass es möglich ist, in modularer Weise über RaaS ein komplettes Angriffsszenario zu organisieren.

Sogenannte Initial Access Broker bieten oft Zugang zu geschützten Systemen, indem sie Sicherheitslücken ausnutzen oder Schwachstellen in Netzwerken identifizieren.[23] Ihre Dienste bilden häufig die Grundlage für einen Ransomware-Angriff, indem sie anderen kriminellen Akteuren den direkten Zugriff auf die Systeme ihrer Opfer ermöglichen. Daneben gibt es Dienstleister, die sich ausschließlich auf die Bereitstellung und Weiterentwicklung von Verschlüsselungssoftware konzentrieren. Diese Dienstleister bieten maßgeschneiderte Verschlüsselungslösungen an, die es den Angreifern erleichtern, die Daten effektiv zu blockieren und die Opfer zur Zahlung des Lösegeldes zu zwingen. Ferner hinaus gibt es spezialisierte Anbieter, die sich um die technische Abwicklung der Lösegeldforderungen küm-

22 *Anderl/Tlapak*, in: Anderl (Hrsg.), #Cybercrime Handbuch für die Praxis, 2023, 3.
23 *Hofmann*, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, 2024, 152.

mern, einschließlich der Bereitstellung sicherer Kommunikationskanäle für die Verhandlungen und der Generierung von Entschlüsselungsschlüsseln nach erfolgter Zahlung.

Das kriminelle Ökosystem umfasst auch unterstützende Dienste, die nicht unmittelbar mit der Durchführung von Angriffen in Verbindung stehen, aber deren Erfolg entscheidend beeinflussen. Ein Beispiel sind die oben genannten Tumbler bzw. Mixer-Dienste, die als Geldwäschedienste dafür sorgen, dass Lösegeldzahlungen, die meist in Kryptowährungen erfolgen, später anonymisiert und in legale Finanzströme überführt werden können. Darüber hinaus gibt es (Darknet-)Plattformen, die als Jobbörsen fungieren und auf denen verschiedene kriminelle Dienstleistungen angeboten werden. Auf diesen Marktplätzen werden Angebote von Akteuren gebündelt, die unterschiedliche Dienstleistungen wie das Schreiben von Schadsoftware, die Verbreitung von Phishing-Kampagnen oder die Bereitstellung von Exploit-Kits anbieten.

All das zeigt, dass „RaaS" die Einstiegshürden für technisch weniger versierte Kriminelle erheblich senkt, da diese auf die Expertise anderer „krimineller Stakeholder" zurückgreifen können. Dies beschleunigt die Verbreitung des kriminellen Geschäftsmodells „Ransomware" zusätzlich.

2.3.2. Ransomware-Serverstrukturen

Das technische Rückgrat eines Ransomware-Angriffs ist erfahrungsgemäß die Infrastruktur sogenannter Command-and-Control-Server (C2-Server). Diese Server fungieren als Schaltstellen, über die infizierte Systeme gesteuert, Verschlüsselungsvorgänge initiiert und exfiltrierte Daten weitergeleitet werden. C2-Server ermöglichen Echtzeitkommunikation zwischen Angreifer und Schadsoftware, koordinieren die Verschlüsselung der Zielsysteme und dienen der Befehlsübermittlung sowie dem Empfang gestohlener Daten. Ransomware-as-a-Service besteht also nicht nur aus Softwaremodulen und kriminellen Dienstleistern, sondern bedarf einer physischen Server-Infrastruktur.

Während viele dieser Server bewusst in Staaten mit geringer internationaler Kooperation platziert wurden, zeigen medienwirksame Erfolge der Strafverfolgungsbehörden aus jüngster Zeit, dass sich ein erheblicher Teil dieser Infrastruktur auch in Europa befand. Dies eröffnete den Behörden neue Handlungsspielräume: Durch gezielte „Takedown"-Aktionen im Rah-

men der Operationen wie „Endgame“[24] oder „Synergia“[25] konnten zentrale Serverstandorte abgeschaltet und damit laufende Ransomware-Kampagnen effektiv unterbrochen werden.

2.4. Häufigkeit

Ransomware-Angriffe haben in den vergangenen Jahren weltweit erheblich zugenommen.[26] Die Angriffsarten- und Abläufe werden von privaten Sicherheitsdienstleistern erfasst und in entsprechenden Berichten zur Verfügung gestellt.[27] Für die Darstellung wurden viele Tatsachenschilderungen von solchen Berichten privater Sicherheitsunternehmen übernommen. Aus wissenschaftlicher Vorsicht ist dabei zu berücksichtigen, dass derartige Dienstleister aus wirtschaftlicher Sicht natürlich motiviert sind, gegenwärtige IT-Gefahren entsprechend darzustellen, weshalb die folgenden Angaben stets mit Vorsicht zu genießen sind.[28] Die Autoren dieses Beitrags sind dennoch vorsichtig zuversichtlich, dass es sich bei den zitierten Aussagen um seriöse Quellen handelt.

Aus dem Sophos-Jahresbericht für das Jahr 2024 ist zu entnehmen, dass 59 % der befragten Unternehmen erfolgreichen Ransomware-Angriffen ausgesetzt waren, bei denen die Angreifer in das System eindringen konnten und eine Datenverschlüsselung erfolgreich durchführten.[29] Frankreich wies mit 74 % die weltweit höchste Ransomware-Angriffsrate auf, dicht gefolgt von Südafrika (69 %) und Italien (68 %). Am unteren Ende

24 Europol Pressemeldung zu Operation „Endgame“, abrufbar unter https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem (06.04.2025).

25 Interpol Pressemeldung zu Operation „Synergia II“, abrufbar unter https://www.interpol.int/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses (06.04.2025).

26 Statt vieler s. *Sohr/Kemmerich*, in: Kipker (Hrsg.), Cybersecurity, 2. Aufl. 2023, Kap. 3 Rz 177.

27 Etwa Sophos, The State of Ransomware 2024, abrufbar unter https://www.sophos.com/en-us/content/state-of-ransomware (08.01.2025).

28 Illustrativ (wenn auch nicht unbedingt exemplarisch): *Khatchadourian*, A Cybersecurity Firm's Sharp Rise and Stunning Collapse, NewYorker, 28.10.2019, Ed. 4.1.2019.

29 Laut Sophos wurden rund 5.000 IT- und Cybersicherheitsverantwortliche von Unternehmen mit einer Größe von 100 bis 5.000 Mitarbeitenden befragt; die Befragung selbst wurde von der Agentur „Vanson Bourne“ zwischen Januar und Februar 2024 durchgeführt: https://news.sophos.com/en-us/2024/05/14/the-role-of-law-enforcement-in-remediating-ransomware-attacks/ (06.04.2025).

der Skala lagen Brasilien (44 %), Japan (51 %) und Australien (54 %) mit vergleichsweise niedrigen Angriffsraten. Während die Zahl der Angriffe in neun Ländern im Vergleich zu 2023 zurückging, stieg sie in fünf europäischen Ländern an, darunter Österreich, Frankreich, Deutschland, Italien und das Vereinigte Königreich.[30]

Ferner betrafen Ransomware-Angriffe verschiedene Branchen (mit wenigen Ausnahmen) relativ gleichmäßig, wobei die Angriffshäufigkeit in 11 der 15 untersuchten Branchen zwischen 60 % und 68 % lag. Eine Ausnahme bilden der Sektor Staat/Lokalverwaltung, in dem nur 34 % der Organisationen betroffen waren, und der Einzelhandel mit 45 %, in dem ebenfalls weniger als die Hälfte der Befragten Angriffe meldeten. Die höchste Angriffsrate verzeichnete hingegen die Zentral-/Bundesregierung mit 68 %. Der Gesundheitssektor erlebte einen Anstieg der Angriffe auf 67 %, in der IT-, Telekommunikations- und Technologiebranche stieg die Rate auf 55 %.[31]

Offenbar werden Lösegeldzahlungen bei Ransomware-Angriffen von Unternehmen häufig erwogen und tatsächlich geleistet. Bei den 1.097 Befragten, deren Organisation das geforderte Lösegeld gezahlt hat, stieg sowohl der Median als auch der Mittelwert deutlich an: Der Median stieg auf 2 Millionen US-Dollar (im Vergleich zu 400.000 US-Dollar aus dem Vorjahr), der Durchschnittswert von Lösegeldzahlungen lag bei rund 3,9 Millionen US-Dollar.[32] Andere Quellen hingegen berichten, dass 2024 die Zahlungen von Lösegeld nach Ransomware-Angriffen gefallen seien.[33]

3. Case-Study: Conti Leak

Nachdem überblicksweise Funktionsweisen und Mechanismen des Phänomens Ransomware dargestellt wurden, liegt der Fokus nun auf den Tätergruppen, die hinter diesen kriminellen Aktivitäten stehen. Ein differenziertes Verständnis der Strukturen, Motivationen und Vorgehensweisen dieser Gruppen ist essentiell, um effektive Gegenstrategien zu entwickeln und die Mechanismen der Cyberkriminalität in ihrer Gesamtheit zu durchdringen.

30 Sophos, The State of Ransomware, 2024, 4.
31 Sophos, The State of Ransomware, 2024, 6.
32 Sophos, The State of Ransomware, 2024, 18.
33 https://www.bleepingcomputer.com/news/security/ransomware-payments-fell-by-35-percent-in-2024-totalling-813-550-000/ (abgerufen am 25.03.2025), in Berufung auf Chainalysis.

Die Analyse erfordert dabei den Rückgriff auf (einigermaßen) verlässliche Studien und Datenquellen, um hochspekulative Annahmen zu vermeiden und empirisch fundierte Aussagen treffen zu können.

Hierfür bietet sich insbesondere der sogenannte Conti-Leak an, der detaillierte Einblicke in die interne Organisation und Arbeitsweise einer der weltweit aktivsten Ransomware-Gruppen namens „Conti" ermöglicht[34] Die Conti-Gruppe, eine der weltweit aktivsten und aggressivsten Ransomware-Organisationen, rückte Anfang 2022 ins Zentrum der Aufmerksamkeit, als interne Daten an die Öffentlichkeit gelangten.[35] Diese Leaks umfassten mehr als 60.000 interne Chatprotokolle, den vollständigen Quellcode der Ransomware sowie Schulungsmaterialien und Tutorials. Die Veröffentlichung der Daten erfolgte vor dem Hintergrund geopolitischer Spannungen: Nachdem die Conti-Gruppe im Zusammenhang mit dem Ukraine-Konflikt ihre Unterstützung für die russische Regierung zum Ausdruck gebracht hatte,[36] reagierte ein Insider, der mutmaßlich pro-ukrainisch eingestellt war, mit der Veröffentlichung der internen Informationen. Diese undichte Stelle bot der Öffentlichkeit und den Strafverfolgungsbehörden einen bislang beispiellosen Einblick in interne Abläufe eines Ransomware-„Konzerns".

3.1. Organisationsstruktur

Entgegen der Vorstellung von Cyberkriminellen als lose agierenden Einzelakteuren zeigt sich, dass Conti als streng hierarchisch strukturierte Organisation agierte, die in vielerlei Hinsicht den Abläufen eines klassischen Unternehmens glich.[37]

---

34 Instruktiv *Paternoster/Nazzari/Jofre/Uberti*, Inside the Leak: Exploring the Structure of the Conti Ransomware Group, Global Crime 1–24/2025, abrufbar unter https://doi.org/10.1080/17440572.2025.2473350 (06.04.2025).

35 Im Mai 2025 wurde die berüchtigte Ransomware-Gruppe LockBit kompromittiert und interne Daten mit Informationen zu Opfern veröffentlicht; diesbezüglich lagen jedoch zum Zeitpunkt der Manuskriptabgabe keine verlässlichen Informationen vor, weshalb hier nur auf den Conti Leak eingegangen wird.

36 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 26.04.2025).

37 Inzwischen ist im Bereich der Ransomware zunehmend ein Modell mit dezentralen Strukturen zu beobachten: Viele Gruppen operieren heute im Rahmen sogenannter Affiliate- oder Franchise-Modelle, bei denen eigenständige Partner – teils mit vertraglich geregelter Gewinnbeteiligung – für die initiale Infektion und teilweise auch für die Lösegeldverhandlungen verantwortlich sind; vgl. *Baker*, Ransomware as a Service (RaaS) explained how it works & examples vom 30.01.2023, abrufbar unter https://w

Herz der Conti-Organisation war eine klare Hierarchie, die Entscheidungsfindung und Arbeitsteilung effizient strukturierte. An der Spitze standen Führungskräfte, die strategische Entscheidungen trafen, wie etwa die Auswahl von Angriffszielen, die Festlegung von Lösegeldforderungen und die Priorisierung technischer Entwicklungen. Diese Anführer waren auch für die Verwaltung der finanziellen Ressourcen zuständig und koordinierten die Verteilung der Gewinne innerhalb der Gruppe. Unterhalb dieser Führungsebene gab es spezialisierte Teams, die jeweils für bestimmte Aufgabenbereiche zuständig waren. Diese Teams arbeiteten weitgehend autonom, aber unter der Aufsicht ihrer jeweiligen Vorgesetzten, die die Umsetzung der Gruppenstrategie sicherstellten. Auffallend ist die detaillierte Dokumentation und Berichterstattung innerhalb der Organisation, um Transparenz und Effizienz zu maximieren.

Die Organisation arbeitete nach einem Modell arbeitsteiliger Strukturen, das sich durch klare Zuständigkeiten und hohe Professionalität auszeichnete. Technische Experten innerhalb der Gruppe widmeten sich der Entwicklung und Weiterentwicklung der Conti-Schadsoftware. Sie waren für die Anpassung an neue Sicherheitsmaßnahmen und die Integration aktueller Exploits verantwortlich, damit die Schadsoftware immer auf dem neuesten Stand war und ihre maximale Wirkung entfalten konnte. Parallel dazu agierten Spezialisten, die sich auf das Eindringen in fremde Netzwerke und Systeme konzentrierten. Diese setzten eine Vielzahl von Techniken ein, darunter gezielte Phishing-Kampagnen und den Einsatz von Exploit-Kits, um Sicherheitslücken auszunutzen. Gelegentlich wurden auch Zugangsdaten von Drittanbietern im Darknet beschafft, wodurch die Gruppe ihre Angriffsfläche vergrößerte und zusätzliche Ressourcen nutzen konnte.

Ein weiterer wichtiger Bereich innerhalb der Organisation betraf die Kommunikation mit den Opfern. Mitarbeiter, die sich auf Verhandlungsstrategien spezialisiert hatten, übernahmen den Kontakt und führten Lösegeldforderungen gezielt durch. Sie bedienten sich manipulativer Taktiken, um Druck auszuüben und die Opfer zur Zahlung zu bewegen. Dabei folgten sie strikten Vorgaben des internen „Playbooks", die auf eine Maximierung der Erfolgsaussichten abzielten. Eine andere „Abteilung" von Experten entwickelten Strategien zur Geldwäsche, insbesondere im Umgang mit Kryptowährungen, die häufig bei Lösegeldzahlungen verlangt wurden. Mithilfe der bereits oben erwähnten Mixer-Diensten und komplexen Transak-

ww.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (06.04.2025).

tionsketten wurde sichergestellt, dass die finanziellen Erträge nur schwer zurückverfolgt werden konnten und letztlich in legale Finanzströme einflossen.

3.2. Onboarding

Die durch den Conti-Leak bekannt gewordenen Schulungsmaterialien zeigen auch die systematische Herangehensweise der Ransomware-Gruppe Conti bei der Schulung ihrer Mitglieder.[38] Ein zentraler Bestandteil des Schulungsprogramms war die Einführung in fortgeschrittene Penetrationstechniken. Neue Mitglieder erhielten detaillierte Handbücher, in denen Schritt für Schritt erklärt wurde, wie man in fremde Netzwerke eindringt, sich Administratorrechte verschafft und persistente Zugänge schafft. Diese Anleitungen beinhalteten auch die Konfiguration von Tools wie AnyDesk für den Fernzugriff und Rclone für die Datenexfiltration, um die Effektivität der Angriffe zu maximieren. Besonderes Augenmerk wurde auf die Verwendung spezieller Software gelegt.

Die Schulungsunterlagen enthielten detaillierte Anweisungen zur Installation und Verwendung von Cobalt Strike, einem bekannten Werkzeug für Penetrationstests, das von der Gruppe für böswillige Zwecke angepasst wurde. Darüber hinaus wurden Techniken wie Kerberoast zur Kompromittierung von Anmeldedaten in Netzwerken sowie Methoden zur Deaktivierung von Sicherheitsmechanismen wie Windows Defender vermittelt, um die Entdeckung der Schadsoftware zu verhindern. Die Schulungsunterlagen gingen über technische Aspekte hinaus und behandelten auch operative Taktiken. Die Mitglieder wurden in Social Engineering geschult, um menschliche Schwächen auszunutzen, sowie in der effektiven Nutzung des Darknets, um zusätzliche Ressourcen zu beschaffen oder erbeutete Daten zu verkaufen.

Diese umfassende Ausbildung stellte sicher, dass die Mitglieder nicht nur über das technische Know-how, sondern auch über das notwendige taktische Verständnis verfügten, um erfolgreiche Angriffe durchzuführen. Die Professionalität des Schulungsprogramms spiegelte sich in der Qualität und Tiefe der zur Verfügung gestellten Materialien wider: Die Unterlagen waren klar strukturiert, praxisorientiert und wurden regelmäßig aktualisiert, um der sich verändernden Sicherheitslandschaft Rechnung zu tragen.

38 Ausführlich dargestellt durch esentire https://www.esentire.com/blog/analysis-of-leaked-conti-intrusion-procedures-by-esentires-threat-response-unit-tru (06.04.2025).

3.3. Kommunikation

Die im Conti-Leak veröffentlichten internen Chat-Protokolle geben einen detaillierten Einblick in die Kommunikations- und Entscheidungsprozesse des Conti-„Konzerns".[39] Die Kommunikation innerhalb der Conti-Gruppe erfolgte hauptsächlich über verschlüsselte Messenger-Dienste, was Sicherheit und Anonymität gewährleisten sollte. Die Protokolle zeigen, dass regelmäßig über den Fortschritt der Angriffe, technische Probleme und finanzielle Angelegenheiten berichtet wurde. Besonders auffällig ist die direkte und teilweise rigide Kommunikation zwischen den verschiedenen Hierarchieebenen. Entscheidungen und Anweisungen wurden klar formuliert und die Ausführenden hatten wenig Spielraum, von diesen Vorgaben abzuweichen. Dies betraf insbesondere die Auswahl der Angriffsziele, die Festlegung der Höhe der Lösegeldforderungen und das technische Ressourcenmanagement.

Trotz (oder gerade wegen) dieser zentralisierten Struktur und der klaren Kommunikation zeigen die Lecks auch interne Spannungen und Konflikte. Ein häufiger Streitpunkt war die Verteilung der Gewinne. Einige Mitglieder äußerten ihre Unzufriedenheit über ungleiche Zahlungen und forderten eine gerechtere Verteilung. Diese Konflikte wurden zum Teil offen in den Chats ausgetragen, wobei das „Management" oft rigoros eingriff, um die Disziplin aufrechtzuerhalten. Ein weiterer Konfliktpunkt betraf die Sicherheitsvorkehrungen. Einige Mitglieder beschwerten sich über die ständige Überwachung oder die Notwendigkeit, ihre Identität zu verbergen, was die Arbeit erschwerte. Diese Beschwerden wurden jedoch selten berücksichtigt, da die Sicherheit der Organisation oberste Priorität hatte.

3.4. Darknet Ökonomie

Die im Conti-Leak enthaltenen Informationen geben nicht nur Einblick in die interne Organisation der Gruppe, sondern auch in das kriminelle Ökosystem des Darknets selbst, in dem sie operierte. Besonders aufschlussreich sind die Strategien, mit denen die Conti-Gruppe über diese Plattformen neue Mitglieder rekrutierte und ihre Strukturen ausbaute.

39 Ausführlich bei Rapid7 unter https://www.rapid7.com/blog/post/2022/03/01/conti-ransomware-group-internal-chats-leaked-over-russia-ukraine-conflict (06.04.2025) sowie Flashpoint unter https://flashpoint.io/blog/history-of-conti-ransomware/ (06.04.2025).

Über spezialisierte Foren und Marktplätze wurden gezielt Spezialisten mit bestimmten technischen oder operativen Fähigkeiten angesprochen. Die Gruppe nutzte die Anonymität dieser Plattformen, um potenzielle Mitglieder anzuwerben, ohne ihre eigene Identität oder ihren Standort preiszugeben. Die von Conti veröffentlichten Stellenangebote waren häufig detailliert und ähnelten Ausschreibungen legaler Unternehmen. Gesucht wurden etwa Entwickler mit Erfahrung in Verschlüsselungstechnologien, Penetrationstester und Experten für Social Engineering. Um das Interesse potenzieller Bewerber zu wecken, wurden attraktive Vergütungen und flexible Arbeitsbedingungen hervorgehoben. Ein typisches Merkmal dieser Ausschreibungen war die Betonung der "Unabhängigkeit" der Mitarbeiter, die häufig als Freelancer arbeiteten und somit nicht fest in die Organisationsstruktur eingebunden waren. Gleichzeitig unterstrich Conti die eigene Professionalität und die langfristigen Möglichkeiten einer Zusammenarbeit, was insbesondere für technikaffine und risikobereite Akteure attraktiv war.[40]

Die Rekrutierungsprozesse der Conti-Gruppe waren ebenso strukturiert wie die betrieblichen Abläufe. Interessenten mussten ihre Fähigkeiten als „Freelancer“ häufig in praktischen Tests unter Beweis stellen. Dabei konnte es sich um die erfolgreiche Durchführung eines Penetrationstests oder die Entwicklung eines spezifischen Softwaretools handeln. Solche Tests dienten nicht nur der Überprüfung der technischen Fähigkeiten, sondern auch als Sicherheitsmechanismus, um zu gewährleisten, dass die Bewerber keine verdeckten Ermittler waren. Neben den technischen Fähigkeiten legte die Gruppe großen Wert auf Loyalität und Diskretion. Die Kandidaten wurden in den ersten Phasen ihrer Tätigkeit intensiv überwacht, und ihre Kommunikation mit anderen Mitgliedern war streng reglementiert. Damit sollten potenzielle Sicherheitsrisiken minimiert und der innere Zusammenhalt der Gruppe gewahrt werden. Nach der Rekrutierung der bewährten Freelancer wurden diese durch ein strukturiertes Onboarding-Programm in die Organisation integriert. Dieses beinhaltete nicht nur Schulungen, wie sie im Leak ausführlich beschrieben sind, sondern auch die schrittweise Einführung in operative Aufgaben. Neue Mitglieder wurden zunächst mit niedrigschwelligen Aufgaben betraut, bevor sie in zentrale Projekte eingebunden wurden. Diese Methodik ermöglichte es der Gruppe, Fähigkeiten

40 *Paternoster/Nazzari/Jofre/Uberti*, Inside the Leak: Exploring the Structure of the Conti Ransomware Group, Global Crime 1–24/2025, abrufbar unter https://doi.org/10.1080/17440572.2025.2473350 (06.04.2025).

und Loyalität der neuen Mitglieder zu testen und ihnen gleichzeitig die Möglichkeit zu geben, sich mit den internen Abläufen vertraut zu machen.[41]

4. Ransomware-Gruppierungen als kriminelle Vereinigungen

Im Folgenden soll die Frage ergründet werden, ob Ransomware-Gruppierungen als kriminelle Vereinigung strafrechtlich belangt werden und welche Herausforderungen sich bei der Rechtsanwendung stellen könnten.

4.1. Einleitende Bemerkungen

Das deutsche Strafrecht kennt für Zusammenschlüsse mehrerer Personen, neben den verschiedenen Beteiligungsmöglichkeiten, zwei Formen: die Bande und die kriminelle Vereinigung.

Die Mitgliedschaft in einer Bande ist ein Tatbestandsmerkmal, aber kein eigener Straftatbestand, sodass die Mitgliedschaft in einer Bande nicht als solches strafbar ist. Vielmehr ist diese in erster Linie strafschärfend, wobei es auch Auswirkungen im Bereich der Nebenfolgen und Zwangsmaßnahmen im Ermittlungsverfahren gibt.[42]

Die kriminelle Vereinigung ist demgegenüber ein eigenständiger Tatbestand. Strafbar macht sich, wer sie gründet, als Mitglied teilnimmt, sie unterstützt (oder für Mitglieder wirbt). Die Konsequenz ist, dass auch eigentlich sozialadäquates Verhalten, wie etwa die Serverwartung, vom Tatbestand erfasst ist, sofern der entsprechende Vorsatz vorliegt.[43] Historisch hat die Norm ihren Ursprung im (preußischen) Staatsschutzrecht, erfasste also in erster Linie staatsfeindliche politische Verbindungen wie die SPD Ende des 19. Jahrhunderts.[44] Wir werden sehen, dass auch die heute geltende Norm diese Entstehungsgeschichte nicht gänzlich abgeschüttelt hat. Ob

41 Check Point Research unter https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/ (06.04.2025).

42 vgl *Ebbinghaus* HRRS 2023/10 S.318 f.

43 Vgl. MüKoStGB/*Schäfer/Anstötz* § 129 Rn. 88; SK-StGB/*Stein/Greco* § 129 Rn. 52,47, 48; LK-StGB/*Krauß* § 129 Rn. 100, 101, 103; BGH NJW 2016, 657, 660.

44 Strafbar waren Verbindungen, die unrechtmäßig die Gesetzesvollziehung/Verwaltung behinderten. Da dies auf die SPD nicht zutraf, bedurfte es des Sozialistengesetzes, auf deren Umgehung SPD (/-nahe Verbindungen) gerichtet waren, um § 129 RStGB anwenden zu können.

Ransomware-Gruppierungen hierunter fallen können, soll Gegenstand des folgenden Abschnitts sein. Der Schwerpunkt wird dabei auf russischsprachigen Gruppierungen liegen, bei denen die Anwendung des § 129 StGB vor den größten Herausforderungen steht.

Eine Vereinigung, wie sie in § 129 II StGB legaldefiniert ist, besteht aus einem personalen, zeitlichen, organisatorischen und einem voluntativen Element.[45] Der Zusammenschluss setzt eine gewisse Organisationsstruktur sowie eine in gewissem Umfang vorhandene instrumentelle Vorausplanung und Koordinierung voraus. Die Vereinigung ist kriminell, wenn ihr Zweck oder ihre Tätigkeit auf die Begehung von Straftaten gerichtet ist.

Als zusätzliche, ungeschriebene Einschränkung des Tatbestandes wird ferner verlangt, dass es sich bei den Straftaten um solche von einigem Gewicht handeln müsse.[46] Teilweise wird dies in § 129 III Nr.2 StGB verortet.[47] Dies soll insbesondere Bagatellkriminalität ausschließen, aber schon die Begehung von Diebstählen im großen Stil wurde als ausreichend angesehen.[48] Daher ist es naheliegend, dass Erpressungen im großen Stil, Ausspähen von Daten, Datenhehlerei, Computersabotage[49] diese Anforderungen erfüllen. Dies gilt auch dann, wenn in dem Bereitstellen der Ransomware und der Infrastruktur lediglich eine Beihilfe gesehen wird, da die Affiliates bei der Opferauswahl und Infiltration der IT Systeme nicht selten eigenständig vorgehen.

Falls es sich bei den Ransomware-Gruppen um eine kriminelle Vereinigung iSd § 129 StGB (idR iVm § 129b StGB, da ausländisch) handelt, so ist nicht nur Mitgliedschaft strafbar, sondern auch deren Unterstützung. Dies hätte allerdings zur Folge, dass die Zahlung von „Lösegeld" zumindest

45 BGH, Urteil vom 3. Dezember 2009 – 3 StR 277/09 –, BGHSt 54, 216–236 Rn. 23; *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385, 388; SK-StGB/*Stein/Greco* § 129 StGB Rn. 7.

46 BGH, Urteil vom 22.2.1995 – 3 StR 583/94-, BGHSt 41, 47–57; LK-StGB/*Krauß* § 129 StGB Rn. 54; SK-StGB/*Stein/Greco* § 129 StGB Rn. 27.

47 *Kuhli/Papenfuß*, KriPoZ 2023, 71,75, sie können sich dabei zwar auf den Willen des Gesetzgebers berufen, welcher mit dieser Einschränkung Sachbeschädigungen aus dem Anwendungsbereich des § 129 StGB heraushalten wollte, die Rspr. & hM sieht es jedoch als ein ungeschriebenes Tatbestandsmerkmal an.

48 BGHSt 57,14.

49 Vgl hierzu BGH ZWH 2022, 22, hier schien es sich um ein Affiliate gehandelt zu haben, § 129 StGB wurde nicht angesprochen, obwohl mehr als drei Personen beteiligt waren; vgl. auch *Eisele* in: Hilgendorf/Kudlich/Valerius (Hrsg.), Handbuch des Strafrechts, 2022, § 63 Rn. 142–145; *Vogelgesang/Möllers*, jM 2016, 381, 383ff.

den Tatbestand des § 129 StGB erfüllt[50] und eine Strafbarkeit des Ransomware-Opfers, das eine Zahlung an die Gruppe tätigt, allenfalls über Rechtfertigungsgründe (insb. Nötigungsnotstand) zu vermeiden wäre[51].

4.2. Organisatorisches Element

An das organisatorische Element werden keine großen Anforderungen gestellt, die Rechtsprechung bejaht dies bereits bei einem Zusammenschluss, der nur in den sozialen Netzwerken existiert, auch dann, wenn dieser „in gewisser Weise unverbindlich ist" und keine besonders ausgestalteten Regeln kennt, solange nur ein koordiniertes Zusammenwirken zur Erreichung des gemeinsamen Ziels vorliegt.[52]

Für einen Teil der Lehre ist das organisatorische Element das maßgebliche Kriterium, um die Bande von der kriminellen Vereinigung abzugrenzen.[53] Nach dieser Auffassung zeichnet sich eine Bande durch deutlich rudimentärere Strukturen aus als eine kriminelle Vereinigung, auch auf die persönliche Bereicherung der Beteiligten gerichteten Zusammenschlüsse könnten so als kriminelle Vereinigung erfasst werden. Dabei wird je-

50 A.A. *Makepeace* StV 2022, 754, 755–756 meinte, dass es dem Zahler idR nicht bewusst sein dürfte, welche Gruppierung genau unterstützt werden würde, daher läge der objektive Tatbestand schon nicht vor, dabei werden die Anforderungen an den objektiven Tatbestand hinsichtlich des Unterstützens einer kriminellen Vereinigung in nicht mehr vertretbarer Weise angehoben, sodass im Ergebnis nur noch die Unterstützung einer bereits gerichtlich als solcher festgestellten kriminellen Vereinigung erfasst wäre, *Makepeace* lehnt auch den Vorsatz dahingehend ab, da ein bloß allgemeines Wissen, dass eine kriminelle Vereinigung hinter der Erpressung stehe nicht ausreiche (aaO S. 756); aber auch LK-StGB/*Krauß* § 129 Rn. 149 verlangen nur, dass sich der Vorsatz darauf bezieht, dass die Unterstützung gerade der betreffenden kriminellen Vereinigung zugute kommt, m.a.W.: wird Lösegeld gezahlt, ist es nicht ersichtlich, wieso sich das Opfer nicht bewusst sein sollte, dass diese Lösegeldzahlung dem Adressaten der Zahlung (Erpresser) auch zugute kommt, damit auch der (ggf. dahinter stehenden) kriminellen Vereinigung; vgl. auch SK-StGB/*Stein/Greco* § 129 StGB Rn. 46: Unterstützen Aufrechterhaltung oder Erhöhung des spezifischen Gefährdungspotentials, keine qualifizierte Vorsatzform (aaO Rn. 52).

51 Unserer Ansicht nach ist die Lösung über den Nötigungsnotstand vorzugswürdig (so auch SK-StGB/*Stein/Greco* § 129 Rn. 53 für Schutzgeldzahlungen allgemein; vgl. *Dittrich/Erdogan*, ZWH 2022, 13, 17; so auch *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385, 388,389, welche auch auf § 129 VI StGB verweisen; ein Anfangsverdacht scheint uns in diesem Kontext aber eher fernliegend, siehe Lösegeldzahlungen bei Cyberangriffen .

52 *Ebbinghaus*, HRRS 10/2023, 318, 320, Fn. 21 m.w.N.

53 *Sinn/Iden/Pörtner*, ZIS 2021 435, 446,447.

doch der Tatbestand in verfassungsrechtlich nicht hinnehmbare Weise verschleift: denn das übergeordnete gemeinsame Interesse, welches der Gesetzgeber in die Legaldefinition in Abs.2 aufgenommen hat, würde in dem Tatbestandsmerkmal der Bezweckung von Straftaten aufgehen. Das übergeordnete Interesse ist es, was ein notwendiges Merkmal für eine Vereinigung ist, die Bezweckung von Straftaten ist es, was der Vereinigung den kriminellen Charakter verleiht.

In der Praxis ergibt sich dabei die Herausforderung, dass Ransomware-Gruppen nicht homogen arbeiten, sondern sich bisweilen zwischen Kerngruppe und Affiliate differenzieren lässt. So setzen gerade russische Ransomware-Gruppierungen häufig auf ein RaaS Modell (s.o.), bei dem es eine Kern-Gruppierung gibt, die Software, Server zur Verfügung stellt, sowie oft auch eine Marke bereitstellt, unter der operiert wird. Die sogenannten Affiliates sind diejenigen, die die Angriffe überwiegend durchführen, teilweise bedienen sie sich auch sogenannter Access-Broker, die ein anvisiertes IT-System bereits infiltriert haben, sodass nur noch die Schadsoftware hochgeladen werden muss. Es ist nicht unüblich, dass ein Affiliate mehrere Anbieter (/Kern-Gruppierungen) nutzen, mehrere Angriffe gleichzeitig durchführen.[54]

Es scheint, als wären die Affiliates nicht in dem erforderlichen Maße in die Kerngruppierung integriert, um von eine umfassende Vereinigung anzunehmen. Denn teilweise agieren die Affiliates in den Dark-Net Foren auch unter eigenem Namen[55]. Sofern also die Kerngruppierung eine kriminelle Vereinigung darstellt, kann die Nutzung von Ransomware durch Affiliates eine Unterstützung der Kerngruppierung darstellen, somit von § 129 I S.2 StGB erfasst werden. Denkbar ist auch, dass es sich bei manchen Affiliates um eigenständige kriminelle Vereinigungen handelt, basierend auf den öffentlich zugänglichen Informationen spricht viel dafür, Affiliates und Kern-Gruppierung zumindest nicht als eine (gemeinsame) kriminelle Vereinigung anzusehen.

---

54 https://analyst1.com/ransomware-diaries-volume-2/ (abgerufen am 27.08.2023); vgl. auch https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/ (abgerufen am 06.04.2025), wonach es hohe Fluktuation bei den ‚Mitglieder' niedrigen Ranges bei Conti gegeben hat, es erscheint daher fraglich, diese als Mitglieder einzustufen, die kriminelle Vereinigung iSd § 129 StGB könnte daher auf höherrangige Mitglieder beschränkt geblieben sein.

55 zB ‚National Hazard Agency' als Name, unter dem ein Affiliate von LockBit auftrat, unbekannt, ob ein oder mehrere Mitglieder hatte, vgl. https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/ (abgerufen am 27.08.2023).

4.3. Übergeordnetes gemeinsames Interesse

Problematisch ist das Element des sog. übergeordneten gemeinsamen Interesses, insbesondere bei wirtschaftskriminellen bzw. auf finanziellen Gewinn ausgerichteten Zusammenschlüssen.[56] Über dieses gemeinsame Interesse erfolgt die Abgrenzung zum bloß strafschärfenden Tatbestandsmerkmal der Bande.[57] Das gemeinsame Interesse darf sich nicht auf die Begehung von Straftaten beschränken (da es sich hierbei um ein anderes konstitutives Merkmal der kriminellen Vereinigung handelt, dass auch vom Vorsatz umfasst sein muss, auch würde andernfalls ein Gleichlauf mit der Bande erfolgen), auch ein (reines) Handeln um eines persönlichen Vorteils willen genügt nach ständiger Rechtsprechung nicht.[58] Im wirtschaftskriminellen Kontext im engeren Sinne (bspw Vorwürfe gegen ehemaligen Vorstand der Wirecard-AG), gibt es große Probleme, da die Strukturen regelmäßig auch legalen Zwecken dienen.[59] Zumindest dieses Problem besteht aber bei den Ransomware-Gruppierungen nicht.

4.3.1. Russische Ransomware-Gruppierungen

Bei Ransomware-Gruppen, die auch politisch Ziele verfolgen dürfte die Bejahung einer kriminellen Vereinigung leichtfallen, zumindest bezüglich der Kerngruppe. Russische Ransomware-Gruppierungen sind wohl überwiegend nicht in den staatlichen Sicherheitsapparat integriert, werden aber von diesem geduldet, solange sich die Tätigkeit auf Opfer außerhalb der russischen Föderationen beschränkt.[60] Die Beschränkung auf das Ausland scheint somit weniger politischen Zielen zu dienen, als vielmehr der Selbst-

56 BGH 3 StR 21/231, Rn.21 juris; BGH, Beschluss vom 9. Februar 2021 – AK 3 und 4/21 –, juris Rn.24.

57 BGH, Urteil vom 2. Juni 2021 – 3 StR 21/21 –, juris Rn.20; BGH, Beschluss vom 2. Juni 2021 – 3 StR 61/21 –, juris Rn.7, st.Rspr.

58 BGH 3 StR 21/231, juris; BGH NJW 2021, 2813, 2815f. BT-Drucks. 18/11275 S. 11; LK/*Krauß* § 129 Rn. 40 f.; SK-StGB/*Stein/Greco* § 129 Rn. 15; *Montenegro*, GA 2019, 489, 502.

59 SK-StGB/*Stein/Greco* § 129 Rn.4,19.

60 Überwiegend das westliche Ausland, aber auch in der südlichen Hemisphäre, zB Brasilien, vgl. *Couretas*, Cyber Operations, 2024, S.1 ff.

erhaltung, dem Schutz vor Strafverfolgung oder zu viel Aufmerksamkeit und Zwangsrekrutierung durch FSB/SVR/GRU.[61]

Es scheint deshalb fraglich, ob die Unterstützungserklärung zugunsten der russischen Regierung für den Überfall auf die Ukraine durch Conti wirklich Ausdruck einer politischen Einstellung oder Zielsetzung ist, da viele der Affiliates, die für das RaaS Geschäft elementar sind, in der Ukraine saßen und entsprechend verärgert waren.[62] Da zeitgleich mit der Invasion der FSB kurzzeitig ein Interesse an Ransomware-Gruppen zeigte,[63] lässt sich dies eher als eine Schutzmaßnahme vor staatlicher Repression deuten. LockBit, eine konkurrierende Ransomware-Gruppe, erklärte etwa kurz nach dem russischen Einmarsch, dass sie unpolitisch sein, ihnen ginge es nur ums Geld: „*We are only interested in money for our harmless and usefull work*"[64].

Die mittlerweile an Bedeutung verlorene EvilCorp, eine andere Ransomware-Gruppe, hat demgegenüber enge Verbindungen zu staatlichen Hackern[65] – hier erscheint es naheliegend, dass nicht nur wirtschaftliche Interessen verfolgt werden. Folglich ist bei Gruppierungen wie EvilCorp, die Verbindungen zu Nachrichtendiensten haben und auch politisch motiviert agieren,[66] die Bejahung einer kriminellen Vereinigung im Ausland naheliegend.

61 Vgl. hierzu jüngst: https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/ (abgerufen am 23.03.2025): BlackBasta hat zuvor russische Banken ins Visier genommen, daraufhin wurden wohl interne Chats geleakt.

62 Vgl. https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).

63 Vgl https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/ (abgerufen am 06.04.2025).

64 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023) Diese Formulierung zeigt die zynische Selbstdarstellung als Post-Pen-tester, also als Programmierer, die Sicherheitslücken aufzeigten und dafür belohnt werden wollen, ein derart abwegiger Vorwand, der durch die Tätigkeit widerlegt ist und keiner näheren Erörterung bedarf.

65 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.23), vgl auch National State Ransomware S. 16f.

66 *Couretas*, Cyber Operations, 2024, S. 86.

4.3.1.1. Das Problem „LockBit"

In Fällen wie bei LockBit,[67] bei denen die Gewinnerzielungsabsicht der Beteiligten im Vordergrund zu stehen *scheint*, ist der typologische Vereinigungsbegriff der Rechtsprechung[68] von Bedeutung: Im Rahmen der Gesetzesreform 2017 hat der Gesetzgeber klargestellt, dass die Anforderungen an das organisatorische Element bei der kriminellen Vereinigung abgesenkt werden sollen.[69] Jedoch kann das gemeinsam verfolgte Interesse der Vereinigung aus objektiven Merkmalen hergeleitet werden, eine stark ausgeprägte Organisationsstruktur spricht dafür, dass nicht nur die persönliche Bereicherung der einzelnen im Vordergrund stehe.[70] So sah der BGH Indizien für ein übergeordnetes gemeinsames Interesse im Bestehen eines Prozesses der einheitlichen Willensbildung, internen Sanktionierung von Verstößen gegen gemeinschaftlich Regeln, eine Gemeinschaftskasse oder der Beanspruchung staatlicher Autorität und Einflussnahme auf Medien,[71] alles Elemente, die sich, wie dargelegt, auch bei Ransomware-Gruppierungen bejahen lassen.[72] In der Callcenter-Entscheidung hat der BGH aufgrund stark ausgeprägter Organisationsstrukturen das Bestehen einer kriminellen Vereinigung für naheliegend gehalten, sodass der Fall an eine Staatsschutzkammer zur weiteren Tatsachenfeststellung überwiesen wurde.[73] Die erste Hawala Entscheidung des BGH[74] wurde z.T. so verstanden, dass als gemeinsames Interesse auch der Selbsterhalt der Organisation in Betracht kommt,

67 Trotz der Stellungnahme Contis nach dem Überfall auf die Ukraine, spricht unserer Meinung viel dafür, dass dies auch auf Conti zutrifft, vgl. https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/ (abgerufen am 06.04.2025).

68 BGH NJW 2021, 2813 ff.; *Ebbinghaus*, HRRS 1/2023,16, 19 f.; SK-StGB/*Stein/Greco* §129 StGB Rn. 27.

69 BT DS 18/11275 S.10; wie aus § 98 I Nr. 6 StPO hervorgeht, weißt auch eine Bande ein organisatorisches Element auf, vgl. *Ebbinghaus* HRRS 1/2023 16, 18f.

70 BGH NJW 2021, 2813, 2814f. st.Rspr., BGHSt 44, 68; BGHSt 54, 216; BGH 2 StR 353/18 Rn.33, juris.

71 Vgl. BGH NJW 2021 2813, 2816; BeckOK-StGB/*Kulhanek* (1.8.24) § 129 Rn.32.

72 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023): Von Dritten moderierte Dark-Net-Foren mit eigenen Streitschlichtungsverfahren, Nutzer-(=Affiliates) Bewertung etc.

73 BGH NJW 2021, 2813.

74 BGH NStZ 2022, 35.

sofern bestimmte Voraussetzungen gegeben sind (in erster Linie eine gut ausgeprägte Struktur).[75]

Doch wäre dies ein Zirkelschluss: Die Vereinigung bestünde, weil die Beteiligten als gemeinsames Interesse bezwecken, das Bestehen der Vereinigung zu gewährleisten. Für die Frage nach dem gemeinsam verfolgten Interesse kommt es aber darauf an, *warum* der Zusammenschluss erhalten werden soll. Auch wenn der BGH derart (miss-) verstanden wird, dass diese Selbsterhaltung ausreiche[76], kann dies nicht überzeugen. Es ist daher begrüßenswert, dass der BGH ein Jahr später, in der zweiten Hawala Entscheidung, hiervon etwas abgerückt ist.[77] Insofern ist auch hier nach dem „Warum" zu fragen, eine Frage, die unter Verweis auf den Selbsterhalt nicht beantwortet wird. Es ist zu klären, warum der Erhalt des Zusammenschlusses angestrebt wird, denn dies ist das gemeinsam verfolgte Interesse, welches Voraussetzung für die Einstufung als Vereinigung iSd § 129 II StGB ist.

Eine ausgeprägte Organisationsstruktur ist also ein starkes Indiz für ein übergeordnetes gemeinsames Interesse. Diese Indizwirkung kann aber widerlegt werden, wenn sich die ausgeprägte Organisationsstruktur anderweitig erklären lässt. Erfordern die von dem Zusammenschluss zu begehenden Vermögensstraftaten etwa eine besonders ausgeprägte Organisationsstruktur, kann diese dadurch erklärt werden, dass so die persönliche Bereicherung der Beteiligten gewährleistet werden soll. Die Indizwirkung der ausgeprägten Struktur für ein übergeordnetes gemeinsames Interesse kann so in dem konkreten Fall auch widerlegt werden. Nur solche, über dieses Maß hinausgehende Strukturen sind ein starkes Indiz, dass es ein übergeordnetes gemeinsames Interesse gibt, da ihre Existenz nicht anders zu erklären ist.

---

75 So zB BeckOK-StGB/*Kulhanek* (1.8.24) § 129 Rn. 32; *Nestler/Schiffner,* Anm. zu BGH NStZ 2022, 35, 38.

76 Nach *Ebbinghaus* differenziert der BGH zwischen der Vereinigung, die das Hawala System betreibt und dem Hawala System selbst. Somit sei der gemeinsam verfolgte Zweck nicht der Selbsterhalt der Vereinigung, sondern der Erhalt des (davon zu unterscheidendem) Hawala-Netzwerks. Auch nach diesem Verständnis bleibt die Entscheidung kritikwürdig, da der BGH es versäumt, die Frage zu beantworten, warum das Hawala System erhalten bleiben solle: reine Gewinnerzielungsabsicht oder ein darüberhinausgehendes Interesse, vgl. *Ebbinghaus* HRRS 1/2023 16, 19, insb. Fn. 42 m.w.N.

77 BGH 3 StR 403/20, HRRS 2022 Nr. 905: Rn.13 nennt Erhalt des Hawala Systems als gemeinsam verfolgten Zweck. Aber in Rn.15 führt BGH nun aus, dass es auch einen altruistischen Zweck gebe, welcher ebenfalls unterstützend heranzuziehen sei.

Dies gilt auch dann, wenn der Zusammenschluss vorgibt, nur wirtschaftliche Zwecke zu verfolgen. Ob die Organisationsstruktur bei Gruppen wie LockBit jedoch über das Maß hinausgeht, dass zur persönlichen Bereicherung der Beteiligten erforderlich ist, ist äußerst fraglich. Somit spricht nachdem bisher Ausgeführtem viel dafür, dass nach der deutschen Rechtslage es sich bei LockBit um Fälle der bandenmäßigen Erpressung oder des bandenmäßigen Betruges handeln würde (soweit es LockBit z.B. nicht möglich ist, die gehackten Daten ins Internet zu stellen), nicht jedoch um eine kriminelle Vereinigung, die u.a. auf Erpressung und Betrug ausgerichtet ist. Denn der gemeinsam verfolgte Zweck, bleibt, sowohl nach Willen des Gesetzgebers als auch nach der Rechtsprechung und herrschenden Meinung, das zentrale Element, um eine Abgrenzung von Bande und krimineller Vereinigung zu ermöglichen.[78]

Dennoch ist nicht völlig ausgeschlossen, dass der BGH, unter Bezugnahme auf die Gesetzesmaterialien[79], auch ein Gewinn und Machtstreben als ausreichend erachtet falls sich, wie bei LockBit oder vergleichbaren Ransomware-Gruppen eine Gruppenidentität gebildet hat, mit eigenem Willensbildungsprozess und Einflussnahme auf Öffentlichkeit. Wie der nächste Abschnitt zeigen wird, ist eine derartige Aufweichung des Tatbestandes nicht erforderlich.

4.3.1.2. Die „Marke“ als Lösung

An diesen grundsätzlichen dogmatischen Zweifeln an der Anwendbarkeit des § 129 StGB auf Ransomware-Gruppierungen wie LockBit, ändert die Existenz einer ‚Marke‘ nur den ersten Blick nichts. Diese ‚Marke‘ oder die Selbstdarstellung in der Öffentlichkeit kann als eine Notwendigkeit für die erfolgreiche Erpressung interpretiert werden: Dem Opfer wird so signalisiert, dass man sich auf die Täter verlassen kann, wenn bezahlt wird, wird alles gut, andernfalls werden die angedrohten Konsequenzen auch wirklich herbeigeführt.

Aber gerade diese Aufmerksamkeit in der Öffentlichkeit führt zu massiven Zahlungserschwerungen, durch internationale Sanktionen, gerade durch das US-amerikanischen Department of Justice, sodass sich ein offen-

78 BGH wistra 2021, 441, 444; BGH, Urteil vom 22. Mai 2019 – 2 StR 353/18 –, juris Rn. 33.

79 BT DS 18/11275, 11.

sives mediales Auftreten nicht allein aus finanziellen Gesichtspunkten erklären lässt. Daher ist es ist naheliegend, dass es auch um Aufmerksamkeit um ihrer selbst willen geht, gerade bei LockBit und dessen ‚Sprecher' LockBitSup[80] nach außen hin. So gesehen erklärt sich einerseits das Bedürfnis, unter einem bestimmten Namen in der Öffentlichkeit aufzutreten, welches es bei rein geheimdienstlichen Akteuren nicht gibt,[81] andererseits auch, dass die Namen selten gewechselt werden, nach zu aufsehenerregenden Taten.[82] Doch wird auch im Fall von internationalen Sanktionen an dem Bedürfnis, unter einer Marke aufzutreten, nicht aufgegeben. Somit lässt sich auch bei Zusammenschlüssen, die wie LockBit in ihrer Selbstdarstellung nur nach finanziellem Gewinn streben, ein gemeinsam verfolgtes Interesse in dem Bedürfnis nach Aufmerksamkeit sehen.

Freilich könnte man dies auch anders interpretieren: Die Aufmerksamkeit, auch wenn sie den unmittelbaren finanziellen Interessen eher schadet, dient (auch) der Rekrutierung von Talent, insb. Programmierern, LockBit veranstaltete im Juni 2020 ein Preisausschreiben für wissenschaftliche Aufsätze mit neuen Strategien für den Einsatz von Ransomware,[83] Probleme hier (insbesondere bei der Entwicklung der neusten LockBit Version), sollen, zusammen mit Ermittlungserfolgen, maßgeblich zu dem jüngsten Bedeutungsverlust von LockBit geführt haben.[84] Doch erfolgt die Rekrutierung über Darknet Foren, der mediale Auftritt außerhalb hiervon ist überzeugender mit einem Geltungsdrang zu erklären, als mit einer rein wirtschaftlichen Zweckverfolgung.

4.3.2. Nordkoreanische Gruppierungen

Gruppierungen aus Nordkorea (wie zB Lazarus) bezwecken in aller erster Linie die Beschaffung von finanziellen Mitteln für den international (nicht

80 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).
81 Namen wie Lazarus für nordkoreanische Hacker-Gruppierungen sind von Sicherheitsunternehmen oder staatlichen Stellen vergeben worden.
82 Häufiger nach betrügerischem Umgang mit Affiliates: https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023), in Bezug auf REvil.
83 https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).
84 https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/ (abgerufen am 27.08.2023).

mehr ganz so) isolierten Staat.[85] Der erste aufsehenerregende flächendeckende Ransomware-Angriff, WannaCry, soll von staatlichen nordkoreanischen Hackern (Lazarus) begangen worden sein.[86] Hier lässt sich das Bestehen einer kriminellen Vereinigung unproblematisch bejahen, da die Mittel dem Staat zugutekommen sollen, für den die Hacker arbeiten.[87] Somit scheint die persönliche Bereicherung der Mitglieder nicht das gemeinsame Interesse des Zusammenschlusses zu sein. Nordkoreanische Hacker sind im Bereich der Ransomware-Gruppierungen weniger stark präsent, traten jüngst als Affiliates auf.[88] Auch frei verfügbare Ransomware wie MAUI wird von nordkoreanischen Einheiten wie APT45 wohl nach wie vor eingesetzt,[89] wenngleich die öffentliche Aufmerksamkeit und die öffentlich bekannten Fallzahlen sind als bei russischsprachigen Ransomware-Gruppierungen.

Nordkoreanische Hackergruppen sind organisatorisch wohl entweder Teil des General Staff Department des Militärs oder des Reconnaissance General Bureau (RGB), erstere ist überwiegend in Sabotage und Informationsbeschaffung, letztere in illegaler Mittelbeschaffung durch Cyberkriminalität tätig,[90] öffentlich verfügbare Informationen sind hier spärlich. Im Bereich der illegalen Mittelbeschaffung ist der Cyberangriff auf die Bangladesch Central Bank am 4.2.2016 erwähnenswert: 10 Monate im System, um Abläufe kennen zu lernen, dann erfolgten Kontoabbuchungen über das

85 Oder auch um Cyberspionage zu finanzieren, vgl. https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage?hl=en (abgerufen am 31.03.2025).

86 https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/;.s.o. Ausnutzung einer von der NSA entdeckten Schwachstelle (Tool, dass diese ausnutzte: EternalBlue) in Windows, welche die NSA aber geheim hielt, um diese Schwachstelle selbst ausnutzen zu können. Hacker(n) unter dem Namen ShadowBroker gelang es, dieses Tool zu stehlen, veröffentlichten es online. Anschließend wurde es für WannaCry von nordkoreanischen Hackern ausgenutzt und verbessert https://www.bleepingcomputer.com/news/security/one-year-after-wannacry-eternalblue-exploit-is-bigger-than-ever/; *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021.

87 *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021.

88 https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-now-deploying-qilin-ransomware/ (abgerufen am 23.03.2025).

89 https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine?hl=en (abgerufen am 31.03.25).

90 *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021; *Couretas*, Cyber Operations, 2024, S. 122f., demnach RGB dem GSD der Armee untergeordnet sei, iVa Mandiant.

SWIFT System bei Federal Reserve am 4.2.2016, iHv fast 1 Mrd. US-$, wenngleich aufgrund eines Zufalls nicht der vollständige Betrag transferiert wurde.[91] Bei der Infiltration der IT Systeme lukrativer Ziele wird raffiniert vorgegangen, beim Lesen der Vorgänge kann man sich einer gewissen Paranoia nicht erwehren.[92]

4.3.3. Chinesische Gruppierungen

Chinesische Gruppierungen sind im Bereich des Ransomware-Geschäfts eher seltener vertreten – hier scheint Wirtschafsspionage sowie die Vorbereitung eventueller Sabotageakte im Krisenfall im Vordergrund zu stehen, genau wie die mit dem russischen SVR in Verbindung gebrachte Gruppierungen sind chinesische Akteure eher advanced persistend threats (APT)[93]. Auch hier handelt es sich um semi-staatliche Akteure, vergleichbar mit den staatlichen Akteuren Nordkoreas. Informationen sind hier sogar für Mutmaßungen zu spärlich.

5. Fazit und Ausblick

Cyberkriminalität ist gut organisiert. Ein maßgeblicher Grund hierfür ist das Problem der Durchsetzung des staatlichen Strafanspruchs und -interesses,[94] da Landesgrenzen von Tätern überschritten werden: In Land A wird agiert, Taten werden aber zu Lasten von Land B begangen, mit

91 *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021, erfolgreich iHv 101 Mio US$; dies war kein Ransomware-Angriff, ausgeführt von BeagleBoyz/Bluenoroff, welche Teil von Lazarus seien, die wiederum eine Abteilung des RGB seien; *Couretas*, Cyber Operations, 2024, S. 124.

92 Lesenswert: *Caesar*, The Incredible Rise of North Korea's Hacking Army, NewYorker, 19.04.2021: Vorspielen eines Bewerbungsverfahren bei einem existierenden Unternehmen, einschließlich Videokonferenz-Interview mit Bewerber und Schauspieler, der dem CIO des Unternehmens ähnelte (& vorgab, dieser zu sein), um das Opfer dazu zu bringen, anschließend eine infizierte PDF Datei zu öffnen.

93 Nationalstate Ransomware S. 19; *Couretas*, Cyber Operations, 2024, S. 105f.

94 Sowie des staatlichen Gewaltmonopols allgemein: Siehe hierzu den folgenden Vorfall (eher ein Gerücht): LockBit führte einen Ransomware-Angriff gegen entrust.com aus, drohte mit der Veröffentlichung interner Daten. Daraufhin erfolgte ein DDoS-Angriff auf die von LockBit zur Veröffentlichung der Daten ihrer Opfer genutzten Server, mit der Nachricht: „DELETE_ENTRUSTCOM_MOTHERFUCKERS"; Quelle: https://analyst1.com/ransomware-diaries-volume-1/ (abgerufen am 27.08.2023).

dem Land A keine engen Beziehungen unterhält. Daher ist es für die Strafverfolgungsbehörden von Land A keine große Priorität, den Aktivitäten Einhalt zu gebieten. Dies ermöglicht festere hierarchische Strukturen, da der Verfolgungsdruck geringer ist. Bei Entdeckung werden die Täter wohl nicht selten von den nationalen Geheimdiensten rekrutiert, um dann zum Erreichen politischer Ziele weiter zu agieren. Die Anwendung von § 129 StGB auf Ransomware-Gruppierungen erscheint auf den ersten Blick sehr naheliegend, doch wie gezeigt wurde, steht schon die Subsumtion vor einem erheblichen Begründungsaufwand. Auf der Grundlage öffentlich bekannter Informationen sind ideologische Ransomware-Gruppen, wie die nordkoreanische Lazarus Gruppe, die sogar in den staatlichen Militärapparat integriert ist, unproblematisch erfasst. Auch bei halbstaatlichen Gruppierungen wie EvilCorp spricht viel für die Bejahung einer kriminellen Vereinigung i.S.v. § 129 StGB. Organisationen wie LockBit propagieren eine reine Gewinnerzielungsabsicht. Die ausgeprägten Organisationsstrukturen können hier kein Indiz für ein gemeinsames Interesse darstellen, da sie notwendig sind für die Gewinnerzielung. Nur wenn der Grad an Organisation über das dafür erforderliche Maß hinausgeht, beziehungsweise nicht allein mit der Gewinnerzielungsabsicht erklären lässt, taugt es als Indiz für ein darüberhinausgehendes gemeinsames Interesse.

Doch zeigt das Auftreten in der Öffentlichkeit, dass es den Beteiligten maßgeblich auch um die Selbstdarstellung geht – in einem Umfang, wie es nicht allein für die Gewinnerzielung erforderlich zu sein scheint. Dies ist unserer Meinung nach ein entscheidendes Argument, mit dem auch nach dem ‚klassischen' (aber nach wie vor gültigen) Vereinigungsbegriff eine kriminelle Vereinigung bejaht werden kann. Dies ist natürlich aus öffentlich bekannten Informationen schwer einzuschätzen, aber bereits aus diesem begrenzten Fundus an Wissen zeigt sich, dass der BGH seine Rechtsprechung zur kriminellen Vereinigung nicht aufgeben müsste, wenn irgendwann einmal die faktischen Hindernisse, die einem Verfahren entgegenstehen, überwunden werden sollten.

Regulierung der Datenlöschung im europäischen Datenschutzrecht

Dominik Schmelz

I. Einleitung

Der Datenschutz stellt ein fundamentales Recht dar, das in der heutigen digitalen Ära von entscheidender Relevanz ist, da die Menge der erfassten Daten sowie die Rechenleistung kontinuierlich zunehmen und somit eine parallele Verarbeitung ermöglichen. Es lässt sich feststellen, dass der Partei, welche über mehr Informationen bezüglich einer anderen Partei verfügt, im Allgemeinen eine Machtposition innewohnt. Das Machtverhältnis ist in dieser Hinsicht als stark unausgewogen zu bewerten. Um eine gerechte digitale Umgebung zu schaffen, ist eine Korrektur dieses Machtungleichgewichts erforderlich. Es ist daher von essentieller Bedeutung, Personen, deren Daten verarbeitet werden, vor den potenziellen Risiken zu schützen oder sie zumindest transparent zu machen.

Insbesondere die Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679, legt großen Wert auf den Schutz personenbezogener Daten durch technische Maßnahmen, um die damit verbundenen Risiken für die Betroffenen zu minimieren. Das Recht auf Löschung personenbezogener Daten ist neben den verschiedenen Auskunftsrechten der Kern der Betroffenenrechte. Kritisch betrachtet fehlen jedoch konkrete Anleitung, Methodik oder Instrumente dazu in der Norm[1] [2].

Diese Konkretisierung der Verpflichtung ist jedoch essenziell, da die durch die DSGVO angestrebte Balance zwischen Datenverarbeitern und Betroffenen nur erreicht werden kann, wenn Verpflichtungen des Datenverarbeiters, welche auf einem Vertrauen auf die korrekte Ausführung basieren, auch einer rechtlichen Verpflichtung entsprechen. Im Gegensatz zu den Auskunftsrechten ist das Löschen von Daten für den Betroffenen

1 *Kühling ea*, Datenschutz-Grundverordnung, BDSG4. Auflage, Art. 17 Rz. 17.

2 *Fritz*, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung, S. 93.

schwerer nachvollziehbar und für den Datenverarbeiter schwerer zu beweisen.

Im Zuge der fortschreitenden Digitalisierung und Datenverarbeitung kommt der Untersuchung der rechtlichen und technischen Rahmenbedingungen sowie deren Wirksamkeit zur Gewährleistung des Schutzes personenbezogener Daten eine entscheidende Bedeutung zu. Der Datenschutz durch Technikgestaltung spielt hierbei eine zentrale Rolle und ist Gegenstand intensiver rechtlicher und technischer Debatten.

Die vorliegende Untersuchung verfolgt das zentrale Ziel, die technischen, rechtlichen und nutzerbezogenen Dimensionen verschiedener Löschmechanismen im Kontext des menschenzentrierten Datenschutzes systematisch zu analysieren. Der menschenzentrierte Ansatz erweist sich hierbei als maßgeblich, da nicht die technischen Spezifikationen oder Implementierungsdetails des Systems im Vordergrund stehen, sondern vielmehr die Erwartungen der Nutzerinnen und Nutzer. Im Fokus steht somit die Frage, inwieweit bestehende technisch-juristische Löschmechanismen den Anforderungen und Bedürfnissen der betroffenen Personen entsprechen. Besondere Aufmerksamkeit gilt dabei der Identifikation möglicher Divergenzen zwischen den technischen Umsetzungsmöglichkeiten und den rechtlichen Vorgaben. Die Ergebnisse dieser Analyse sollen nicht nur dazu beitragen, potenzielle Herausforderungen aufzuzeigen, sondern auch praxisorientierte Empfehlungen für die Verbesserung des Datenschutzes zu liefern. Dabei soll insbesondere die folgende Forschungsfrage beantwortet werden:

> *Inwieweit erfüllen verschiedene juristisch-technische Löschmechanismen im menschenzentrierten Datenschutz die technischen Anforderungen, sind rechtlich konform?*

Um eine detaillierte Analyse der juristisch-technischen Löschmechanismen im Rahmen des menschenzentrierten Datenschutzes zu ermöglichen, werden folgende Unterforschungsfragen untersucht:

- Welche Löschmechanismen existieren?
- Inwieweit ist die Konformität der Löschmechanismen zur DSGVO gegeben?

Die erste Unterforschungsfrage zielt darauf ab, die technischen Spezifikationen zu identifizieren, die für die effektive Umsetzung von Löschmechanismen im Datenschutz relevant sind. Hierbei sollen insbesondere aktuelle technische Standards und Normen sowie ihre Anwendbarkeit auf verschiedene Datenkontexte analysiert werden.

Die zweite Unterforschungsfrage befasst sich mit der juristischen Konformität der vorhandenen Löschmechanismen. Es sollen Rechtsnormen, Kommentare und Urteile untersucht werden, um herauszufinden, wie verschiedene Mechanismen den Anforderungen der Datenschutzgesetze, insbesondere der DSGVO, entsprechen und ob mögliche rechtliche Interpretationen konsistent angewendet werden.

Die methodische Vorgehensweise dieser Arbeit basiert auf einem ganzheitlichen Ansatz, der sowohl rechtliche als auch technische Aspekte berücksichtigt. Es wird daher eine Kombination aus qualitativen und quantitativen Methoden der Natur- und Geisteswissenschaften angewendet, um eine umfassende Bewertung der Löschmechanismen vorzunehmen. Dabei werden rechtliche Textanalysen und technische Bewertungen durchgeführt.

Die vorliegende Arbeit ist wie folgt strukturiert: Nach der Einleitung, in der der Hintergrund, die Zielsetzung, die Forschungsfragen, die Methodik und der Aufbau der Arbeit dargelegt werden, folgt der theoretische Hintergrund. In diesem Abschnitt werden die relevanten rechtlichen Konzepte, technischen Standards und die bisherige Literatur dargestellt. Die Diskussion der Ergebnisse im Kontext der Forschungsfragen und des theoretischen Hintergrunds führt zu Schlussfolgerungen, in denen die wichtigsten Erkenntnisse zusammengefasst und praktische sowie theoretische Implikationen diskutiert werden.

Hinweis: Zur besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

II. Juristische Analyse

Die Datenschutz-Grundverordnung (DSGVO) fungiert als rechtlicher Rahmen zur Gewährleistung des Schutzes personenbezogener Daten innerhalb der Europäischen Union. Das Ziel besteht in der Gewährleistung des Schutzes der Privatsphäre sowie der Förderung des freien Datenverkehrs innerhalb des Binnenmarktes. Auf nationaler Ebene wird das österreichische Datenschutzgesetz (DSG) als Instrument eingesetzt, um spezifisch nationale Anforderungen und Gegebenheiten zu berücksichtigen.

Von besonderer Relevanz ist hierbei Art. 17 DSGVO, der das Recht auf Löschung, auch bekannt als das „Recht auf Vergessenwerden", normiert.

Diese Bestimmung wird im österreichischen Datenschutzgesetz durch § 1 Z. 3 DSG als Verfassungsbestimmung weiter konkretisiert, was ihre herausragende Bedeutung im nationalen Rechtsrahmen unterstreicht.

Eine explizite Legaldefinition des Begriffs „Löschen" ist in der DSGVO sowie dem aktuellen österreichischen DSG jedoch nicht enthalten. Die fehlende Definition des Begriffs „Löschrecht" wirft wesentliche Fragen hinsichtlich der praktischen Umsetzung und der rechtlichen Implikationen auf. Die vorliegende Untersuchung widmet sich der Fragestellung, wie der Begriff des Löschens im Kontext moderner digitaler Technologien und der damit verbundenen Datenverarbeitung zu interpretieren und anzuwenden ist.

Ziel der vorliegenden Untersuchung ist die Analyse des Zwecks und der Tragweite des Rechts auf Löschung gemäß Art. 17 DSGVO sowie im Kontext des DSG. Der Fokus der Untersuchung liegt auf der teleologischen und historischen Auslegung, mit deren Hilfe der gesetzgeberische Wille und die zugrunde liegenden Ziele dieser Normen erfasst werden sollen. Ziel dieser Vorgehensweise ist es, die Anwendung der Normen in der Praxis zu erleichtern.

A. Primärquellen

Das sogenannte „Recht auf Vergessenwerden" ist als fundamentales Recht der informationellen Selbstbestimmung zu begreifen. Das in Art. 17 implementierte „Recht auf Löschung" ermöglicht die Löschung personenbezogener Daten auf Verlangen des Betroffenen oder wenn der Zweck der weiteren Aufbehaltung entfällt, wobei bestimmte Ausnahmen bestehen. Die Löschung personenbezogener Daten ist erforderlich, wenn diese für die ursprünglichen Zwecke nicht mehr erforderlich sind, die betroffene Person ihre Einwilligung widerruft (Art. 17 Abs. 1 lit. b), Widerspruch gegen die Verarbeitung einlegt (Art. 21 Abs. 1), die Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 lit. d) oder eine rechtliche Verpflichtung zur Löschung besteht (Art. 17 Abs. 1 lit. e).

Sofern die Löschung aufgrund der Komplexität der Anfrage länger als einen Monat in Anspruch nimmt, ist der Verantwortliche dazu verpflichtet, den Betroffenen darüber in Kenntnis zu setzen (Art. 12 Abs. 3).

Im Falle veröffentlichter Daten ist es die Pflicht des Verantwortlichen, unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, einschließlich technischer Maß-

nahmen, zu ergreifen, um andere Verantwortliche darüber zu informieren, dass die betroffene Person die Löschung sämtlicher Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt (Art. 17 Abs. 2). Erwägungsgrund 66 konkretisiert das Recht auf Löschung aus Art. 17 Abs. 2 der DSGVO, indem er festlegt, dass der Verantwortliche unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel angemessene Maßnahmen treffen sollte, um andere Verantwortliche, die die Daten verarbeiten, über den Löschungsantrag zu informieren. Gemäß Erwägungsgrund 65 wird das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten im Kindesalter explizit dargelegt. Es sei darauf hingewiesen, dass die betroffene Person dieses Recht insbesondere dann ausüben kann, wenn die Daten im Kindesalter erhoben wurden und eine Löschung zu einem späteren Zeitpunkt erfolgen soll.

§ 4 Z 4 DSG[3] erlaubt dem Verantwortlichen, die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO („Recht auf Einschränkung der Verarbeitung") einzuschränken, wenn die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen kann, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann. Das bedeutet, dass Daten, wenn es technisch nicht möglich ist, sie zu löschen, zeitweilig auch nur eine Einschränkung der Verarbeitung erfolgen darf.

Gemäß Art. 24 Abs. 1 verlangt der risikobasierte Ansatz vom Verantwortlichen, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen angemessene technische und organisatorische Maßnahmen zu ergreifen. Der Aufwand soll im Verhältnis zu dem Risiko (für den Betroffenen) und den Kosten der Implementierung stehen, wobei ein hohes Maß an Schutz und Datensicherheit gewährleistet sein muss (Art. 25 Abs. 1).

Gemäß Art. 32 Abs. 1 lit. b werden Verantwortliche und Auftragsverarbeiter dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Dies umfasst die Gewährleistung der Vertraulichkeit, Inte-

3 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), Fassung vom 29.06.2024, Art. 2 §4.

grität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Die Vertraulichkeit ist im Hinblick der Löschung wichtig, denn sie stellt sicher, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben und dass diese Daten vor unbefugter Offenlegung geschützt sind. Die Integrität gewährleistet, dass die Daten korrekt und unverändert bleiben, indem Maßnahmen ergriffen werden, um unbefugte Änderungen zu verhindern, so zum Beispiel durch eine partielle Löschung. Verfügbarkeit bedeutet, dass personenbezogene Daten bei Bedarf zur Verfügung stehen und nicht unbefugt blockiert oder gelöscht werden können. Die Belastbarkeit bezieht sich auf die Fähigkeit des Systems, einem Angriff oder einer Störung standzuhalten und seine Funktionen auch unter widrigen Bedingungen aufrechtzuerhalten. Die Überlastung eines Systems darf also auch nicht zu einem Verlust von Daten führen.

Art. 25 Abs. 1 schreibt vor, dass Verantwortliche und Auftragsverarbeiter bereits bei der Planung von Verarbeitungsvorgängen technische und organisatorische Maßnahmen, unter Berücksichtigung der Risiken für die Betroffenen und der Implementierungskosten, ergreifen müssen, um die Datenschutzgrundsätze zu gewährleisten. Dabei sind insbesondere die Prinzipien „Datenschutz durch Technikgestaltung" bzw. „Datenschutz durch datenschutzfreundliche Voreinstellungen" zu berücksichtigen[4]. Die Implementierung solcher Maßnahmen von Beginn an ermöglicht eine effektive Umsetzung des Datenschutzes und trägt dazu bei, Datenschutzverletzungen zu verhindern. „Datenschutz durch Technikgestaltung" bezieht sich auf die systematische Integration von Datenschutzprinzipien in die Entwicklung von Produkten, Systemen und Prozessen von deren Anfangsphase an. Datenschutz durch datenschutzfreundliche Voreinstellungen[5] bedeutet, dass standardmäßig die höchstmöglichen Datenschutzeinstellungen angewendet werden sollen, ohne dass der Benutzer aktiv eingreifen muss.

Es sei darauf hingewiesen, dass Löschkonzepte, die mitunter in der Praxis Anwendung finden, nicht unmittelbar aus der DSGVO resultieren. Gemäß Art. 5 Abs. 1 unterliegt die Verarbeitung personenbezogener Daten dem Grundsatz der Speicherbegrenzung. Das Löschkonzept fungiert in diesem Zusammenhang als Instrument, um dieser Verpflichtung systema-

4 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), OJ L 2016/119 [DSGVO], ErwG 78.

5 ebd, Art. 25 Abs. 1.

tisch, risikoorientiert und dokumentierbar nachzukommen und eben zu dokumentieren, wann und wie gelöscht wird. Diese Verpflichtung ergibt sich aus dem Prinzip der Rechenschaftspflicht nach Art. 5 Abs. 2, wonach der Verantwortliche die Einhaltung aller Grundsätze der Datenverarbeitung nachweisen muss.

Die Bestimmungen der Artikel 32 und 25 sowie die entsprechenden Erwägungsgründe verdeutlichen die Relevanz adäquater technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten. Diese Maßnahmen sind von entscheidender Relevanz für die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten im Rahmen der Datenverarbeitung. Die nachfolgend erörterten Leitlinien des European Data Protection Board (EDPB) stellen eine zusätzliche Orientierungshilfe für die praktische Umsetzung dieser Anforderungen dar.

Art. 32 Abs. 1 fordert die Berücksichtigung des Stands der Technik bei der Implementierung von Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. In Bezug auf das Löschen von Daten bedeutet Stand der Technik, dass Verantwortliche aktuelle Technologien und Verfahren einsetzen sollen, um die sichere und vollständige Löschung personenbezogener Daten zu gewährleisten. Diese müssen laut Abs. 1 lit. d regelmäßig geprüft und ggf. nachgebessert werden. In seinem Kommentar erörtert Piltz, dass gemäß Art. 32 Abs. 1 DSGVO der „Stand der Technik" eine autonome und einheitliche Interpretation innerhalb der EU erfordert, die unabhängig von nationalen Gesetzen ist. Die exakte Bedeutung des Terminus „Stand der Technik" bleibt indes unklar, insbesondere, ob dieser neueste technologische Entwicklungen einschließt oder ob branchenübliche Standards ausreichen. Die Argumentation fußt auf der Prämisse, dass es sich höchstwahrscheinlich nicht um den höchstmöglichen Technologiestandard handelt, da der EuGH diesen nur bei Verwendung des Begriffs „Stand der Wissenschaft und Technik" annimmt.

Piltz meint, es seien „Empfehlungen staatlicher Stellen zu berücksichtigen wie etwa die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI)"[6]. Und die „enge Einbindung des BSI in den gesamten Verfahrensablauf beim Ausbau und Betrieb der IT kann die durch Art. 32 Abs. 1 angeordnete Berücksichtigung des Stands der Technik

6 *Piltz* in Datenschutz-Grundverordnung: VO (EU) 2016/679: Bundesdatenschutzgesetz: Kommentar, Art. 32 Rz. 19.

sichern“[7]. Einer der Löschstandards des BSI wird in Abschnitt III.F „BSI Grundschutz CON.6„ beschrieben.

B. Kommentare und Leitlinien

Die rechtlichen Rahmenbedingungen für die Löschung personenbezogener Daten gemäß der DSGVO erfahren durch nationale Entscheidungen eine Präzisierung. Artikel 17 und 12 der DSGVO geben keine spezifischen Methoden für die Löschung vor. Die Kommentare zum Art. 17 fokussieren sich primär auf die Voraussetzungen und Ausnahmen der Löschverpflichtung. In einigen Fällen erfolgt eine detaillierte Auseinandersetzung mit spezifischen Zeiträumen und Benachrichtigungen. Eine Diskussion über die Modalitäten der Löschung ist eine Seltenheit.

Die österreichische Datenschutzbehörde (DSB) stellt fest, dass die Löschung erreicht ist, wenn „die Verarbeitung und Nutzung der personenbezogenen Daten einer betroffenen Person [...] nicht mehr möglich ist“[8]. Dies beinhaltet sowohl physische als auch digitale Daten, wie vom OGH bestätigt wird[9]. Bei der Anonymisierung als eine zulässige Löschmethode muss „sichergestellt werden, dass weder der Verantwortliche selbst noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann“[10]. Des Weiteren wurde von der DSB entschieden, dass eine zeitweilige Löschung ausreicht, also, dass die Möglichkeit einer Rekonstruktion der Daten zu einem späteren Zeitpunkt, mit besseren technischen Möglichkeiten, nicht ausreicht, um keine Löschung durch Anonymisierung darzustellen[11]. Darüber hinaus wurde dies im selbigen Bescheid verallgemeinert beschrieben, dass generell keine „völlige Irreversibilität“[12], was einer Vernichtung der Daten nahekommt, gefordert ist. Knyrim sieht auch diese Irreversibilität nicht als notwendig, definiert aber die „physische Löschung“ neben der Anonymisierung als Löschung, sodass „Daten unter

7 ebd, Art. 32 Rz. 19.
8 Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018, *DSB-D123.270/0009-DSB/2018*.
9 *Fritz*, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung.
10 ebd.
11 Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018, *DSB-D123.270/0009-DSB/2018*.
12 ebd.

Anwendung üblicher Verfahren nicht mehr ausgelesen werden können“[13]. Des Weiteren wird von Knyrim definiert, dass physische Medien durch Zerstörung des Datenträgers vernichtet werden.

Der Terminus „Vernichtung“ von Daten im Sinne des Art. 4 Abs. 12 zur Definition der „Verletzung des Schutzes personenbezogener Daten“ bzw. eines Data Breaches wurde von der EDPB frei aus dem Englischen übersetzt als „wenn die Daten nicht mehr existieren oder nicht mehr in einer Form vorliegen, die für den für die Verarbeitung Verantwortlichen von Nutzen ist“[14] definiert. Abbildung 1 stellt die verschiedenen Begriffe in Relation zum Grad des Personenzuges dar.

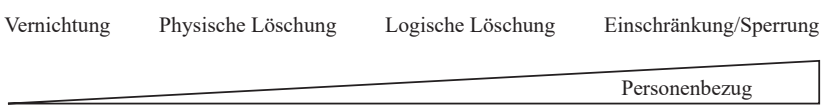

Abbildung 1 – Grade des Personenbezugs von Löschmaßnahmen

Zur Fragestellung der örtlichen Begrenzung beschäftigen sich Feiler und Forgo mit der Löschung aus Suchmaschinen und kommen in Referenz auf C-507/17 zum Schluss, dass es „kein Recht auf globale Löschung“ gibt, also eine Sperre des Datenzugriffs aus dem EWR ausreichend ist und dass generell eine Reduzierung der Verarbeitungstätigkeit auf ein Maß, dass die DSGVO nicht mehr Anwendung findet, einer Löschung nach DSGVO gleichkommt[15]. Knyrim differenziert das „Verarbeitungsverbot“ bzw die „Einschränkung“ auch zur Löschung, welches durch einen „Sperrvermerk bewerkstelligt werden“[16] kann. Er setzt dieses mit der „logischen Löschung“ gleich[17]. Kamann und Braun argumentieren, dass aus Art. 17 DSGVO, welcher beschreibt, dass der Betroffene die Löschung seiner personenbezogenen Daten verlangen kann, folgt, dass die betroffene Person den Umfang ihres Löschverlangens selbst bestimmen darf, wie etwa durch die Beschrän-

13 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 17 Rz. 63.
14 *EDPB*, Guidelines 9/2022 on personal data breach notification under GDPR Guidelines 9/2022: Data Breaches.
15 *Feiler/Forgó*, EU-DSGVO und DSG2. Auflage, Rz. 7.
16 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 17 Rz. 63.
17 ebd, Art. 4 Rz. 42.

kung auf bestimmte Daten, Datenkategorien, Verarbeitungsformen, Zwecke oder Teilverarbeitungsvorgänge[18].

Rechtlich ist eine geographische Einschränkung als Äquivalenz zur Löschung im örtlichen Anwendungsbereich nachvollziehbar, aber wegen der Tatsache, dass die Daten wiederum nicht unwiderruflich gelöscht sind, kann aus einer technischen Sicht, nur von einer „Einschränkung" ausgegangen werden, denn die Daten sind, zum Beispiel bei der Verwendung einer nicht Europäischen IP-Adresse wiederum öffentlich zugänglich. Das bedeutet, dass die Maßnahme nicht nur theoretisch, sondern auch leicht praktisch durch einen Laien aufgehoben werden kann. Knyrim beschreibt dieses Verfahren genauso als einen Spezialfall des Löschens und bezeichnet es als „delisting" [19] in Referenz auf C-131/12. Welches Verfahren zur Löschung verwendet wird, und damit wie sicher diese Löschung ist, kann laut Fritz nicht durch den Betroffenen verlangt werden. Er stellt klar, dass „kein Wahlrecht der Betroffenen hinsichtlich der Löschungsmethode besteht"[20]. Die EDPB formuliert den Begriff des „Rechts auf Auslistung" in ihrer Leitlinie 5/2019[21] zu dem Thema auf Basis des selbigen Urteils. Sie halten fest, dass Löschanträge, in diesem Fall „Auslistungsanträge" laut der Meinung des EDPB „nicht zur vollständigen Löschung der personenbezogenen Daten" führen, sondern eben nur eine Zugriffbeschränkung, sodass bei einer Suche nach einem Namen diese Ergebnisse nicht mehr gefunden werden, aber jegliche technische Speicherung der Daten (Index, Cache etc.) weiter erhalten bleibt, mit Ausnahmen wie zum Beispiel, dass der indizierte Webseitenbetreiber das indizieren der betroffenen Seite fortan verbietet. Dies wird über eine Datei „robots.txt" auf der Webseite automatisiert kundgetan. Neben weiteren Ausnahmen, bei denen die Löschung sofort passieren muss, werden auch Ausnahmen zur Behaltung der Daten formuliert, wie das Recht auf freie Meinungsäußerung.

Stellungnahmen und Empfehlungen, wie beispielsweise die Leitlinie 4/2019 des European Data Protection Board (EDPB), bieten praktische Hil-

18 *Braun/Kamann* in DS-GVO: Datenschutz-Grundverordnung: Kommentar, Art. 17 Rn. 72.

19 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 17 Rz. 63/1.

20 *Fritz*, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung.

21 *EDPB*, Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO Leitlinien 5/2019 zum Recht auf Auslistung.

fe für die technische Umsetzung der Datenschutzanforderungen gemäß der DSGVO[22]. Die Leitlinien 4/2019 des EDPB zu Art. 25 DSGVO bieten eine detaillierte Analyse und praktische Anleitungen für die Umsetzung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Sie umfasst die Pflicht des Verantwortlichen zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 25 Abs. 1 sowie die Verarbeitung nur erforderlicher personenbezogener Daten gemäß Art. 25 Abs. 2. Die Leitlinien behandeln verschiedene Aspekte, darunter Transparenz, Rechtmäßigkeit, Datenminimierung, Integrität, Vertraulichkeit und Rechenschaftspflicht.

Die technisch-organisatorischen Maßnahmen, inklusive dem dokumentierten Löschkonzept und damit den inkludierten Löschmechanismen müssen laut Art. 32 Abs. 1 lit. d regelmäßig überprüft werden. Zudem enthält sie Empfehlungen zur Zertifizierung nach Art. 25 Abs. 3 und Hinweise zur Durchsetzung von Art. 25 sowie deren Auswirkungen und Art. 32 Abs. 3 ähnlich lautende Empfehlungen zur Zertifizierung. Daher sind Verfahren und technische Normen wie in Kapitel III beschrieben, die in Zertifizierungen Anwendung finden, sinnvoll bei der Implementierung dieser Konzepte zu beachten.

C. Entscheidungen

In Fällen von besonderer Relevanz hinsichtlich der Vertraulichkeit sowie der Datenlöschung im Kontext der DSGVO bzw. der des DSG wurden wegweisende Entscheidungen durch den Europäischen Gerichtshof (EuGH), den österreichischen Obersten Gerichtshof (OGH) und die österreichische Datenschutzbehörde (DSB) getroffen.

Im Fall vom 15. April 2010 6Ob41/10p[23] entschied der OGH, dass eine „logische Löschung" nicht ausreicht und die Daten physisch gelöscht werden müssen, um eine Rekonstruktion unmöglich zu machen. Diese Entscheidung unterstreicht die Notwendigkeit einer irreversiblen Datenlöschung, um den Anforderungen des DSG 2000 zu entsprechen. In diesem Urteil wird die „logische Löschung" als „eine Maßnahme, mit der erreicht wird, dass Daten innerhalb der EDV-Anlage nicht mehr zur Verfügung

22 *EDPB*, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Leitlinien 4/2019 zu Artikel 25.

23 Oberster Gerichtshof 15.04.2010, 6Ob41/10p, *6Ob41/10p*.

stehen, unkenntlich gemacht werden sowie durch das Betriebssystem als nicht mehr vorhanden interpretiert werden“[24] definiert. Es wird klargestellt, dass ein rein logisches Löschen nicht ausreicht, um den Anforderungen von „Löschen“ zu genügen. Des Weiteren wird der Begriff „Sperre“ in Anlehnung an § 3 des Pre-DSGVO BDSG als „das Kennzeichnen gespeicherter personenbezogener Daten […], um ihre weitere Verarbeitung oder Nutzung einzuschränken“[25] definiert und klargestellt, dass auch diese nicht den Anforderungen von „Löschen“ zu genügen. Einzig das von der Vorinstanz bereits geurteilte „physische Löschen“ sei als „Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist“[26], ausreichend. Des Weiteren wird festgestellt, dass die historische Interpretation, dass die Entfernung der Definition bei der Reformation des DSG 1978 zum DSG 2000 nicht bedeute, dass Löschen so interpretiert werden solle, dass der Betroffene schlechter gestellt werde.

Am 13. September 2012 bestätigte der OGH in einem weiteren Fall 6Ob107/12x[27], dass Daten aus einer Wirtschaftsdatenbank ebenfalls physisch gelöscht werden müssen, wenn der Betroffene dies fordert. Diese Entscheidung verdeutlicht die strikte Anwendung des physischen Löschens gegenüber bloßem Sperren der Daten, um den Datenschutz vollständig zu gewährleisten.

In einem Bescheid vom 5. Dezember 2018, DSB-D123.270/0009-DSB/2018[28] entschied die DSB, dass auch die Anonymisierung, also die Entfernung des Personenbezugs, als Löschung gelten kann. Dies bietet eine praktikable Alternative zur physischen Löschung, solange die Daten nicht mehr einer bestimmten Person zugeordnet werden können.

Zur „delisting“ Diskussion entschied der EuGH im Fall vom 8. Dezember 2022, Rechtssache C-460/20[29], dass ein Suchmaschinenbetreiber Links zu Inhalten mit offensichtlich unrichtigen Angaben auf Antrag der betroffenen Person aus der Ergebnisliste entfernen muss, ohne dass zuvor ein gerichtliches Verfahren gegen den Inhalteanbieter erforderlich ist. Die Löschung betrifft ausschließlich die De-Indexierung der Links und Vorschau-

24 ebd.
25 ebd.
26 ebd.
27 Oberster Gerichtshof 13.09.2012, 6Ob107/12x, *6Ob107/12x*.
28 Datenschutzbehörde 13.12.2018, DSB-D122.995/0003-DSB/2018, *DSB-D122.995/0003-DSB/2018*.
29 Europäischer Gerichtshof Rechtssache C-460/20, *TU und RE gegen Google LLC*.

bilder durch die Suchmaschine; eine Entfernung der Inhalte selbst ist nicht erforderlich.

Im Fall vom 13. Mai 2014, C-131/12[30], entschied der EuGH, dass Personen von Suchmaschinenbetreibern wie Google die Löschung von Links zu rechtmäßig veröffentlichten Informationen verlangen können, wenn diese bei Namenssuche erscheinen und ihre Grundrechte – insbesondere auf Datenschutz und Privatsphäre – verletzen. Dieses „Recht auf Vergessenwerden" gilt auch dann, wenn die Originalinformationen online bleiben und unabhängig von einem vorherigen Antrag an die Website selbst.

Im Fall vom 27. Oktober 2022, C-129/21[31] entschied der EuGH, dass ein Antrag eines Teilnehmers, seine personenbezogenen Daten aus öffentlich zugänglichen Teilnehmerverzeichnissen entfernen zu lassen, als Ausübung des Rechts auf Löschung gemäß Art. 17 DSGVO zu werten ist. Der Widerruf einer zuvor erteilten Einwilligung zur Veröffentlichung dieser Daten verpflichtet den Verantwortlichen zur unverzüglichen Löschung, sofern keine andere Rechtsgrundlage besteht (Art. 17 Abs. 1 lit. b DSGVO). Die Art der Umsetzung, wie etwa durch technische Maßnahmen oder die Änderung eines internen Kennungscodes, steht der rechtlichen Bewertung als „Löschung" nicht entgegen, sofern der Zugang zu den Daten faktisch beendet wird.

Im Bescheid der Datenschutzbehörde vom 13. Dezember 2018, DSB-D122.995/0003-DSB/2018[32] wurde entschieden, dass der Verantwortliche verpflichtet ist, die personenbezogenen Daten des Beschwerdeführers entweder zu löschen oder zu anonymisieren, wenn eine längere Speicherung als die gesetzlich erlaubte Frist erfolgt ist. Die DSB betont, dass die Anonymisierung als Löschmethode akzeptiert wird, solange der Personenbezug nicht ohne unverhältnismäßigen Aufwand wiederhergestellt werden kann. Die Einhaltung der Speicherfristen und die unverzügliche Umsetzung der Löschung oder Anonymisierung innerhalb von zwei Wochen wurden besonders hervorgehoben.

Im Urteil T-557/20[33] des EuGH wird die Pseudonymisierung, welche bisher als Datenschutzmaßnahme, jedoch nicht als Ausnahme von der

30 *Google Spain SL und Google Inc gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*, No. Rechtssache C-131/12.

31 EuGH Rechtssache C-129/21, *Proximus NV gegen Gegevensbeschermingsautoriteit*.

32 Datenschutzbehörde 13.12.2018, DSB-D122.995/0003-DSB/2018, *DSB-D122.995/0003-DSB/2018*.

33 EuGH Rechtssache T-557/20, *Einheitlicher Abwicklungsausschuss gegen Europäischer Datenschutzbeauftragter*.

DSGVO galt, relativiert. Bisher waren lediglich anonyme Daten von der DSGVO ausgenommen und die Lehrmeinung, ob ein relativistischer Ansatz oder ein absoluter Ansatz bei der Pseudonymisierung anzuwenden ist, unklar[34]. Der relativistische Ansatz behauptet, dass es bei der Beurteilung des Personenzuges von vermeintlich personenbezogenen Daten für eine Partei ausreiche, die durch diese Partei zugreifbaren Daten in Betracht zu ziehen, im Gegensatz zum absoluten Ansatz, bei dem alle generell verfügbaren, also auch jene Daten bei Dritten, in Betracht gezogen werden müssen. Das Urteil T-557/20 stützt sich auf ein Urteil von 2016 C-582/14[35], in welchem IP-Adressen als personenbezogenes Datum angesehen wurden. Dort wurde aber auch festgehalten, dass die Möglichkeit bestände, dass der Verantwortliche legalen Zugriff auf die anonymisierenden Daten hätte, nämlich die Zuordnung der dynamischen IP-Adresse zu einer natürlichen Person bzw. deren Haushalt. Oft wird dieses Urteil missverstanden und eben IP-Adressen als generell personenbezogen interpretiert, also faktisch das Gegenteil, nämlich der absolute Ansatz, statt des ebendort beschriebenen relativistischen Ansatzes. Im vorliegenden aktuelleren Urteil aus 2023 T-557/20[36] wurde die damals fälschlicherweise als absoluter Ansatz interpretierte Entscheidung nun eindeutig klargestellt: Die EDSB muss, um festzustellen, ob es sich um personenbezogene Daten handelt, die Überprüfung vornehmen, ob das Unternehmen, dem die Daten zur Verfügung gestellt wurden, rechtlich befugt war, auf zusätzliche Informationen zuzugreifen, die für die Rückidentifizierung der betroffenen Personen erforderlich sind und ob dieser Zugriff auch tatsächlich durchführbar war. Daraus kann geschlossen werden, dass ein pseudonymisiertes Datum nur dann personenbezogen ist, wenn der Verantwortliche den Betroffenen rückidentifizieren könnte.

Das Urteil C-340/21[37] des EuGH erörtert aber dieses Risiko und die Fragestellung der Beweislast und Dokumentationspflicht von Unternehmen im Zusammenhang mit ihren Cybersicherheitsmaßnahmen im Kontext des Datenschutzes. Insbesondere wird betont, dass gemäß Art. 82 Abs. 1 der bloße Umstand, dass eine betroffene Person infolge eines Verstoßes gegen diese Verordnung befürchtet, dass ihre personenbezogenen Daten

34 *Piska/Bierbauer* in Blockchain Rules, Rn. 7.4.
35 EuGH Rechtssache C-582/14, *Patrick Breyer gegen Bundesrepublik Deutschland*.
36 EuGH Rechtssache T-557/20, *Einheitlicher Abwicklungsausschuss gegen Europäischer Datenschutzbeauftragter*.
37 Europäischer Gerichtshof Rechtssache C-340/21, *VB gegen Natsionalna agentsia za prihodite*.

durch Dritte missbräuchlich verwendet werden könnten, einen immateriellen Schaden im Sinne dieser Bestimmung darstellen kann. Damit wird die Befürchtung, welche unter Aussetzung des Risikos einhergeht, als Schaden anerkannt. Das in dem Urteil beschriebene Risiko ist wohlgemerkt nicht aus einem Löschvorgang herleitbar, sondern beruht auf einer unbefugten Offenlegung nach einem Cyberangriff. Dennoch ist das sichere Löschen eine Maßnahme zur dort verletzten Vertraulichkeit (Art. 5 Abs. 1 DSGVO), weil etwaige unbefugte nach einem unsicheren Löschen Zugriff auf die Daten erhalten könnten, ähnlich der beschriebenen unbefugten Offenlegung.

Das Urteil C-687/21[38] des EuGH befasst sich mit der Frage, ob der Verantwortliche für die Verarbeitung von Gesundheitsdaten gemäß Art. 9 Abs. 2 lit. h dazu verpflichtet ist, sicherzustellen, dass kein Kollege Zugang zu diesen Daten hat, also Vertraulichkeit herzustellen. Der EuGH entschied, dass eine solche Pflicht nicht unmittelbar aus den genannten Bestimmungen hervorgeht. Jedoch könnte ein Mitgliedstaat gemäß Art. 9 Abs. 4 eine solche Regelung erlassen oder der Verantwortliche könnte gemäß den Grundsätzen der Integrität und Vertraulichkeit in Art. 5 Abs. 1 lit. f und Art. 32 Abs. 1 lit. a und b dazu verpflichtet sein.

Abschließend lässt sich feststellen, dass die Entscheidungen des EuGH, OGH und der DSB sowohl vor als auch nach Einführung der DSGVO einen signifikanten Einfluss auf die Interpretation und Anwendung des Datenschutzrechts hatten. Die frühen Entscheidungen des OGH, wie das Urteil 6Ob41/10p aus 2010 und 6Ob107/12x aus 2012, legten den Fokus auf die Notwendigkeit der physischen Löschung von Daten, um rechtlichen Anforderungen zu genügen.

Die jüngeren Entscheidungen des EuGH, wie T-557/20 und C-582/14, zeichnen jedoch ein komplexeres Bild. Während der Fall C-582/14 die Möglichkeit der Behandlung von IP-Adressen als personenbezogene Daten thematisiert, widmet sich der Fall T-557/20 der Anwendung der Pseudonymisierung und relativiert damit vorherige, restriktive Ansätze. Diese Urteile legen nahe, dass sich die Rechtsprechung von einer strikten, klaren Linie hin zu einer differenzierteren Betrachtung bewegt. Zwar ermöglicht dies eine präzisere Anpassung an die technischen Realitäten, jedoch resultieren daraus auch Unsicherheiten.

38 EuGH Rechtssache C-687/21, *BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH*.

D. Interpretation auf Basis des Normzwecks

Die teleologische Extension des Begriffs „Löschen" im Kontext der DSGVO und des DSG ist von grundlegender Bedeutung für die Auslegung und Umsetzung dieser Normen. Die DSGVO und das DSG zielen darauf ab, den Schutz personenbezogener Daten zu gewährleisten und das Recht auf Privatsphäre zu schützen. Gemäß der Rechtsprechung des Europäischen Gerichtshofs (EuGH) konstituiert das „Recht auf Vergessenwerden" eine zentrale Komponente des Datenschutzes.

Grundsätze und Prinzipien der DSGVO umfassen nach Art. 5 die Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Diese Maßnahmen dienen dazu, dass die betroffene Person Risiken einschätzen und diese selbst beeinflussen kann. Der risikobasierte Ansatz zieht sich durch die gesamte DSGVO, und ist speziell bei der Bewertung von technisch organisatorischen Maßnahmen und Datenschutz-Folgenabschätzungen[39] zu erkennen. Artikel 25 der DSGVO führt das Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ein, das darauf abzielt, Risiken für die Rechte und Freiheiten der betroffenen Personen durch geeignete technische und organisatorische Maßnahmen zu minimieren. Die Risiken für die betroffene Person sind bei der Verarbeitung personenbezogener Daten erheblich. Diese können Identitätsdiebstahl, Diskriminierung oder unberechtigte Profilbildung umfassen, wobei letztere eine Interessenabwägung benötigen[40]. Die vollständige, unwiderrufliche Löschung der Daten reduziert dieses Risiko effektiv auf null, indem sie sicherstellt, dass die Daten nicht wiederhergestellt oder für unzulässige Zwecke verwendet werden können. Jedoch berücksichtigt die DSGVO auch die Perspektive der Verantwortlichen und Auftragsverarbeiter. Es wird anerkannt, dass die Umsetzung von technisch organisatorischen Maßnahmen Ressourcen und Aufwendungen bedürfen, die bei der Auswahl der Maßnahmen Berücksichtigung finden dürfen. Das Telos der DSGVO zeigt deutlich, dass der Aufwand für die Risikobewältigung in einem angemessenen Verhältnis zu dem Risiko für die Betroffenen stehen muss[41]. Dies bedeutet, dass eine Risiko- und Aufwandsabschätzung unerlässlich ist, um

39 DSGVO, ErwG. 84.
40 *Albrecht* in Datenschutzrecht: DSGVO mit BDSG, Art. 6 Rz. 105-115.
41 DSGVO, ErwG. 84.

eine proportionale und effektive Umsetzung der Datenschutzmaßnahmen zu gewährleisten. Die Verantwortlichen sind verpflichtet, eine Risikoanalyse durchzuführen, um die potenziellen Auswirkungen der Datenverarbeitung auf die Betroffenen zu bewerten und entsprechende Maßnahmen zur Risikominderung zu ergreifen. Diese Maßnahmen sollten sowohl wirksam als auch verhältnismäßig sein, um den Aufwand der Verantwortlichen zu minimieren, ohne die Sicherheit und den Schutz der personenbezogenen Daten zu gefährden. Diese Balance zwischen Aufwand und Risikoreduzierung ist ein zentraler Bestandteil des Datenschutzkonzepts der DSGVO und spiegelt den pragmatischen Ansatz wider, den die Verordnung verfolgt.

Ein praxisnaher Ansatz zur Risiko- und Aufwandsabschätzung umfasst die Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Risiken für die Rechte und Freiheiten natürlicher Personen. Auf dieser Grundlage können Verantwortliche und Auftragsverarbeiter Maßnahmen ergreifen, die nicht nur den gesetzlichen Anforderungen entsprechen, sondern auch praktikabel und effizient in der Umsetzung sind.

Diese Prinzipien der DSGVO bilden die Grundlage für die Auslegung des Begriffs „Löschen". Zur Abgrenzung des tatsächlich vereinbaren Risikos hilft die Einordnung des Löschens als äußerste Reduktion der Vereinbarkeit der Daten. Im Spektrum dieser Betrachtung stehen die in der DSGVO verwendeten Begriffe Anonymisierung, Pseudonymisierung und indirekt- und direkt personenbezogene Daten (siehe Abbildung 2).

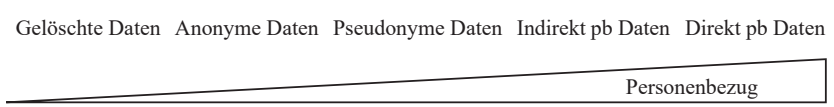

Abbildung 2 – Grade des Personenbezugs von Daten anhand DSGVO-Terminologie

Nahe zur Löschung, im Sinne des Grades des Personenbezuges, steht die Anonymisierung. Dieser Prozess, gemäß Erwägungsgrund 26 DSGVO, soll sicherstellen, dass die betroffene Person nicht identifiziert werden kann. Bei der Anonymisierung werden personenbezogene Daten so verändert, dass sie nicht mehr einer identifizierbaren natürlichen Person zugeordnet

werden können[42]. Dadurch wird ein noch hohes Maß an Datenschutz gewährleistet.

Die daraus resultierenden anonymisierten Daten unterliegen auch nicht mehr der DSGVO[43]. Dabei ist jedoch nicht jedes technische Verfahren gleich zu bewerten. Voigt und Von dem Bussche[44] unterscheiden in Referenz auf WP 216 zwei Kategorien von Anonymisierungen: Randomisierung und Verallgemeinerung. Die Randomisierung ist ein Verfahren, das die Präzision der Daten verändert, um die Reidentifizierbarkeit der betroffenen Person auszuschließen. Gemäß der vorliegenden Literatur wird unter dem Begriff der „Verallgemeinerung" die Modifikation der Merkmale von Daten verstanden, die durch eine Anpassung des Bezugspunkts oder der Granularität erfolgt. Zudem wird korrekterweise festgestellt, dass nicht jede Anonymisierungstechnik den gleichen Grad an Personenbezug entfernt. Es wird empfohlen, eine Anonymisierung anhand des Risikos zu wählen.

Im Vergleich dazu ist die Pseudonymisierung gemäß Art. 4 Abs. 5 eine Methode, bei der personenbezogene Daten ohne Zuhilfenahme zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, jedoch immer noch einem Risiko der Reidentifikation unterliegen können, wenn diese zusätzlichen Informationen zugänglich sind[45]. Pseudonymisierung wird zwar als technische und organisatorische Maßnahme (TOM) angesehen, die das Risiko für die betroffene Person reduziert, jedoch fallen die resultierenden Daten dennoch unter die DSGVO[46].

Der relativistische Ansatz (wie in den Urteilen T-557/20 und C-582/14 beschrieben), welcher davon ausgeht, dass es ausreiche, dass pseudonyme Daten aus der Sicht einer Partei anonym sein können, ohne dabei die Daten von anderen zu berücksichtigen, und damit das Risiko für den Betroffenen als vernachlässigbar bewertet, solange keine direkte Verbindung besteht, wird in der Diskussion näher behandelt.

42 *EDPB*, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Leitlinien 4/2019 zu Artikel 25, Rn. 26.
43 DSGVO, ErwG. 26.
44 *Voigt/Von Dem Bussche*, EU-Datenschutz-Grundverordnung (DSGVO), S. 16.
45 *Kühling ea*, Datenschutz-Grundverordnung, BDSG4. Auflage.
46 DSGVO, ErwG. 28.

E. Historische Analyse

Die Analyse der Änderungen im § 3 des Datenschutzgesetzes 1978 (DSG1978) zwischen den Versionen von 1980-1987[47] und 1987-1999[48] offenbart eine Erweiterung und Präzisierung der Methoden zum Löschen von Daten. In der Fassung von 1980 definiert das Gesetz das Löschen von Daten als „das Unkenntlichmachen von erfaßten oder gespeicherten Daten ohne die Möglichkeit ihrer Rekonstruktion“ [49]. Diese Definition konzentriert sich ausschließlich auf das physische Löschen, ohne spezifische Techniken zu differenzieren oder das logische Löschen zu adressieren.

Die Version von 1987 hingegen führt eine explizite Unterscheidung zwischen physischem und logischem Löschen ein. Das physische Löschen wird als „Unkenntlichmachen von Daten in der Weise, daß eine Rekonstruktion nicht möglich ist“[50] beschrieben, während das logische Löschen als „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen“[51] definiert wird (§ 3, DSG1978 Fassung 1987). Diese Differenzierung reflektiert eine Anpassung an technologische Entwicklungen und die wachsende Bedeutung von Software und digitalen Datenspeichern im Vergleich zu rein physischen Speichermedien.

Die differenzierte Betrachtung der Löschmethoden ermöglicht eine umfassendere und flexiblere Regulierung des Datenschutzes, die sowohl physische als auch digitale Realitäten abdeckt. Dieser Wandel in der Gesetzgebung kann als Reaktion auf die zunehmende Verbreitung von Computertechnologie und die Entwicklung komplexer Datenverarbeitungssysteme interpretiert werden, welche neue Risiken und Potenziale für Datenschutzverletzungen bergen.

Die im Datenschutzgesetz 1978, speziell in der Version von 1987, angeführten Bestimmungen zu den Löschmethoden von Daten, verdeutlichen eine klare und bewusste Unterscheidung zwischen physischer und logischer Löschung. Der Paragraph § 27 Z 2 konkretisiert diese Unterscheidung und stellt zudem sicher, dass die logische Löschung nur als vorübergehende

47 Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1980 01.01.1980.
48 Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1987 01.07.1987.
49 Datenschutzgesetz – DSG1978 (1980), § 3.
50 Datenschutzgesetz – DSG1978 (1987), § 3.
51 ebd, § 3.

Maßnahme dient, bis die physische Löschung unter wirtschaftlich vertretbaren Bedingungen umgesetzt werden kann.

Die in § 3 dargelegten Definitionen sowie die in § 27 Z 2 enthaltenen weiterführenden Regelungen verdeutlichen, dass der Gesetzgeber beide Löschmethoden als eigenständige und signifikante Prozesse im Kontext des Datenschutzes erachtet. Die physische Löschung wird als endgültige Maßnahme zur Datenvernichtung verstanden, bei der die Daten unwiederbringlich entfernt werden. Die logische Löschung wird als eine vorübergehende Einschränkung des Zugriffs auf die Daten definiert, bis die Bedingungen für eine physische Löschung gegeben sind.

Die temporäre Natur der logischen Löschung wird in § 27 Z 2 explizit betont, indem klargestellt wird, dass diese Methode nur bis zum nächstmöglichen, wirtschaftlich gerechtfertigten Zeitpunkt zur physischen Löschung angewendet werden darf. Diese Haltung reflektiert die Auffassung, dass die logische Löschung zwar als eine effektive Sofortmaßnahme zur Gewährleistung der Privatsphäre und des Datenschutzes erachtet wird, jedoch nicht als dauerhafte Lösung betrachtet wird. Der Gesetzgeber verdeutlicht mit dieser Regelung sein Ziel, einen dauerhaften Schutz personenbezogener Daten zu gewährleisten, der nur durch die irreversible physische Löschung der Daten erreicht werden kann.

Zusammenfassend lässt sich konstatieren, dass durch die Regelungen des DSG 1987 und insbesondere durch die spezifischen Vorgaben des § 27 Z 2 eine deutliche Unterscheidung und Hierarchisierung der Löschmethoden erfolgt. Die vorliegende Vorgehensweise berücksichtigt sowohl die technologische Entwicklung als auch die ökonomische Realität. Zudem wird ein hohes Maß an Datenschutz gewährleistet, da die logische Löschung lediglich eine temporäre Maßnahme darstellt, die bis zur Umsetzung der physischen Löschung dient.

F. Zwischenfazit

In der vorliegenden Analyse des Datenschutzes unter besonderer Berücksichtigung der Löschung personenbezogener Daten wurden verschiedenste Aspekte und deren Auswirkungen im Kontext der DSGVO und des österreichischen DSG beleuchtet.

Die Analyse der Rechtslage zur Löschung personenbezogener Daten im Lichte der DSGVO und des österreichischen DSG zeigt ein differenziertes Bild, das durch ein Spannungsverhältnis zwischen technischer Rea-

lität, rechtlicher Auslegung und normativer Offenheit geprägt ist. Eine Legaldefinition des Begriffs „Löschen" ist weder im Unionsrecht noch im nationalen Datenschutzgesetz enthalten. Diese Unbestimmtheit ist kein gesetzgeberisches Versehen, sondern Ausdruck eines bewusst gewählten Gestaltungsfreiraums für die Verantwortlichen. Der Begriff wird funktional interpretiert und ermöglicht eine an den spezifischen Gegebenheiten des Einzelfalls orientierte Auswahl geeigneter Maßnahmen, vorausgesetzt, diese genügen den datenschutzrechtlichen Zielvorgaben. Der rechtliche Rahmen wird durch die Grundsätze der Speicherbegrenzung (Art. 5 Abs. 1), der Rechenschaftspflicht (Art. 5 Abs. 2), der technischen und organisatorischen Sicherheit (Art. 32) sowie der Technikgestaltung (Art. 25) definiert.

Innerhalb dieses Rahmens ist eine Bandbreite zulässiger Löschformen anerkannt: von der physischen Datenvernichtung über softwarebasierte logische Löschung bis hin zur Anonymisierung. Dabei ist von entscheidender Relevanz, ob die Maßnahme tatsächlich und dauerhaft zur Beendigung der Verfügbarkeit personenbezogener Daten führt. Die historische Entwicklung, insbesondere die Differenzierung zwischen physischem und logischem Löschen im DSG 1987, unterstreicht, dass der österreichische Gesetzgeber bereits früh ein abgestuftes System zulässiger Löschmaßnahmen etabliert hat, wobei die logische Löschung ausdrücklich nur als temporäre Maßnahme anerkannt wurde. Die vor Inkrafttreten der DSGVO getroffenen Entscheidungen des OGH betonten daher konsequent die Notwendigkeit der physischen Unkenntlichmachung. Erst mit der Rechtsprechung des Europäischen Gerichtshofs, insbesondere der Sache T-557/20, wurde ein flexiblerer Zugriff eröffnet. Eine wirksame Anonymisierung oder auch eine risikoadjustierte Pseudonymisierung können in bestimmten Konstellationen als „Löschung" im Sinne der DSGVO angesehen werden, sofern das Risiko der Reidentifikation für den konkreten Verantwortlichen gegen null tendiert.

Diese Entwicklung darf jedoch nicht als Beliebigkeit missverstanden werden. Der weite Begriff des Löschens ist durch das Zusammenspiel von Risikoorientierung, Stand der Technik und Verhältnismäßigkeit begrenzt. Ein rechtskonformes Löschkonzept hat die Aufgabe, diesen Rahmen zu dokumentieren und eine Überprüfbarkeit zu gewährleisten. Die DSGVO verlangt keine absolute Irreversibilität, verlangt jedoch effektive Maßnahmen, die im Lichte der konkreten Gefährdungssituation angemessen und durchsetzbar sind. Die zulässigen Methoden der Datenlöschung umfassen demnach die physische Vernichtung als Goldstandard, restriktive logische Zugriffsbeschränkungen sowie die Anonymisierung. Die Auswahl der Me-

thode ist dabei abhängig von Zweck, Risiko, Umsetzbarkeit und dem jeweiligen Stand der Technik. Diese abgestufte Struktur ist Ausdruck eines modernen, technologieoffenen Datenschutzverständnisses, das weder durch formale Definitionen überreguliert noch durch vollständige Vagheit unterminiert wird. Stattdessen wird dem Verantwortlichen ein normativ gerahmter, aber technisch adaptiver Handlungsspielraum eingeräumt. Dies gewährleistet, dass sowohl dem Schutzziel der DSGVO als auch den realen Verarbeitungsbedingungen Genüge getan wird. Eine potenzielle Weiterentwicklung im Sinne der DSGVO sowie die Abgrenzung zur Überregulierung werden am Ende dieser Arbeit diskutiert.

III. Technische Analyse

Bei der sicheren Datenlöschung spielen technische Standards eine entscheidende Rolle, um sicherzustellen, dass Daten vollständig und irreversibel entfernt werden. Technische Standards erlauben eine einheitliche, von Standardisierungsinstituten oder Behörden verifizierte Methode. Die folgenden Abschnitte beschreiben technische Mechanismen Daten zu löschen.

A. Löschen durch das Betriebssystem

Ein Betriebssystem ist eine spezielle Software, die eine Abstraktionsschicht zwischen Hardware und Software bildet. Dadurch wird die eigenständige Implementierung grundlegender Funktionen sowie das Löschen obsolet. Die Implementierung des Löschvorgangs kann je nach Hardwarekonfiguration variieren. Es ist evident, dass jedes Betriebssystem eigene, spezifische Softwarelösungen aufweist, um Daten auf einer Hardware zu lagern und zu organisieren. Die gegenwärtig vorherrschende Form der Datenorganisation erfolgt in der Regel in Dateien. Dateien sind als abgeschlossene Daten mit Metainformationen definiert. Zu diesen Metainformationen zählen beispielsweise der Dateiname, das Erstellungsdatum oder das Format der Datei. Die vorliegende Untersuchung kommt zu dem Schluss, dass die gängigste Art der Organisation in hierarchischen Ordnerstrukturen besteht. Um diese abzubilden, bedient sich das Betriebssystem einer Software, nämlich dem Dateisystem. Im Grunde hilft das Dateisystem dem Benutzer und Programmen gleichermaßen Dateien mit einer Adresse, im Falle von

hierarchischen Ordnerstrukturen werden diese Pfade genannt, anzulegen, zu verändern, zu lesen oder zu löschen[52]. Dabei spielt die zuvor erwähnte Abbildung dieser Pfade auf Hardwareebene eine wichtige Rolle. So werden Daten auf einer Compact Disk (CD) anders abgelegt als auf einer Solid State Disc (SSD).

Die Löschmechanismen auf Betriebssystemebene sind also je Dateisystem unterschiedlich. Daher werden in den folgenden Unterabschnitten die drei gängigsten Dateisysteme und deren Löschmechanismen betrachtet.

1. NTFS

Das New Technology File System (NTFS) findet vornehmlich in Windows-basierten Betriebssystemen Anwendung und ist aufgrund seiner erweiterten Funktionalitäten und Stabilität weit verbreitet. Die Anwendung findet sowohl in Unternehmensservern als auch in herkömmlichen Windows-Workstations Verwendung.

Grundlegend arbeitet NTFS mit einer Master File Table (MFT), in der jede Datei und jedes Verzeichnis durch eine eindeutige Datei-ID und Metadaten beschrieben wird. Diese Metadaten umfassen Informationen wie Dateinamen, Größe, Erstellungsdatum und Dateiattribute[53]. NTFS unterstützt auch Journaling, das Änderungen an Dateien und Verzeichnissen protokolliert, um die Datenintegrität zu gewährleisten und eine schnelle Wiederherstellung nach einem Systemausfall zu ermöglichen. Des Weiteren ermöglicht NTFS Dateikomprimierung, Verschlüsselung und die Verwaltung von Zugriffsrechten. Durch die Verwendung von Clustern als Grundeinheit der Speicherung und die dynamische Zuweisung von Speicherplatz kann NTFS effizient große und kleine Dateien handhaben.

Beim Löschen einer Datei in NTFS wird der entsprechende Eintrag in der MFT als gelöscht markiert, die Datei selbst bleibt physisch auf dem Datenträger bestehen, bis sie von neuen Daten überschrieben wird. Der Speicherplatz der gelöschten Datei wird als verfügbar markiert und kann für neue Dateien genutzt werden. Um die Daten endgültig zu entfernen, muss der Speicherplatz mehrfach überschrieben oder ein spezielles Löschprogramm verwendet werden, das eine sichere Datenvernichtung gewährleistet.

52 *Silberschatz/Galvin/Gagne*, Operating system conceptsNinth edition.
53 *Bettany/Halsey*, Windows File System Troubleshooting.

2. ext4

Das Dateisystem ext4 (Fourth Extended Filesystem) findet vornehmlich in Linux-basierten Betriebssystemen Anwendung und repräsentiert eines der am häufigsten eingesetzten Dateisysteme in der Linux-Umgebung, sowohl auf Servern als auch auf Desktop- und mobilen Geräten. Aufgrund seiner Stabilität und Effizienz findet es weite Verbreitung und wird von zahlreichen Distributionen als Standarddateisystem eingesetzt.

Ext4 arbeitet mit einem erweiterten Superblock, der grundlegende Informationen über das Dateisystem enthält, sowie mit Inodes, die Metadaten jeder Datei speichern[54]. Diese Metadaten umfassen Dateigröße, Zugriffsrechte, Zeitstempel und Zeiger auf die Datenblöcke, in denen die eigentlichen Dateiinhalte gespeichert sind. Ext4 unterstützt sowohl Extents als auch Blockgruppen, was die Verwaltung von Speicherplatz effizienter macht und die Fragmentierung reduziert. Das Dateisystem verwendet ein Journal, um Änderungen zu protokollieren und die Konsistenz des Dateisystems nach unerwarteten Ausfällen sicherzustellen. Des Weiteren bietet ext4 Unterstützung für große Dateisysteme und Dateien, verzögerte Zuordnung (Delayed Allocation) und Multiblock-Allokation, um die Schreibvorgänge zu optimieren.

Beim Löschen einer Datei in ext4 wird der entsprechende Inode als frei markiert und die Referenzen auf die zugehörigen Datenblöcke werden entfernt, wodurch der Speicherplatz freigegeben wird.

54 *Baun*, Operating Systems / Betriebssysteme.

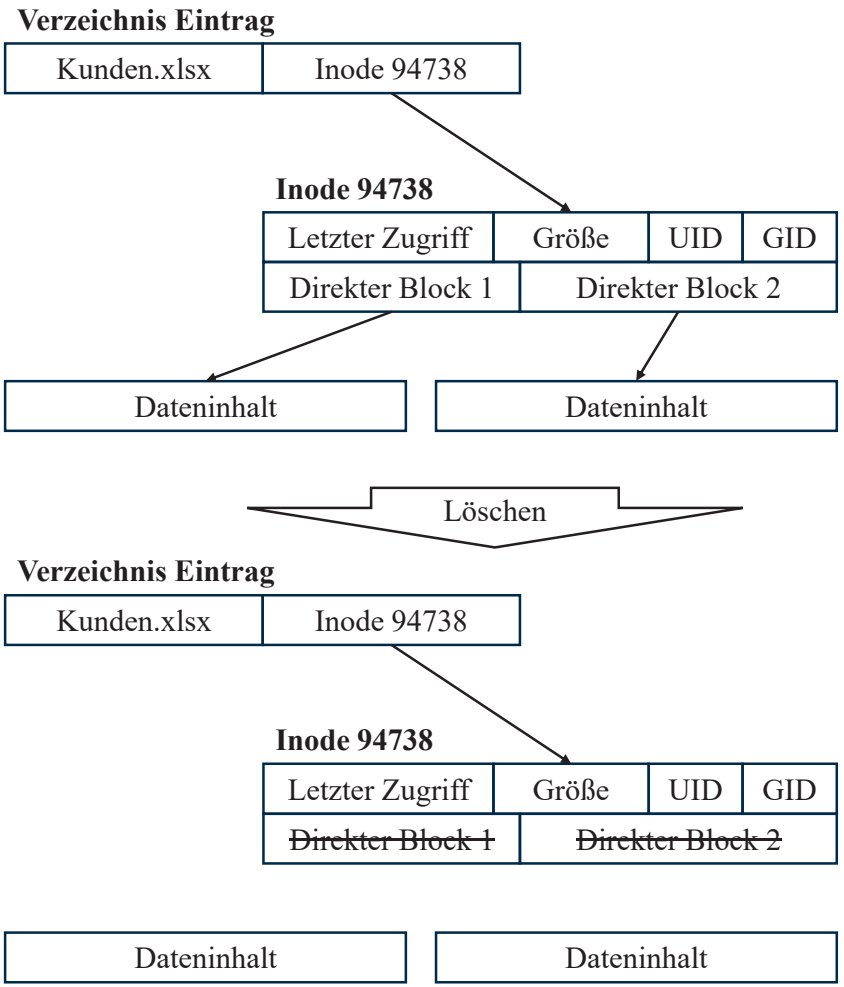

Abbildung 3 – Löschung einer Datei auf ext4 Dateisystemen

Abbildung 3 stellt die Löschung einer Datei auf einem ext4 Dateisystem dar. Eine einfache Datei („Kunden.xlsx“) besteht aus einem Verzeichniseintrag, der auf einen Inode zeigt, dieser beinhaltet die Metadaten (Zugriff, Rechte, Größe etc.), aber auch die Referenzen auf die tatsächlichen Speicherorte (zur Simplifizierung nur direkte Blöcke). Beim Löschen werden nun die Metadaten angepasst, die Referenzen gelöscht, aber die eigentlichen Daten

(Dateninhalte) nicht gelöscht. Die eigentlichen Daten bleiben auf dem Datenträger bestehen, bis sie von neuen Daten überschrieben werden. Um die Daten endgültig zu entfernen, ist es notwendig, den Speicherplatz zu überschreiben oder ein spezielles Löschprogramm zu verwenden, das eine sichere Datenvernichtung durchführt. Ein verschlüsseltes Dateisystem kann die Löschung auch sicherer machen.

3. APFS

Das Apple File System (APFS) wird hauptsächlich in Apple Produkten, wie macOS, iOS, watchOS und tvOS, verwendet und ist aufgrund seiner fortschrittlichen Funktionen und Leistung weit verbreitet. Es wurde entwickelt, um die speziellen Anforderungen moderner Applegeräte zu erfüllen und wird als Standarddateisystem genutzt.

Grundlegend basiert APFS auf einem 64-Bit-Architekturdesign und verwendet eine Kopier-auf-Schreib-Strategie (Copy-on-Write), um die Integrität von Daten bei Schreiboperationen zu gewährleisten. Es unterstützt Snapshots, die den Zustand des Dateisystems zu einem bestimmten Zeitpunkt erfassen und so eine schnelle und effiziente Datenwiederherstellung ermöglichen. Das Dateisystem ist auch für Flash-/SSD-Speicher optimiert, was zu schnellerem Zugriff und geringerer Latenz führt. APFS verwendet eine Baummodellstruktur (B-Trees) für das Management von Dateien und Metadaten, die die Effizienz bei der Datenorganisation und -suche verbessert. Zudem bietet es erweiterte Funktionen wie Verschlüsselung auf Dateiebene, effiziente Klon Erstellung und Space Sharing, wodurch mehrere Volumes denselben physischen Speicherplatz teilen können.

Beim Löschen einer Datei in APFS wird der entsprechende Verzeichniseintrag entfernt und die Speicherblöcke, die die Datei enthalten, werden als verfügbar markiert, aber die Daten selbst bleiben physisch vorhanden, bis sie überschrieben werden. APFS kann mithilfe seiner nativen Verschlüsselungsfunktionen dafür sorgen, dass gelöschte Daten schwerer wiederherstellbar sind, indem es verschlüsselte Blöcke unbrauchbar macht. Für eine endgültige Entfernung der Daten muss der Speicherplatz überschrieben oder ein spezielles Tool verwendet werden, das sichere Löschungsvorgänge durchführt.

B. NIST SP 800–88

Der Standard des US-Amerikanischen National Institute of Standards and Technology (NIST) bietet umfassende Richtlinien zur „Mediensanierung", die speziell auf die Löschung von Daten abzielen. NIST SP 800-88[55] unterscheidet zwischen drei Sanierungstypen: Löschen [„Clear"], Bereinigen [„Purge"] und Zerstören [„Destroy"]. Jede Methode ist für spezifische Szenarien und Medientypen geeignet. Beim Löschen werden Daten so überschrieben, dass sie durch Standarddateisystemmethoden nicht mehr zugänglich sind. Das Bereinigen erfolgt durch Methoden, die eine Wiederherstellung der Daten durch spezialisierte Techniken verhindern sollen. Das Zerstören von Medien führt dazu, dass eine Wiederherstellung der Daten unmöglich wird, sei es durch physikalische Zerstörung oder durch chemische Prozesse. Techniker müssen die Art der zu löschenden Daten sowie den erforderlichen Sicherheitsgrad berücksichtigen, um die geeignete Sanierungsmethode auszuwählen.

C. DoD 5220.22-M

Der Standard 5220.22-M[56] des US-Verteidigungsministeriums ist einer der bekanntesten und am häufigsten verwendeten Ansätze zur Datenlöschung. Er beschreibt ein Verfahren, bei dem Daten auf magnetischen Medien dreimal überschrieben werden. Jeder Durchgang verwendet ein anderes Muster, um alle Spuren der ursprünglichen Daten zu entfernen. Obwohl dieser Standard in einigen Kreisen als veraltet angesehen wird, bietet er immer noch eine solide Basis für die sichere Datenlöschung, besonders wenn kombinierte Überlagerungsmethoden verwendet werden. Für Techniker ist es wichtig, sich der Kritik bewusst zu sein und gegebenenfalls zusätzliche Maßnahmen zur Datensicherheit zu ergreifen.

Der Aufwand der Implementierung der DoD 5220.22-M ist zum Beispiel unter Windows mit Microsoft Sysinternals mittels SDelete[57] relativ gering. Es kann über die Microsoft Webseite gratis bezogen werden und über die

55 *National Institute of Standards and Technology*, Guidelines for Media Sanitization (SP 800-88).

56 *Department of Defense*, National Industrial Security Program Operating Manual (5220.22-M).

57 Microsoft Sysinternals, SDelete, https://learn.microsoft.com/de-de/sysinternals/downloads/sdelete

Eingabeaufforderung ausgeführt, in verschiedene Programme oder mittels Drittsoftware in das Windows Kontextmenü integriert werden, um mittels eines Rechtsklicks jede Datei sicher zu löschen.

Unter Linux kann der Befehl „scrub“[58] herangezogen werden, um sowohl DoD als auch BSI konform Dateien zu löschen.

D. ISO/IEC 27040:2024

Der ISO-Standard 27040:2024[59] konzentriert sich auf die Sicherheitsaspekte von Speichersystemen und umfasst Richtlinien für das sichere Löschen von Daten. Er bietet einen Rahmen für das Einrichten, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in Speichersystemen. Der Standard behandelt spezifische Techniken und Methoden zur Datenlöschung und betont die Bedeutung von Verfahren, die sicherstellen, dass Daten nicht wiederhergestellt werden können. Für Techniker, die mit der Speichersicherheit arbeiten, ist dieser Standard eine wertvolle Ressource, um aktuelle und effektive Praktiken zu implementieren.

Diese Standards bieten nicht nur Richtlinien für die praktische Durchführung der Datenlöschung, sondern betonen auch die Wichtigkeit einer sorgfältigen Planung und Durchführung im Prozess der Datenvernichtung, um die Sicherheit von Informationen zu gewährleisten.

E. DIN 66399

Die Deutsche Industrie Norm 66399[60] konzentriert sich auf die sichere Vernichtung von Datenträgern und legt Anforderungen an Verfahren und Maschinen zur Datenlöschung fest. Gemäß der Definition werden Schutzklassen, Sicherheitsstufen und Materialkategorien festgelegt, um den Schutzbedarf sensibler Daten strukturiert zu erfassen. Die Norm differenziert zwischen sieben Sicherheitsstufen, wobei die erste Stufe lediglich für allgemeine Informationen vorgesehen ist, während die siebte Stufe den höchsten Schutz für geheime Daten gewährleistet. Die Einteilung von Datenträgern

58 Scrub, https://linux.die.net/man/1/scrub

59 *International Organization for Standardization*, Information technology – Security techniques – Storage security (ISO/IEC 27040:2024).

60 DIN SPEC 66399-3:2013-02, Büro- und Datentechnik – Vernichten von Datenträgern, DIN SPEC 66399-3.

erfolgt in sechs Materialkategorien, darunter Papier, optische Medien und magnetische Datenträger.

Die vorliegende Norm DIN 66399 findet ausschließlich Anwendung auf die physische Vernichtung von Datenträgern. Das softwarebasierte Löschen von Daten auf Festplatten oder in Anwendungen ist hingegen nicht Gegenstand der Norm.

F. BSI Grundschutz CON.6

Das IT-Grundschutz-Konzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI) stellt einen strukturierten Ansatz zur Identifizierung und Implementierung von Sicherheitsmaßnahmen in Organisationen bereit. Der BSI-Grundschutz-Baustein CON.6 „Löschen und Vernichten" umfasst Richtlinien und Verfahren für das sichere Löschen und Vernichten von Informationen auf unterschiedlichen Datenträgern. Hierzu zählen sowohl physische Medien, wie etwa Papier und Filme, als auch digitale Speichermedien, zu denen Festplatten und SSDs zählen. Das Ziel besteht darin, den Zugriff auf sensible Daten zu verhindern und die Einhaltung der Datenschutzgesetze zu gewährleisten.

Im Rahmen des BSI-Grundschutz-Bausteins CON.6 wird spezifiziert, dass nicht verschlüsselte, digitale wiederbeschreibbare Datenträger „vollständig mit einem Datenstrom aus Zufallswerten (z. Bsp. PRNG Stream) überschrieben werden"[61] müssen. Für verschlüsselte Datenträger gilt, dass sie „durch ein sicheres Löschen des Schlüssels unter Beachtung des Kryptokonzepts gelöscht werden"[62] müssen, um die Integrität der Datenlöschung zu gewährleisten.

Damit gibt die CON.6 konkrete und detaillierte Anweisungen zur sicheren und datenschutzkonformen Löschung digitaler Datenträger, um Vertraulichkeit und Integrität von Daten zu gewährleisten.

G. Verschlüsselung und Löschung des Schlüssels

Eine technisch-organisatorische Löschung kann durch die Verschlüsselung des Datensatzes oder der Datei vor der Speicherung und die separate Spei-

61 *Bundesamt für Sicherheit in der Informationstechnik*, CON.6 Löschen und Vernichten, Edition 2023.

62 ebd.

cherung des Schlüssels und anschließende Löschung des Schlüssels erreicht werden. Der Löschmechanismus, der auf der Verschlüsselung und anschließenden Löschung des Schlüssels basiert, wird in mehreren Jurisdiktionen als legal gelehrt und wird als effektive Methode zur sicheren Datenlöschung beschrieben.

Verschlüsselung und anschließende Schlüssellöschung (auch „Crypto-Shredding" genannt) ist eine Methode, um personenbezogene Daten faktisch momentan unzugänglich zu machen. Diese Methode wird oft als sicher und praktikabel angesehen, insbesondere für cloudbasierte Systeme, bei denen vollständige Kontrolle über die physische Löschung nicht möglich ist. Auch werden diese bei unveränderlichen Datenspeichern wie z.B. Blockchain Technologien angewandt.

Anderl und Schelling beschreiben in genau diesem Kontext ein Verfahren, bei dem personenbezogene Daten verschlüsselt auf einer öffentlichen Blockchain abgelegt werden und die dazugehörigen Schlüssel „off-chain", also bei dem Verantwortlichen selbst, in einer Datenbank gespeichert werden[63]. Das hätte eine „subjektiv anonymisierende Wirkung", da nur der Verantwortliche den Schlüssel kenne und die Daten verarbeiten könnte. Eine etwaige, durch die DSGVO notwendige, Löschung würde dann durch Löschen des Schlüssels passieren. Die Daten auf der Blockchain „durch Löschung des Schlüssels dauerhaft anonymisiert".

Dobrauz-Saldapenna und Rosenauer sehen im selben Blockchain Kontext die Verschlüsselung und Veröffentlichung von personenbezogenen Daten differenzierter, wenn auch nicht abschließend geklärt. Sie meinen es sei „zu prüfen, ob die Daten durch die Verschlüsselung als irreversibel anonymisiert gelten"[64], aber kommen weiters zu dem Schluss „Verschlüsselung oder Pseudonymisierung der Daten und die anschließende Vernichtung des Schlüssels."[65] seien eine Möglichkeit, um dem Recht auf Vergessenwerden nachzukommen, weil eine Entschlüsselung „technisch sehr Aufwändig", aber demnach möglich wäre. Sie sprechen dabei also das „Knacken" der Verschlüsselung an, welches meist mit „Brute Forcing", also dem Ausprobieren von allen Kombinationen bei intakten Verschlüsselungsverfahren, die korrekt implementiert wurden, gelöst wird. Dies benötigt auch die besagte Rechenleistung.

63 *Anderl/Schelling* in #Blockchain in der Rechtspraxis, S. 102.
64 *Dobrauz-Saldapenna/Rosenauer* in Datenschutz: Recht und Praxis, Rz. 17.
65 ebd, Rz. 37.

Piska und Bierbauer beschreiben ein ähnliches Verfahren „Key-Escrow", indem im Grunde auch ein Schlüssel verwendet wird, um Daten nachträglich zu anonymisieren und kommen zum Schluss, dass dies im „vollen Einklang mit den gebotenen Löschkriterien der DSGVO"[66] stehe und bereits von einigen Startups verwendet werde.

Tatsächlich werden die Daten unzugänglich gemacht. Obwohl die Methode der Schlüssellöschung viele Vorteile bietet, gibt es auch einige Herausforderungen:

Verwaltung der Verschlüsselungsschlüssel: Die Gewährleistung der Sicherheit ist dabei in hohem Maße von einer sicheren Verwaltung und Aufbewahrung der Schlüssel abhängig. Ein kompromittierter Schlüssel könnte potenziell zur Wiederherstellung der Daten führen.

Restdaten in Speichern: Nach der Löschung des Schlüssels sind die Risiken identisch mit denen bei der Löschung aller Daten, sofern diese nicht adäquat gelöscht werden. Es verbleiben Überreste, die nicht durch das einfache Löschen des Schlüssels unzugänglich gemacht werden können.

Sicherheit des Verschlüsselungsverfahrens: Es sei darauf hingewiesen, dass selbst im Falle des Nicht-Diebstahls des Schlüssels ein unsicheres Verschlüsselungsverfahren dazu führen kann, dass ein Dritter unberechtigten Zugriff auf die Daten erhält. Einerseits kann dies auf eine Sicherheitslücke im Verschlüsselungsverfahren zurückzuführen sein, andererseits auf eine unzureichende Schlüssellänge mit der Zeit. In einigen Fällen kann zudem eine bereits erwähnte „Brute-Force"-Attacke Anwendung finden. Dies kann insbesondere bei veröffentlichten oder auf einem unveränderlichen Medium gespeicherten Daten gravierende Konsequenzen nach sich ziehen, da eine nachträgliche Aktualisierung des Verschlüsselungsverfahrens bzw. der Schlüssellänge unmöglich ist.

Evidenz hierzu gibt die Technische Richtlinie (TR) des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Es publiziert in seiner TR-02102-1 kontinuierlich Empfehlungen zu kryptografischen Verfahren inklusive empfohlene Schlüssellängen. Ein Vergleich der Ausgabe von

66 *Piska/Bierbauer* in Blockchain Rules Rz. 7.49.

2021[67] und 2024[68] zeigt, dass bei einem der häufigsten verwendeten asymmetrischen Verschlüsselungsverfahren RSA (Rivest-Shamir-Adleman) die Schlüssellängenempfehlung von 2000 Bits Länge auf 3000 Bits Länge (also Faktor 1,5) innerhalb von nur drei Jahren erweitert wurde. Durch steigende Rechenleistung wird es daher passieren, dass gewisse Schlüssellängen nicht mehr als ausreichend angesehen werden, weil die Daten ohne viel Aufwand entschlüsselt werden können und Daten, die heute als sicher verschlüsselt galten, morgen nicht mehr sicher sind.

Zusammenfassend lässt sich festhalten, dass das Verfahren technisch-juristisch einer gewissen probabilistischen Absicherung entspricht, die nur begrenzt und unter einer (diskutablen) Wahrscheinlichkeit Gültigkeit besitzt. Aus technisch-juristischer Perspektive besteht demnach eine Verbindung der Daten (Personenbezug), die künstlich (durch Verschlüsselung) zuerst probabilistisch subjektiv und nach Löschung des Schlüssels probabilistisch objektiv getrennt wurde. Dies impliziert, dass es sich um Daten handelt, deren Verknüpfung zum gegenwärtigen Zeitpunkt nicht möglich ist. Wolff und Brink behandeln jene Daten und argumentieren die Möglichkeit eines vorbeugenden Unterlassungsanspruches, „wenn sich die rechtswidrige Datenverarbeitung hinreichend konkret anbahnt“[69]. Ob die Anbahnung hinreichend konkret ist, wird in der Diskussion behandelt.

H. Wiederherstellung von Daten

Daten, die auf Dateisystemebene gelöscht wurden, können oft durch spezielle Wiederherstellungssoftware wiederhergestellt werden, solange die Datenblöcke noch nicht überschrieben wurden. Diese Software durchsucht den Datenträger nach nicht referenzierten, aber noch vorhandenen Datenblöcken und rekonstruiert daraus die ursprünglichen Dateien. Das ist möglich, weil das Löschen in vielen Dateisystemen lediglich die Verweise auf die Daten entfernt, nicht aber die Daten selbst. Ein Expertenwissen oder ein hoher Aufwand ist dabei nicht notwendig.

67 *BSI*, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)2021-01 S. 28.

68 *BSI*, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)2024-01 S. 32.

69 *Wolff/Brink*, BeckOK DatenschutzR48. Edition BeckOK Datenschutzrecht, Art. 17 Rz. 77b.

Betriebssysteme wie Windows, Linux und macOS verwenden unterschiedliche Dateisysteme (NTFS, ext4, APFS) zum Löschen von Dateien, wobei die Daten häufig nur als gelöscht markiert werden und physisch auf dem Datenträger verbleiben, bis sie überschrieben werden. Spezielle Wiederherstellungssoftware kann diese Daten rekonstruieren, solange sie nicht überschrieben wurden.

Verfahren wie die oben genannten Standards des NIST, DoD, ISO oder BSI haben unterschiedliche Anwendungsgebiete im Sinne der Medien (Dokumente, Festplatten, SSD, etc.). Gemein haben sie aber, dass sie eine Reduktion des Risikos der Wiederherstellung der Daten schaffen.

I. Zwischenfazit

Die Analyse der technischen Methoden zur Datenlöschung zeigt, dass das Löschen von Daten, abhängig von den verwendeten Dateisystemen und Speichertechnologien, in den meisten Fällen nicht zu einer endgültigen und unwiederbringlichen Löschung der Daten führt. Vielmehr bleiben die Daten in den meisten Dateisystemen physisch auf dem Datenträger bestehen, bis sie von neue Daten überschrieben werden. Dies unterstreicht die Notwendigkeit, spezialisierter Löschverfahren oder Software, um die sichere und irreversible Vernichtung von Daten zu gewährleisten. Die gängigen Dateisysteme wie NTFS, ext4 und APFS markieren beim Löschen einer Datei primär die zugehörigen Metadaten als gelöscht und stellen den Speicherplatz für zukünftige Schreiboperationen zur Verfügung. Diese Vorgehensweise birgt jedoch erhebliche Risiken, da die eigentlichen Daten weiterhin auf dem Datenträger vorhanden bleiben und mit entsprechender Wiederherstellungssoftware rekonstruiert werden können. Dies ist besonders kritisch in Szenarien, in denen eine vollständige und rechtssichere Datenvernichtung erforderlich ist, um Datenschutzvorgaben und regulatorische Anforderungen zu erfüllen.

Normative Standards wie NIST SP 800–88, DoD 5220.22-M und ISO/IEC 27040:2024 bieten detaillierte Vorgaben für die sichere Löschung von Daten und betonen die Bedeutung der Auswahl geeigneter Methoden je nach Sicherheitsanforderungen und Medientyp. Während einige dieser Standards, insbesondere DoD 5220.22-M, als veraltet gelten, bleiben sie weiterhin eine Grundlage für die praktische Umsetzung sicherer Datenlöschung. Dennoch müssen Techniker die Aktualität und Relevanz dieser Normen kontinuierlich überprüfen, um sicherzustellen, dass die angewand-

ten Methoden den neuesten technologischen Entwicklungen und Bedrohungsszenarien entsprechen.

Die Verschlüsselung und anschließende Löschung des Schlüssels (Crypto-Shredding) stellt eine technisch-organisatorische Methode dar, die insbesondere in cloudbasierten und blockchainbasierten Systemen Anwendung findet. Diese Methode wird oft als sicher und praktikabel angesehen, da sie die Daten faktisch unzugänglich macht. Allerdings weist sie auch wesentliche Schwächen auf, insbesondere in Bezug auf die sichere Verwaltung der Verschlüsselungsschlüssel, die verbleibenden Restdaten auf den Speichern und die Langzeitsicherheit des Verschlüsselungsverfahrens selbst. Da die Sicherheit stark von der Stärke und Verwaltung der Schlüssel sowie der Integrität des Verschlüsselungsalgorithmus abhängt, stellt dies eine probabilistische Absicherung dar, deren langfristige Wirksamkeit unsicher ist.

Was die beschriebenen Verfahren zur Datenlöschung gemeinsam haben, ist, dass sie aus der grundlegenden Notwendigkeit entstanden sind, Daten unzugänglich zu machen. Technologische Gegebenheiten, Innovationen und veränderte Rahmenbedingungen haben zur Entwicklung und Weiterentwicklung dieser Lösungen geführt. Abhängig von der Risikobereitschaft des Anwenders können günstige und schnelle Verfahren in bestimmten Kontexten ausreichend sein. Allerdings gilt: Je kritischer oder sensibler die Daten sind, desto sicherere und umfassendere Verfahren sollten angewendet werden. Technisch gesehen, existieren diese fortschrittlichen Lösungen bereits. Ob und wie diese jedoch eingesetzt werden sollten oder müssen, wird in der abschließenden Diskussion behandelt.

V. Strukturierte Analyse

Die Ergebnisse der Analyse werden anschließend bewertet und in tabellarischer Form präsentiert, um die Ergebnisse der Analyse zu veranschaulichen. In der nachfolgenden Diskussion erfolgt eine Analyse der Klassifikation diverser Löschmethoden und Standards hinsichtlich ihrer Zuordnung zu physischen und logischen Löschverfahren (vgl. Kapitel II du III). Tabelle 1 zeigt die Ergebnisse der Analyse zwischen den technischen Löschmethoden (siehe Kapitel II) anhand der juristischen Definitionen von physischem und logischem Löschen (siehe Kapitel IIII.E).

Tabelle 2 – Ergebnisse der Analyse der technischen Löschmethoden anhand der juristischen Definitionen von physischem und logischem Löschen

	Physisches Löschen	Logisches Löschen
Löschen durch das Betriebssystem		●
NIST SP 800–88	●	●
DoD 5220.22-M	●	
ISO/IEC 27040:2024	●	
BSI Grundschutz CON.6	●	
Verschlüsselung und Löschung des Schlüssels		●

Löschen durch das Betriebssystem wird ausschließlich als logische Löschmethode klassifiziert. Diese Methode impliziert, dass die Datenverweise im Dateisystem entfernt werden, während die physischen Daten auf dem Datenträger bestehen bleiben, bis sie durch neue Daten überschrieben werden. Dies entspricht den konventionellen Funktionen moderner Betriebssysteme, die nicht unmittelbar die physikalische Zerstörung der Daten vornehmen, sondern lediglich ihre Zugänglichkeit limitieren.

Der **NIST SP 800–88** Standard ist sowohl unter physischem als auch logischem Löschen kategorisiert. Diese doppelte Zuordnung spiegelt die umfassenden Richtlinien des Standards wider, der Techniken für das Überschreiben von Daten sowie für deren physische Zerstörung umfasst. Dieser Standard bietet somit eine flexible Grundlage für die Implementierung von Datenlöschvorgängen, die sowohl die Unzugänglichkeit als auch die endgültige Zerstörung der Daten sicherstellen können.

DoD 5220.22-M wird ausschließlich als eine Methode des physischen Löschens geführt. Obwohl dieser Standard auch das Überschreiben von Daten beinhaltet, welches als logische Löschmethode betrachtet werden könnte, dominiert in der Praxis die Perzeption seiner Rolle bei der gründlichen und irreversiblen Zerstörung von Daten.

ISO/IEC 27040:2024 wird ebenfalls nur unter physischem Löschen geführt. Der Standard konzentriert sich auf die Sicherheit von Speicherdiensten und inkludiert Anleitungen sowohl für das physische als auch für das logische Löschen, jedoch mit einem starken Akzent auf die physische Vernichtung der Speichermedien.

Der **BSI Grundschutz CON.6** wird konsequent als physische Löschmethode aufgeführt. Dies reflektiert die Schwerpunktsetzung des Bausteins

auf sichere Vernichtungsprozesse, die sicherstellen, dass die Daten nicht nur unzugänglich gemacht, sondern auch physisch zerstört werden.

Schließlich wird die **Verschlüsselung und Löschung des Schlüssels** eindeutig als logische Löschmethode kategorisiert. Diese Methode macht Daten durch die Entfernung des Schlüssels unlesbar, ohne die Notwendigkeit einer physischen Zerstörung der Daten selbst, die typisch für logische Löschverfahren ist.

Diese Klassifikationen verdeutlichen die breite Palette von Löschmethoden, die in der Informationssicherheit zur Anwendung kommen, und reflektieren die Vielfalt der Ansätze zur Datenlöschung, die von rein softwarebasierten Lösungen bis hin zu physischen Vernichtungsprozessen reichen.

Die Betrachtung und tabellarische Analyse der verschiedenen technischen Löschmethoden im Kontext der gesetzlichen Vorgaben und der gesellschaftlichen Erwartungen, wie in den Kapiteln II und III dargestellt, erlauben eine systematische Evaluierung der Effektivität und Anwendbarkeit der einzelnen Verfahren. Die differenzierte Darstellung in Tabelle 1 verdeutlicht die spezifischen Stärken und Einschränkungen jeder Methode in Bezug auf physische und logische Löschprozesse sowie deren Ausrichtung auf Endgültigkeit, Sicherheit, Transparenz, Datenintegrität, Zuverlässigkeit, Schnelligkeit, einfache Durchführung, Regelkonformität, Nachvollziehbarkeit und das Fehlen einer Selbstzerstörungsfunktion. Diese strukturierte Analyse bietet nicht nur einen klaren Überblick über die vorhandenen technologischen Möglichkeiten und deren rechtliche Adäquanz, sondern legt auch den Grundstein für weiterführende Forschungen, die auf der Optimierung von Löschverfahren basieren könnten, um sowohl technologische als auch rechtliche Anforderungen effizienter zu adressieren und die Resilienz von Datenschutzmaßnahmen in einer sich ständig weiterentwickelnden digitalen Landschaft zu stärken.

VI. Diskussion

Die vorliegende Untersuchung kommt zu dem Schluss, dass sowohl die DSGVO als auch das österreichische DSG einen umfassenden, jedoch in Bezug auf den Begriff des „Löschens" unpräzisen Rechtsrahmen bieten. Eine klare Definition des Begriffs ist essenziell, insbesondere im Hinblick auf dessen praktische Umsetzung. Die fehlende klare Definition hat zur Folge, dass Unternehmen und Organisationen Unsicherheiten haben, da

unklar bleibt, welche Maßnahmen tatsächlich als „Löschen" im Sinne der Gesetzgebung zu betrachten sind. Dies erschwert nicht nur die Einhaltung der gesetzlichen Vorgaben, sondern erhöht auch das Risiko von Fehlinterpretationen und möglichen Sanktionen. Zudem können unterschiedliche Interpretationen dazu führen, dass Unternehmen unterschiedliche Lösungsansätze verfolgen. Dies kann zu einer uneinheitlichen Umsetzung und potenziellen Nachteilen im Wettbewerb führen. Darüber hinaus erschwert die unpräzise Definition die Entwicklung standardisierter technischer Lösungen, was insbesondere bei neuen Technologien wie der Blockchain problematisch ist, da dort eine physische Löschung oft nicht möglich ist. Eine präzise und konsistente Definition wäre daher von essenzieller Bedeutung, um Rechtssicherheit zu gewährleisten und eine effektive und konsistente Umsetzung der gesetzlichen Anforderungen zu gewährleisten. Die DSGVO normiert mit dem Recht auf Löschung nach Art. 17 eine bußgeldbewehrte Pflicht, unterlässt es jedoch, den Begriff „Löschen" inhaltlich zu konkretisieren. Angesichts der in Art. 83 ausgesprochenen Sanktionsandrohung ist eine eindeutige, normative Festlegung erforderlich. Diese Festlegung ermöglicht es dem Adressatenkreis, das gesetzlich Gebotene zu erkennen und rechtssicher umzusetzen. Die fehlende Differenzierung zwischen physischem und logischem Löschen eröffnet einen weiten Interpretationsspielraum, der mit rechtsstaatlichen Anforderungen an Normklarheit und Rechtsfolgensicherheit unvereinbar ist.

Die teleologische Auslegung des Begriffs „Löschen" ist von zentraler Bedeutung, um den gesetzgeberischen Willen zu erfassen und die Ziele des Datenschutzes zu erreichen. Die Analyse hat ergeben, dass eine einheitliche Auslegung im Rahmen der DSGVO nicht vorliegt. Die mangelnde Klarheit bezüglich der Art der Löschung (logisch vs. physisch) kann in der Praxis zu Unsicherheiten führen. In der digitalen Welt, in der Daten bei verschiedenen Verantwortlichen vorliegen oder als unveränderlich gelten (z. B. Blockchain), besteht ein Bedarf an klareren Regelungen.

Die Entscheidungen des EuGH, OGH und der österreichischen DSB zeigen eine gewisse **Uneinheitlichkeit in der Bewertung von Löschmethoden**. Diese Unterschiede führen zu Unsicherheiten bei der praktischen Anwendung und Interpretation des Löschrechts.

Die technische Untersuchung zeigt, dass die Anwendung unzureichender Löschmethoden, insbesondere der bloßen logischen Löschung, potenziell schwerwiegende Risiken für die betroffenen Personen birgt. Dies verdeutlicht die Relevanz eines risikobasierten Ansatzes. Die fortschreitende technologische Entwicklung bedingt eine kontinuierliche Anpassung der

rechtlichen Rahmenbedingungen, um den effektiven Schutz personenbezogener Daten zu gewährleisten. Dies ist insbesondere im Kontext der Löschung und Pseudonymisierung von Daten von signifikanter Relevanz. Die vorliegende Arbeit kommt zu dem Schluss, dass die Verschlüsselung und Löschung des Schlüssels als eine juristisch akzeptierte Alternative zur physischen Löschung zu betrachten ist. Allerdings sind damit auch Herausforderungen und Risiken verbunden.

Gemäß der DSGVO ist ein dem Aufwand des Verantwortlichen angemessenes Verhältnis zu dem Risiko des Betroffenen erforderlich, auch in Bezug auf die Implementierung von Löschmethoden. Dies stellt die Verantwortlichen vor Herausforderungen, erfordert jedoch auch eine präzise gesetzliche Regelung.

Das Kernproblem besteht darin, dass Verantwortliche nicht nur die Verarbeitungstätigkeiten, sondern auch die damit verbundenen Risiken im Kontext der Datenlöschung vollumfänglich verstehen und darauf basierend eine geeignete Lösung auswählen müssen, sei es durch technische Systeme oder organisatorische Maßnahmen. Je weniger technisch versiert der Verantwortliche ist, desto mehr ist er auf validierte Standards und standardisierte Systeme angewiesen, die, wie in Kapitel III dargelegt, bereits existieren.

Die gegenwärtige Interpretation des Begriffs „Löschen" durch die DSB und den EuGH lässt jedoch Spielraum für Verantwortliche, die, obwohl sie das Risiko der Datenverarbeitung durchaus verstehen, versuchen, den Aufwand zu minimieren. Dies eröffnet die Möglichkeit, den Begriff des Löschens im Sinne einer beneficium sibi tribuendi zulasten der Betroffenen möglichst weit zu fassen. Hierdurch etablieren große Unternehmen Quasi-Standards, denen kleinere Unternehmen aus Kostengründen folgen, da individuelle Implementierungen wirtschaftlich kaum tragbar sind. Dies führt zu einer de facto Harmonisierung durch wirtschaftliche Macht, anstatt durch klare gesetzliche Vorgaben, was den Schutzzweck der DSGVO zu unterlaufen droht. Derzeitige Unsicherheiten über die datenschutzrechtliche Zulässigkeit bestimmter Löschmethoden führen zu einer strukturellen Ungleichheit zwischen datenverarbeitenden Stellen. Große Unternehmen sind regelmäßig in der Lage, eigene technische Standards zu etablieren und durchzusetzen, während kleinere Verantwortliche sich mangels Ressourcen an diese faktischen Quasi-Normen anlehnen müssen. Eine verbindliche und differenzierende Definition der Löschmethoden würde nicht nur Rechtssicherheit schaffen, sondern auch Chancengleichheit im Wettbewerb und gleichmäßige Rechtsanwendung gewährleisten.

Die Ergebnisse zeigen, dass eine **gesetzliche Präzisierung des Begriffs „Löschen" erforderlich** ist, um den praktischen Anforderungen gerecht zu werden. Eine klare Unterscheidung zwischen logischer und physischer Löschung wäre notwendig. Die Rechtsprechung hat bereits wichtige Impulse zur Auslegung des Löschrechts gegeben, doch bleibt eine endgültige Klärung aus. Die Arbeit legt nahe, dass die Zukunft des Löschrechts von einer stärkeren Differenzierung der Löschmethoden und einer präziseren gesetzlichen Regelung abhängen wird. Eine Anpassung der Gesetzgebung an die technologische Realität ist unerlässlich. Die Gerichte haben dabei sowohl physische Löschung als auch Anonymisierung als wirksame Methoden anerkannt; logische Löschung ist uneinheitlich ausgelegt.

Im Rahmen der Implementierung der Löschung ist es unerlässlich, die Vorgaben des Standes der Technik zu berücksichtigen (Art. 32). In vorliegender Arbeit werden technische Standards erörtert, darunter auch der BSI-Grundschutz CON.6. Es wird explizit darauf hingewiesen, dass dieser kontinuierlich aktualisiert wird und daher wird empfohlen, seine Implementierung zu prüfen.

Die Abwägung der Risiken und Implementierungskosten des Stands der Technik darf zur Auswahl der Technik herangezogen werden. Jedoch kann mit der Implementierung einfacher Mittel (wie in Abschnitt III.C dargestellt) eine Lösung zum sicheren Löschen umgesetzt werden, die sowohl von Benutzern als auch Programmen verwendet werden kann.

Art. 32 Abs. 1 lit. d fordert auch eine regelmäßige Überprüfung dieser Maßnahmen. Sollten also Verfahren eingesetzt werden, die technisch nur kurzlebig sind, so müssen diese spätestens bei der nächsten Prüfung gewechselt werden. Somit ist nicht nur aus technisch-juristischer Sicht, sondern auch aus wirtschaftlicher Sicht eine weitsichtige Auswahl der Verfahren sinnvoll.

Die Ergebnisse der Arbeit legen nahe, dass **logische Löschung aus technischer Sicht eine kurzlebige und stark risikobehaftete Methode ist** und daher **im Falle der Löschung von personenbezogenen Daten ein Risiko für den Betroffenen darstellt und sollte daher nicht als Löschen im Sinne der DSGVO ausgelegt werden**. Löschverfahren sollten mit dem Stand der Technik vereinbar sein, und in der bereits zum Einsatz des Verfahrens absehbaren Zukunft nicht zu einer Deanonymisierung führen.

Des Weiteren liegt nahe, dass ein risikobasierter Ansatz erforderlich ist, um zu definieren, zu welchem Zeitpunkt und auf welche Art und Weise die Löschung von Daten erfolgen sollte. Diese Vorgehensweise steht im Einklang mit den Grundprinzipien der DSGVO, welche eine Abwägung

zwischen Risiko und Aufwand fordern. Eine Differenzierung zwischen dem physischen und logischen Löschen könnte dieses Risiko in der Implementierung darstellen.

Die vorliegende Arbeit kommt zu dem Schluss, dass der Gesetzestext derzeit eine Unklarheit aufweist, die durch eine Interpretation zugunsten einer logischen Löschung im Sinne des Löschbegriffes der DSGVO überkompensiert wird. Die vorliegende Untersuchung kommt zu dem Schluss, dass klare Vorgaben für technische und organisatorische Maßnahmen erforderlich sind, um die Löschung von Daten sicher und effektiv zu gestalten. Dies entspricht den fundamentalen Prinzipien sowie den Anforderungen der DSGVO.

Die Kosten und eingesetzten Ressourcen, die mit der Umsetzung effektiver Löschmethoden verbunden sind, müssen im Verhältnis zum Datenschutzrisiko stehen. Ein risikobasierter Ansatz ermöglicht eine wirtschaftlich sinnvolle Umsetzung. Die Gefahr der Reidentifikation pseudonymisierter Daten stellt ein erhebliches Risiko dar, das bei der Auslegung und Umsetzung des Löschrechts berücksichtigt werden muss. Dies unterstreicht die Bedeutung eines strikten Datenschutzes. Die Arbeit legt nahe, dass der Gesetzestext dahingehend präzisiert werden sollte, dass zwischen logischer und physischer Löschung unterschieden wird. Dies würde sowohl die Rechtssicherheit erhöhen als auch die praktische Umsetzung erleichtern.

Die in der Forschungsfrage „*Inwieweit erfüllen verschiedene juristisch-technische Löschmechanismen im menschenzentrierten Datenschutz die technischen Anforderungen, sind rechtlich konform und entsprechen den Erwartungen der Benutzer?*“ aufgeworfene Thematik spiegelt sich umfassend in der Analyse der Löschmechanismen wider. Diese Diskussion reflektiert, dass die betrachteten Methoden eine Spannbreite von streng regelkonformen bis hin zu benutzerzentrierten Lösungen aufzeigen. Während einige Methoden wie NIST SP 800-88 und BSI Grundschutz CON.6 durch ihre umfassenden Richtlinien und strengen Protokolle hohe Sicherheit und Endgültigkeit der Datenlöschung garantieren und somit technische Anforderungen sowie rechtliche Konformität hervorragend erfüllen, zeigt die Analyse auch, dass Methoden wie das Löschen durch das Betriebssystem vor allem auf die Benutzererwartungen mit ihrer Schnelligkeit und einfachen Durchführung abzielen. Die umfassende Bewertung aller Methoden hinsichtlich verschiedener Kriterien ermöglicht es, die komplexen Interdependenzen zwischen technischer Machbarkeit, rechtlicher Notwendigkeit und Benutzerakzeptanz herauszuarbeiten und somit einen ganzheitlichen

Blick auf den aktuellen Stand der Technik und dessen Eignung im Rahmen des Datenschutzes zu bieten.

A. Implikationen für die Rechtswissenschaft und Praxis

Die aktuelle juristische Interpretation des Löschbegriffs, wie er in der DSGVO verwendet wird, offenbart signifikante technische Risiken für die Betroffenen. Die Ergebnisse der vorliegenden Analysen verdeutlichen, dass eine konsequente Unterscheidung zwischen logischem und physischem Löschen notwendig ist, um den Schutz personenbezogener Daten effektiv zu gewährleisten. Diese Notwendigkeit manifestiert sich insbesondere bei der Analyse der historischen Entwicklung der rechtlichen Rahmenbedingungen zur Datenlöschung, insbesondere der Änderungen, die im österreichischen Datenschutzgesetz (DSG) 1978 implementiert wurden.

Die Revision des DSG im Jahr 1987 führte präzise Definitionen für das physische und das logische Löschen ein. Physisches Löschen wurde als „Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist", definiert, während das logische Löschen als „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen" beschrieben wurde. Diese Differenzierung reflektierte eine fortschrittliche Anerkennung der technologischen Realitäten sowie der Notwendigkeit, sowohl den Zugriff als auch die Existenz der Daten selbst zu kontrollieren.

Die aktuelle Auslegung der DSGVO bietet jedoch keine solch klaren Abgrenzungen. Dies stellt ein Risiko dar, weil logisches Löschen, also die bloße Sperrung der Daten ohne deren physische Zerstörung[70], den Daten subjektiv einen Schutzstatus verleiht, der objektiv nicht gegeben ist. Die Daten bleiben physisch vorhanden und potenziell rekonstruierbar, was insbesondere bei mangelnder physischer Sicherung der Datenträger ein erhebliches Sicherheitsrisiko bedeutet. Darüber hinaus folgt die Notwendigkeit einer ausdrücklichen Unterscheidung aus dem unionsrechtlich verankerten Prinzip des effektiven Grundrechtsschutzes und den datenschutzrechtlichen Vorgaben der Art. 5 und Art. 17 DSGVO. Das Ziel der Löschpflicht ist nicht lediglich die Zugriffsbeschränkung, sondern die tatsächliche Beendigung der Verfügbarkeit personenbezogener Daten. Logische Löschmethoden, die lediglich die Adressierung oder Sichtbarkeit der Daten aufheben, lassen

70 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 4 Rz. 42.

die physische Existenz der Information unberührt. Diese verbleibende Rekonstruierbarkeit widerspricht dem Schutzzweck des Art. 17 DSGVO, insbesondere bei sensiblen Datenkategorien. Eine Löschmaßnahme kann nur dann als effektiv gelten, wenn sie die Möglichkeit des Wiederzugriffs technisch ausschließt. Dies ist ausschließlich durch physische oder kryptographisch finalisierende Maßnahmen gewährleistbar.

Es wird daher vorgeschlagen, eine rechtliche Revision der DSGVO zu erwägen, die eine ähnliche Differenzierung zwischen physischem und logischem Löschen einführt, wie sie bereits im österreichischen DSG von 1987 vorhanden war. Eine solche Änderung würde die juristische Klarheit erhöhen und sicherstellen, dass die technische Handhabung von Datenlöschungen den tatsächlichen Anforderungen des Datenschutzes entspricht. Konkret sollte die DSGVO um die Definitionen des physischen Löschens als „Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist" und des logischen Löschens als „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen" ergänzt werden. Gleichzeitig ist jedoch auch das Verhältnismäßigkeitsprinzip zu beachten. Eine ausnahmslose Pflicht zur physischen Löschung würde in bestimmten technischen Konstellationen, etwa bei unveränderlichen Speichermodellen wie der Blockchain, zu unüberwindbaren Umsetzungshindernissen führen. Die Zulässigkeit logischer Löschung sollte daher gesetzlich eng gefasst und nur für solche Ausnahmefälle vorgesehen werden, in denen physische Vernichtung derzeit technisch unmöglich oder unzumutbar ist. Eine solche Regelung wahrt die erforderliche Flexibilität, ohne den Schutzzweck des Datenschutzrechts zu unterlaufen, und stellt ein ausgewogenes Verhältnis zwischen den Interessen der betroffenen Personen und den faktischen Möglichkeiten der Verantwortlichen her.

Des Weiteren ist es angebracht, klarzustellen, **dass logisches Löschen nur als temporäre Maßnahme in streng geregelten Ausnahmefällen zulässig sein sollte**. Diese Einschränkung würde die Rechtssicherheit für die Datenverarbeiter erhöhen und die Rechte der betroffenen Personen effektiver schützen. Die Inkorporation dieser klaren und differenzierten Definitionen würde dazu beitragen, die Lücke zwischen der rechtlichen Regelung und der technischen Praxis zu schließen und somit den Datenschutz auf ein neues, zeitgemäßes Niveau zu heben.

Die vorgeschlagenen Änderungen dienen nicht nur der Stärkung des Schutzes der Betroffenen, sondern auch der Bereitstellung klarer rechtlicher Rahmenbedingungen für die Verantwortlichen. In der Folge könnten Datenverarbeitungsprozesse sowohl effizienter als auch konformer gestaltet

werden, wodurch die Vertrauenswürdigkeit und Rechtskonformität der Datenverarbeitung im digitalen Zeitalter gefördert werden würde.

B. Abwägung zwischen Heteronomie, Überregulierung und Risiken

Um eine Überregulierung zu vermeiden, sollte geprüft werden, ob eine detaillierte Regulierung zur Definition der Löschbegriffe tatsächlich notwendig ist. Brownsword betont, dass die regulatorische Herausforderung darin besteht, „nützliche Innovationen zu fördern und gleichzeitig inakzeptable Risiken für Mensch und Umwelt zu kontrollieren“[71]. Aus technologischer Perspektive ist der Löschbegriff im Gegensatz zur Selbstverantwortung und der damit verbundenen Flexibilität bei der Implementierung weniger einschränkend. Die vorliegende Untersuchung zielt darauf ab, den Terminus „Löschung“ einer präzisen Definition zu unterziehen. Sofern sich aus technischer Sicht, wie es beispielsweise bei der später erwähnten Technologie unveränderlicher Speicher, wie etwa der Blockchain-Technologie, nicht realisieren lässt, wäre eine logische Löschung im Sinne der DSGVO und DSG bis zu dem Zeitpunkt ausreichend, an dem eine physische Löschung möglich wird. Eine differenzierte Definition von physischem und logischem Löschen kann mit dem technologischen Fortschritt Schritt halten, indem sie Raum für Anpassungen lässt, ohne dass ständig neue, restriktive Regelungen eingeführt werden müssen. Allein der Umstand, dass die vorgeschlagene Definition über mehrere Generationen der Automatisierung und Digitalisierung immer noch zutreffend ist, ist eine starke Evidenz dafür, dass diese technologieneutral und nicht zu speziell ist. Dies unterstützt die Balance zwischen Sicherheit und Innovationsförderung. Ein starker Eingriff in die Innovation ist durch die Abgrenzung der bereits etablierten Verfahren daher nicht zu erwarten. Die Risiken, gegen die abgewogen werden muss, bleiben jedoch, wie bereits erwähnt, evident.

Es sei jedoch die Frage aufgeworfen, ob eine zu detaillierte Ausdifferenzierung des Löschbegriffs nicht paradoxerweise zu den von der Verhaltensökonomie beschriebenen Effekten wie Überregulierung und reduzierter Eigenverantwortung führen könnte. Insbesondere der Peltzman-Effekt[72] könnte in diesem Zusammenhang relevant werden, wenn Datenverarbeitende aufgrund explizit definierter Löschvorgänge eine falsche Sicherheit

71 *Brownsword*, Rethinking Law, Regulation, and Technology, Übers. d. Verf., S. 6.
72 *Specht*, The Journal of SH&E Research 4 (2007) 3.

empfinden und infolgedessen eine kritische Auseinandersetzung mit Risiken und dem tatsächlichen Schutz personenbezogener Daten vernachlässigen. Die rechtliche Notwendigkeit, präzise und unmissverständlich zu definieren, was unter Löschung zu verstehen ist, könnte daher in einer unerwünschten Heteronomie resultieren, bei der der Fokus mehr auf die Einhaltung spezifischer Vorgaben als auf das übergeordnete Ziel des Datenschutzes gelegt wird. Diese Überlegungen bedürfen einer sorgfältigen Abwägung, um sowohl die Compliance als auch die datenschutzrechtliche Sensibilisierung zu fördern.

C. Limitationen der Studie und mögliche Verbesserungen

Die Studie basiert auf einer begrenzten Anzahl von Quellen und könnte durch die Einbeziehung weiterer empirischer Daten oder expliziter Studien verbessert werden, um umfassendere Ergebnisse zu erzielen. Eine Limitation der Studie ist das Fehlen empirischer Untersuchungen, die die praktische Umsetzung der Löschvorschriften in verschiedenen Organisationen analysieren. Eine vertiefte Analyse der technischen Aspekte der Datenlöschung, insbesondere in Bezug auf moderne Technologien (KI, Blockchain etc.), könnte die Studie ergänzen. Die vorliegende Untersuchung fokussiert sich auf eine Auswahl von Gerichtsurteilen. Eine umfassendere Analyse könnte zu einer detaillierteren Bewertung der Rechtsprechung führen. Die vorliegende Studie fokussiert sich in hohem Maße auf das EU-Recht und könnte durch einen Vergleich mit internationalen Datenschutzregelungen ergänzt werden. Die vorliegende Untersuchung könnte durch die Berücksichtigung von Sonderfällen, wie beispielsweise der Löschung von publizierten oder verteilten Daten, detailliertere Informationen liefern. So wäre es möglich, die Notwendigkeit einer spezialisierten Regelung für diese zu ermitteln. Eine wesentliche Limitation besteht in der Vernachlässigung einer Analyse der langfristigen Implikationen der Löschung von Daten, insbesondere unter Berücksichtigung des Datenschutzes und der Datensicherheit. Eine vertiefte Analyse der Perspektive der betroffenen Personen könnte zu einem besseren Verständnis der Auswirkungen der Löschung auf die individuellen Rechte beitragen.

D. Ausblick für zukünftige Forschung

Zukünftige Forschung könnte empirische Studien berücksichtigen, um die tatsächliche Umsetzung und Wirksamkeit von Löschmaßnahmen in der Praxis zu evaluieren. Es besteht Bedarf an der Entwicklung klarer, praxisorientierter Leitlinien für die Datenlöschung für Unternehmen, die sowohl logische als auch physische Löschmethoden umfassen. Die Auswahl der adäquaten Löschmethode für die entsprechende Risikoklasse soll auf diese Weise optimiert werden.

Die Implikationen neuer Technologien auf die Datenlöschung sollten einer verstärkten Untersuchung unterzogen werden, um rechtliche und technische Anpassungen frühzeitig zu identifizieren. Entwicklungen im Bereich der Quantencomputer und -algorithmen können potenziell zu abrupten Veränderungen im Risikoprofil spezifischer Verfahren führen. Unternehmen, die technische Datenschutzmaßnahmen implementieren, sollten in die Lage versetzt werden, diese Entwicklungen einfach aufzufinden und zu konsumieren, um entsprechende Änderungen vorzunehmen.

Mit weiterer Forschung und praxisnaher Entwicklung könnte damit Unternehmen geholfen werden, ihren Verpflichtungen, speziell auch, aber nicht beschränkt auf Löschrechte nachzukommen und diese technisch-juristisch sicher zu implementieren.

E. Zusammenfassung der Diskussion

In Anbetracht der **ratio legis der DSGVO**, welche primär darauf abzielt, eine ausgewogene Balance zwischen den Rechten der betroffenen Personen und den Pflichten der Verantwortlichen zu schaffen, ist es unerlässlich, dass die **Risiken**, denen die Betroffenen ausgesetzt sind, sowohl für diesen **transparent** als auch **minimiert** werden. Die DSGVO verfolgt das Ziel, die Grundrechte der betroffenen Personen zu schützen und zugleich den Verantwortlichen eine gewissenhafte Abwägung von Aufwand und Risiko zu erlauben.

Die derzeitige Interpretation führt zu einer **Erhöhung des Risikos** eines möglichen Verstoßes gegen die Datenminimierung, Transparenz, Speicherbegrenzung, Integrität und allen voran **Vertraulichkeit** der betroffenen Daten (vgl. Art. 5, welcher die Grundsätze und Prinzipien der DSGVO beschreibt). Die gesellschaftliche Erwartungshaltung, vor allem Endgültigkeit, Sicherheit und Transparenz, deckt sich stark mit diesen Grundsätzen, aber

nicht mit der derzeitigen Interpretation dieser. Der teleologische Ansatz erfordert, dass die etablierten, standardisierten Verfahren, welche zur Reduktion dieses Risikos beitragen und bereits lange etabliert sowie technisch unaufwändig implementierbar sind, vollumfänglich Berücksichtigung finden.

Die **historische Exegese** zeigt zudem, dass eine ähnliche Problematik bereits im DSG1978 durch eine gesetzliche Klarstellung im Jahr 1987 adressiert wurde. Diese Gesetzeserweiterung diente der Präzisierung und Verbesserung des Datenschutzes und es ist daher nur folgerichtig, eine vergleichbare Erweiterung für die DSGVO anzustreben, um dem ursprünglichen gesetzgeberischen Willen gerecht zu werden und die Schutzintention der Norm zu wahren.

VII. Conclusio

Die vorliegende Arbeit zielte darauf ab, die Eignung juristisch-technischer Löschmechanismen im menschenzentrierten Datenschutz zu bewerten. Die vorliegenden Ergebnisse zeigen, dass logische Löschmethoden mit technischen Risiken assoziiert sind, während das physische Löschen eine sicherere Alternative darstellt.

Die vorliegende Untersuchung kommt zu dem Schluss, dass der Begriff des „Löschens" in der DSGVO sowie im österreichischen DSG rechtlich nicht präzise definiert ist. Diese Unbestimmtheit erweist sich insbesondere im Kontext der technischen Umsetzung als problematisch. Eine Analyse der Rechtsprechung des EuGH, OGH und der österreichischen Datenschutzbehörde offenbart eine uneinheitliche Auslegung und Anwendung des Löschbegriffs, insbesondere hinsichtlich der Abgrenzung zwischen physischer und logischer Löschung. Die Tatsache, dass die logische Löschung als rein programmtechnische Zugriffsbeschränkung keinen tatsächlichen Datenverlust verursacht, steht im Spannungsverhältnis zum in Art. 17 DSGVO normierten Anspruch auf Löschung und den Grundprinzipien des Datenschutzrechts, insbesondere dem der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO. Gemäß der technischen Analyse ist festzustellen, dass insbesondere logische Löschmethoden das Risiko einer Reidentifikation personenbezogener Daten nicht hinreichend ausschließen. Somit kann in bestimmten Fällen keine endgültige Löschung der Daten gewährleistet werden. Gemäß dem Stand der Technik, wie er in Art. 32 DSGVO und in einschlägigen Standards wie dem BSI Grundschutz CON.6 konkretisiert

ist, ist eine risikoadäquate Auswahl und Überprüfung der eingesetzten Verfahren erforderlich. In diesem Zusammenhang ist die von der DSGVO geforderte Verhältnisbestimmung zwischen dem Aufwand für den Verantwortlichen und dem Risiko für die betroffene Person von maßgeblicher Relevanz. Die Ergebnisse der Untersuchung legen nahe, dass eine gesetzliche Präzisierung des Begriffs „Löschen" erforderlich ist, insbesondere durch die ausdrückliche Unterscheidung zwischen logischem und physischem Löschen. Eine solche Differenzierung würde nicht nur die Kohärenz der Auslegung fördern, sondern auch eine unionsweit einheitliche und effektive Anwendung des Löschrechts gewährleisten. Der Gesetzgeber sieht sich folglich in der Pflicht, den Löschbegriff normativ zu präzisieren, um den datenschutzrechtlichen Schutzzielen zu entsprechen und bestehende Auslegungsspielräume im Sinne der Betroffeneninteressen zu limitieren.

VIII. Rechtsquellenverzeichnis

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), OJ L 2016/119 [DSGVO].

Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1980.

Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1987.

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), Fassung vom 29.06.2024.

IX. Literaturverzeichnis

Albrecht, in Datenschutzrecht: DSGVO mit BDSG (2019).

Anderl/Schelling, in #Blockchain in der Rechtspraxis (2020).

Baun, Operating Systems / Betriebssysteme – Bilingual Edition: English – German / Zweisprachige Ausgabe: Englisch – Deutsch (2020) http://link.springer.com/10.1007/978-3-658-29785-5 [Operating Systems / Betriebssysteme].

Bettany/Halsey, Windows File System Troubleshooting (2015).

Brand ea, in Datenschutz-Grundverordnung: VO (EU) 2016/679: Bundesdatenschutzgesetz: Kommentar (2022).

M. Braun/Kamann, in DS-GVO: Datenschutz-Grundverordnung: Kommentar (2024).

Brownsword, Rethinking Law, Regulation, and Technology (03.04.2022) https://www.elgaronline.com/view/9781800886469.xml.

BSI, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)[2024-01] (2024) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=5.

BSI, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)[2021-01] (2021) https://web.archive.org/web/20220120061112/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf;jsessionid=5FAA6C5F75A71422772001A3C9EED482.internet481?__blob=publicationFile&v=2.

Bundesamt für Sicherheit in der Informationstechnik, CON.6 Löschen und Vernichten, Edition 2023 (2023) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2023.pdf?__blob=publicationFile&v=2.

Department of Defense, National Industrial Security Program Operating Manual (5220.22-M) (2006).

DIN SPEC 66399-3:2013-02, Büro- und Datentechnik – Vernichten von Datenträgern https://dx.doi.org/10.31030/1935106 [DIN SPEC 66399-3].

Dobrauz-Saldapenna/Rosenauer, in Datenschutz: Recht und Praxis (2020).

Dodge/Kitchin, Outlines of a World Coming into Existence – Pervasive Computing and the Ethics of Forgetting, Environment and Planning B: Planning and Design 34 (06.2007) 3, 431 ['Outlines of a World Coming into Existence'].

EDPB, Guidelines 9/2022 on personal data breach notification under GDPR (2022).

EDPB, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (2020).

EDPB, Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO (2020).

Feiler/Forgó, EU-DSGVO und DSG – EU-Datenschutz-Grundverordnung und Datenschutzgesetz: Kommentar[2. Auflage] (2022) [EU-DSGVO und DSG].

Fritz, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung, Datenschutzrecht Jahrbuch 2022 (19.01.2023).

Gürses/Troncoso/Diaz, Engineering privacy by design, Computers, Privacy & Data Protection (CPDP) 14 (2011).

Halsey/Bettany, Windows file system troubleshooting, Expert's voice in Microsoft Windows (2015).

International Organization for Standardization, Information technology – Security techniques – Storage security (ISO/IEC 27040:2024) (Published: ISO/IEC 27040:2024 2024).

Knyrim, Der DatKomm, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online.

Koops, Forgetting Footprints, Shunning Shadows – A Critical Analysis of the „Right to Be Forgotten" in Big Data Practice, SSRN Electronic Journal 2011 http://www.ssrn.com/abstract=1986719 [Forgetting Footprints, Shunning Shadows].

Kranenborg, Article 17 Right to erasure ('right to be forgotten'), in *Kuner ea* (Hrsg), The EU General Data Protection Regulation (GDPR) (13.02.2020) 475 https://academic.oup.com/book/41324/chapter/352298059.

Kühling ea, Datenschutz-Grundverordnung, BDSG – Kommentar[4. Auflage] (2024) [Datenschutz-Grundverordnung, BDSG].

Mayer-Schönberger, The Virtue of Forgetting in the Digital Age (2011) https://doi.org/10.1515/9781400838455.

National Institute of Standards and Technology, Guidelines for Media Sanitization (SP 800-88) (2014).

Nepal ea, Editorial – Human-Centric Security and Privacy, Frontiers in Big Data 5 (17.02.2022) https://www.frontiersin.org/articles/10.3389/fdata.2022.848058/full [Editorial].

Nissenbaum, Privacy in context – technology, policy, and the integrity of social life (2010) [Privacy in context].

Norman, The design of everyday things[Revised and expanded edition] (2013).

Piltz, Sicherheit personenbezogener Daten, in Datenschutz-Grundverordnung: VO (EU) 2016/679: Bundesdatenschutzgesetz: Kommentar (2022).

Piska (Hrsg), Blockchain rules – das FinTech-Handbuch[2. Auflage] (2024) [Blockchain rules].

Piska/Bierbauer, in Blockchain Rules (2024).

Purtova, The Law of Everything – Broad Concept of Personal Data and Future of EU Data Protection Law, Law, Innovation and Technology 10 (2018) 1, 40.

Silberschatz/Galvin/Gagne, Operating system concepts[Ninth edition] (2013).

Specht, The Peltzman effect – Do safety regulations increase unsafe behavior, The Journal of SH&E Research 4 (2007) 3.

Tzanou, The unexpected consequences of the EU Right to Be Forgotten – Internet search engines as fundamental rights adjudicators, in Personal Data Protection and Legal Developments in the European Union (2020) 279.

Voigt/Von Dem Bussche, EU-Datenschutz-Grundverordnung (DSGVO) (2018) http://link.springer.com/10.1007/978-3-662-56187-4.

Wolff/Brink, BeckOK Datenschutzrecht[48. Edition] (2023).

CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB, GDPR Enforcement Tracker – List of GDPR fines, (abgefragt 8. 3. 2024).

X. Entscheidungsverzeichnis

EuGH 26. 4. 2023, Rechtssache T-557/20, *Einheitlicher Abwicklungsausschuss gegen Europäischer Datenschutzbeauftragter*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020TJ0557&qid=1709927171181.

EuGH 19.10.2016, Rechtssache C-582/14, *Patrick Breyer gegen Bundesrepublik Deutschland*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CJ0582.

EuGH 16.7.2020, Rechtssache C-311/18, *Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62018CJ0311&qid=1709931086167.

EuGH 27 Oktober 2022, Rechtssache C-129/21, *Proximus NV gegen Gegevensbeschermingsautoriteit*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0129&qid=1751209049981.

EuGH 5.12.2023, Rechtssache C-807/21, *Deutsche Wohnen SE gegen Staatsanwaltschaft Berlin*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0807&qid=1709927140384.

EuGH 14.12.2023, Rechtssache C-456/22, *VX und AT gegen Gemeinde Ummendorf*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62022CJ0456&qid=1709930921739.

EuGH 25.01.2024, Rechtssache C-687/21, *BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0687&qid=1709926727671.

Europäischer Gerichtshof 8 Dezember 2022, Rechtssache C-460/20, *TU und RE gegen Google LLC*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020CJ0460&qid=1751208855425.

Europäischer Gerichtshof 14.10.2023, Rechtssache C-340/21, *VB gegen Natsionalna agentsia za prihodite*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0340&qid=1709927018251.

Bescheid (AEPD) 28.07.2023 (Bescheid PS/00331/2022 der Spanischen Datenschutzbehörde (AEPD)).

Bescheid (HDPA) 27.01.2022 (Bescheid 4/2022 der Griechischen Datenschutzbehörde (HDPA)).

Beschluss (EDSA) (Verbindlicher Beschluss 2/2022 zur Streitigkeit nach Artikel 65 Absatz 1 Buchstabe a der DSGVO über den Beschlussentwurf der irischen Aufsichtsbehörde bezüglich Meta Platforms Ireland Limited (Instagram)) [28.7.2022].

Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018, *DSB-D123.270/0009-DSB/2018*, https://www.ris.bka.gv.at/JudikaturEntscheidung.wxe?Abfrage=Dsk&Dokumentnummer=DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.

Datenschutzbehörde 13.12.2018, DSB-D122.995/0003-DSB/2018, *DSB-D122.995/0003-DSB/2018*, https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181213_DSB_D122_995_0003_DSB_2018_00/DSBT_20181213_DSB_D122_995_0003_DSB_2018_00.html.

Oberster Gerichtshof 15.04.2010, 6Ob41/10p, *6Ob41/10p*, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20100415_OGH0002_0060OB00041_10P0000_000&Suchworte=RS0125838.

Oberster Gerichtshof 13.09.2012, 6Ob107/12x, *6Ob107/12x*, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20120913_OGH0002_0060OB00107_12X0000_000&Suchworte=6Ob107/12x.

Google Spain SL und Google Inc gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, No. Rechtssache C-131/12 (EuGH 13 Mai 2014), https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62012CJ0131.

Krimineller oder Sündenbock? Strafrechtliche Verantwortlichkeit des CISO durch Unterlassen

Sophia Salm

§ 1 Einleitung[*]

Im Zeitalter der Digitalisierung benutzen immer mehr Unternehmen digitale Systeme zur Steuerung physischer Infrastruktur und zur Datenspeicherung. Damit werden die Einkommensquellen und Assets der Unternehmen, sensible Daten von natürlichen und juristischen Personen sowie Infrastruktur von öffentlichem Interesse der Gefahr digitaler Übergriffe ausgesetzt. Deren Schutz unter dem Begriff «Cybersecurity» oder «Cybersicherheit» wird somit immer wichtiger. Der schweizerische Gesetzgeber reagierte unter anderem, indem er die sogenannten «Computertatbestände» wie Art. 144bis StGB, Art. 147 StGB und weitere Strafnormen wie Art. 61 DSG und Art. 69a URG ausarbeitete. Auf der Seite der Unternehmen wird als Reaktion immer häufiger die Position des Chief Information Security Officer, kurz «CISO», eingeführt.

Der CISO ist in einem Unternehmen oder einer Organisation für die Cybersicherheit verantwortlich. Diese beinhaltet den Schutz elektronischer Systeme, Informationen und physischer Infrastruktur vor digitalen Angriffen.[1] Häufige Attacken sind beispielsweise Malware, welche auf Ausspähung gerichtet ist,[2] oder DDoS Angriffe, deren Ziel die Überlastung der Kapazität einer digitalen Infrastruktur – zum Beispiel Websites – sind, um so die

---

* Der nachfolgende Beitrag wurde als Masterarbeit im Rahmen des Masterstudiums der Rechtswissenschaften an der Universität Zürich am 15.4.2024 eingereicht. Der Inhalt befindet sich auf dem Stand der Einreichung. Für die Veröffentlichung wurden die Formalien inklusive Literaturverweise zum Stichtag 21.2.2025 aktualisiert. Auch sämtliche Internetlinks wurden an diesem Tag zuletzt aufgerufen. Ich bedanke mich bei Herrn Dr. iur. Lukas Staffler, L.L.M (London) für die Betreuung der Arbeit und die Ermöglichung, an der Publikation mitzuwirken. Zur besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet. Die verwendeten Personenbezeichnungen beziehen sich gleichermassen auf alle Geschlechter.

1 Brockhaus isits AG; CISA What is Cybersecurity?; vgl. BWL Minimalstandard, S. 10.

2 Pieth Wirtschaftsstrafrecht, S. 130, 139.

Verfügbarkeit dieser zu stören.[3] Resultate solcher Cyber-Angriffe sind oft massive finanzielle Schäden in Form verlorener Assets oder der Einschränkung möglichen Gewinns, die Gefährdung von Daten sowie Rufschäden.[4] Die Strafverfolgung der Cyberkriminellen ist allerdings schwierig, da deren Identität oft unbekannt und schwierig zu eruieren ist. Die Täter sind häufig Teil grösserer Organisationen und handeln aus dem Ausland.[5] Daher ist ein Rückgriff auf andere Verantwortliche, deren Identität bekannt ist und die sich in der Schweiz befinden, kriminalpolitisch wünschenswert. Hierfür kommt der CISO in Frage.

Aufgrund der Neuheit der Position variieren die spezifischen Aufgaben des CISO in der Praxis. Grundsätzlich ist er dazu verpflichtet, eine Informationssicherheits-Strategie auszuarbeiten und diese Massnahmen gemeinsam mit der IT(-Sicherheits)-Abteilung umzusetzen und zu überwachen. Dazu gehört auch die Schulung von Mitarbeitern zu Cybersicherheitsthemen. Ausserhalb dieser «Informatik-Aufgaben» dient er als Bindeglied zwischen der Organisationsleitung und der Informationssicherheit. In diesem Zusammenhang muss er regelmässig der Leitung Bericht erstatten, diese beraten und mit internen oder externen Institutionen zusammenarbeiten. Somit muss der CISO neben technischem Wissen zur Informationssicherheit auch über geschäftliches Wissen und Durchsetzungsvermögen verfügen. Bezüglich seines Bereichs ist er berechtigt, Entscheidungen zu treffen. Weitreichende Risikoentscheidungen werden jedoch seiner Entscheidungsmacht entzogen.[6]

Vor diesem Hintergrund wird dieser Beitrag der Frage nachgehen, inwiefern der CISO im Rahmen des StGB durch unechte Unterlassung zur Verantwortung gezogen werden kann. Hierfür werden zunächst die potenziell einschlägigen Straftatbestände des besonderen Teils dargelegt. Aufgrund der thematischen Nähe werden dabei auch Tatbestände des DSG vorgestellt und erklärt, weshalb der Fokus auf das StGB, nicht das DSG gesetzt wurde. Der Hauptteil des Beitrags wird sich mit dem allgemeinen Teil des

3 BACS Halbjahresbericht 2024/I, S. 26; Pieth Wirtschaftsstrafrecht, S. 131.

4 BACS Halbjahresbericht 2024/I, S. 4; Proofpoint 2024 Report, S. 11: vgl. FINMA Aufsichtsmitteilung 05/2020, S. 2 f.: Die FINMA sieht bei Betroffenheit systemrelevanter Institute zusätzlich die Funktionsfähigkeit der Finanzmärkte über die einzelnen Unternehmen hinaus gefährdet; Kaspersky Lab What it Takes to Be a CISO, S. 12; Wipro State of Cybersecurity, S. 52.

5 NCSC Allgemeine Bedrohungsformen, S. 4 ff.; Pieth Wirtschaftsstrafrecht, S. 148 f.

6 Zum Ganzen: CISO-Alliance Berufsbild CISO, S. 5 ff.; Heidrick & Struggles 2024 Survey, S. 14; Kaspersky Lab What it Takes to Be a CISO, S. 5, 8.

Strafrechts – die Begehung durch Unterlassen – beschäftigen. Dabei werden unter anderem verschiedene Garantenstellungen diskutiert. In diesem Zusammenhang wird die Rolle des CISO mit der des Compliance Officers und des Datenschutzberaters verglichen werden.

§ 2 Verhältnis des StGB zu den Strafbestimmungen des DSG

Die potenziell anwendbaren Tatbestände sind nicht auf die nachfolgend aufgelisteten Artikel begrenzt. Diese wurden lediglich exemplarisch herausgegriffen. Um das grosse Spektrum der Aufgaben des CISO darzustellen, wurden vier Tatbestände gewählt, die je eine Kategorie repräsentieren. So werden im folgenden Abschnitt ein Daten- beziehungsweise Computerdelikt, ein Eigentumsdelikt, ein Vermögensdelikt und ein Freiheitsdelikt näher beleuchtet. Ziel hierbei ist es, einen kurzen Überblick des jeweiligen Tatbestands und mögliche Anwendungsbeispiele zu geben.

Straftatbestände wie Art. 143 StGB oder Art. 146 StGB wurden trotz ihrer Häufigkeit in der Praxis bewusst ausgeschlossen, weil sie eine Bereicherungsabsicht fordern. Auch bei der Begehung durch Unterlassen muss der Täter, hier der CISO, diese erfüllen.[7] In den wenigsten Fällen wird ein CISO jedoch mit direktem Vorsatz, geschweige denn mit der Absicht, sich selbst oder jemand anderem einen Vermögensvorteil[8] dadurch zu verschaffen, handeln.

A. Potenziell einschlägige Straftatbestände des StGB

I. Unbefugtes Eindringen in ein Datenverarbeitungssystem

Gemäss Art. 143bis StGB macht sich strafbar, wer unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt. Bezüglich der Sicherung ist die Schwelle relativ tief; die Sicherungsmassnahme muss nicht zwingend den üblichen Standard der jeweiligen Branche erreichen, so dass auch einfache Massnahmen ge-

7 Niggli/Muskens BSK StGB, Art. 11 Rn. 145.
8 Maeder/Niggli BSK StGB, Art. 146 Rn. 261; Stratenwerth/Bommer Strafrecht BT I, § 15 Rn. 62.

nügen.[9] Sicherheitslücken schliessen die besondere Sicherung nicht aus.[10] Ein CISO, der also zwar Sicherheitsmassnahmen wie Passwörter einführt, jedoch in Kauf nimmt, dass diese einfach überwindbar sind, könnte möglicherweise diesen Tatbestand durch Unterlassen erfüllen. Art. 143bis StGB schützt die Freiheit des Berechtigten, zu entscheiden, wer Zugang zu einem Datenverarbeitungssystem beziehungsweise den darin enthaltenen Daten hat.[11] Auch als «Computerfrieden» umschrieben, wird damit die Unverletzlichkeit des eigenen Computers geschützt.[12]

Bei den meisten Cyberangriffen wird dieser Tatbestand erfüllt sein. Zur Installierung von Viren dringt man in ein Datenverarbeitungssystem ein. Die Benutzung von Malware ist auf die Ausspähung der Daten in Verarbeitungssystemen gerichtet. Bei Phishing Angriffen wird sodann oft die Eingabe von Anmeldedaten durch das Opfer erschlichen, damit mithilfe dieser Anmeldedaten in das Datenverarbeitungssystem eingedrungen werden kann.[13] Auch bei einem erfolgreichen Phishing Angriff kann folglich der Tatbestand erfüllt werden. Der CISO könnte sich in den vorgenannten Beispielen durch Unterlassen strafbar machen, indem er den Angriff nicht verhindert.

II. Sachbeschädigung

Art. 144 StGB stellt die Beschädigung, Zerstörung oder das Unbrauchbarmachen einer Sache, an der ein fremdes Eigentums-, Gebrauchs- oder Nutzniessungsrecht besteht, unter Strafe. Der Eingriff in die Substanz selbst ist nicht notwendig, solange die Funktionsfähigkeit beziehungsweise Brauchbarkeit beeinträchtigt wird.[14] Geschützt wird in erster Linie die unbeeinträchtigte tatsächliche Herrschaftsmacht über eine Sache.[15]

Auf den ersten Blick scheint dieses Delikt nicht passend, um einen Cyberangriff abzudecken. Jedoch soll hier aufgezeigt werden, dass die Arbeit des CISO sich nicht auf die virtuelle Welt beschränkt, sondern sich auch

9 BGE 145 IV 185 E. 2.2.2; Weissenberger BSK StGB, Art. 143 Rn. 19, Art. 143bis Rn. 14.
10 Weissenberger BSK StGB, Art. 143bis Rn. 15.
11 Weissenberger BSK StGB, Art. 143bis Rn. 5.
12 BGer 6B_456/2007 vom 18.3.2008 E. 4.2.
13 BACS Halbjahresbericht 2024/I, S. 11 ff.
14 Stratenwerth/Bommer Strafrecht BT I, § 14 Rn. 53 f.; Weissenberger BSK StGB, Art. 144 Rn. 38.
15 Weissenberger BSK StGB, Art. 144 Rn. 2; vgl. Stratenwerth/Bommer Strafrecht BT I, § 14 Rn. 48.

auf die physische Welt auswirken kann. Ein denkbares Szenario wäre beispielsweise ein Angriff auf Systeme, welche physische Infrastruktur steuern, wodurch diese über einen längeren Zeitraum ausgeschaltet werden und deren Funktionsfähigkeit aufgehoben wird.[16] Die Frage ist auch hier, ob der CISO diesen Angriff hätte verhindern müssen, wodurch er sich durch Unterlassen strafbar gemacht hat.

III. Ungetreue Geschäftsbesorgung

Nach Art. 158 Ziff. 1 StGB macht sich des Treubruchs strafbar, wer aufgrund eines Rechtsgeschäfts mit der Vermögensverwaltung für einen anderen oder mit der Beaufsichtigung solcher betraut ist, und dabei unter Pflichtverletzung zulässt, dass der andere am Vermögen geschädigt wird. Im Gegensatz zu den anderen genannten Tatbeständen handelt es sich dabei um ein echtes Unterlassungsdelikt.[17] Die für die unechte Unterlassung benötigte Garantenstellung wird hier mit der Sondereigenschaft des Vermögensverwalters ersetzt.[18] Geschützt wird dadurch fremdes Vermögen.[19]

Hauptfrage hier ist, ob der CISO als Vermögensverwalter im Sinne des Art. 158 Ziff. 1 StGB zu qualifizieren ist. Weiter vorausgesetzt wäre dann, dass aufgrund seiner Pflichtverletzung ein Cyberangriff erfolgt, der zu einem Vermögensschaden führt. Denkbar wäre zum Beispiel eine Lösegeldzahlung aufgrund einer Ransomware Attacke oder der unterbliebene Gewinn, wenn ein Webshop durch einen DDoS Angriff ausser Betrieb gesetzt wird.[20] Da diese Arbeit den Fokus auf die Garantenstellung des unechten Unterlassungsdelikts setzt, wird dieser Tatbestand nicht weiter besprochen. Trotzdem ist er aufgrund der thematischen Nähe erwähnenswert.

16 Woodtli SRF: Beim Unternehmen Swisswindows realisierte sich diese Gefahr im Jahr 2019, als ein Cyberangriff auf computergesteuerte Maschinen einen mehrwöchigen Produktionsstillstand auslöste.
17 Stratenwerth Strafrecht AT I, § 14 Rn. 8.
18 Niggli BSK StGB, Art. 158 Rn. 10, 125; Pieth Wirtschaftsstrafrecht, S. 114.
19 Niggli BSK StGB, Art. 158 Rn. 9.
20 Woodtli SRF: Das Unternehmen Comparis beispielsweise zahlte 2021 als Reaktion auf einen Ransomware Angriff Lösegeld.

IV. Nötigung

Eine Nötigung im Sinne des Art. 181 StGB ist gegeben, wenn durch Gewalt, Androhung ernstlicher Nachteile oder durch andere Beschränkung der Handlungsfreiheit ein Tun, Unterlassen oder Dulden abgenötigt wird. Geschütztes Rechtsgut ist dabei die Freiheit der Willensbildung, -entschliessung und -betätigung.[21] Die Erpressung gemäss Art. 156 StGB würde zwar bei Verlangen einer Geldzahlung vorgehen, jedoch benötigt diese im Gegensatz zur Nötigung eine Bereicherungsabsicht, weshalb sie hier für den CISO ausgeschlossen wurde.[22] Die Nötigung ist subsidiär anwendbar.[23]

Cyberangriffe wie Ransomware und DDoS zielen oft auf ein Tun oder Dulden der Geschädigten ab. Bei Ransomware wird die Publizierung von gestohlenen Daten angedroht oder Daten werden im Computersystem der Opfer verschlüsselt. Erst bei Erfüllung der erzwungenen Handlung – oft die Zahlung von Geld – werden die Daten entschlüsselt.[24] Bei DDoS Überfällen könnte sich der Nötigungserfolg im Dulden des damit verbundenen (Reputations-)Schadens durch das Unternehmen beziehungsweise im Dulden durch die Kunden, nicht auf die Website zugreifen zu können, manifestieren. Es würde sich dabei um eine Art Sitzblockade im Internet handeln. Möglich ist auch, dass ein Handeln des angegriffenen Unternehmens verlangt wird.[25] Auch hier stellt sich die Frage, ob der CISO durch Unterlassen trotz Handlungspflicht die Nötigung ermöglichte.

B. Überblick der DSG Strafbestimmungen

Nach Art. 1 DSG sind die geschützten Rechtsgüter der Persönlichkeitsschutz und die Grundrechte von natürlichen Personen. Art. 60 ff. DSG enthält die Strafbestimmungen, welche einen Teil des Nebenstrafrechts darstellen.

---

21 BGE 106 IV 125 E. 2a; Delnon/Rüdy BSK StGB, Art. 181 Rn. 5; Stratenwerth/Bommer Strafrecht BT I, § 5 Rn. 1.

22 Vgl. § 2.

23 Delnon/Rüdy BSK StGB, Art. 181 Rn. 71; Stratenwerth/Bommer Strafrecht BT I, § 5 Rn. 19.

24 BACS Halbjahresbericht 2024/I, S. 16.

25 Mozur New York Times: 2015 wurde das Unternehmen GitHub Opfer eines mehrtägigen DDoS Angriffs. Gemäss GitHub wollten die Angreifer, vermutlich der chinesische Staat, das Unternehmen dazu nötigen, zwei Websites, für die GitHub Webhosting betrieb, zu entfernen.

Für den CISO besonders relevant sind Art. 61 und Art. 64 DSG – die Verletzung von Sorgfaltspflichten und Widerhandlungen in Geschäftsbetrieben. Art. 64 Abs. 1 DSG verweist auf Art. 6 und 7 VStrR. Diese besagen, dass bei Widerhandlungen in Ausübung geschäftlicher Verrichtungen für einen anderen die Strafbestimmungen auf die natürlichen Personen anwendbar sind, welche die Tat verübt haben. Art. 64 DSG führt damit eine strafrechtliche Geschäftsherrenhaftung ein.[26] Art. 61 DSG umfasst unter anderem das Nichteinhalten der Mindestanforderungen an die Datensicherheit (lit. c). Da der CISO für die Cybersicherheit verantwortlich ist, welche die Gewährleistung der Datensicherheit einschliesst, wird insbesondere diese Variante für seine strafrechtliche Verantwortlichkeit relevant sein.

C. Zwischenfazit

Der Anwendungsbereich des StGB ist weiter als der des DSG. Das StGB schützt auch juristische Personen als Geschädigte, nicht nur natürliche Personen wie das DSG. Die Strafbestimmungen des DSG zielen nur auf den Datenschutz spezifisch ab, während das StGB den weiteren Bereich der Cybersicherheit abdeckt. Dadurch wird eine grössere Bandbreite von Rechtsgütern wie die Herrschaftsmacht über eine Sache, das Vermögen sowie die freie Willensbildung und -betätigung des einzelnen Menschen geschützt. Im Gegensatz dazu deckt das DSG nur den Persönlichkeitsschutz. Die Stellung des DSG als Nebenstrafrecht kommt zudem durch das tiefere Strafmass im DSG zum Ausdruck.

Das StGB geht auch bezüglich der geschützten Rechtsgüter in Verbindung mit Daten weiter als das DSG. So schützt Art. 143bis StGB beispielsweise die Entscheidungsfreiheit des Computerberechtigten, nicht nur des Dateneigentümers. Damit werden nicht nur die Betroffenen, sondern auch die Datenverantwortlichen geschützt. Der Unrechtsgehalt eines Cyberangriffs kann daher nicht allein anhand der DSG-Straftatbestände abgegolten werden.

Aus diesen Gründen können die Straftatbestände des StGB die Bandbreite der mit Cybersicherheit verbundenen Gefahren besser repräsentieren als das DSG allein. Daher wird zum Zweck dieser Arbeit nur die Strafbarkeit des CISO im Rahmen des StGB untersucht.

26 Gassmann OK DSG, Art. 64 Rn. 2; Simmler OFK DSG, Art. 64 Rn. 5.

§ 3 Strafbarkeit des CISO durch Unterlassen

Die meisten potenziell einschlägigen Straftatbestände sind Handlungsdelikte.[27] In der Praxis wird jedoch die aktive Tatbegehung nur äusserst selten vorkommen. Viel wahrscheinlicher ist die Begehung durch Unterlassen, beispielsweise indem Sicherheitslücken nicht behoben werden und dadurch Angriffe von Dritten ermöglicht werden. Nachdem also oben ein Überblick der BT-Straftatbestände gegeben wurde, muss nun gemäss dem allgemeinen Teil ermittelt werden, ob der CISO durch Unterlassen für das deliktische Verhalten der Cyberangreifer strafrechtlich verantwortlich gemacht werden kann.

A. Überblick des unechten Unterlassungsdelikts

Objektiv wird ein Unterlassen vorausgesetzt. Dieses wird nach herrschender Lehre anhand der Subsidiaritätstheorie bestimmt, wonach zuerst ein aktives Tun zu prüfen ist und erst bei Fehlen dessen ein Unterlassen in Frage kommt.[28] Das Unterlassen muss anschliessend zu einem tatbestandsmässigen Erfolg führen.[29]

Nach Art. 11 Abs. 2 StGB muss der Täter eine Garantenstellung innehaben. Diese kann namentlich aufgrund Gesetzes (lit. a), Vertrages (lit. b), einer freiwillig eingegangenen Gefahrengemeinschaft (lit. c) oder durch Schaffung einer Gefahr (lit. d) entstehen. Sie verpflichtet den Garanten zu handeln, um den Eintritt des tatbestandsmässigen Erfolgs abzuwenden.[30]

Zusätzlich wird eine hypothetische Kausalität verlangt. Gefragt wird hier, ob der Erfolg ausgeblieben wäre, hätte der Täter die unterlassene Handlung vorgenommen.[31] Die Tatmacht – die Möglichkeit, die gebotene Handlung vorzunehmen und dadurch den Erfolg abzuwenden – ist auch Vorausset-

27 Vgl. § 2.A.

28 BGE 129 IV 119 E. 2.2; BGE 115 IV 199 E. 2a; Niggli/Muskens BSK StGB, Art. 11 Rn. 53;
Trechsel/Noll/Pieth Strafrecht AT I, S. 236; a.M. Donatsch/Godenzi/Tag Strafrecht I, S. 315 f.

29 Donatsch/Godenzi/Tag Strafrecht I, S. 338 f.; Trechsel/Noll/Pieth Strafrecht AT I, S. 234.

30 BGE 105 IV 172 E. 4a; Donatsch/Godenzi/Tag Strafrecht I, S. 322; Niggli/Muskens BSK StGB, Art. 11 Rn. 67.

31 BGE 117 IV 130 E. 2a; BGE 108 IV 3 E. 2; Trechsel/Noll/Pieth Strafrecht AT I, S. 250.

zung der unechten Unterlassung.[32] Weiter wird gemäss Art. 11 Abs. 3 StGB die Vorwurfsidentität vorausgesetzt. Demnach muss dem unterlassenden Täter derselbe Vorwurf gemacht werden können, wie wenn er die Tat durch aktives Tun begangen hätte.

Subjektiv wird je nach Tatbestand Vorsatz oder Fahrlässigkeit genügen. Die vorgenannten potenziell einschlägigen Straftatbestände müssen alle in Verbindung mit Art. 12 Abs. 1 StGB vorsätzlich begangen werden. Der Täter muss also die Verwirklichung des Straftatbestands durch einen Dritten erkennen beziehungsweise voraussehen, sie aber trotz seiner Garantenpflicht nicht aufheben oder verhindern, weil er sie mindestens in Kauf nimmt.[33]

B. Garantenstellung des CISO

Die grösste Problematik bezüglich der Strafbarkeit des CISO durch Unterlassen liegt in der Frage, ob er eine Garantenpflicht hat. Hierfür muss zuerst die Hierarchie des CISO bestimmt werden. Ausgehend davon werden verschiedene Arten der Garantenstellung näher beleuchtet, um zu ermitteln, ob der CISO diese erfüllt.

I. Hierarchie des CISO

Weil die Position des CISO neu ist, kann keine pauschale Beurteilung seiner Stellung gemacht werden. Jede Organisation interpretiert die Rolle anders, räumt dem CISO einen unterschiedlichen Ermessensspielraum ein und teilt die Verantwortung anders auf. Teils soll der Verwaltungsrat für Cyberrisiken verantwortlich sein, teils ausschliesslich die Informatik-Abteilung und damit der CISO. Sogar innerhalb der einzelnen Unternehmen kann Unklarheit herrschen.[34]

In wenigen Unternehmen wird der CISO als Teil des Verwaltungsrats eingebunden.[35] Die Mehrheit der CISOs sind nicht direkt dem CEO un-

32 BGE 96 IV E. II.4a; Stratenwerth Strafrecht AT I, § 14 Rn. 41; Trechsel/Noll/Pieth Strafrecht AT I, S. 249 f.

33 BGE 105 IV 172 E. 4b.

34 Zum Ganzen: Hunziker/Trachsel EXPERTfocus, S. 613: Kommentiert wird zusätzlich, dass die alleinige Verantwortung der Informatik-Abteilung widerrechtlich sei.

35 Hunziker/Trachsel EXPERTfocus, S. 614: Ein CISO aus 18 befragten Schweizer Unternehmen; Kaspersky Lab What it Takes to Be a CISO, S. 14: 26 % der CISOs von 250 weltweit befragten Unternehmen.

terstellt, sondern unterstehen dem CIO oder einer anderen Person unterhalb des CEO.[36] Damit ist der CISO mutmasslich auch nicht Teil der Geschäftsleitung. Dies könnte ein Grund sein, weshalb nur eine bescheidene Mehrheit des CISOs von 58 % global beziehungsweise 64 % in Europa sich angemessen in Geschäftsentscheidungen eingebunden fühlt.[37] Dabei ist jedoch unklar, ob der CISO eine beratende Rolle hat, wobei seine Vorschläge durch die Geschäftsleitung abgesegnet werden müssen, oder ob der CISO eigenständig Entscheidungen treffen kann. Die Daten wurden länderübergreifend gesammelt, weshalb eine direkte Übertragung dieser Zahlen auf die Position eines CISO in der Schweiz nur mit einem gewissen Vorbehalt möglich ist. Jedoch deuten die Daten auf Tendenzen, welche vor allem grössere schweizerische Unternehmen vermutlich übernehmen.

In Übereinstimmung mit der oben aufgezeigten Mehrheit wird für die nachfolgenden Ausführungen angenommen, dass der CISO nicht im Verwaltungsrat ist und einer Person unterhalb des CEO unterstellt ist. Ob diese Person den Titel des CIO oder einen anderen Titel trägt, ist für die Zwecke dieser Arbeit unerheblich. Hintergrund dieser Annahme ist auch, dass der CISO sonst wie jedes andere Verwaltungsrats- oder Geschäftsleitungsmitglied verantwortlich wäre; seine Pflichten spezifisch als CISO wären weniger entscheidend.

II. Obhutsgarantenstellung aus Vertrag

Die Garantenstellung, die zunächst in Frage kommt, ist eine aus Vertrag gemäss Art. 11 Abs. 2 lit. b StGB. Hierfür reicht jedoch nicht jede vertragliche Handlungspflicht.[38] Vielmehr muss dadurch eine gesteigerte Verantwortung begründet werden, die grundsätzlich als Hauptpflicht erscheint.[39] Es muss sich um eine qualifizierte Rechtspflicht handeln.[40]

In Lehre und Praxis wird zwischen zwei Formen der Garantenpflicht unterschieden: die Obhutsgarantenstellung und die Sicherungs- beziehungs-

36 Heidrick & Struggles 2024 Survey, S. 11 48 % der 416 weltweit befragten CISOs unterstehen dem CIO, während nur 14 % direkt dem CEO Bericht erstatten; Wipro State of Cybersecurity, S. 23, 50: 51 % der circa 110 befragten Organisationen in Europa beziehungsweise 54 % der 345 Organisationen global unterstehen dem CIO.

37 Kaspersky Lab What it Takes to Be a CISO, S. 13 f.

38 BGE 140 IV 11 E. 2.4.2; Stratenwerth Strafrecht AT I, § 14 Rn. 17.

39 Niggli/Muskens BSK StGB, Art. 11 Rn. 82 f.; Stratenwerth Strafrecht AT I, § 14 Rn. 17 f.

40 BGE 141 IV 249 E. 1.1; BGE 120 IV 98 E. 2c; BGE 113 IV 68 E. 5a.

weise Überwachungsgarantenstellung. Erstere ist gegeben, wenn ein bestimmtes Rechtsgut vor unbestimmt vielen Gefahren geschützt wird, während zweitere die Überwachung einer bestimmten Gefahrenquelle zum Schutze unbestimmt vieler Rechtsgüter erfasst.[41]

Der CISO ist verpflcihtet ein Rechtsgut – die digitalen Assets des Unternehmens, mit dem er vertraglich verbunden ist – vor Gefahren zu schützen. Diese Gefahren sind digitale Angriffe, welche von einer Vielzahl von Tätern und auf verschiedene Arten ausgeführt werden. Damit kommt nur eine Obhutsgarantenstellung in Frage.

Ein Arbeitnehmer kann Garant aufgrund seines Arbeitsvertrags sein, wenn die entsprechenden Kompetenzen delegiert werden. Massgeblich ist die tatsächliche Herrschaft und Verantwortung für die Gefahrenquelle.[42] Eine pauschale Garantenstellung rein aufgrund seiner Treuepflicht wird wegen der Voraussetzung einer qualifizierten Rechtspflicht abgelehnt.[43] Ist der CISO nicht Teil der Geschäftsleitung, so ist sein Verhältnis zum Unternehmen ein arbeitsrechtliches. Fraglich ist dann, ob ihm als Arbeitnehmer die Verantwortung über die digitalen Assets delegiert wurde beziehungsweise delegiert werden kann.

Für die Garantenstellung spricht, dass er bei der Auswahl und Implementierung der Sicherheitstechnologien mithilft und Cybersicherheitsprozesse überwacht.[44] Er hat somit eine tatsächliche Möglichkeit einzugreifen und das Unternehmen zu schützen. Allerdings ist er nicht die einzige Person, welche für die Implementierung verantwortlich ist, und dies ist nur ein Teil seiner vielen Aufgaben.

Dagegen spricht vor allem die gesetzlich geregelte Verantwortung des Verwaltungsrats. Gemäss Art. 716a Abs. 1 OR gehören zu den unübertragbaren Aufgaben des Verwaltungsrats die Oberleitung der Geschäftsleitung (Ziff. 1), die Festlegung der Organisation (Ziff. 2) und die Ausgestaltung der Finanzkontrolle sowie Finanzplanung (Ziff. 3).

Die Oberleitung umfasst unter anderem die Implementierung eines Risikomanagements.[45] Die Risiken resultierend aus Cybervorfällen vermehren sich mit der schnellen und teils rechtlich unkontrollierten Entwicklung

41 Zum Ganzen: BGE 113 IV 68 E. 5b; Stratenwerth Strafrecht AT I, § 14 Rn. 13; Trechsel/Noll/Pieth Strafrecht AT I, S. 238 f.
42 BGer 6B_405/2013 vom 19. Mai 2014 E. 1.3.2.
43 BGE 113 IV 68 E. 6a; Donatsch/Godenzi/Tag Strafrecht I, S. 329.
44 CISO-Alliance Berufsbild CISO, S. 7; Kaspersky Lab What it Takes to Be a CISO, S. 5.
45 Watter/Pellanda BSK OR, Art. 716a Rn. 6; vgl. Hunziker/Trachsel EXPERTfocus, S. 613.

neuer Technologien.[46] Dies ist auch ersichtlich aus der stetig wachsenden Cyberkriminalität und den vermehrten Meldungen von Cybervorfällen.[47] Die Privatwirtschaft nennt heutzutage Cyber-Spionage und -Krieg als fünfthöchstes beziehungsweise langfristig als vierthöchstes Risiko.[48] Cyberrisiken müssen somit ohne Zweifel im Risikomanagement berücksichtigt werden.[49] Dadurch gehören Themen wie Cybersicherheitsmassnahmen und Risikoappetit bezüglich Cyberrisiken zu den unübertragbaren Aufgaben des Verwaltungsrats.[50]

In Fällen, in denen die Verantwortlichkeit intern nicht geregelt oder unklar ist, haftet auch wiederum der Verwaltungsrat für die ungenügende Festlegung der Organisation. Schliesslich spricht auch die Verantwortlichkeit über die Finanzplanung für eine Verantwortlichkeit für Cybersicherheit. Da Cybervorfälle hohe finanzielle Schäden mit sich ziehen können und Massnahmen ein gewisses Budget benötigen, müssen diese auch bei der Ausarbeitung einer Finanzplanung mitberücksichtigt werden.[51] All dies weist darauf hin, dass die Verantwortlichkeit nicht an den CISO delegiert werden kann.

Weiter wird in einem Rundschreiben der FINMA die Ausgestaltung einer geeigneten Technologieinfrastruktur explizit als Aufgabe der Geschäftsleitung genannt.[52] In einem anderen Rundschreiben wird die Genehmigung und Überwachung von Strategien für den Umgang mit Cyber-Risiken dem Oberleitungsorgan auferlegt.[53] Zudem wird die Geschäftsleitung dazu verpflichtet, Verwundbarkeitsanalysen und Penetrationstests durchführen

46 Vgl. WEF Global Risk Report, S. 38 f., 54.

47 BFS Digitale Kriminalität; BFS Gemeldete Cyber-Vorfälle: Wobei beachtet werden muss, dass auch andere Faktoren, wie beispielsweise eine erhöhte Sensibilisierung der Bevölkerung bezüglich Cybersicherheit, das Meldeverhalten beeinflussen können; FINMA Aufsichtsmitteilung 03/2024, S. 3.

48 WEF Global Risk Report, S. 17, 46: Zusätzlich nannten 2024 71 % von befragten Chief Risk Officers Cyberrisiken als grosse Bedrohung für ihre Unternehmen.

49 So auch BWL Minimalstandard, S. 5; FINMA Aufsichtsmitteilung 03/2024, S. 6; FINMA Rundschreiben 2023/1, Rz. 23.

50 So auch CISO-Alliance Berufsbild CISO, S. 5, 7, wonach die «Responsibility» an den CISO delegiert wird, jedoch die «Accountability» bei der Organisationsleitung bleibt und der CISO keine Risikoentscheidungen trifft; Hunziker/Trachsel EXPERTfocus, S. 613.

51 Vgl. Kaspersky Lab What it Takes to Be a CISO, S. 19: CISOs arbeiten auch mit Finanzabteilungen zusammen.

52 FINMA Rundschreiben 2017/1, Rz. 50.

53 FINMA Rundschreiben 2023/1, Rz. 24.

zu lassen.[54] Zwar sind beide Rundschreiben nur für gewisse Branchen anwendbar,[55] jedoch kann die darin festgehaltene Pflichtenverteilung für Unternehmen, welche die gleiche Gesellschaftsform nutzen, als Anhaltspunkt berücksichtigt werden.

Für die strafrechtliche Verantwortlichkeit ist zwar nach wohl herrschender Lehre nicht massgeblich, ob der Vertrag zivilrechtlich gültig ist, sondern nur die faktische Übernahme.[56] Diese wird im Einzelfall geprüft werden müssen. Jedoch ist die zivilrechtliche Undelegierbarkeit ein starkes Indiz für die tatsächliche Organisation. Grundsätzlich ist somit eine Garantenstellung aus Vertrag abzulehnen.

III. Garantenstellung aus Ingerenz

Die Garantenstellung nach Art. 11 Abs. 2 lit. d StGB verpflichtet diejenige Person, die eine Gefahr schafft oder vergrössert dazu, alle zumutbaren Massnahmen zu ergreifen, um die Gefahr abzuwenden.[57] Da eine solche Situation schnell entstehen kann, wird in der Lehre für Zurückhaltung plädiert.[58] Kein Garant ist unter anderem derjenige, deren Handlung die zulässige Risikogrenze nicht überschritten hat.[59] Zudem wird die Garantenstellung durch die Eigenverantwortung des Gefährdeten eingeschränkt.[60]

Eine Garantenstellung des CISO aus Ingerenz ist denkbar, wenn der CISO eine Sicherheitslücke trotz deren Kenntnis nicht beseitigt beziehungsweise keine weitere Person zur Beseitigung auffordert. Dabei muss unterschieden werden zwischen Lücken, die der CISO selbst durch mangelhafte Cybersicherheitsmassnahmen herbeigeführt hat und Lücken, die nicht durch sein Verhalten entstanden sind.

---

54 FINMA Rundschreiben 2023/1, Rz. 69.

55 FINMA Rundschreiben 2017/1, Rz. 1; FINMA Rundschreiben 2023/1, Rz. 2.

56 Donatsch/Godenzi/Tag Strafrecht I, S. 330; Stratenwerth Strafrecht AT I, § 14 Rn. 18 f.; Trechsel/Noll/Pieth Strafrecht AT I, S. 242; a.M. Von Rotz Garantenstellung des Compliance Officers, S. 94.

57 BGE 134 IV 255 E. 4.2.2; Niggli/Muskens BSK StGB, Art. 11 Rn. 92.

58 Niggli/Muskens BSK StGB, Art. 11 Rn. 95; Stratenwerth Strafrecht AT I, § 14 Rn. 22.

59 BGE 134 IV 255 E. 4.2.2; Donatsch/Forster/Schwarzenegger Strafrecht/Roxin, S. 558, 560 f.; Stratenwerth Strafrecht AT I, § 14 Rn. 24 f.

60 Donatsch/Forster/Schwarzenegger Strafrecht/Roxin, S. 562 f.; Donatsch/Godenzi/Tag Strafrecht I, S. 333; Stratenwerth Strafrecht AT I, § 14 Rn. 25; Trechsel/Noll/Pieth Strafrecht AT I, S. 245 f.

Ist eine Sicherheitslücke auf die Handlung des CISO zurückzuführen, hat er die Gefahr geschaffen. Somit könnte potenziell eine Garantenstellung für ihn bejaht werden, wonach er verpflichtet wäre, alle geeigneten Massnahmen zu treffen, um die adäquat kausalen Folgen der Untätigkeit zu verhindern.[61]

Lehre und Rechtsprechung befürworten teils eine auf dem Vertrauensgrundsatz basierende Sichtweise, wonach darauf vertraut werden kann, dass Dritte sich rechtmässig verhalten.[62] Demnach könnte der CISO darauf vertrauen, dass Cyberkriminelle die Sicherheitslücke nicht ausnutzen werden, wodurch er keine Garantenstellung hätte. Gegen die Anwendbarkeit des Grundsatzes in diesem Fall scheint zunächst das hohe Volumen von Cyberangriffen zu sprechen. Da eine grosse Anzahl von Unternehmen betroffen ist, besteht ein hohes Risiko einer Cyberattacke. Auf der anderen Seite ist jedoch auch eine grosse Menge von Sicherheitslücken festzustellen, welche zwar existieren, aber noch nicht für Angriffe benutzt wurden.[63] Nur weil eine Lücke besteht, wird diese folglich nicht zwingend ausgenutzt werden. Der Vertrauensgrundsatz kann somit durchaus Grund für die Verneinung einer Garantenstellung sein.

Wenn eine höhere leitende Person über die Sicherheitslücke benachrichtigt wird – dies kann der CIO oder der Verwaltungsrat sein –, muss zudem die Eigenverantwortung dieser Person berücksichtigt werden. Wird von ihr nichts getan, um die Lücke zu schliessen, beispielsweise durch Beauftragung externer Hilfskräfte oder Zuteilung weiterer Ressourcen, muss bei einer Cyber-Attacke die Garantenstellung des CISO verneint werden.

Die Eigenverantwortung des Unternehmens kann die Garantenstellung des CISO auch ausschliessen, wenn er sich innerhalb der vorgegebenen Risikogrenze hält. Der Risikoappetit – der Umfang der tolerierten Cyberrisiken – soll von der Organisationsleitung im Rahmen des Risikomanagements definiert werden.[64] Hält sich der CISO mit seinen Handlungen innerhalb dieses Rahmens, wird keine Garantenstellung begründbar sein, da vorrangig das Unternehmen hierfür die Verantwortung übernehmen muss.

---

61 BGE 134 IV 255 E. 4.2.2 Trechsel/Noll/Pieth Strafrecht AT I, S. 244.

62 BGE 120 IV 300 E. 3d.bb; Donatsch/Forster/Schwarzenegger Strafrecht/Roxin, S. 558 f.; vgl. auch Donatsch/Godenzi/Tag Strafrecht I, S. 369 f.

63 Donzé/Humbel/Plüss NZZ am Sonntag, S. 11: Im Juni 2023 zählten Sicherheits-Scans 106'000 Server mit Sicherheitslücken im Schweizer Netz.

64 BWL Minimalstandard, S. 6; FINMA Rundschreiben 2023/1; Hunziker/Trachsel EXPERTfocus, S. 613.

Zu beachten ist weiter, wie die Sicherheitslücke zustande kam. Denkbar ist, dass der CISO eine Sicherheitsmassnahme implementierte, um eine Lücke zu reparieren, wodurch jedoch an einer anderen Stelle erneut eine Sicherheitslücke entstand. In diesem Fall stellt sich die Frage, ob die zulässige Risikogrenze überschritten wurde. Wenn zuvor genügende Tests gemacht wurden und diese Folge unvorhersehbar war, kann argumentiert werden, dass eine solche Konsequenz als inhärentes Risiko der IT-Infrastruktur zu dulden ist und die zulässige Risikogrenze folglich nicht übertreten wurde.

Ist die Schaffung der Sicherheitslücke nicht auf den CISO zurückzuführen, beispielsweise weil ein verwendetes Programm nach einer Aktualisierung nicht mehr sicher ist, stellt sich die Frage, ob das reine Aufrechterhalten auch eine Garantenstellung begründet. Dafür könnte die Bejahung der Garantenstellung von Skiliftunternehmen, welche Massnahmen vor Naturgefahren vorkehren müssen, sprechen.[65] Die Gefahr in Form einer Lawinengefahr an sich wurde nicht vom Unternehmen selbst geschaffen. Im Urteil wird das Schaffen der Gefahr durch das Unternehmen darin gesehen, dass es Skipisten in einem Gebiet erstellt, wo eine Naturgefahr herrscht. Dies ist jedoch nicht vergleichbar mit der Situation eines CISO. Zwar hat er sich dafür entschieden, ein digitales Mittel zu benutzen, das Cybergefahren bergen könnte, aber dies wird aufgrund der Natur einer sich schnell entwickelnden Cybersicherheitsindustrie bei jeder Option der Fall sein. Das Skiliftunternehmen hätte in Theorie die Alternative, Skipisten an einem anderen Ort ohne Lawinengefahr zu eröffnen oder weniger Pisten zu erstellen, wodurch keine Gefahr geschaffen werden würde. Der CISO, der einer Geschäftsführung unterstellt ist, kann jedoch nicht eigenhändig entscheiden, keine digitalen Dienstleistungen anzubieten.

Gegen die Begründung der Garantenstellung durch reines Aufrechterhalten einer Gefahr spricht der Gesetzeswortlaut, der nur die Schaffung dieser Gefahr nennt. Eine solche Ausdehnung des Wortlautes würde zu einer uferlosen Strafbarkeit führen, wobei das Einhalten des Bestimmtheitsgebots problematisch wäre. Auch die Rechtsprechung impliziert, dass ein reines Aufrechterhalten nicht genügt, indem eine Garantenstellung ausgeschlossen ist, wenn die Person die Gefahr weder schuf noch erhöhte.[66] Der CISO kann also kein Garant sein, wenn die Entstehung der Sicherheitslücke nicht ihm zuzurechnen ist.

65 BGE 115 IV 189 E. 3a.
66 BGE 134 IV 255 E. 4.2.2.

IV. Geschäftsherrenhaftung

Die Geschäftsherrenhaftung kann auch eine Garantenstellung begründen. Trotz fehlender ausdrücklicher gesetzlicher Verankerung ist sie in Lehre und Rechtsprechung etabliert.[67] Allerdings ist in Hinblick auf das Legalitätsprinzip eine engere Auslegung geboten.[68] Bei dieser Haftung wird der Geschäftsherr für eine unter seiner Aufsicht begangene Straftat verantwortlich gemacht, auch wenn er diese nicht aktiv förderte, sondern lediglich nicht verhinderte.[69] Geschäftsherr ist, wer in einem Verantwortlichkeitsbereich des Unternehmens tatsächliche Leitungsaufgaben ausübt.[70]

Zuerst muss geprüft werden, ob der CISO als Geschäftsherr qualifiziert werden kann. Der CISO leitet in vielen Fällen entweder die Informatik- oder die IT-Sicherheitsabteilung.[71] Jedoch ist unklar, inwieweit er tatsächliche Entscheidungsbefugnisse über die Abteilung hat. Grundsätzlich ist seine Aufgabe in erster Linie als Brücke zwischen Informatik und Organisationsleitung zu verstehen. Bei der Ausarbeitung von Informationssicherheitsmassnahmen arbeitet er mit der Abteilung zusammen, was tendenziell auf eine horizontale, nicht vertikale Hierarchie deutet. Zusätzlich untersteht der CISO selbst einer Person, welche unterhalb der obersten Geschäftsführung steht.

So wie seine Position in dieser Arbeit definiert wurde, muss die Stellung des CISO als Geschäftsherr abgelehnt werden. Jedoch kann bei einer anderen hierarchischen Organisation durchaus eine strafrechtliche Geschäftsherrenhaftung in Frage kommen. In Betracht käme dafür beispielsweise die Konstellation, in welcher der CISO in den Verwaltungsrat eingebunden ist.

V. Vergleich zum Compliance Officer

Der Begriff der «Compliance» umfasst «die Einhaltung von gesetzlichen regulatorischen und internen Vorschriften sowie die Beachtung von markt-

67 BGE 96 IV 155 E. II.4a; Donatsch/Godenzi/Tag Strafrecht I, S. 399; Stratenwerth Strafrecht AT I, § 14 Rn. 31; Trechsel/Noll/Pieth Strafrecht AT I, S. 246.
68 BGE 105 IV 172 E. 4a; vgl. auch Stratenwerth Strafrecht AT I, § 14 Rn. 31.
69 BGE 96 IV 155 E. 4a; Stratenwerth Strafrecht AT I, § 14 Rn. 31; Trechsel/Noll/Pieth Strafrecht AT I, S. 249.
70 BGE 113 IV 68 E. 7; BGE 105 IV 172 E. 4a; Stratenwerth Strafrecht AT I, § 14 Rn. 31.
71 Kaspersky Lab What it Takes to Be a CISO, S. 7; vgl. Heidrick & Struggles 2024 Survey, S. 13.

üblichen Standards und Standesregeln».[72] Dazu gehört unter anderem die Verhinderung von strafrechtlichen Taten, begangen durch Organe und Mitarbeiter des Unternehmens.[73]

Die Garantenstellung des Compliance Officers wurde vor Bundesgericht bezüglich der Geldwäscherei nach Art. 305bis StGB bejaht.[74] Die unterlassene Handlung war dabei das Versäumen, verdächtige Vermögenswerte bezüglich ihrer Herkunft zu prüfen sowie diese bei der Geschäftsleitung zu melden.[75] Argumentiert wurde mit den Sorgfaltspflichten nach Art. 3–8 GwG, der Meldepflicht bei Verdacht auf Geldwäscherei gemäss Art. 9 GwG, den Pflichten im EBK-RS 98/1 und den internen Richtlinien der betroffenen Bank.[76] Das Bundesgericht stützte sich dabei auf eine Mindermeinung in der Lehre, weshalb dieser Entscheid stark kritisiert wird.[77]

Die Entscheidungskompetenz des Compliance Officers ist nicht einheitlich geregelt, sondern variiert nach Unternehmen. In einem Urteil, in dem die Verletzung der Meldepflicht in Art. 9 GwG bejaht wurde, gab der Compliance Officer an, dass er nicht angewiesen werden konnte, eine Meldung zu unterlassen.[78] Er war diesbezüglich weisungsfrei und entscheidungsbefugt.[79] Im oben angesprochenen Bundesgerichtsentscheid wurde erwähnt, dass ein Verdachtsfall der Geschäftsleitung zur Entscheidung über die Meldung oder Sperrung der verdächtigen Konten vorgelegt hätte werden müssen.[80] Dies impliziert, dass der Compliance Officer in diesem Fall bezüglich der Meldung nicht alleine entscheidungsbefugt war. Eine so grosse Entscheidungsmacht wie im ersten Fall ist beim CISO zu verneinen, da dieser nicht zu weitreichenden Entscheidungen befugt ist. Stattdessen nähert sich die Position des CISO der des Compliance Officers im zweiten Fall an, in dem solche Entscheidungen der Geschäftsleitung vorgelegt werden müssen.

72 FINMA Rundschreiben 2017/1, Rz. 7.
73 Nagel SJZ 117/2021, S. 104; Pieth Wirtschaftsstrafrecht, S. 77; Von Rotz Garantenstellung des Compliance Officers, S. 12.
74 BGE 136 IV 188 E. 6.2.2.
75 BGE 136 IV 188 E. 6.3.4.
76 BGE 136 IV 188 E. 6.2.1.1 ff.
77 Übersicht der verschiedenen Kritikpunkte in BGE 136 IV 188 E. 6.2.1; Von Rotz Garantenstellung des Compliance Officers, S. 172 f.
78 BStGer SK.2019.55 vom 28.7.2020 E. 2.3.21, 2.4.2.2.
79 BStGer SK.2019.55 vom 28.7.2020 E. 2.4.2.2.
80 BGE 136 IV 188 E. 6.3.2.

In den oben angesprochenen Urteilen wurde mit der gesetzlichen Meldepflicht nach Art. 9 GwG argumentiert. Fraglich ist, ob eine ähnliche Pflicht für den CISO bestehen könnte.

Gemäss Art. 29 Abs. 2 FINMAG müssen die Beaufsichtigten der FINMA unverzüglich Vorkommnisse melden, die für die Aufsicht von wesentlicher Bedeutung sind. Die FINMA konkretisierte, dass damit auch eine Meldepflicht von erfolgreichen Cyberattacken besteht, soweit sie wesentlich sind.[81] Zu ermitteln ist zunächst, wer verantwortlich für die Meldung ist.

Die Bestimmung im FINMAG nennt nur «Die Beaufsichtigten», aber nicht, wer innerhalb eines Unternehmens diese Meldung erstatten muss. In der Botschaft wird für juristische Personen erwähnt, die Organe seien Adressaten der Meldepflicht.[82] Die Botschaft führt auch aus, dass dieser Artikel dem damals geltenden Art. 47 Abs. 3 aVAG entspreche.[83] Demnach musste die Geschäftsleitung des Unternehmens die Aufsichtsbehörde informieren. Daraus ergibt sich, dass der CISO nicht Adressat der Meldepflicht ist. Eine gleichartige gesetzliche Meldepflicht wie die nach Art. 9 GwG ist für den CISO nicht ersichtlich.

Ein Unterschied zwischen dem CISO und Compliance Officer liegt im Umfang der Gefahren. Bei Cyberkriminellen handelt es sich um eine grosse Menge von bösartigen Angreifern, die unermüdlich und kontinuierlich versuchen, einen Angriff durchzuführen. Aufgrund der schnellen Entwicklung im IT-Bereich muss sich der CISO auf eine grosse Variation von Angriffen und neuen Technologien vorbereiten. Der Compliance Officer dagegen wird selten auf «Angreifer» stossen, welche im gleichen Mass konstant auf die Verletzung des Unternehmens zielen. Vielmehr handelt es sich mehrheitlich um fahrlässig oder eventualvorsätzlich handelnde Täter, welche nicht die gleichen Mittel und die Zielstrebigkeit wie Cyberangreifer haben. Einem Compliance Officer kann es daher eher zugemutet werden, einen strafrechtlich relevanten Vorfall zu verhindern.

Ein weiterer Vergleichspunkt ist die Interessenslage der beiden Positionen. Der Compliance Officer wird teilweise gegen die Interessen der Geschäftsleitung handeln müssen. Hält sich ein Unternehmen beispielsweise aus Vermögensinteressen nicht an gesetzliche Vorgaben, muss der Compliance Officer trotz Druck der Geschäftsleitung Meldung bei den

81 FINMA Aufsichtsmitteilung 05/2020, S. 2.
82 Botschaft 2006, S. 2880.
83 Botschaft 2006, S. 2880.

Behörden erstatten.[84] Der Compliance Officer hat damit auch eine Aufdeckungs- und Überwachungsfunktion bezüglich Handlungen der Geschäftsleitung.[85] Eine solche Aufdeckungsfunktion ist beim CISO zu verneinen. Jedes Unternehmen hat grundsätzlich ein Interesse daran, Cyberangriffe zu verhindern, um Schäden abzuwenden. Auch wenn die Geschäftsleitung vereinzelt nicht die konkreten Vorschläge des CISO gutheisst, wird sie trotzdem ihr Gesamtinteresse mit dem des CISO teilen. Dies ermöglicht, dass die Unternehmensleitung selbst die Verantwortlichkeit trägt.

Der CISO und der Compliance Officer können je nach Fall eine ähnliche Entscheidungsmacht haben. Zudem können für beide interne Richtlinien bestehen, welche den Officern eine Sorgfaltspflicht vorschreiben. Jedoch sind beim CISO keine gesetzlichen Sorgfalts- oder Meldepflichten erkennbar und es handelt sich um nicht vergleichbare Gefahren. Zusätzlich muss auch berücksichtigt werden, dass die Garantenstellung des Compliance Officers nur bezüglich der Geldwäscherei durch das Bundesgericht bestätigt wurde.[86] Aus diesen Gründen kann die für den Compliance Officer bejahte Garantenstellung nicht analog auf den CISO übertragen werden.

VI. Vergleich zum Datenschutzberater

Der Datenschutzberater kann gemäss Art. 10 Abs. 1 DSG fakultativ durch das Unternehmen eingesetzt werden. Er dient nach Art. 10 Abs. 2 DSG als Anlaufstelle für betroffene natürliche Personen und für Behörden. Seine Aufgaben umfassen insbesondere die Schulung und Beratung des Unternehmens bezüglich Datenschutzes (lit. a) und die Mitwirkung bei der Anwendung der Datenschutzvorschriften (lit. b). Eine Meldepflicht wurde nicht normiert, weshalb er eine rein unterstützende Funktion hat.[87]

Der Datenschutzberater trägt grundsätzlich nicht die alleinige Entscheidungsgewalt und somit auch nicht die Verantwortung für die datenschutzkonforme Datenbearbeitung. Letztere liegt gemäss Botschaft und Lehre weiterhin allein beim verantwortlichen Unternehmen.[88] Während der CI-

84 Vgl. Nagel SJZ 117/2021, S. 104 f.
85 Vgl. Von Rotz Garantenstellung des Compliance Officers, S. 31 f.
86 Vgl. Von Rotz Garantenstellung des Compliance Officers, S. 176: Die allgemeine Garantenstellung bleibt ungeklärt.
87 Balthasar OK DSG, Art. 10 Rn. 26 f.; Sury OFK DSG, Art. 10 Rn. 1.
88 Zum Ganzen: Botschaft 2017, S. 7033; Balthasar OK DSG, Art. 10 Rn. 29; a.M. Sury OFK DSG, Art. 10 Rn. 32 f.

SO etwas mehr Entscheidungsmacht hat als der Datenschutzberater, trägt das Unternehmen auch gegenüber dem CISO die Verantwortung für grössere Entscheidungen.[89] Nur innerhalb des Bereichs der Cybersicherheit ist er entscheidungsbefugt. In diesem Sinne sind die beiden Rollen daher vergleichbar.

Der Datenschutzberater muss gemäss Art. 10 Abs. 3 DSG lit. a fachlich unabhängig und weisungsungebunden sein. Dies wird in lit. b unterstrichen mit dem Verbot, andere Tätigkeiten auszuüben, welche unvereinbar mit der Aufgabe als Datenschutzberater sind. Grund dahinter ist die Vermeidung eines Interessenkonflikts. Die Lehre bejaht unter anderem einen Interessenkonflikt, wenn der Berater zugleich Leiter der IT-Abteilung ist.[90] Die Botschaft nennt als erlaubte Nebentätigkeit explizit den Informationssicherheitsbeauftragten.[91] Der CISO ist als Arbeitnehmer weisungsgebunden. Er schuldet seinem Arbeitgeber eine Treuepflicht nach Art. 321a Abs. 1 OR und muss seine Weisungen gemäss Art. 321d Abs. 2 OR befolgen. Dies wirkt sich auf die Beurteilung der Garantenstellung aus. Je nach Einzelfall wird diese Abhängigkeit zwar mehr oder weniger zum Vorschein kommen. Im Allgemeinen handelt es sich hierbei aber um einen grossen Unterschied zum Datenschutzberater.

Der Datenschutzberater dient gemäss Gesetzeswortlaut und in Anbetracht des Zwecks des DSG primär zum Schutz des Betroffenen. Auch die vorausgesetzte Unabhängigkeit deutet daraufhin, dass er – auch wenn er vom Unternehmen angestellt wird – nicht die Interessen des Unternehmens zu vertreten hat, sondern die derjenigen Personen, deren Daten bearbeitet werden. Der CISO vertritt im Gegensatz dazu primär die Interessen des Unternehmens. In seiner Funktion soll er schwere Folgen von Cyberangriffen verhindern. Primär stimmt das Interesse der Betroffenen, ihre Personendaten zu schützen, mit dem des Unternehmens, einen Reputationsschaden zu verhindern, überein. Daher bestätigt mutmasslich die Botschaft auch eine Vereinbarkeit der beiden Positionen. Jedoch dient der CISO auch beispielsweise zum Schutz vor finanziellen Schäden, was vorrangig ein Unternehmensinteresse darstellt. So verfolgt der CISO nicht vollständig deckungsgleiche Ziele wie der Datenschutzberater.

89 Siehe § 1.

90 Balthasar OK DSG, Art. 10 DSG Rn. 34; vgl. auch CISO-Alliance Berufsbild CISO, S. 5.

91 Botschaft 2018, S. 7033 f.

Eine Analogie zwischen dem Datenschutzberater und dem CISO ist aufgrund der unterschiedlichen Abhängigkeitsgraden und Interessensetzungen nicht möglich. Sie haben jedoch eine ähnliche Position hinsichtlich der Entscheidungsmacht und sind beide mit den Herausforderungen der Datensicherheit und damit dem IT-Bereich konfrontiert. Im Gegensatz zum Compliance Officer haben sie auch keine gesetzlichen Meldepflichten. Der Vergleich zum Datenschutzberater ist somit geeigneter als der zum Compliance Officer.

C. Weitere Voraussetzungen der unechten Unterlassung

Selbst wenn eine Garantenstellung zu bejahen wäre, müssten, wie oben im Kapitel § 3 A. aufgezeigt, weitere Voraussetzungen für die Strafbarkeit erfüllt sein. Nachfolgend werden die Tatmacht und der subjektive Tatbestand – zwei Voraussetzungen, deren Bejahung im Falle des CISO problematisch sein könnte – näher analysiert.

I. Tatmacht

Die Tatmacht setzt voraus, dass die gebotene Handlung, um den tatbestandsmässigen Erfolg abzuwenden, dem Täter möglich sein musste.[92] Das Vorhandensein der Tatmacht wird stark vom Einzelfall abhängen. Trotzdem können gewisse Pauschalisierungen gemacht werden.

In vielen Fällen wird die Tatmacht aufgrund fehlender Ressourcen wegfallen. Hat der CISO keine finanziellen oder personellen Mittel, um eine Sicherheitslücke zu schliessen oder diese gar zu bemerken, wird es ihm nicht möglich sein, einen Cyberangriff zu verhindern. Da das Gebiet der Cybersecurity neu ist, werden die finanziellen Ausgaben im Zusammenhang mit der Cybersicherheit nicht genügend im Budget des Unternehmens berücksichtigt.[93] Dazu kommt, dass Cybersicherheit oft als Teil der Infor-

92 Donatsch/Godenzi/Tag Strafrecht I, S. 338; Niggli/Muskens BSK StGB, Art. 11 Rn. 120; Stratenwerth Strafrecht AT I, § 14 Rn. 41.

93 Heidrick & Struggles 2024 Survey, S. 27: 41 % der CISOs verneinen, dass ihnen genügend Ressourcen zur Verfügung gestellt werden; Hunziker/Trachsel EXPERTfocus, S. 615; vgl. Proofpoint 2024 Report, S. 14: Die Mehrheit der ca. 1600 befragten CISOs berichten abnehmende Budgets für die Cybersicherheit aufgrund negativer Wirtschaftsentwicklungen.

matik gesehen wird und damit lediglich einen kleinen Teil des Gesamtbudgets für die Informatik erhält.[94] Selbst der Schweizer Bund räumt nur ein bescheidenes Budget für die eigene Cybersicherheit ein.[95] Aber auch wenn genügend finanzielle Mittel zur Verfügung gestellt werden, fehlt oft fachkundiges Personal, welches eingestellt werden kann, um den CISO zu unterstützen.[96]

Des Weiteren stellen Cyberbedrohungen ein neueres Phänomen dar, wobei die Täter teils höchst professionell arbeiten und viele Ressourcen zur Verfügung haben.[97] Für diese Einzeltäter, Organisationen oder gar staatlich unterstützten Akteure stellt das Ausnutzen von Sicherheitslücken ihre Haupttätigkeit dar, wodurch sie sich schnell weiterentwickeln und effektiv handeln können. Im Gegensatz dazu haben CISOs eine Vielzahl von Aufgaben, welche sie erfüllen, und sie müssen antizipierend handeln. Die Effizienz der Cyberkriminellen zeigt sich auch an der grossen Menge von erfolgten Cyberangriffen.[98] Aufgrund der hohen Anzahl ist es unmöglich, jede einzelne Sicherheitslücke zu schliessen.[99] Sogar staatliche Institutionen werden davon betroffen und können Opfer solcher Angriffe sein.[100] Wenn selbst Staaten überfordert sind, werden sicherlich CISOs von privaten Unternehmen nicht in der Lage sein, sämtliche Angriffe zu verhindern.[101]

Schliesslich ist auch zu beachten, dass der CISO nicht Kontrolle über alle Faktoren hat, welche zu erfolgreichen Cyberangriffen führen können. Häu-

94 FINMA Aufsichtsmitteilung 03/2024, S. 5; Wipro State of Cybersecurity, S. 23: 13 % der europäischen Organisationen ordnen über 12 % des Informatikbudgets der Cybersicherheit zu.

95 Donzé/Humbel/Plüss NZZ am Sonntag, S. 11.

96 Kaspersky Lab What it Takes to Be a CISO, S. 15 f.; vgl. auch Heidrick & Struggles 2024 Survey, S. 23; Wipro State of Cybersecurity, S. 17.

97 NCSC Allgemeine Bedrohungsformen, S. 3 ff.

98 BACS Halbjahresbericht 2024/I, S. 6; BFS Digitale Kriminalität.

99 Vgl. Donzé/Humbel/Plüss NZZ am Sonntag, S. 11.

100 BACS Halbjahresbericht 2024/I, S. 34 ff.: Im Kontext der Europawahlen beispielsweise fanden 2024 erfolgreiche Cyberangriffe auf Websites niederländischer und deutscher Parteien statt. 2022 und 2023 verschafften sich Cybertäter Zugriff auf das niederländische Verteidigungsministerium und 2024 wurden E-Mail-Konten französischer diplomatischer Einrichtungen kompromittiert. Auch Schweizer Parlamentarier waren 2021 betroffen; vgl. WEF Global Risk Report, S. 30, 90: Die Schweiz nannte Cyberunsicherheit – gemeint werden Risiken wie beispielsweise Cyber-Spionage – als fünfthöchste Bedrohung.

101 Vgl. auch Kaspersky Lab What it Takes to Be a CISO, S. 11: 86 % der befragten CISOs halten Verletzungen der Cybersicherheit für unvermeidlich; Proofpoint 2024 Report, S. 4 f.: 70 % der CISOs fühlen sich in den nächsten 12 Monaten dem Risiko eines Cyberangriffs ausgesetzt.

fige Attacken sind solche, wo Arbeitnehmer des Unternehmens getäuscht werden und dadurch Zugang zum System erlangt wird.[102] Eine grosse Aufgabe des CISO beinhaltet dementsprechend die Schulung der Arbeitnehmer. Aber auch wenn diese durchgeführt wird, ist schlussendlich jeder einzelne Arbeitnehmer dafür verantwortlich, das erlernte Wissen auch umzusetzen. Wird trotz ausreichender Bemühungen des CISO beispielsweise ein E-Mail Link angewählt, hat der CISO keine Tatmacht darüber.

Die Tatmacht wird folglich in den meisten Fällen verneint werden müssen, wodurch die Strafbarkeit des CISO auch aufgrund dieser Voraussetzung ausgeschlossen wird.

II. Subjektiver Tatbestand

Selbst wenn der objektive Tatbestand bejaht wäre, müsste der subjektive Tatbestand erfüllt sein. Die meisten einschlägigen Tatbestände sind nicht unter der Fahrlässigkeit strafbar, weshalb der CISO mindestens mit Eventualvorsatz handeln müsste.[103]

Zur Abgrenzung von der Fahrlässigkeit dient in erster Linie die Willenskomponente. Dabei nimmt ein eventualvorsätzlich handelnder Täter den Erfolg in Kauf, während ein fahrlässig handelnder Täter darauf vertraut, der Erfolg werde nicht eintreten.[104] Gemäss Rechtsprechung muss für die Abgrenzung zwischen Eventualvorsatz und Fahrlässigkeit zusätzlich die Grösse des dem Täter bekannten Risikos der Tatbestandsverwirklichung und die Schwere der Sorgfaltspflichtverletzung berücksichtigt werden.[105]

Das Risiko eines Cybervorfalls ist sehr hoch.[106] Besteht eine Sicherheitslücke, ist wahrscheinlich, dass Cyberkriminelle versuchen werden, diese auszunutzen. Dies ist dem CISO vermutlich bewusst. Eine schwere Sorgfaltspflichtverletzung ist denkbar, wenn ein CISO trotz Kenntnis keine interne Meldung über ein Cyberrisiko, welches er selbst nicht beseitigen kann, erstattet. Tut er dies zwar, aber die Geschäftsleitung bleibt untätig, könnte eine schwere Pflichtverletzung begründet werden, wenn er nicht

102 Proofpoint 2024 Report, S. 9 f.: 42 % der CISOs nennen unvorsichtige Arbeitnehmer, 36 % auch vorsätzlich handelnde Arbeitnehmer als Grund für Datenverlust; vgl. FINMA Aufsichtsmitteilung 03/2024, S. 6 f.

103 Siehe § 3 A.

104 Statt vieler: BGE 96 IV 99.

105 BGE 125 IV 242 E. 3c; BGE 119 IV E. 5a.

106 Vgl. §3 B.II; §3 C.I.

erneut nachfragt.[107] Das Bundesgericht würde in diesen Fällen vermutlich den Eventualvorsatz bejahen.

Eine solche Überdehnung des Vorsatzes erscheint problematisch. Durch die Annahme, die Inkaufnahme sei bei hohem Risiko gegeben, wird die Willenskomponente obsolet. Der CISO wird meistens nicht in Kauf nehmen, dass ein Cyberangriff geschieht. Stattdessen ist es naheliegender, dass er mit dem Gedanken, er habe mehr Zeit, die Sicherheitslücke nicht zeitnah meldet oder handelt. Denn vom reinen Entdecken einer Sicherheitslücke kann nicht auf einen unmittelbaren Cyberangriff geschlossen werden, insbesondere, wenn diese Lücke zuvor bereits länger bestand. Der CISO wird somit mutmasslich darauf vertrauen, dass ein zwischenzeitlicher Angriff ausbleiben wird. Daher wird hier die Meinung vertreten, der subjektive Tatbestand müsste in den überwiegenden Fällen verneint werden.

§ 4 Hinterfragung des Strafbedürfnisses

Das Strafrecht soll eine ultima ratio darstellen. Im Falle einer Sorgfaltspflichtverletzung durch den CISO, welche zu einem Schaden für das Unternehmen führt, kann der CISO bei Bedarf aufgrund seines Vertrags zivilrechtlich zur Haftung gezogen werden. Geschieht dies nicht, muss davon ausgegangen werden, dass das Bedürfnis des Unternehmens fehlt, keine Sorgfaltspflichtverletzung eingetreten ist oder dass der CISO kein Verschulden trägt. Daher ist fraglich, ob eine strafrechtliche Regelung nötig ist.

Besonders bei einer weiten und daher unbestimmten Strafbestimmung wie Art. 11 StGB muss Zurückhaltung geboten werden. Natürlich besteht ein Strafbedürfnis der Öffentlichkeit, die ein Interesse an Datensicherheit hat, der geschädigten Unternehmen und gewissermassen des Staates, da auch dieser Ziel von Cyberangriffen ist. Nur weil der primäre Täter – der Cyberkriminelle selbst – schwierig zu greifen ist, kann jedoch nicht stattdessen eine andere Person als Sündenbock dienen. Es ist Natur eines Rechtsstaats, dass nicht immer jemand strafrechtlich zur Verantwortung gezogen werden kann. Dies im Interesse, dass niemand fälschlicherweise bestraft wird.

Die Argumente, den CISO strafrechtlich verantwortlich zu machen, sind sodann zu stark auf das Resultat – also die Strafbarkeit – ausgerichtet.

107 Vgl. CISO-Alliance Berufsbild CISO, S. 6: Der CISO muss Durchsetzungsvermögen haben.

Die Auslegung des Strafrechts aus der Perspektive, man wolle lediglich ein befriedigendes Ergebnis, ist zu verneinen, da dies eine Überdehnung des in Art. 1 StGB statuierten Legalitätsprinzips bedeutet. Damit wäre nicht mehr voraussehbar, welches Verhalten strafrechtliche Folgen mit sich ziehen kann.

Zuletzt muss der Zweck der strafrechtlichen Bestimmungen betont werden. Anhand des Strafrechts sollen rechtswidrige Cyberangriffe verhindert oder zumindest deren Folgen minimieret werden. Da Cyberattacken aber so häufig sind, müssen CISOs unterstützt werden, anstatt sie durch ein hohes Risiko strafrechtlicher Verurteilungen abzuschrecken. Eine strafrechtliche Verantwortlichkeit des CISO wäre also für die Verhinderung von Cyberangriffen kontraproduktiv und würde sich somit gegen die Zielsetzung des Strafrechts richten.

§ 5 Fazit

Ziel dieses Beitrags war es, die Strafbarkeit des CISO im Rahmen des StGB durch unechte Unterlassung zu analysieren. Aus dem besonderen Teil des StGB wurden vier Tatbestände identifiziert, welche bei einem Cybervorfall relevant sein könnten: Das unbefugte Eindringen in ein Datenverarbeitungssystem, die Sachbeschädigung, die ungetreue Geschäftsbesorgung und die Nötigung.

Die Analyse der Garantenstellung ergab, dass der CISO grundsätzlich keine vertragliche Garantenstellung innehaben kann, da die Verantwortlichkeit für die Cybersicherheit zum Risikomanagement gehört. Dieses ist gemäss Art. 716a Abs. 1 OR eine unübertragbare Aufgabe des Verwaltungsrats. Für die Garantenstellung aus Ingerenz wurde differenziert, ob die Sicherheitslücke auf das Verhalten des CISO zurückzuführen ist. Ist dies zu bejahen, kann man eine Garantenstellung unter anderem aufgrund des Vertrauensgrundsatzes und der Eigenverantwortung des Unternehmens ausschliessen. Das reine Aufrechterhalten einer Lücke, die der CISO nicht zu verantworten hat, begründet auch keine Garantenstellung, da nur die Schaffung oder Erhöhung einer Gefahr strafbar wäre. Weiter wurde die Geschäftsherrenhaftung wegen der fehlenden Geschäftsherreneigenschaft abgelehnt. In den Vergleichen zum Compliance Officer und Datenschutzberater ergab sich schliesslich, dass eine direkte Analogie grundsätzlich nicht möglich ist.

Für die Strafbarkeit ist zusätzlich die Tatmacht nötig. Diese wird regelmässig verneint werden müssen aufgrund des grossen Umfangs der Cyberbedrohungen und aufgrund mangelnder Ressourcen. Somit wird die Strafbarkeit des CISO spätestens hier abgelehnt. Der auch vorausgesetzte Eventualvorsatz würde gemäss Bundesgericht vermutlich bejaht werden, ist nach der hier vertretenen Ansicht aber zu verneinen.

Zuletzt wurde besprochen, ob eine Strafbarkeit des CISO erwünscht wäre. Zwar besteht ein Strafbedürfnis, weil die primären Täter von Cyberangriffen schwer zu fassen sind. Jedoch muss unter anderem beachtet werden, dass eine Strafbarkeit nur zu einem ungewollten Mangel an CISOs führen könnte. Würde eine Strafbarkeit des CISO folglich entgegen der präsentierten Meinung bejaht werden, würde er lediglich als Sündenbock für die Taten von Cyberkriminellen dienen.

Literaturverzeichnis

Bieri Adrian/Powell Julian (Hrsg.), Orell Füssli Kommentar DSG. Kommentar zum Schweizerischen Datenschutzgesetz mit weiteren Erlassen, Zürich 2023.

Brockhaus Annika, IT-Sicherheit, Informationssicherheit und Cyber-Sicherheit: Wo liegen die Unterschiede?, isits AG International School of IT Security 2019, https://www.is-its.org/it-security-blog/it-sicherheit-informationssicherheit-cyber-sicherheit-unterschiede.

Bundesamt für Cybersicherheit (BACS), Halbjahresbericht 2024/I (Januar – Juni). Cybersischerheit: Lage in der Schweiz und International, 2024, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2024-1.html.

Bundesamt für Statistik (BFS), Digitale Kriminalität, BFS-Nummer gr-d-16.04 – 12b-ind, 2024, https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/strategieindikatoren/sicherheit-vertrauen/digitale-kriminalitaet.html.

Bundesamt für Statistik (BFS), Gemeldete Cyber-Vorfälle, BFS-Nummer gr-d-16.04 – 12a-ind, 2024, https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft/strategieindikatoren/sicherheit-vertrauen/cyber-vorfaelle.html.

Bundesamt für wirtschaftliche Landesversorgung (BWL), Minimalstandard zur Verbesserung der IKT-Resilienz, 2023, https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html.

Cybersecurity & Infrastructure Security Agency (CISA), What is Cybersecurity?, 2021, https://www.cisa.gov/news-events/news/what-cybersecurity.

CISO-Alliance, Berufsbild CISO, Ausgabe 03/2024, https://www.ciso-alliance.de/fileadmin/downloads/Berufsbilder/1_-_Berufsbild_CISO_v1.0.pdf.

Donatsch Andreas/Godenzi Gunhild/Tag Brigitte, Strafrecht I. Verbrechenslehre, 10. Aufl., Zürich/Genf 2022.

Donzé René/Humbel Georg/Plüss Mirko, Hackerangriffe: Ungeschützt im Auge des Hurrikans, NZZ am Sonntag vom 18.6.2023, Nr. 25, S.11.

Eidgenössische Bankenkommission, Rundschreiben betreffend Richtlinien zur Bekämpfung und Verhinderung der Geldwäscherei vom 26. März 1998. EBK-RS 98/1 Geldwäscherei, https://www.finma.ch/FinmaArchiv/ebk/d/publik/mitteil/1998/m3-98-2.pdf.

Eidgenössische Finanzmarktaufsicht (FINMA), Aufsichtsmitteilung 03/2024. Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen, 2024, https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03–2024.pdf?sc_lang=de&hash=666EEE255C04FB42F01BFD0BC6C80191.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2023/1. Operationelle Risiken und Resilienz – Banken. Management der operationellen Risiken und Sicherstellung der operationellen Resilienz, 2022, https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023–01–20221207.pdf.

Eidgenössische Finanzmarktaufsicht (FINMA), Aufsichtsmitteilung 05/2020. Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG, 2020, https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05–2020.pdf.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2017/1. Corporate Governance – Banken. Corporate Governance, Risikomanagement und interne Kontrollen bei Banken, 2016, https://www.finma.ch/de/~/media/finma/dokumente/rundschreiben-archiv/2017/rs-17-01/finma-rs-2017-01-20210506_de.pdf?sc_lang=de&hash=7F530363D0237EC203704EFC8E32C624.

Heidrick & Struggles, 2024 Global Chief Information Security Officer Organization and Compensation Survey, 2024, https://www.heidrick.com/-/media/heidrickcom/publications-and-reports/2024-global-ciso-organization-and-compensation-survey.pdf.

Hunziker Stefan/Trachsel Viviane, Cyber Risk Governance in Schweizer Unternehmen. Kernbotschaften einer Studie aus der Sicht von Risk Manager und CISO, EXPERTfocus Dezember 2022, S. 612–616, https://doi.org/10.5281/zenodo.8386970.

Kaspersky Lab, What it Takes to Be a CISO: Success and Leadership in Corporate IT Security, 2018, https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/05/15131106/What-It-Takes-to-Be-a-CISO_-Success-and-Leadership-in-Corporate-IT-Security-2018.pdf.

Mozur Paul, China Appears to Attack GitHub by Diverting Web Traffic, The New York Times vom 30.3.2015, https://www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html?smid=url-share.

Nagel Thomas, Interessenkonflikte des Compliance Officers. Mit besonderer Betrachtung der Meldepflicht nach Art. 9 GwG, SJZ 117/2021, S. 102–109.

Nationales Zentrum für Cybersicherheit (NCSC), Allgemeine Bedrohungsformen, Täter und Werkzeuge, 2021, https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/allgemeine-bedrohungsformen.html.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar. Strafrecht II. Art. 137–392 StGB, Jugendstrafgesetz, 4. Aufl., Basel 2019.

Pieth Mark, Wirtschaftsstrafrecht, Basel 2016.

Proofpoint, Report 2024 Voice of the CISO. Global Insights into CISO Challenges, Expectations and Priorities, 2024, https://nationalcioreview.com/wp-content/uploads/2024/06/pfpt-us-wp-voice-of-the-CISO-report.pdf.

Roxin Claus, Ingerenz und objektive Zurechnung, in Donatsch Andreas/Forster Marc/Schwarzenegger Christian (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte. Festschrift für Stefan Trechsel, Zürich et. al, S. 551–567.

Steiner Thomas/Morand Anne-Sophie/Hürlimann Daniel (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz, 2023, https://doi.org/10.17176/20230825-095533-0, https://doi.org/10.17176/20230812-163522-0.

Stratenwerth Günter, Schweizerisches Strafrecht. Allgemeiner Teil I: Die Straftat, 5. Aufl., Bern 2024.

Stratenwerth Günther/Bommer Felix, Schweizerisches Strafrecht. Besonderer Teil I: Straftaten gegen Individualinteressen, 8. Aufl., Bern 2022.

Trechsel Stefan/Noll Peter/Pieth Mark, Schweizerisches Strafrecht Allgemeiner Teil I. Allgemeine Voraussetzungen der Strafbarkeit, 7. Aufl., Zürich et al. 2017.

Von Rotz Madeleine, Die Garantenstellung und die Garantenpflicht des Compliance Officers einer Bank unter Berücksichtigung der strafrechtlichen Bestimmungen des Finanzmarktrechts, Zürich 2019.

Watter Rolf/Vogt Hans-Ueli (Hrsg.), Basler Kommentar. Obligationenrecht II. Art. 530–964 OR inkl. Schlussbestimmungen, 6. Aufl., Basel 2024.

Wipro, State of Cybersecurity Report. Cyber Resilience in an Age of Continuous Disruption, 2023, https://www.wipro.com/cybersecurity/state-of-cybersecurity-report-2023/.

Woodtli Nadine, Cyberattacken nehmen zu. So brutal erpressen Hacker Schweizer Firmen, SRF vom 13.10.2021, https://www.srf.ch/news/schweiz/cyberattacken-nehmen-zu-so-brutal-erpressen-hacker-schweizer-firmen.

World Economic Forum (WEF), The Global Risks Report 2025. 20th Edition. Insight Report, 2025, https://www.weforum.org/publications/global-risks-report-2025/.

Materialienverzeichnis

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff., https://www.fedlex.admin.ch/eli/fga/2017/2057/de.

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 1. Februar 2006, BBl 2006 2829 ff., https://www.fedlex.admin.ch/eli/fga/2006/303/de.

Zur Kriminalisierung politischer Desinformation

Lukas Staffler

Politische Desinformation im digitalen Raum stellt eine wachsende Bedrohung für demokratische Prozesse dar. Der Beitrag beleuchtet aktuelle Beispiele und analysiert die Mechanismen hinter Viralität und Empörungsökonomie. Er diskutiert, ob und wie strafrechtliche Massnahmen gegen manipulativ lancierte Falschinformationen angemessen sein können. Dabei wird eine grundlegend und vergleichend angelegte Analyse verfolgt, die rechtsvergleichende Beispiele etwa aus Österreich, Deutschland und Italien einbezieht, jedoch insbesondere mit Blick auf die verfassungsrechtlichen und strafrechtlichen Rahmenbedingungen der Schweiz argumentiert. Es wird aufgezeigt, dass prozedurale Ansätze wie Transparenzpflichten strafrechtlichen Verboten vorzuziehen sind.

Einleitung

Im Zeitalter der Informationsgesellschaft[1], in dem Daten zum wichtigsten Rohstoff und Informationen zu den wertvollsten Gütern zählen,[2] erscheint gerade das Phänomen politischer Desinformation für demokratische Rechtsstaaten als vitale Bedrohung[3]. Desinformation, also «*die absichtliche Erstellung und Weitergabe falscher und/oder manipulierter Informationen, die darauf abzielen, das Publikum zu täuschen und in die Irre zu führen, sei es, um Schaden anzurichten, sei es, um politischen, persönlichen*

1 Zum Begriff der Informationsgesellschaft, der das kommunikative Zusammenwirken gesellschaftlicher Kräfte auf der Grundlage von Informations- und Kommunikationstechnologien beschreibt, s. bereits Mayer-Schönberger (2001), 383 ff.; überblicksweise bei Steinbicker (2011), 7 ff. und passim; lesenswert – im Zusammenhang mit der fortschreitenden Digitalisierung und Algorithmisierung – im Übrigen Nassehi (2019), passim sowie Gille et. al. (2024), 136.

2 So etwa Schünemann (2019), 620; s.a. Staffler (2018), 269.

3 Analytisch zum Gefährdungspotential von Desinformation bei Baade (2023), 409 ff.

oder finanziellen Gewinn zu erzielen»,[4] wird das Potential zugeschrieben, nicht nur den demokratischen Diskurs zeitnahe vor einem Wahlereignis akut zu «vergiften», sondern die Diskursfähigkeit des *demos* insgesamt und nachhaltig zu beeinträchtigen.[5]

Angesichts dieses Phänomens, das weltweit auf dem Vormarsch ist, spricht der US-amerikanische Soziologe und Politikwissenschaftler Larry J. Diamond von einer Phase «*demokratischer Rezession*».[6] Wozu Desinformation führen kann, zeigte sich beim Sturm auf das US-Kapitol vom 6. Januar 2021, dem die beharrliche Lüge über den gestohlenen Wahlsieg bei der US-Präsidentschaftswahl von 2020 des damaligen Amtsinhabers Donald Trump voranging.[7]

Dabei ist zu berücksichtigen, dass Desinformation längst nicht mehr nur als Problem der gesellschaftlichen Kommunikation oder der Medienverantwortung gesehen wird, sondern zunehmend auch als sicherheitsrechtliche Herausforderung. Im erweiterten Verständnis moderner Cybersicherheit umfasst dieser Begriff nicht nur den Schutz technischer Infrastrukturen, sondern auch die Resilienz demokratischer Prozesse gegenüber gezielten Informationsangriffen. Denn Desinformation zielt auf die «kognitive Sphäre» digital vernetzter Gesellschaften, sie gefährdet das Vertrauen in öffentliche Kommunikation, destabilisiert die politische Willensbildung und kann, insbesondere im Kontext orchestrierter Kampagnen staatsnaher Akteure, als Teil hybrider Einflussnahme verstanden werden. Cybersicherheit bedeutet in diesem Zusammenhang nicht nur Systemschutz, sondern auch Schutz vor strategischer Manipulation in digitalen Öffentlichkeiten. Der strafrechtliche Umgang mit politischer Desinformation ist daher nicht zu-

4 So lautet die Definition des UK House of Commons, Disinformation and ‚fake news': Government Response to the Committee's Fifh Report of Session 2017–19, 23 Oktober 2018, HC 1630 Government response to Interim Report, Bericht vom 23. Oktober 2018, 2 („*In our work we have defined disinformation as the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain*"); für weitergehende Überlegungen zum Begriff der Desinformation s. Baade (2023), 404 ff.; Baade (2022), 201; Frattolillo (2021), 214, 217; Zimmermann/Kohring (2018), 526, 527 ff.

5 Instruktiv Baade (2023), 399, 403 ff. sowie die Beiträge in Uhle (2018) und Hueso (2021) 121 ff.

6 Diamond (2015), 141 ff.

7 Überblicksweise bei Keil (2022), 13, 46; ausführliche Rekonstruktion der Ereignisse vom 6. Januar 2021 bei Haberman (2022) sowie Thiele (2022), 1 ff.

letzt auch eine Frage der rechtlichen Absicherung zentraler Elemente der demokratischen Sicherheitsarchitektur im digitalen Zeitalter.

Vor diesem Hintergrund verwundert es nicht, dass von verschiedenen Seiten der Zivilgesellschaft der Ruf nach einer unmittelbaren Kriminalisierung von politischer Desinformation lauter wird. In diesem Beitrag wird der Frage nachgegangen, ob man diesem Ruf nach Strafrecht folgen sollte.

Zwei Präzisierungen gehen dieser Untersuchung voraus. Erstens richtet sich die Untersuchung ausdrücklich auf politische Desinformation im digitalen bzw. Online-Segment. Hintergrund dafür ist, dass gerade das Internet und insb. die sog. sozialen Netzwerke zu zentralen Plattformen politischer Kommunikation geworden sind. Eine Vielzahl politischer Akteure – von Einzelpersonen über Interessengruppen bis hin zu ganzen Kampagnenteams – nutzt diese Kanäle, um ihre Botschaften schnell und teils automatisiert an grosse Personenkreise zu verbreiten. Umgekehrt ist die Empfängerseite im Online-Bereich erheblich grösser als in herkömmlichen Offline-Medien. Gerade wegen der hohen Reichweite und der vergleichsweise geringen Regulierungsschwelle erscheinen Untersuchungen zu digitaler politischer Desinformation als besonders dringlich.

Zweitens fokussiert dieser Beitrag auf einfache politische Desinformation und blendet eine spezifische Unterkategorie, die man als qualifizierte Desinformation bezeichnen könnte, bewusst aus. Unter qualifizierter Desinformation sollen hier solche Phänomene verstanden werden, die mittels technisch aufwendiger audiovisueller Manipulation – insbesondere sog. Deepfake-Technologien[8] – eine Täuschung herbeiführen. Deepfakes ermöglichen es, Bilder oder Videos von Personen täuschend echt zu verändern, ihnen bestimmte Aussagen in den Mund zu legen oder Handlungen zuzuweisen, die sie in Wirklichkeit nie begangen haben. Dadurch wird ein besonders hohes Mass an Irreführungspotenzial geschaffen, weil

8 Bei Deepfake-Technologien können mittels Einsatz von Bild- und Video-Technologien modifizierte bzw. manipulierte Bild-, Video- oder Audioaufnahmen erstellt werden. Durch den Einsatz von leistungsstarker Software können dann beispielsweise die gesprochenen Worte einer Person in einer Videoaufnahme durch völlig neue, maschinengenerierte Worte mit stimmlicher Anpassung und authentisch aussehender Mimik geschaffen werden. Aktuell sind diese technologisch erstellten Desinformationen noch nicht weit verbreitet, ihre Realisierung zeichnet sich aber im Zeitalter von Künstlicher Intelligenz langsam aber sicher ab. Ihr Täuschungspotential ist – anders als bei einfacher politischer Desinformation – enorm hoch, ihr Einsatz setzt aber auch entsprechend hohes Know-How voraus, siehe Brown (2020), 1 ff.; Kumkar/Rapp (2022), 199 ff.; Lantwin (2020), 78 ff.

menschliche Wahrnehmung gerade bei visuellen Inhalten davon ausgeht, etwas «authentisch» Gesehenes oder Gehörtes zu erfassen. Solche hochtechnologischen Varianten stellen zwar zweifelsfrei ein ernstzunehmendes Gefährdungsszenario für die demokratische Meinungsbildung dar, können in diesem Beitrag allerdings nicht vertieft behandelt werden.[9] Der Schwerpunkt liegt stattdessen auf einfache Desinformationspraktiken, die zwar nicht per se auf fortgeschrittener audiovisueller Manipulation beruhen, jedoch gleichwohl politische Diskurse nachhaltig beeinflussen und den Ruf nach strafrechtlichen Gegenmassnahmen lauter werden lassen.

Wahlstrafrecht als Demokratieschutzstrafrecht?

Die anhaltende Verbreitung manipulativer Informationen auf Social-Media-Plattformen belebt die Diskussion um staatliche Intervention und Strafbarkeit von Desinformation wiederholt neu. Da fraglich ist, inwiefern sich Desinformation durch grosse Plattform-Unternehmen mittels freiwilliger Selbstverpflichtung effizient bekämpfen lässt,[10] wird in rechtspolitischen und -wissenschaftlichen Debatten grundsätzlich die Forderung vorgetragen, wonach sich die Legislative dem Phänomen von Desinformation annehmen sollte,[11] wobei auch ausdrücklich strafrechtliche Massnahmen befürwortet werden.[12] Zumal sich Desinformation politischer Art gegen die politische Debattenkultur, gegen den Wählerwillen sowie die Glaubwürdigkeit von politischen Akteuren richtet und damit die Grundfesten de-

9 Im Übrigen adressiert der europäische AI Act gerade die Deepfake-Technologie ausdrücklich, siehe ErwG 134 sowie Art. 3 Nr. 60 und zentral Art. 50 Abs. 4 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz; dazu im Überblick etwa Staffler (2025).

10 Mansell et a. (2025), 113, 116; So hat beispielsweise YouTube Anfang Juni 2023 eine neue Unternehmensrichtlinie erlassen, wonach die Videoplattform „keine Inhalte mehr entfernen [will], die falsche Behauptungen über weitverbreiteten Betrug, Fehler oder Pannen bei der Präsidentschaftswahl 2020 und anderen vergangenen US-Wahlen aufstellen“: https://blog.youtube/inside-youtube/us-election-misinformation-update-2023/ (zuletzt abgerufen am 01.01.2025).

11 Etwa Krzywon (2021), 673, 676; s.a. Frattolillo (2021), 220 ff.

12 Siehe den Überblick an unterschiedlichen Stellungnahmen bei Preuß (2021), 171 m.w.N.

mokratischer Meinungsbildung[13] erschüttert, stellt sich im Ausgangspunkt zunächst die Frage, ob Straftatbestände zum Schutz demokratischer Wahlen derartige schädliche Phänomene bereits erfassen. Konkret: Könnte der strafrechtliche Schutz vor Desinformation über die Vergehenstatbestände gegen den Volkswillen des Schweizerischen StGB in Art. 279 ff. StGB gelingen?

Tatsächlich scheint der Kontext des schweizerischen politischen Systems mit seinen starken direktdemokratischen Elementen[14] die Bejahung der gestellten Frage nahezulegen. Dies lässt die verfassungsrechtliche Zentralnorm[15] zum Schutz politischer Rechte in Art. 34 Abs. 2 BV[16] zumindest auf den ersten Blick vermuten, die die Garantie der freien Willensbildung und der unverfälschten Stimmabgabe enthält.[17] So heisst es in ständiger Rechtsprechung des schweizerischen Höchstgerichts, dass «kein Abstimmungs- und Wahlergebnis anerkannt [werden soll], welches nicht den freien Willen der Stimmbürger zuverlässig und unverfälscht zum Ausdruck bringt».[18] Der wissenschaftlichen Kommentarliteratur zu Art. 34 BV ist zu entnehmen, dass das einschlägige schweizerische Demokratieverständnis seinen Legitimationsanspruch nicht allein auf formell-korrekt abgewickelte Wahlveranstaltungen, sondern «ebenso auf die *materielle Qualität des Willensbildungsprozesses* abstellt».[19] Die Bundesverfassung gehe vom Leitbild der politischen Autonomie seiner Bürgerinnen und Bürger aus und traue ihnen zu, «zwischen den verschiedenen gegensätzlichen Auffassungen zu unterscheiden, unter den Meinungen auszuwählen, Übertreibungen als solche zu erkennen und vernunftgemäss zu entscheiden».[20] Gleichzeitig wird betont, dass Art. 34 BV keine normativen Anstandsregeln für den politischen Diskurses formuliert.[21] Gerade bei politischer Kommunikation von Priva-

13 Instruktiv Iben (2021), 35 ff.
14 Statt vieler Kley (2020), 85 ff. sowie Moeckli (2020), 487 ff.; überblicksweise bei Canova/Giardini (2023), 57, 58 ff. m.w.N.
15 Der Schutz des Wählerwillens ist auf Verfassungsebene durch weitere Garantien geschützt, etwa über die Glaubens- und Gewissensfreiheit (Art. 15 BV) oder den Informationsauftrag von Radio und Fernsehen (Art. 93 BV).
16 Art. 34 Abs. 2 BV: „Die Garantie der politischen Rechte schützt die freie Willensbildung und die unverfälschte Stimmabgabe."
17 Instruktiv Coeni (2019), 3, 8–13; s.a. Steinmann/Besson (2023), N 22.
18 Ständige Rechtsprechung seit BGE 75 I 244, 245; vgl. etwa BGE 124 I 55, 57, E. 2a; BGE 140 I 394, 402, E. 8.2.; BGE 141 II 297, 299, E. 5.2.
19 Tschannen (2015), N 2 (Hervorhebungen im Original).
20 BGE 98 Ia 73, 80, E. 3b.
21 Tschannen (2015), N 37.

ten im Kontext von Wahlvorgängen sollen Behörden offensichtlich falsche oder irreführende Informationen richtigstellen, allerdings nur subsidiär und falls dies für die Sicherstellung des Anspruchs auf freie Willensbildung notwendig erscheint.[22] Richtigerweise wird hier grosse Zurückhaltung vor behördlichen Interventionen[23] angemahnt, weil ansonsten die involvierten Grundrechte zu sehr beeinträchtigt werden würden.[24]

Diese Zurückhaltung kann eine Erklärung dafür liefern, warum das schweizerische Strafrecht in Umsetzung der verfassungsrechtlichen Vorgaben von Art. 34 BV gegenüber politischer Desinformationskampagnen, welche auf die Beeinflussung des Wählerwillens abzielen, letztlich zahnlos bleibt. Denn die Vergehenstatbestände in Art. 279 ff. StGB betreffen primär die Art und Weise der Ausübung der politischen Rechte durch die Stimm- und Wahlberechtigten,[25] nicht jedoch die Manipulation von Informationen

22 Vgl. BGE 135 I 292, 295, E. 4.1.: „Nach der bundesgerichtlichen Rechtsprechung können private Informationen im Vorfeld von Sachabstimmungen in unzulässiger Weise die Willensbildung der Stimmberechtigten beeinflussen. Von einer unzulässigen Einwirkung wird etwa dann gesprochen, wenn mittels privater Publikation in einem so späten Zeitpunkt mit offensichtlich unwahren und irreführenden Angaben in den Abstimmungskampf eingegriffen wird, dass es den Stimmberechtigten nach den Umständen unmöglich ist, sich aus anderen Quellen ein zuverlässiges Bild von den tatsächlichen Verhältnissen zu machen. In Anbetracht der Meinungsäusserungsfreiheit wird eine derartige Beeinträchtigung nicht leichthin angenommen. Da insbesondere gewisse übertreibende oder gar unwahre Behauptungen kaum vermieden werden können und weil den Stimmberechtigten ein Urteil über die bekundeten Meinungen und Übertreibungen zugetraut werden darf, fällt die Aufhebung einer Abstimmung *nur unter grösster Zurückhaltung und bei ganz schwerwiegenden Verstössen* in Betracht" (eigene Hervorhebungen); s.a. BGer, Urt. v. 20.01.2011, 1C_472/2010, E. 4.: „Nach ständiger Praxis des Bundesgerichts muss es sich um eine *schwerwiegende Irreführung* der Stimmbürger über eine *entscheidwesentliche Tatsache* oder einen Hauptpunkt der Vorlage handeln; überdies wird verlangt, dass die irreführenden Informationen die Stimmbürger so *knapp vor dem Stimmakt* erreichen, dass es dem Bürger nach den Umständen unmöglich ist, sich aus andern Quellen ein zuverlässiges Bild von den tatsächlichen Verhältnissen zu machen" (eigene Hervorhebungen).

23 Behördliche Interventionen sind insb. zur Gewährleistung der freien Willensbildung möglich, nämlich zur Richtigstellung offensichtlich falscher Informationen durch Private im Vorfeld eines Wahlgangs; BGE 118 Ia 259, 261 ff.; die genaueren Anforderungen an die Kommunikation von Behörden werden in Art. 10a des Bundesgesetzes über die politischen Rechte näherer konkretisiert; vgl. dazu Steinmann (1996), 255, 265 ff. sowie Töndury (2011), 341 ff.; jeweils m.w.N.

24 Tschannen (2015), N 37; kritisch etwa Coeni (2019), 3, 12 f.

25 Aus der Rechtsprechung s. BGE 121 I 138, 141 f.; aus der Literatur s. Wehrle (2018a), N 5; diesbezüglich uneindeutig Trechsel/Vest (2021), N 1: „Geschütztes Rechtsgut ist die *eigenverantwortliche Ausübung* der politischen Rechte durch die Stimm- und Wahlberechtigten bei der Willensbildung und der Stimmabgabe" (eigene Hervorhebungen).

in demokratischen Debatten.[26] Als verbotene Handlungen sind die durch Gewalt oder Androhung ernstlicher Nachteile hervorgerufene Hinderung oder Störung von Wahlen und Abstimmungen (Art. 279 StGB)[27] oder von Stimmabgaben (Art. 280 StGB), die Bestechung zum Zwecke einer bestimmten Stimm- oder Wahlabgabe (Art. 281 StGB) sowie die Verletzung des Abstimmungs- und Wahlgeheimnisses (Art. 283 StGB) erfasst. Die Wahlfälschung (Art. 282 StGB) betrifft nicht die Manipulation des genuinen Wählerwillens vor der Stimmabgabe durch Desinformation, sondern das Verfälschen von Stimmregistern, Wahlergebnissen oder Abstimmungen.[28] Auch Art. 282bis StGB («Stimmenfang») ist hinsichtlich Desinformationskampagnen nicht einschlägig, weil der Tatbestand allein das planmässige Ausfüllen, Ändern oder Einsammeln von Wahl- oder Stimmzetteln erfasst.[29] Obwohl also die Tatbestände als Vergehen gegen den Volkswillen beschrieben werden, schützt das Strafrecht primär äusserlich-formelle Manifestation («Ausübung») des politischen Volkswillens[30] – nicht aber die innerliche Bildung der politischen Präferenzen. Wahlstrafrecht ist also *de lege lata* nicht als Demokratieschutzstrafrecht zur Bekämpfung von Desinformation ausgestaltet. Vielmehr scheint das Gemeinwesen davon auszugehen, dass innerhalb des Wahlvolkes hinreichend kritische Auffassungskraft und Denkvermögen vorherrscht, um Manipulationen durch einfache Desinformation zu widerstehen.

Mit diesem Regelungszugang von Desinformation ist die Schweiz nicht allein, denn dieser Befund lässt sich durchaus auch auf Deutschland[31] und andere mitteleuropäische Rechtsordnungen übertragen. Eine Ausnahme bildet Österreich, das mit § 264 StGB einen Straftatbestand gegen «falsche Nachrichten» bei einer Wahl oder Volksabstimmung bereithält (sogleich *infra*).

---

26 Lubishtani/Flattet (2019), 710, 716.

27 Fuhrer/Ronc (2020a), N 6.

28 Fuhrer/Ronc (2020b), N 1. beschreiben das Rechtsgut treffend als „richtige Feststellung des Volkswillens"; s.a. Wehrle (2018b), N 1.

29 Wehrle (2018c), N 1; BGE 138 IV 70 spricht davon, dass die Norm Verhaltensweise verbietet, welche die persönliche Stimmabgabe beeinflussen und insofern den Volksentscheid verfälschen können. Die Norm wurde 1976 anlässlich der Erleichterung der brieflichen Stimmabgabe eingeführt, vgl. BBl 1975, 1359.

30 Wehrle (2018a), N 5.

31 So die Einschätzung gegenüber dem deutschen StGB durch Eder-Rieder (2019), N 7; s.a. Rückert (2018), 2018, 167, 171 f.

Aktueller Stand der Debatte

Während das schweizerische (Wahl-)Strafrecht mit Blick auf Desinformation also zahnlos bleibt, zeigt der Blick in die wissenschaftliche Literatur, dass die Frage zur Kriminalisierung der Desinformation seit dem Jahr 2017 und damit insbesondere infolge der 2016 ergangenen Wahl von Donald Trump zum US-Präsidenten, die von massivem Einsatz von Desinformation begleitet war,[32] in den (Straf-)Rechtswissenschaften vermehrt diskutiert wird.[33] Gerade in der Anfangsphase der rechtswissenschaftlichen Betrachtung waren insbesondere drei verschiedene kriminalpolitische Ansätze zu beobachten, die sich zur Kriminalisierung einfacher politischer Desinformation äusserten.[34]

Ein erster Ansatz tritt für eine möglichst umfassende Strafbarkeit zur Verbreitung von politischer Desinformation ein.[35] Ein zweiter Ansatz will demgegenüber nur qualifizierte Arten von Desinformation unter Strafe stellen, etwa im Rahmen eines Sonderdelikts, welches lediglich Garanten oder bestimmte Tathandlungen, an deren Vornahme niemand ein berechtigtes Interesse haben kann, erfasst.[36] Dieser Ansatz intendiert also die Kriminalisierung von besonders gefährlichen Phänomenen von politischer Desinformation. In eine derartige kriminalpolitische Richtung geht der österreichische Straftatbestand in § 264 öStGB, der die Verbreitung falscher Nachrichten in einer qualifizierten Öffentlichkeit dann unter Strafe stellt, wenn die Äusserung zu einem Zeitpunkt getätigt wird, in welchem eine

32 Statt vieler s. Baade (2022), 201, 202 f.; Sirakov (2017), 1, 2 ff.; Böller u.a. (2020), 7, 8 ff.

33 Überblicksweise bei Preuß (2021), 171 ff. m.w.N.

34 So die Einteilung von Hoven (2017), 718, 738 ff.

35 Hoven (2017), 718, 739 weist auf den (letztlich nicht realisierten) Entwurf von Art. 656-bis Abs. 1 des italienischen Strafgesetzbuches und meine eigene Übersetzung davon in Staffler (2017), hin, wonach mit Geldbusse bis zu EUR 5.000 bestraft werden soll, „wer falsche, übertriebene oder tendenziöse Nachrichten über offenkundig haltlose oder unwahre Daten bzw. Fakten über die sozialen Medien oder andere Webseiten, die nicht zum sog. Online-Journalismus gehören, veröffentlicht oder verbreiten, sofern der Sachverhalt keine schwere Straftat darstellt."

36 So etwa Schünemann (2019), 627 ff.; Preuß (2021), 177 ff. sowie Schreiber (2022), wobei letzterer die Strafbarkeit „von politischen Fake News [befürwortet], die sich im Hinblick auf die individuelle und öffentliche politische Meinungsbildung sowie die Legitimation des staatlichen Willensbildungsprozesses – als allesamt essentielle Elemente der Volkssouveränität – als am schädlichsten entpuppen" (S. 317); vgl. auch Mafi-Gudarzi (2019), 65, 68.

Gegenäusserung nicht mehr wirksam verbreitet werden kann.[37] Zudem ist der italienische Straftatbestand in Art. 656 iStGB zu nennen, der die Veröffentlichung oder Verbreitung falscher, übertriebener oder tendenziöser Nachrichten kriminalisiert, welche die öffentliche Ordnung verwirren können. Ein dritter Ansatz will punktuelle Anpassungen der geltenden Strafbestimmungen vornehmen,[38] etwa die Ausdehnung der Ehrschutzdelikte auf den Schutz politischer Reputation.[39]

Doch die Debatte hat nicht nur in den Strafrechtswissenschaften, sondern auch in anderen wissenschaftlichen Disziplinen[40] an Fahrt aufgenommen:[41] Die Fragen zur Phänomenologie von Desinformation und ihrer «Bekämpfung»[42] beschäftigt parlamentarische Untersuchungsausschüsse[43] und Gesetzgeber in westlichen Demokratien (einschliesslich der Europäischen Union)[44], aber auch internationale Expertenkommissio-

37 Sadoghi (2022), N 4, 6; als geschütztes Rechtsgut wird hierbei „die Reinheit und Freiheit der demokratischen Willensbildung" genannt, wobei als Schutzobjekt „ein größerer Personenkreis von Wahl- und Abstimmungsberechtigten" genannt wird: beide Zitate nach Eder-Rieder (2019), N 5. Im Übrigen hat der österreichische Strafgesetzgeber den Straftatbestand in § 276 öStGB zur absichtlichen Verbreitung eines Gerüchts, wobei der Täter wusste, dass es falsch und geeignet war, eine grössere Personengruppe zu beunruhigen und dadurch die öffentliche Ordnung zu gefährden, zum Jahresende 2015 gestrichen – der Tatbestand war seit seiner Einführung im Jahr 1975 nie zum Einsatz gekommen.

38 Rostalski (2017), 436, 445.

39 Hoven (2017), 718, 742 f.

40 Für einen Überblick zum kommunikationswissenschaftlichen Forschungsstand s. Hohlfeld (2020), 179, 182 ff. m.w.N.

41 Hervorzuheben ist etwa Habermas (2021), 470 ff., der konstatiert, dass soziale Netzwerke nicht zu mehr Austausch und Kommunikation von Individuen und damit zu mehr Demokratie führen, sondern vielmehr anarchische und tribalistische Halböffentlichkeiten schufen.

42 Die verschärfte Rhetorik eines „Bekämpfungsstrafrechts" kritisiert zurecht Pieth (2014), 264, 267 ff. mit zahlreichen Beispielen; s. auch Pawlik (2008), 25 ff. zum Strafrecht als Kampfinstrument.

43 So befasste sich ein Untersuchungsausschuss des Unterhauses des Parlaments des Vereinigten Königreichs mit Desinformation und „Fake News", s. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (zuletzt abgerufen am 5.10.2022); vgl. auch die Aussage des Whistleblowers Christopher Wylie in Bezug auf Cambridge Analytica, abrufbar unter https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Wylie%20Testimony.pdf (zuletzt abgerufen am 5.10.2022).

44 Borgi/Bleyer-Simon (2021), 531 ff.; Stehliková (2020), 49 ff.

nen[45] und selbst den UN-Sicherheitsrat[46]. Einige nationale Gesetzgeber haben sich dem Phänomen angenommen und (ausserstrafrechtliche) Massnahmen erlassen, wie etwa Frankreich mit einem speditiven Unterlassungsverfahren im Rechtsschutzwege[47] oder die USA mit einem Gesetzesentwurf zur Verstärkung von Transparenz und Rechenschaftspflichten für politische Werbung[48]. Auch die Europäische Union hat sich diesem Thema angenommen und Verordnung[49] lanciert,[50] der Transparenzpflichten über Art. 16 des Entwurfs mit Sanktionen flankiert. Auch die Schweiz hat reagiert und strafbewährte Transparenzpflichten bei der Politikfinanzierung in ihr Bundesgesetz über die politischen Rechte (BPR) implementiert: Seit 23. Oktober 2022 gelten gemäss Art. 76b ff. BPR entsprechende Offenlegungspflichten samt Kontrollmechanismen,[51] die in Art. 76j BPR mit Strafbestimmungen flankiert werden.

Diese legislativen Trends[52] sind damit zu erklären, dass Desinformation zwar als besonders demokratie-schädlich empfunden wird, jedoch bislang die Schwellen etablierter Straftatbestände unterschreitet. Denn es handelt sich um Inhalte, die als störend («*awful but lawful*») zu bezeichnen sind, weil sie an sich legal sind, allerdings aufgrund ihres Kontextes und in Manipulationsabsicht lanciert werden, um politische Diskurse in einer bestimmten Weise zu beeinflussen. Um in dieser Debatte eine Stellungnahme zum Kriminalisierungsbedarf von politischer Desinformation zu artikulieren, soll das Phänomen von Desinformation anhand des bisherigen Kennt-

45 So beschäftigte sich das „Committee of Experts on the integrity of online information" des Europarates in seinem zweiten Meeting im Oktober 2022 mit einem Entwurf zur „Guidance not on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner", MSI-INF (2022)05 v. 8. Juni 2022.

46 Baade (2022), 201, 203 f.

47 Loi n° 2018–1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information; gleichwohl stellt das Gesetz nach Art. L. 163–2 irreführende Behauptungen und Unterstellungen über politische Parteien und deren Akteure für den Zeitraum von drei Monaten vor einer Wahl unter Strafe; vgl. Iben (2021), 409 f.

48 S. 1356 – Honest Ads Act.

49 Verordnung (EU) 2024/900 vom 13.3.2024 über die Transparenz und das Targeting politischer Werbung.

50 Zum Stand des EU-Gesetzes siehe Holznagel, Political Advertising and Disinformation, Verfassungsblog vom 23. März 2023, abrufbar unter https://verfassungsblog.de/political-advertising-and-disinformation/ (zuletzt abgerufen am 06.06.2023).

51 Überblicksweise bei Aeschimann/Schaub (2023), 1 ff.

52 Ein Panorama zu den legislativen Trends findet sich im Bericht der Venedigkommission vom 7. Oktober 2022, CDL-Pl(2022)032, S. 5 ff.

nisstandes in Forschung und Praxis näher betrachtet werden. Denn erst nach einer deskriptiv-analytisch Erfassung des Phänomens kann darüber diskutiert werden, inwiefern Desinformation mit strafrechtlichen Mitteln verfolgt werden sollte.

Das Phänomen Desinformation

Um das Phänomen von Desinformation näher zu analysieren, ist zunächst kurz auf den technologischen Kontext einzugehen, wo Desinformation wohl am häufigsten auftritt, nämlich in den sog. sozialen Netzwerken.[53] Soziale Netzwerke, wie etwa Facebook, X (ehemals Twitter) oder Telegram, sind digitale Internetdienste, die sich als Plattformen[54] zum Austausch von Informationen und zum Aufbau von Beziehungen anbieten.[55] Ihre soziale Akzeptanz und massive Verbreitung[56] gelang in den frühen 2000er Jahren, als immer grössere Bevölkerungsteile Zugang zum Internet erhielten und sich Bereiche privater Kommunikation auf die neuen Plattformen verlagerten.[57]

Mit Blick auf politische Kommunikation sind die sozialen Netzwerke mit dem Versprechen angetreten, Informationen zu demokratisieren[58], indem die Internet-Plattformen frei zugängliche Informationsflüsse ohne Intermediäre (z.B. Presse) zwischen dem unmittelbaren Wahlvolk einerseits und den Institutionen des Staates bzw. den politischen Akteuren andererseits zulassen.[59] Diese oft als «Demokratisierung» deklarierte Entwicklung von Informationsflüssen über das Internet[60] und das Geschäftsmodell sozia-

53 Im Kontext von Desinformation s. insb. Preuß (2021), 80 ff. m.w.N.; s.a. Frischhut (2024), 109, 115.

54 Hierzu Ebersberger/Dachs (2024), 75 f.

55 Ähnlich die Duden-Definition von „Social Network“: „Portal im Internet, das Kontakte zwischen Menschen vermittelt und die Pflege von persönlichen Beziehungen über ein entsprechendes Netzwerk ermöglicht.“, abrufbar unter https://www.duden.de/rechtschreibung/Social_Network (zuletzt abgerufen am 05.10.2022).

56 Zur Ökonomik digitale MNE s. Ebersberger/Dachs (2024), 69 ff.

57 Habermas (2022), 48 ff. gibt einen Überblick über den gewandelten Medienkonsum und stellt fest, dass gerade in jüngerer Zeit Misstrauen gegenüber den Medien (wegen vermeintlichen politischen oder wirtschaftlichen Druckes) ausbreitet.

58 Inzwischen gehen Forschende wie Golumbia (2024) davon aus, dass die Idee eines digitalen Raumes von Meinungsaustausch durch Großkonzerne einen antidemokratischen Gestus darstellen.

59 Vgl. Kubiciel M., (2020), 159 f.; Thiel (2022), 41, 51.

60 Vgl. diesbezüglich Studie von Schroeder (2022).

ler Medien,[61] deren Dienste offenbar gebührenfrei[62] genutzt werden können, hat den Kommunikationsplattformen einerseits Massentauglichkeit beschert, andererseits die staatliche Reglementierung lange Zeit zurückgehalten. Ging man ab 2004 davon aus, dass soziale Plattformen gewöhnliche Webseiten seien, gelangte man in den frühen 2010er Jahren ins Staunen über das demokratische Potential dieser Medien, weil ihnen eine massgebliche Rolle beim sog. «Arabischen Frühling» zugeschrieben wurde.[63] Spätestens mit dem «Cambridge Analytica»-Skandal erfolgte in der zweiten Hälfte der 2010er Jahre ein Umdenken, als verschiedene Staaten legislative Massnahmen ergriffen, um den vermeintlich rechtsfreien Raum wieder einzufangen. Die Social-Media-Plattformen wurden als «*partner in crime fighting*» aufgefasst und sollten als Durchsetzer staatlicher Regeln in Stellung gebracht werden.[64] Ende der 2010er Jahre folgte die grosse Resignation, weil man erkennen musste, dass die Bekämpfung von «*awful but lawful*» – Inhalte staatlich nicht zu bewerkstelligen ist und man letztlich auf die Durchsetzung der «Hausordnung» durch Social-Media- Akteure angewiesen ist. Neuerdings besteht die Herausforderung, professionelle Wahlmanipulatoren wie etwa das israelische Unternehmen «Team Jorge»[65], rechtlich in Schranken zu weisen und auf diese Weise demokratische Strukturen zu schützen.

Vor dem Hintergrund dieser summarisch dargestellten Entwicklung erscheint es für die Analyse des strafrechtlichen Interventionsbedarfs zum Schutz von Demokratie gegen einfache Desinformation hilfreich, eine Literaturauswertung über empirische Befunde zu Desinformation durchzuführen. Auf diese Weise soll die Komplexität von Desinformation reduziert und phänomenologische Pathologien offengelegt werden, an denen der (Straf-)Gesetzgeber möglicherweise ansetzen könnte.

---

61 Grundlegend Degischer/Wallnöfer (2024), 87, 88 ff. 95 ff., 97.

62 Tatsächlich gründen die Geschäftsmodelle vieler kostenloser Internet-Plattformen auf datenökonomischen Prinzipien, sodass letztlich Nutzer die Inanspruchnahme kostenloser Plattformdienstleistungen mit ihren (personenbezogenen) Daten bezahlen; statt vieler s. Schmitz/Buschuew (2022), 171 ff.; Lohsse/Schulze/Saudenmayer (2020).

63 Instruktiv Wolff (2013), 163, 170 ff. sowie die Beiträge in Demmelhuber/Paul/Reinkowski (2017).

64 Balkin (2014), 2296 ff.; Balkin (2018), 1149 ff. bezeichnet diesen Regulierungsansatz der neuen Digital-Infrastruktur als „New School Speech Regulation".

65 Zum israelischen Unternehmen „Team Jorge", dessen Praktiken und Geschäftsmodelle im Frühjahr 2023 durch Investigativ-Recherchen aufgedeckt wurden, s. Stark/Zimmermann (2023).

Psychometrik als dahinterliegende «Mechanik»

Psychometrik bzw. Psychographie ist ein Zweig der Psychologie, der das Forschungsanliegen verfolgt, die Persönlichkeit eines Menschen zu vermessen. Die psychologische «Vermessung» von Persönlichkeit fusst auf einer Methode, die in den 1980er Jahren entwickelt wurde[66] und heute als sog. «OCEAN»-Methode bekannt ist.[67] Ausgangspunkt ist die Grundannahme, wonach Charakterzüge und Entscheidungen von Menschen anhand von fünf Persönlichkeitsdimensionen einordbar sind. Die fünf einschlägigen Persönlichkeitsmerkmale sind Offenheit (wie aufgeschlossen ist die betreffende Person gegenüber Neuem?), Gewissenhaftigkeit (wie perfektionistisch ist die betreffende Person?), Extraversion (wie gesellig ist die betreffende Person?), Verträglichkeit (wie rücksichtsvoll bzw. kooperativ ist die betreffende Person) und Neurotizismus (wie verletzlich ist die betreffende Person). Auf dieser Basis – so lautet die Forschungsthese – lässt sich relativ bestimmt vorhersagen, welche Bedürfnisse und Ängste die betreffende Person hat und welches Verhalten die betreffende Person tendenziell an den Tag legen wird. Tatsächlich liess sich die empirische Nachweisbarkeit dieses Forschungsansatzes lange Zeit nicht feststellen, weil die Bestimmung der Dimensionen von individuellen Personen nur auf Grundlage eines komplizierten und gleichzeitig überaus persönlichen Fragebogens zu erheben ist. Der Praxisabgleich scheiterte in den 1980er Jahren insofern an der Beschaffung der Datengrundlage zur Verifikation der Theorie.

Das Problem der Datenbeschaffung wurde durch den technischen Fortschritt gelöst. Ab 2004, dem Gründungsjahr von Facebook, etablieren sich soziale Netzwerke und eröffnete damit neue Forschungsmöglichkeiten. So wurde an der University of Cambridge das erste Psychometrie-Labor gegründet und Michal Kosinski, damals ein Student aus Warschau, tat sich mit seinem Studienkollegen David Stillwell zusammen, um den OCEAN-Fragebogen für das damals noch überschaubare soziale Netzwerk Facebook massentauglich zu gestalten. Über eine Quiz-Applikation mit dem Namen «*My.Personality*», das ihren Nutzern ein Persönlichkeitsprofil zur Verfügung stellt, beabsichtigten die Forscher die Auswertung von Frage-

66 Das Model geht auf die Forschung von Robert R. McCrae und Oliver P. John zurück, s. insb. den Überblick bei McCrae/John (1992), 175 ff.; siehe auch Costa/McCrae (1992); McAdams (1992), 329 ff.; Wiggins (1996).

67 Einführend zum OCEAN-Model, das auch als "Big Five Model" oder „Five Factor Model" bezeichnet wird, Matz/Chan/Kosinski (2016), 35 ff. m.w.N.

bögen, um die angegebenen Antwortergebnissen hinsichtlich der OCEAN-Werte zu kalkulieren und die erhobenen Daten mit anderen eingeholten Daten (Art der auf Facebook ergangenen Kommunikation sowie die bekannten individuellen Persönlichkeitsmerkmale) abzugleichen, welche die Personen auf ihrer Facebook-Seiten teilen. Das auf diese Weise gestaltete Quiz verteilen die Forscher virtuell an ihre Studienfreunde. Tatsächlich ging die Applikation viral, d.h. sie wurde über die Studienfreunde hinaus weiter geteilt und letztlich von mehreren Millionen Nutzern ausgefüllt, sodass die Forschenden über ihre Applikation über einen grossen Datensatz verfügten. Dies ermöglichte den Forschenden, Korrelationen in den Datenpunkten zu identifizieren, etwa zur Musikpräferenz heterosexueller Personen oder Themenpräferenzen von introvertierten Personen.[68]

In der Folgezeit intensivierten die Forscher ihre Experimente und erzielten durchaus spektakuläre Ergebnisse. Berühmt wurde die 2012 ergangene Pressemitteilung, wonach aus durchschnittlich 68 Likes aus Facebook-Profilen die Hautfarbe der betroffenen Person mit 95 % Treffsicherheit, die Frage zur Homosexualität der betreffenden Person mit 88 % und die Frage nach der politischen Zugehörigkeit zur demokratischen oder republikanischer Partei mit 85 % Treffsicherheit ermittelt werden konnte.[69] Durch die Verfeinerung der Datensätze waren die Forscher zuletzt in der Lage, Menschen allein auf Grundlage ihres Profilfotos in den sozialen Medien[70] oder über die Auswertung der Kontakte laut sozialem Netzwerk nach den OCEAN-Kriterien einzuordnen.[71]

Welches wirtschaftliche Potential in diesem Forschungsfortschritt erhoben werden kann, wird augenscheinlich, wenn man sich das Geschäftsmodel von kostenlosen[72] sozialen Medien und Suchmaschinen verdeutlicht: Es geht um den Verkauf von Werbung, die bei diesen Online-Medien besonders raffiniert erscheinen, weil diese Medien einen hohen Grad an Personalisierung ermöglichen. Klassische Werbung in Massenmedien (Plakate, Werbetafeln, Werbespots) orientierten sich zwar an ihrer Zielgruppe (z.B. «Frauen»), doch war es wirtschaftlich kaum sinnvoll, eine zu hohe

68 Vgl. Cantador et. al. (2013); Kosinski/Stillwell/Graepel (2013), 5802 ff.
69 Vgl. statt vieler Sterne (2017), 256 m.w.N.
70 Segalin et al. (2017).
71 Jüngst hat Kosinski offengelegt, dass Gesichtserkennungssoftware die politische Orientierung offenlegen kann: Kosinski (2021).
72 Wie oben bereits aufgezeigt, wird der Verzicht auf monetäre Gegenleistung durch die Preisgabe und Verarbeitung personenbezogener Nutzerdaten ersetzt; instruktiv Knüppel (2022), 39 ff.

Spezifikation der Werbebotschaft vorzunehmen, welche der Diversifikation von Interessen innerhalb dieser Zielgruppe Rechnung trägt. Während es bei wirtschaftlicher Werbung wirtschaftlich interessante Spezifikationen geben mag (z.B. die Bewerbung bestimmter Produkten für «schwangere Frauen»), folgt politische Werbung anderen Logiken und anderen Bedürfnissen: Politische Wahlbotschaften sollen das Zielpublikum insb. in Zeiträumen unmittelbar vor einer Wahl ansprechen; gleichzeitig ist aber die individuell angesprochene Zielperson in ihren politisch-relevanten Interessen divers.[73] Damit politische Werbung ihren individuellen Adressaten möglichst auf eine personalisierte Weise erreicht, bedarf es aufwendiger Mechanismen (z.B. gezielte Ansprache durch Wahlhelfende). Der Modellierung von Persönlichkeitsprofilen von potentiellen Wählerinnen und Wählern könnte bereits im Vorfeld enorme Bedeutung zukommen: Indem die konkret anzusprechende Person nach gewissen Kriterien eingeordnet wird, wird es ermöglicht, die Nuancen der eigenen Wahlbotschaft zuzuschneiden. Während also beispielsweise Wähler A familienpolitische Aspekte primär interessieren, ist es für Wählerin B der Staatshaushalt.

Tatsächlich wurde ein derartiges Vorgehen in der US-Präsidentschaftskampagne von Barack Obama im Jahr 2008 gewählt, wo der Wahlkampf mittels Unterstützung von Persönlichkeitsprofilen und darauf zugeschnittenen Gesprächsleitfäden für die Wahlhelfenden geführt wurde.[74] Jenen Wählerinnen und Wählern, die nach entsprechendem Persönlichkeit-Profiling neuen bzw. progressiven politischen Ideen tendenziell offenstanden, konnten die von der Obama-Kampagne lancierten politischen Botschaften von «Veränderung» und «Fortschritt» besser kommuniziert werden, während konservativere Wählerinnen und Wähler mit politischen Botschaften zu «Stabilität» und «Tradition» angesprochen werden sollten. Möglichst austarierte Persönlichkeitsprofile zur Ansprache individueller potentieller Wähler sollte nach dem Erfolg von Barack Obama von 2008 zum Repertoire politischer Wahlen von grösseren Dimensionen gehören. Die Erstellung derartiger Persönlichkeitsprofile gestaltet sich allerdings enorm aufwendig, wie die frühe Forschung in den 1980er Jahren zum OCEAN-Model gezeigt hatte. Mit der Anwendung des OCEAN-Models auf Datensätze von

73 Thieltges/Serrano (2021), 3 ff.

74 Instruktiv zur Obama-Kampagne etwa Bimber (2014), 130 ff. (mit Blick auf die Ansprache von Wählerinnen und Wähler im Jahr 2008 auf S. 141).

sozialen Medien würde sich neues Potential für personalisierbare Politikwerbung ergeben.[75]

Die potentiellen wirtschaftlichen Möglichkeiten, welche die Forschung durch die Daten aus den sozialen Netzwerken erhielt, blieben nicht unbemerkt.[76] Der Mutterkonzern von Cambridge Analytica, ein britisch-US-amerikanisches Unternehmen namens «Strategic Communications Laboratories» (SCL),[77] nahm mit Kosinski Kontakt zwecks möglicher Zusammenarbeit auf. Das Geschäftsmodell von SCL war die Verhaltensforschung und strategische Kommunikation mit besonderem Schwerpunkt auf Aushebung und Analyse von Daten, um auf diese Weise Kommunikationsmassnahmen zu entwerfen, die für bestimmte Zielgruppen mit dem Ziel massgeschneidert wurden, Verhaltensänderungen im Sinne der SCL-Kunden zu bewirken. Das Unternehmen bot also Wahlmanagement i.S.e. Marketings auf Basis eines psychologischen Modells an. Aufgrund eines universitätsinternen Konflikts zwischen Kosinski und einem Kollegen (Kogan), der für SCL auftrat, kam diese Zusammenarbeit nicht zustande.[78] Das 2014 gegründete Tochterunternehmen von SCL, die politische Beratungsfirma «Cambridge Analytica»[79], adaptierte auch ohne Kosinskis Mitwirkung mithilfe anderer Vorhersagemodelle[80] das OCEAN-Model, indem über Facebook und einen durch dieses Unternehmen (zumindest) tolerierten Fehler[81] massenhaft Da-

75 Vgl. Frenkel/Kang (2021), die nachzeichnen, wie personalisierte Werbung als Geschäftsmodel erkannt wurde.

76 Die folgenden Informationen entstammen der Complaint der US-Federal Trade Commission, die anlässlich des Cambridge Analytica-Skandals ein Verfahren gegen Aleksander Kogan und Alexander Nix initiierte, welches mit Vergleichen endete: United States of America before the Federal Trade Commission, Kogan and Nix, Nr. 182 3106 u. 182 3107, abrufbar unter https://www.ftc.gov/system/files/documents/cases/182_3106_kogan-nix_complaint.pdf (zuletzt abgerufen am 01.01.2025); sowie der schriftlichen Einlassung von Aleksander Kogan vor dem britischen Untersuchungsausschuss, abrufbar unter: https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/Written-evidence-Aleksandr-Kogan.pdf (zuletzt abgerufen am 01.01.2025); unterstützend wurde auf die Whistleblower-Erzählungen von Kaiser (2020) zurückgegriffen.

77 Wylie (2019), 39.

78 Zur Struktur von SCL s. Wylie (2019), 93 ff., 136 f., 166; Briant (2022).

79 Eingehend Caroll (2021), 41 ff.

80 Wylie (2019), 45 ff.

81 So deckte der britische Guardian im Jahr 2019 auf, dass Facebook bereits 2015 von der Ausnutzung von Datenlecks durch Cambridge Analytica für die Ted Cruz-Kampagne wusste. Doch bis August 2016 unternahm Facebook keine ernsthaften Schritte gegen Cambridge Analytica; lediglich ein anwaltliches Schreiben mit der Aufforderung zur Löschung aller erhobenen Daten wurde gegenüber Cambridge Analytica ausgestellt,

ten eingeholt[82] und darauf basierend Persönlichkeitsprofile erstellt wurden, die letztlich für politisches Micro-Targeting genutzt werden sollten.[83] Der erste erfolgreiche Einsatz, der medial bekannt wurde, war die Unterstützung der politischen Kampagne von Ted Cruz in den Vorwahlen rund um die US-Präsidentschaft 2016.[84] Doch das Know-How sollte in noch wesentlich grösseren Kontexten zur Anwendung kommen.[85]

Beispiel 1: Brexit-Kampagne 2016

Wie allgemeinhin bekannt, ging es beim sog. «Brexit» um den EU-Austritt des Vereinigten Königreichs. 2013 hatte der damalige UK-Premierminister David Cameron aus wahlkampftaktischen Gründen einen Volksentscheid über den Verbleib seines Landes in der EU angekündigt.[86] Der Volksentscheid selbst erfolgte am 23. Juni 2016,[87] wobei 51,89 % der Wahlbeteiligten für den EU-Austritt stimmten, der letztlich auf der Grundlage von Art. 50 EUV am 31. Januar 2020 erfolgte.[88]

Für die vorliegende Untersuchung ist die politische Kampagne der Befürworter des EU-Austritts („leave.eu"), insb. unter der Leitung von Nigel Farage, näher zu betrachten.[89] Relativ früh im Wahlkampf gab Farage bekannt, dass seine Kampagne zur Unterstützung ihres Wahlkampfs ein Big Data Unternehmen namens Cambridge Analytica angeheuert hatte, dessen Kernkompetenz ein damals neuartiges politisches Marketing durch zielgruppenbasierte Ansprache von Wahlberechtigten (sog. Micro-Targeting)[90] auf der Grundlage des psychologischen OCEAN-Modells darstellt.[91]

---

worauf die Firma affermativ antwortete – eine Kontrolle der Löschung wurde allerdings nicht vorgenommen: Wong (2019).

82 Cadwalladr/Graham-Harrison (2018).

83 Vgl. Mansell et a. (2025), 33, 79 f.; Staffler (2022), 19.

84 Venturini/Rogers (2019), 532, 534.

85 Zu den Phänomenen derartiger Wahlmanipulationen s. Reimann (2023), 27 ff.

86 Die Rede vom 23. Januar 2013 ist über diesem Link abrufbar: https://www.bbc.com/news/av/uk-politics-21156905 (zuletzt abgerufen am 19.10.2022).

87 Ausführlich Streinz (2020), 95 ff. sowie Sturm (2016), 878 ff.

88 Ausführliche Analysen zum Brexit finden sich bei Kadelbach (2019), 9 ff.; Pernice/Guerra Martins (2019); Terchechte (2020), 425 f.; Winkelmann/Griebel (2018).

89 Instruktiv Bale/Wager (2015), 217 ff.; Prentoulis (2022), 55, 62 ff.; Zabel (2017), 275 f.

90 Instruktiv Towfigh/Luckey (2022), 61 ff.; Baade (2023), 415 f.

91 Bakir (2020), 1, 8 f.

Wie Cambridge Analytica den Brexit-Wahlkampf beeinflusste, lässt sich konkret anhand verschiedener Werbebotschaften illustrieren, die Unterlagen der britischen parlamentarischen Untersuchungsausschüsse[92] sowie der Literatur[93] zu entnehmen sind: So wurden mittels Micro-Targeting Liebhaberinnen und Liebhabern von Tee die Anzeige eingeblendet, wonach die Europäische Union Wasserkocher verbieten will. Mitglieder und Sympathisanten von Tierschutzvereinigungen wurde suggeriert, dass die EU das Schlachten von Robbenbabys erlauben will. Ausländer- und islamfeindlichen Personen wurden Anzeigen eingeblendet, wonach die Türkei kurz vor einem EU-Beitritt stünde und daher ohne Brexit mehrere Millionen Muslime aus der Türkei in die EU (und insofern auch nach Grossbritannien) einwandern würden. Alle drei Beispiele waren Erfindungen der Brexit-Kampagne.

Betrachtet man diese Beispiele auf einer analytischen Ebene, so zeigt sich, dass die drei genannten Werbebotschaften nicht nur Unwahrheit als Gemeinsamkeit aufweisen. Eine wichtige Gemeinsamkeit besteht auch im Lancieren emotionaler Botschaften, die sich stark an Facetten der Identität des angesprochenen Zielpublikums richten. Tee gilt als britisches Nationalgetränk; Tierschutz ist ein klassisches humanistisches Anliegen; die religiöse Zugehörigkeit ist ein identitätsstiftendes Merkmal vieler Menschen. Offenbar wurde von den politischen Kampagnen-Verantwortlichen versucht, die Brexit-Frage als Frage einer Identitätspolitik zu deuten. Dies ist vor dem Hintergrund zu sehen, dass Politikwissenschaftler die Ansicht vertreten, wonach Identitätspolitik[94] ein probates Mittel ist, um Aufmerksamkeit im politischen Wettbewerb zu binden[95] und um Wählerschaft zu mobilisieren.[96]

---

92 Siehe etwa House of Commons, Disinformation and 'fake news': Final Report, 18. Februar 2019, abrufbar unter https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (zuletzt abgerufen am 05.10.2022).

93 Siehe Shipman (2016), 183 ff. m.w.N.

94 Zum Begriffsverständnis von „Identitätspolitik" s. Priester (2019), 11, 13 ff.; Schubert/Schwiertz (2021), 565, 569 ff.

95 Dass gerade Desinformation bei der Generierung von Aufmerksamkeit im politischen Kontext durchaus erfolgversprechend ist, zeigt eine US-amerikanische Anekdote. Als am 9. September 2009 US-Präsident Barack Obama vor beiden Kammern des Kongresses erklärte, es sei nicht beabsichtigt, illegale Eingewanderte in das geplante Gesundheitssystem mit einzubeziehen (was der Wahrheit entsprach), unterbrach ihn der republikanische US-Abgeordnete Joe Wilson aus South Carolina von seinem Sitzplatz aus, indem er rief „Sie lügen", s. Benson (2011), 22, 27 (der Autor spricht diesbezüglich von „*incivility*" als einer „*rhetorical tactic*"). Der Abgeordnete

Beispiel 2: Trump-Wahlkampf 2016

Als im September 2016 der US-Präsidentschaftswahlkampf in die Endrunde ging, sprach der CEO von Cambridge-Analytica, Alexander Nix, auf dem Concordia Summit über seine Erfahrungen aus seiner Unterstützung für den Ted Cruz-Wahlkampf in Iowa, wonach dessen Wahlerfolg auf die Zunahme ländlicher Wählerschaft und Rückgang der Stimmabgabe durch afroamerikanische Personen zurückzuführen sei.[97] Laut Nix hatte diesbezüglich das Unternehmen persönliche Datensätze von Wählerinnen und Wählern aus vielfältigen Quellen wie etwa Grundbucheinträgen, Bonuskarten, Wählerverzeichnissen, Mitgliedschaften oder Zeitungsabonnements gekauft, um sie mit Wählerlisten der republikanischen Partei und Onlinedaten aus Facebook abzugleichen und daraus eine Zuordnung nach dem OCEAN-Persönlichkeitsprofil zu generieren. Anschaulich lässt sich das Prinzip mit dem Beispiel der geographischen Dichte von Biomärkten verdeutlichen – offenbar besteht eine Korrelation zur Biomarkt-Dichte und der Dichte demokratischer Wählerschaft in derselben Gegend.[98] Nix sprach davon, dass seine Firma Psychogramme von allen erwachsenen US-Bürgerinnen und Bürgern (und insofern von 220 Millionen Menschen) erstellt hatte, die unter anderem Alter, Adresse, Interessen und politische Neigungen enthielten. Anhand der jeweiligen Klassifikation wurden dann spezifische politische Werbebotschaften geschaltet. Damit die Unterstützung durch das Datenunternehmen funktionieren konnte, bedurfte jedes Cluster von Wahlberechtigten einer eigens zugeschnittenen politischen Botschaft. Entsprechend war Donald Trump mit seinen widersprüchlichen und unwahren Botschaften[99] ein idealer Produzent zielgerichteter Botschaften.[100]

---

wurde hierfür durch das Repräsentantenhaus gerügt und entschuldigte sich – sein Zwischenruf bescherte ihm allerdings jede Menge Aufmerksamkeit und innert kurzer Zeit eine Vielzahl an beachtlichen Wahlkampfspenden: Klein (2020), 268 ff.

96 Klein (2020), 235 ff., der betont, dass Politiker auf Polarisierung und Empörung setzen, um Wählerstimmen zu verbuchen; dabei spielt die Identitätspolitik eine herausragende Rolle.

97 Eine Videodokumentation des Vortrages ist unter folgendem Link abrufbar: https://youtu.be/n8Dd5aVXLCc (zuletzt abgerufen am 05.06.2023).

98 Klein (2020), 155 ff.

99 König (2022), 121, 125 f.; vgl. auch Güldenzopf/Voigt (2016), 24 ff.

100 Vgl. Oswald (2020), 61, 70 ff.; Shaw (2016), 15 ff.

Wie bereits der Obama-Wahlkampf von 2008 vorgezeichnet hatte,[101] stellte das Cambridge Analytica-Team für die Wahlhelfenden von Trump eine Software (App) für Hausbesuche bereit, wodurch sich schon im Vorfeld erkennen liess, welche politische Einstellung und welchen Persönlichkeitstyp die Bewohner des jeweiligen Hauses hatten. Je nach Persönlichkeitstyp stand ein entsprechend vorgefertigter Gesprächsleitfaden bereit und die Reaktionen, die die Wahlhelfer entgegennahmen, wurden wiederum in der App rückgemeldet, sodass die neuen Daten zurück zu Cambridge Analytica flossen, um die Algorithmen zu verfeinern. Darüber hinaus versuchten Nix und sein Unternehmen, die Botschaften an die Empfänger psychologisch optimal anzupassen. Dazu differenzierten sie die Adressaten nach Kleinstgruppen für Micro-Targeting auf sozialen Medien. Es ging dabei weniger darum, die bereits überzeugten Wähler für den unterstützten Kandidaten in ihrer Meinung zu verfestigen, sondern eher darum, potentielle Wähler der gegnerischen Kandidatin von der Wahlurne fernzuhalten.[102] So wurde die Einwohnerinnen und Einwohner im Stadtteil Little Haiti von Miami durch das Team von Trump mit Nachrichten über das Versagen der Clinton Stiftung nach dem Erdbeben in Haiti versorgt. An Facebook-Profile von afroamerikanischen Bürgerinnen und Bürgern wurden Videos gesendet, in denen Hillary Clinton schwarze Männer als Raubtiere bezeichnete.[103]

Neben dieser Kampagne durch Micro-Targeting, die vom Wahlkampfteam rund um Cambridge Analytica ausging, erhielt Donald Trump in einem heiklen Moment seines holprigen Wahlkampfs unerwartete Unterstützung aus dem Ausland in Form von Desinformation. Laut dem Historiker Timothy Snyder wurde rund eine halbe Stunde, nachdem ein Video-Transkript mit Donald Trumps vulgären Bemerkungen über Frauen erschien, wonach er Frauen ungestraft zwischen die Beine fassen könne, durch Russland in den sozialen Medien die gehackten E-Mails von John Podesta (dem damaligen Wahlkampfleiter von Hillary Clinton) veröffentlicht, wohl mit dem Ziel, die Öffentlichkeit vom peinlichen Auftritt Trumps abzulenken.[104] Derartige Muster, nämlich desinformative Schützenhilfe aus

101 Instruktiv Horst (2009), 107, 122 ff., 135 ff., 138 f.; Kornelius (2009), 296 ff. Jungherr (2016), 3 ff.; Weiss (2008).
102 Vgl. Jungherr (2016), 3 ff.; Shaw (2016), 15 ff.
103 Ausführlich zum Negativ Campaining insb. Thelen (2020), 121 ff., 130 ff.
104 Snyder (2018).

Russland, finden sich im Übrigen auch in jüngerer Zeit wieder, etwa im Zusammenhang mit den Parlamentswahlen in Ungarn im Jahr 2022.[105]

Der Ausgang der US-Präsidentschaftswahl von 2016 ist bekannt. Donald Trump gewann das Votum um die US-Präsidentschaft äussert knapp vor Hillary Clinton.[106] Tatsächlich legen inzwischen Studien nahe, dass politische Desinformation die Wahlentscheidung bei demokratischen Abstimmungen beeinflussen kann.[107] Insofern verwundert es nicht, dass Desinformation als Mittel zur politischen Kampagne auch jenseits des Atlantiks entdeckt wurde und eingesetzt wird.[108]

Beispiel 3: Kurz-Wahlkampf 2017

Der bisherige Eindruck zur Wählerschaft-Demobilisierung aus Brexit- und Trump-Kampagnen darf allerdings nicht darüber hinwegtäuschen, dass Desinformation auch dazu genutzt werden kann, um das eigene Wählerschaft-Potential zu mobilisieren. Das zeigt ein Fallbeispiel aus Österreich zu den dortigen Parlamentswahlen von 2017 mit Blick auf Sebastian Kurz. Im Vorfeld der Parlamentswahlen von 2017 hatte die Österreichische Volkspartei (ÖVP) mit einem Umfragetief als drittstärkste wahlkämpfende Partei zu ringen. Mit der Übernahme des Parteivorsitzes von Sebastian Kurz und seiner Schwerpunktsetzung auf klassische Politikthemen populistischer rechter Strömungen[109] änderten sich die Umfragewerte zugunsten der ÖVP. Sie wurde insb. von einem bestimmten Meinungsforschungsinstitut mit einem deutlichen Vorsprung von rund 15 % auf die konkurrierenden Parteien angegeben. Im Zuge der (noch immer laufenden) strafrechtlichen Aufarbeitung von Korruptionsvorwürfen aus dem Umfeld des ehemaligen österreichischen Bundeskanzlers kam infolge von Kronzeugenaussagen[110] ans Licht, wonach eine Meinungsforscherin gegen Geld geschönte Umfragewerte erstellt hatte, die dann in den Medien präsentiert wurden, um den

105 So der Medienmonitor Mérték (2022); vgl. Levitsky/Ziblatt (2018), 105 f.
106 Eine ausführliche Analyse hierzu findet sich bei Levitsky/Ziblatt (2018), 68 ff.
107 Allcott/Gentzkow (2017), 211 ff.; Zimmermann/Kohring (2018), 23, 33; jeweils m.w.N.
108 Vgl. die Fallstudien bei Sängerlaub/Meier/Ruhl (2018); s. fernier Vorberg (2023), 103 ff.
109 Hoven (2020), 101 ff. m.w.N. Instruktiv zum Wahlkampf von Sebastian Kurz aus politikwissenschaftlicher Sicht bei Strobl (2018).
110 Ausführlich Konzett/Klenk/Staudinger/Tóth (2022).

politischen Wettbewerber Kurz bei den Wählerinnen und Wählern bekannt zu machen und seine Siegeschancen zu steigern. Einschlägige politische Kommunikationsstrategien sind inzwischen in der Literatur eindrücklich beschrieben worden. So veröffentlichte 2022 Gerald Fleischmann, der Chefkommunikator von Sebastian Kurz, sein Buch über die politische Einflussnahme auf die mediale Berichterstattung. In seinem Werk beschreibt er unter anderem eine gängige politische Ablenkungstaktik namens «strategisch notwendigen Unsinn», mit der für die Regierung harmlose Randnotizen gezielt in Medien mit dem Ziel untergebracht werden, Empörung in den sozialen Medien zu generieren, um auf diese Weise von grossen problematischen Themen abzulenken.[111]

Desinformation zwischen Mobilisierung von eigenen und Demobilisierung von gegnerischen Wählern

Zusammenfassend lässt sich festhalten, dass Desinformation grundsätzlich von personalisierten Werbebotschaften für den politischen Diskurs lebt. Dafür ist zuerst der (legale oder illegale) Zugriff auf personenbezogene Daten erforderlich,[112] um auf dieser Datenbasis Wählerschaftsprofile zu erstellen und damit personalisierte Wählerinnen-Ansprache vornehmen zu können. Die Vorgehensweise verläuft in zwei Schritten: Im ersten Schritt werden auf der Grundlage von Datenanalysen verschiedene Zielgruppen nach politischen Gesichtspunkten definiert. Im zweiten Schritt bekommen diese Personengruppen massgeschneiderte Botschaften, die zu ihrem Umfeld passen.

Die dargelegten Fallbeispiele zeigen, dass es sowohl darum geht, durch Desinformation eigene Wählergruppen zu mobilisieren, als auch umgekehrt gegnerische Wählergruppen zu demobilisieren.[113] Oft erscheint es insb. notwendig, den tatsächlichen Absender oder Auftraggeber politischer Botschaften zu verschleiern. Denn hätten die Wählerinnen und Wähler von Hillary Clinton erkennen können, dass die Werbebotschaften von einer

111 Fleischmann (2023).

112 Dieser Ausgangspunkt legt offen, dass das Potential politischer Online-Werbung von der Existenz personenbezogener Daten lebt; insofern attestiert die Dissertation von Wittner (2022), 99 ff., dem Recht auf Datenschutz eine besondere demokratietheoretische Bedeutung.

113 Vgl. diesbezüglich die multiperspektivische Betrachtung in der Publikation der Landesanstalt für Medien NRW (2020).

Trump-nahestehenden politischen Organisation kamen, hätten sie die Werbung kritisch einordnen können. In diesem Kontext tritt das Phänomen des sog. «Astroturfing» erschwerend hinzu. Astroturfing meint, dass der Werbende oder Auftraggeber als neutraler Akteur oder als NGO auftritt, um der eigenen Botschaft mehr Überzeugungskraft zu verleihen.[114] Insofern gehört Desinformation offenbar zum «Werkzeugkasten» der politischen Machtergreifung. Unabhängig vom demobilisierenden Potential von potentiellen Wahlgegnerinnen oder vom mobilisierenden Potential der eigenen Wählerschaft erscheint hierbei die Informationsasymmetrie zwischen Werbendem (bzw. Auftraggeber) und dem Werbeempfänger als eines der zentralen Kernprobleme von Desinformation.[115]

Analyse des Phänomens «politische Desinformation»

Einfache politische Desinformation beeinflusst den politischen Meinungsbildungsprozess, indem gezielt der Informationsgehalt von Tatsachen in Frage gestellt wird. Durch Desinformation wird die Grenze legitimer Meinung verschoben, weil die (an sich unstrittige) Integrität der Faktenlage, auf die sich bezieht, nicht mehr respektiert wird.[116] Aus der Analyse zur Phänomenologie lassen sich folgende Charakterzüge von Desinformation ableiten.

Unwahrhafte politische Kommunikation

Ein wesentliches Element von Desinformation ist Kommunikation[117] – es geht um politische Kommunikation bzw. Einflussnahme auf den politischen Diskurs. In dieser Kommunikation werden irreführende Informationen einer breiten Masse kommuniziert. Ein wichtiger Bestandteil von einfacher politischer Desinformation ist zudem die Unwahrhaftigkeit. Desinformation muss nicht notwendigerweise empirisch falsche Information

114 Zerback/Töpfl (2022), 399 ff.; eindrücklich bei Mansell et a. (2025), 147, 166.
115 So Tufekci (2015), 203, 207 ff., die dies als „algorithmic harms" bezeichnet.
116 Siehe Arendt (1972), 57 f.: Meinungen sind legitim, „solange sie die Integrität der Tatbestände, auf die sie sich beziehen, respektieren. Meinungsfreiheit ist eine Farce, wenn Informationen über Tatsachen nicht garantiert ist."; s.a. Mahlmann (2023), 9, 22 f.
117 Ebenso Zimmermann/Kohring (2018), 530 ff.

sein, denn auch evidenz-basierte Information kann zu Desinformation führen, wenn sie aus dem Kontext gerissen und damit in ihrem Informationsgehalt verzerrt wird.[118] Während also Unwahrheit nicht als essentielles Charakteristikum für Desinformation taugt, kommt dem Element der «Unwahrhaftigkeit», d.h. dem Umstand, wonach der Urheber selbst nicht an die Gültigkeit seiner verbreiteten Tatsachenbehauptung glaubt, erhebliche Bedeutung zu. Dies erscheint als das zentrale Unterscheidungsmerkmal von Desinformation gegenüber unwissentlicher Fehl- bzw. Falschinformation (etwa redaktionelle Fehler, die unbewusst aufgrund von Geld- oder Zeitmangel passieren): Letztere stellt zwar gleich wie Desinformation eine potentiell irreführende Information dar, ihr fehlt jedoch das der Desinformation innewohnende intentionale Element.[119] Denn während der Urheber von fahrlässiger Fehlinformation an die Gültigkeit seiner verbreiteten Tatsachenbehauptung glaubt, tut dies der Urheber von Desinformation gerade nicht.[120] Letztlich verkehrt einfache politische Desinformation liberale Grundrechte wie das Meinungsfreiheitsrecht oder das Recht auf politische Öffentlichkeitsinformation ins Gegenteil: Unter dem Vorwand von Grundrechteschutz werden freiheitsgefährdende Inhalte für antidemokratische Zwecke verbreitet.[121]

Unterminierung von Kompromisshaftigkeit

Damit zielt Desinformation auf das Herz demokratischer Ordnungen: Demokratische Ordnungen sind nämlich inhärent kompromisshaft und erfordern von den Individuen einer pluralistischen Gemeinschaft ein Mindestmass an Toleranz. Demokratische Regierungsformen agieren nicht mit dem Ziel des expertokratisch besten Ergebnisses. Vielmehr wird das ausdifferenzierte und nach Abwägung mit unterschiedlichen Interessen zu treffende Ergebnis gesucht, das infolge von Vermittlungen und Kompromissen unter

118 Instruktiv Entman (1993), 51 ff.; Entman/Usher (2018), 298 ff.; vgl. auch Zimmermann/Kohring (2018), 526, 533, 534, 535.

119 Bader/Jansen/Rinsdorf (2020), 33, 42 ff. heben treffend die Eigenschaft von Fake-News als „Pseudo-Journalismus" hervor.

120 Instruktiv Frattolillo (2021), 217; Gunjic (2020), 179, 181 f.; Hartmann (2019), 81, 82 ff.

121 Rotte (2022), 69, 76.

Inklusion eines möglichst breiten Meinungsaustausches gefunden wird.[122] In den Worten von Hans Kelsen ist der Kompromiss das Herz der Demokratie, nämlich das «Zurückstellen dessen, was die zu Verbindenden trennt, zugunsten dessen, was sie verbindet.»[123]

Dieser Anspruch an die demokratische Herrschaftsform kommt nicht nur im direktdemokratischen System der Schweiz par excellence zum Ausdruck, sondern findet auch in normativen Leitbildern europäischer Gesellschaften, wie etwa der Europäischen Union, seinen Niederschlag. So heisst es in Art. 2 EUV, dass die europäische Gesellschaft eine sei, «die sich durch Pluralismus, Nichtdiskriminierung, Toleranz, Gerechtigkeit, Solidarität und die Gleichheit von Frauen und Männer auszeichnet», unter den Werten «der Achtung der Menschenwürde, Freiheit, Demokratie, Gleichheit, Rechtsstaatlichkeit und Wahrung der Menschenrechte einschliesslich der Rechte der Personen, die Minderheiten angehören». Dies sind jene Grundprinzipien, auf deren Basis hoheitliche Herrschaftsakte durchzuführen sind. Weil den aufgezählten Werten ein relational-personales Verständnis inhärent ist, bedarf Herrschaftsausübung unter diesen Prämissen keine Majoritätsdiktatur, sondern Diskursivität und (noch viel wichtiger) Kompromisshaftigkeit. Kompromisshaftigkeit ist deshalb das demokratische Herz der europäischen Gesellschaft.[124] Angesichts dieser Prämissen wird politische Desinformation zur Zerstörung demokratischer Kompromisshaftigkeit genutzt.[125] Denn Desinformation zielt unmittelbar auf «legale Diffamierung» des politischen Gegners (mit dem Ziel, gegnerische Wählerschaft vom Urnengang abzuhalten) und Polarisierung[126] (mit dem Ziel zur Generierung neuer und Konsolidierung bestehender Wählerschaft) ab. Mittelfristig bezweckt Desinformation die Erosion demokratischer Gesprächs- und Kompromissbereitschaft: Wer den politischen Gegner als Feind brandmarkt, kann seiner Wählerschaft nicht mehr glaubwürdig Kompromisse

122 Statt vieler s. Mahlmann (2023), 9, 20 ff., 30 ff. m.w.N.; s.a. Mansell et a. (2025), 55 f., 156.

123 Kelsen (1929), 57.

124 V. Bogdandy (2022), 15.

125 Vor diesem Hintergrund her stösst Desinformation gerade im US-amerikanischen Politiksystem auf fruchtbaren Boden: denn das heutige politische System definiert sich aus seiner partisanship (Kompromiss ist demnach ein Verrat an der Sache); das europäische Modell hingegen aus der Pluralität seiner Vermittlungen (Kompromiss als politische Tugend): Martin (2016), 199 ff.

126 Instruktiv aus öffentlich-rechtlicher Sicht die Beiträge in Uhle/Friehe (2022) sowie Baade (2023), 565 ff.

verkaufen, die mit diesem «Feind» ausgehandelt wurden.[127] Daher ist es für die Zwecke erfolgreicher Desinformationskampagnen nicht nötig, ein bestimmtes falsches Narrativ zu fördern – es genügt, viele verschiedene (sogar untereinander unvereinbare) Narrative zu erzeugen, die dann die Wahrheitsfindung unmöglich erscheinen lassen. Dies lässt sich durch moderne digitale Kommunikationsmittel sehr einfach und überaus breitenwirksam bewerkstelligen.[128] Die verschiedenen Ausprägungen von einfacher politischer Desinformation gründen gleichzeitig auf dem Potential von sozialen Netzwerken, als Online-Plattformen Informationen ungefiltert und ohne (redaktionelle) Intermediäre algorithmengestützt nach ökonomischen Gesichtspunkten verbreiten zu können.[129] Das wirft die Frage auf, welche ökonomischen Gesichtspunkte für die algorithmische Verbreitung von Desinformationen auf grossen Online-Plattformen ausschlaggebend sind.

Empörungsökonomie und Empörungsdemokratie

Das Geschäftsmodell von sozialen Medien (z.B. Facebook oder Twitter), aber auch von grossen Online-Dienstleistern wie Suchplattformen (z.B. Google oder Bing), welche gebührenfrei genutzt werden können, ist die Nutzung von Kundendaten zum Verkauf von personalisierter Online-Werbung (sog. Micro-Targeting).[130] Ziel ist es, Plattform-Nutzende möglichst lange auf der eigenen Datenplattform zu halten, denn dadurch kann das Datenunternehmen mehr digitale Werbeflächen verkaufen und gleichzeitig mehr Daten sammeln. Dass die Datensammlung letztlich auch ausdrücklich das Geschäftsmodell von Social-Media-Plattformen darstellt, haben nicht zuletzt zuletzt Whistleblower eindrücklich dargelegt.[131] Für die Plattformen stellte sich hier die Frage, wie das Erlebnis von Nutzerinnen und Nutzer auf sozialen Netzwerken zeitlich verlängert werden könnte, damit Online-Werbung entsprechend lukrativ platziert werden kann.

127 Deutlich Levitsky/Ziblatt (2018), 204: „Von Newt Gingrich bis zu Donald Trump haben republikanische Politiker gelernt, dass es in einer polarisierten Gesellschaft nützlich sein kann, den politischen Gegner als Feind zu brandmarken. Denn Politik als Kriegsführung zu betreiben wirkt auf diejenigen anziehen, die viel zu verlieren haben."; s.a. Baade (2023), 411.

128 Baade (2023), 411 m.w.N.

129 Überblicksweise zur digitalen Revolution für die öffentliche Kommunikation s. Saxer (2020) 2371, 2372 ff.

130 Habermas (2022), 54; Schemmel (2018), 501, 508; ausführlich Laux (2024), 335 ff.

131 Frenkel/Kang (2021).

In der Medienforschung[132] findet sich diesbezüglich das Erklärungsangebot der Empörungsökonomie.[133] Demnach wird versucht, die Aufmerksamkeit von Medienkonsumenten anzuziehen, indem man Empörung schürt.[134] Das Erklärungsmodel fusst auf psychologische Grundkenntnissen, wonach einerseits Menschen emotionalen Reizen mehr Aufmerksamkeit zuwenden als nicht-emotionalen Impulsen[135] und andererseits Empörung per se menschliche Mitteilungsbedürfnisse auslöst.[136] Für Medienunternehmen lohnt es sich demnach, ihre Meldungen in dystopischem Stil zu veröffentlichen, um dadurch Medienkonsumenten länger auf ihren Plattformen zu halten, sie zu Interaktionen[137] zu animieren und sie letztlich zum Klicken auf Werbung zu veranlassen.[138]

Dieses Erklärungsmodell für Erfolgsfaktoren von Informationsdienstleistungen in sozialen Netzwerken lässt sich plausibel für Desinformation in sozialen Netzwerke fruchtbar machen.[139] In sozialen Medien ist es technisch sehr einfach, dem durch Empörung ausgelösten zwischenmenschlichen Mitteilungsbedürfnis nachzukommen – der «Gefällt mir»-Button ist ein wichtiger Bestandteil des Geschäftsmodells sozialer Netzwerke.[140] So teilte Facebook selbst in einer Pressemitteilung mit, dass das Engagement von Facebook-Nutzern exponentiell ansteige, je näher der Inhalt an illegale oder von der Plattform verbotene Inhalte herankommt.[141] Inzwischen ist

132 Überblick bei Högden/Krämer/Meinert/Schaewitz (2020), 77 ff.; zentral etwa Pörksen (2018); zuletzt Mansell et a. (2025), 57, 80.

133 Instruktiv Klein (2020); vgl. auch Pörksen (2018), der allerdings von „Empörungsdemokratie" spricht.

134 Khan/Pozen (2019), 497, 505; Paal (2018), 567; Drexl (2019); vgl. Bader/Jansen/Rinsdorf (2020), 33 ff., die Fake-News als ein Geschäft mit der Angst darstellen.

135 S. insb. Högden/Krämer/Meinert/Schaewitz (2020), 77, 81: „Oftmals werden Falschnachrichten so konzipiert und kommuniziert, dass sie die Emotionen und Gefühle der Rezipientinnen ansprechen anstatt Fakten zu transportieren."

136 Instruktiv Fichter (2021), 26 ff sowie Hong (2022), 126, 161 f.

137 Inzwischen lässt sich in Sozialen Medien gezielt provozierende oder polarisierende Stellungnahmen (sog. „Rage-Baiting") beobachten, um starke emotionale Reaktionen wie Wut oder Empörung auszulösen; das Ziel ist dabei, die Interaktionsrate auf sozialen Medien oder Webseiten zu erhöhen, indem Menschen dazu gebracht werden, Inhalte zu kommentieren, zu teilen oder darauf zu reagieren – auch wenn diese Reaktionen negativ sind.

138 So die Kernaussage der Soziologin Tufekci (2012); vgl. auch Mafi-Gudarzi (2019), 65 f. m.w.N.

139 Insofern spricht Preuß (2021), 75 von Fake-News als „Lockstoff".

140 Hartmann (2019), 81, 88 f.

141 Zuckerberg (2018).

bekannt, dass Facebook über seine Algorithmen den sog. News-Feed kuratiert und reisserische Inhalte ausdrücklich begünstigt.[142]

Doch dieses Phänomen beschränkt sich nicht auf soziale Medien. Auch bei Online-Suchmaschinen scheint das Geschäftsmodel der Empörungsökonomie zu verfangen,[143] zumindest besteht gegenüber der automatischen Suchwort-Vervollständigung gewisser Suchmaschinen bereits seit längerem ein diesbezüglicher Verdacht.[144] So hatte der Suchalgorithmus von Google mehrere Wochen vor dem Sturm auf das US-Kapitol am 6. Januar 2021 bei der automatischen Vervollständigung des Schlagwortes «Bürgerkrieg» Vervollständigungsempfehlungen wie «Bürgerkrieg kommt», «Bürgerkrieg ist da» oder «Bürgerkrieg ist unvermeidlich» angezeigt. Ein interessantes Randdetail besteht darin, dass diese Vorschläge zur Autovervollständigung nicht mit dem entsprechenden Volumen von Nutzeranfragen übereinstimmte,[145] weshalb der logische Schluss naheliegt, dass diese Vorschläge algorithmisch nach empörungsökonomischen Grundsätzen kuratiert sind. Ähnliche Beobachtungen liessen sich auch bei anderen Plattformen nachweisen.[146] So empfahl der Suchalgorithmus der Verkaufsplattform Amazon während der Covid-19-Pandemie eine Vielzahl von Büchern mit Verschwörungstheorien.[147]

Welche Schlussfolgerungen ergeben sich auf der Grundlage der vermeintlichen Demokratisierung des Informationsflusses, der in Wahrheit die Ausschaltung redaktioneller Intermediäre bezweckt und die algorithmengestützte Verbreitung von «*lawful but awful*»-Inhalten unterstützt? Erstens bewirkt das Weglassen eines redaktionellen Intermediärs, dass objektive Sachverhalte und Fakten hinter «*paywalls*» von qualitativ hochwertigen Journalismus-Produkten verschwinden, während Lügen kostenfrei zugänglich sind.[148] Die Medienvielfalt als essentielles Instrument demokratischer Meinungsbildung wird verzerrt, weil qualitative Quellen und Informatio-

142 Frenkel/Kang (2021).
143 Vgl. die ausführliche Studie bei Hao (2021).
144 Siehe etwa die Studien über Korelationen zwischen Autovervollständigung und Stereotypen bei Baker/Potts (2013), 187 ff.; Roy/Ayalon (2020), 1020 ff.; hinsichtlich Verschwörungstheorien bei Al-Rawi/Celestini/Steward/Worku (2022).
145 Chaslot (2021).
146 Für eine Auswertung zur Verbreitung von Verschwörungstheorien auf der digitalen Videoplattform YouTube s. Allgaier (2022), 83, 88 ff.
147 Rudl (2021).
148 So die dramatisch zugespitzte Formulierung des Chefredakteurs von „Current Affairs" Robinson (2020).

nen nur gegen Bezahlung, (nicht als solche gekennzeichnete) Desinformationen hingegen massenhaft auf den sozialen Medien und Online-Suchmaschinen zu finden sind. Zweitens haben die Informationen, die aus der Empörungsökonomie stammen, einen anderen inhaltlichen Gehalt: Anders als für den staatsbürgerlichen Wahlakt so wichtige Faktenvermittlung bzw. Unterstützung von Meinungs- und Willensbildung zeigen Desinformationskampagnen, dass ihr Kerngeschäft gerade emotionale Botschaften (im Negativen wie im Positiven) darstellen. Die Überzeugungskraft von Desinformations-Beiträgen hängt von der benützten Sprache, der Kombination mit entsprechenden Bildern und dem entsprechenden Kontext ab. Insofern wird durch Desinformationskampagnen in sozialen Medien der ursprüngliche Informationsauftrag der vierten Gewalt, nämlich zur Meinungs- und Willensbildung des informierten Staatsbürgers beizutragen, verzerrt, indem um die Aufmerksamkeit (nicht von Bürgerinnen und Bürgern, sondern) von Konsumenten zum Zweck kommerzieller Dienstleistungen konkurriert wird.[149] Insgesamt besteht also die Gefahr, dass das Zeitalter der digitale Informationsgesellschaft der Ära einer Empörungsdemokratie Bahn bricht.[150]

Soll gegen die vitale Demokratiebedrohung das schärfste Instrument des Staates in Stellung gebracht werden?

Wenn Desinformation das Herzstück der Demokratie angreift, liegt es nahe, dass der demokratische Rechtsstaat sein schärfstes Schwert in Stellung bringt, um dieser vitalen Bedrohung zu begegnen. Konkrete Diskussionsentwürfe für neu zu schaffende Straftatbestände zur unmittelbaren Kriminalisierung von einfacher politischer Desinformation wurden etwa von Bernd Schünemann[151], Tabea Preuß[152] und Markus Schreiber[153] formuliert.

149 Ähnlich Habermas (2022), 57, in diese Konkurrenzsituation zwischen der Presse und den Online-Plattformen treffend beschreibt.

150 Schick (2020), 9 f. zeichnet das dystopische Bild einer „Infokalypse" vor.

151 Schünemann (2019), 639: «Gefährdung der Demokratie und des Friedens durch Falschnachrichten:
(1) Ein Amtsträger, der öffentlich eine falsche Tatsache behauptet, die geeignet ist, zum Hass gegen andere aufzustacheln, Wahlberechtigte bei ihrer Stimmabgabe zu beeinflussen, einen schweren Nachteil für das internationale Ansehen oder die äußere Sicherheit der Bundesrepublik Deutschland zu verursachen, insbesondere ihre friedlichen Beziehungen zu anderen Staaten zu beeinträchtigen, oder einen großen Personenkreis zu beunruhigen und dadurch die öffentliche Ordnung zu stören, wird mit Freiheitsstrafe nicht unter einem Jahr bestraft.

Unabhängig davon, inwiefern man die konkreten Diskussionsentwürfe zustimmungswürdig findet,[154] sollte jedenfalls darüber reflektiert werden, ob das Strafrecht tatsächlich das Mittel der Wahl zur «Bekämpfung» von einfacher politischer Desinformation sein sollte. Im Folgenden sollen dazu einige Argumente näher betrachtet werden.

(2) Wer die in Absatz 1 bezeichnete Handlung als Mitarbeiter von Rundfunk- und Fernsehanstalten, überregionaler Presse, Nachrichtenagenturen oder gewerblichen Internetplattformen vornimmt, wird mit Freiheitsstrafe bis zu fünf Jahren bestraft.
(3) Wer als Mitwirkender einer Rundfunk- oder Fernsehsendung, Verfasser von Leserbriefen oder im Internet die in Absatz 1 bezeichneten Handlungen gemeinschaftlich mit anderen oder unter besonderen Zurüstungen absichtlich vornimmt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(4) [Regelung für minderschwere Fälle, gestaffelt nach den Absätzen 1 bis 3].».

152 Preuß (2021), 178 mit ihrem Vorschlag eines neuen § 126a StGB zur Störung des öffentlichen Friedens durch falsche Tatsachen: «(1) Wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, eine falsche Tatsache veröffentlicht oder öffentlich verbreitet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Gefängnisstrafe bestraft.
(2) Wer die Tat nach Absatz 1 in einer Weise begeht, die geeignet ist, die äußere Sicherheit oder die internationale Reputation der Bundesrepublik zu gefährden oder ihre internationalen Beziehungen negativ zu beeinflussen, einen anderen zu veranlassen, sein Wahlrecht in einembestimmten Sinne auszuüben oder gegen eine nationale, rassische, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zuge-hörigkeit zu einer vorbezeichneten Gruppe oder zu einem Teil der Bevölkerung zum Hass aufzustacheln, wird mit Freiheitsstrafe nichtunter einem Jahr bestraft.».

153 Schreiber (2022), 293: «Politische Einflussnahme durch Falschinformation: Wer wider besseres Wissen öffentlich eine unwahre Tatsache mit Wahrheitsanspruch, die geeignet ist, Wahlberechtigte bei der Ausübung ihres Wahlrechts in einem bestimmten Sinn zu beeinflussen, unter Verwendung eines reichweitenvergrößernden Computerprogramms behauptet oder verbreitet, wird (…) bestraft.»; der Autor entwickelt seinen konkreten Vorschlag in Auseinandersetzung mit dem Textvorschlag von Schünemann, dessen Sonderdelikt er für derzeit nicht legitimierbar hält, weshalb sein Gegenentwurf auf strafrechtlich relevante Gefährlichkeit von Desinformation für vitale Momente einer Demokratie beschränkt bleibt: Schreiber (2022), 301 ff., 309.

154 Vgl. Kusche (2020), 421, 431, der Tatbestandsfragen als neuralgischen Punkt des Kriminalisierungsvorhabens bei Fake News identifiziert.

Vorzüge strafrechtlicher Regulierung

Symbolhaftigkeit der Reaktion auf demokratie-vitale Bedrohung

Befürworterinnen und Befürworter der Kriminalisierung von politischer Desinformation gehen vom honorigen Anliegen aus, den demokratischen Rechtsstaat zu beschützen: Sie anerkennen die vitale Bedrohung, die durch Desinformationskampagnen ausgehen und bringen gegen diese das Strafrecht als schärfste Schwert des Staates in Stellung.[155] Anders gewendet, rechtfertigt sich der Einsatz von Strafrecht als besondere Reaktion auf ein qualifiziertes rechtliches Fehlverhalten.[156] Politische Desinformation stellt insofern ein strafwürdiges Handlungsunrecht dar.

Doch auch wenn man weniger die Bedrohungskapazität von Desinformation i.S.d. Handlungsunrechts fokussiert, sondern das Angriffsobjekt selbst i.S.d. Erfolgsunrechts betrachtet, könnte man mit dieser Überlegung auf den Einsatz von Strafrecht als staatliche Reaktion rekurrieren, nämlich wenn man staatliche Strafe als Reaktionsmöglichkeit zur Verteidigung des Rechts per se auffasst.[157] Denn durch Desinformation wird der demokratische Entscheidungsfindungsprozess unmittelbar angegriffen, was sich unter anderem auf die politische Zusammensetzung des Legislativorgans und darüber hinaus auf weitere Staatsorgane auswirkt. Vor dem Hintergrund, dass der Erfolg von Desinformationskampagnen von weiteren Umständen wie der Passivität politischer Gegnern, bestimmter Gatekeeper (z.B. politische Parteigremien oder journalistische Medien)[158] und der Wählerschaft selbst (die Demokratie nur noch «duldet», nicht jedoch aktiv dafür eintritt)[159] abhängt, würde eine strafrechtliche Verurteilung von Desinformation sowohl hinsichtlich der Mikro- als auch zur Makrodimension eine hohe Symbolkraft aufweisen, mit der die vitale Bedrohung der Demokratie gerade hinsichtlich der Makrodimension von Desinformation bekämpft werden kann.

155 Schünemann (2019), 620 ff.; Schreiber (2022), passim.
156 Vgl. Günther H.-L.(1983), 394.
157 Instruktiv Sauer (2021), 63 f., wenngleich mit dem ausserstrafrechtlichen Blick auf hoheitliche Rechtsverletzungen.
158 Baade (2023), 420 m.w.N.
159 Vgl. die These von Baurmann (2022).

Nutzung strafrechtlicher Verfolgungsinstrumentarien

Ein weiterer wichtiger Vorzug strafrechtlicher Verfolgbarkeit von politischer Desinformation liegt im Potenzial von ermittlungstechnischen Möglichkeiten, die Strafverfolgungsbehörden zur Aufklärung von Straftaten und Identifikation von Tätern einsetzen zu können, sofern aufgrund der Strafdrohung entsprechende Zwangsmassnahmen zur Verfügung stehen. So können Strafverfolgungsbehörden die Urheber anonymer Desinformationskampagnen durch das zur Verfügung stehende Instrumentarium an invasiven Ermittlungsmassnahmen wesentlich besser ausfindig machen als private Akteure auf dem zivilprozessualen Weg.[160] Doch nicht nur bei der Identifikation, sondern auch bei der Repression derartiger Taten können strafrechtliche Reaktionsmöglichkeiten wirkungsvoll sein, seien es solche, die sich gegen den Täter selbst oder aber gegen mit der Tat zusammenhängende Gegenstände oder Informationen richten. Die Invasivität strafrechtlicher Mittel hat daher durchaus Vorzüge gegenüber anderen rechtlichen Reaktionsmöglichkeiten.

Der Einsatz von Strafrecht ermöglicht insofern die Bekämpfung eines sozial schädlichen Phänomens durch die geballte staatliche Herrschaftsmacht. Insofern verwundert es auch nicht, wenn gerade autokratische Systeme im Strafrecht eines der ersten Mittel zur Bekämpfung Andersdenkender und politischer Opponenten erblicken.[161] Ob sich dies demokratische Rechtsstaaten liberaler Tradition ebenso leisten können oder sollen, steht freilich auf einem anderen Blatt.

Abschreckungseffekt

Die vorher skizzierte Nutzung von Staatsmacht zur Bekämpfung von Desinformation zum Schutz des Einzelnen und der Gesellschaft intendiert letztlich auch die Abschreckung vor der Begehung von Straftaten, nämlich in zwei unterschiedlichen Ausprägungen: Es geht einerseits um die Abschreckung des individuellen Täters vor der Begehung weiterer Strafen (Spezialprävention), andererseits um die Kommunikation mit der Allge-

160 Vgl. Staffler (2021), 217, 221 im Zusammenhang mit der Identifizierung von „Produktpiraten".

161 Mit Blick auf die Ausrichtung des NS-Strafrechts im Dritten Reich eindrücklich Ambos (2019), 44 ff.; mit Blick auf sozialistische Diktaturen Mirschel (2021), 69 ff. sowie Gerlant (2021), 271 ff.; allgemeinhin Mahlmann (2023), 9, 33.

meinheit, die durch Strafdrohung und -vollzug von der Übertretung der gesetzlichen Verbote abgehalten werden soll (negative Generalprävention).[162] Wenn aus Anlass von Desinformation strafrechtliche Ermittlungen, medienwirksame Gerichtsverfahren und schliesslich strafrechtliche Verurteilungen ergehen, ist dies nicht nur ein kommunikativer Akt gegenüber dem einzelnen Täter und den von seiner Tat betroffenen Opfern, sondern auch eine in die Zukunft gerichtete Kommunikation, die potenziell tatgeneigte Personen abschrecken soll. Ob allgemeinhin das Strafrecht generalpräventive Wirkungen nachweisbar entfaltet, ist ungelöst und braucht hier nicht näher reflektiert werden. Mit Blick auf autoritäre Regime zeigt sich zumindest, dass strafrechtliche Mittel einen derartigen abschreckenden Effekt intendieren, der teilweise wohl auch gelingt. Doch selbst dort kann der Abschreckungseffekt in Zweifel gezogen werden, gerade wenn Urheber von vermeintlich gefährlichen Informationen als ausländische Agenten oder Spione diffamiert werden, weil man ihnen nicht auf eine andere Weise habhaft wird.[163]

Solidarisierung durch Strafausspruch

Ein weiteres Argument zugunsten der Kriminalisierung einfacher politisches Desinformation ergibt sich aus der (individuellen) Opferperspektive und betrifft insofern allein die Mikrodimension von Desinformation. Personen wie das oben beschriebene Beispiel der deutschen Aussenministerin (N 20), die von Desinformationskampagnen betroffen sind, würden sich naheliegenderweise durch eine strafrechtliche Verurteilung der betreffenden Täter wohl weniger eine Genugtuung im Hinblick auf die konkret ausgesprochene Strafe, als vielmehr den mit dem staatlichen Strafausspruch einhergehenden kommunikativen Akt der Solidarisierung wünschen: Durch die strafrechtliche Verurteilung des Täters stellt sich die Rechtsordnung symbolisch an die Seite des Opfers.[164] In den Worten des Soziologen Reemtsma hat das Strafrecht «klarzustellen, auf wessen Seite

162 Roxin/Greco (2020), § 3 N 11 ff., 21 ff.; vgl. im Überblick auch Papathanasiou (2019), 151, 157 f. m.w.N.

163 Das zeigt sich letztlich auch am System Putins, das gerade Anfang September 2022 erhebliche Risse bekommen hat.

164 Staffler (2020), 53, 69 ff. m.w.N.

das Recht und auf wessen Seite das Unrecht ist.»[165] Dieser Gedanke fusst auf einer Konzeption von Strafrecht, die das expressive Element des Strafausspruchs im Sinne einer gesellschaftlichen Kommunikation über gesetzte soziale Mindeststandards betont.[166] Diese Konzeption von Strafrecht verfängt insb. auch ausserhalb der Strafrechtswissenschaften, namentlich in der Verfassungstheorie.[167]

Auch wenn dieser Ansatz gerade in Bezug auf konkrete Einzelfälle vielversprechend scheint, ist er in seiner Allgemeinheit eher unbrauchbar. Denn mangels eines fassbaren kollektiven Schadens bzw. einer geschädigten Gruppe gibt es wohl kein hinreichend konkretisierbares «kollektives Opfer» der Desinformation, welches die Solidarisierung durch einen Strafausspruch für sich in Anspruch nehmen könnte. Der Grundgedanke von Solidarisierung durch Strafausspruch orientiert sich primär an der Perspektive von Individuen, weniger an Kollektiven.[168]

165 Hassemer/Reemtsma (2002), 163; ähnlich auch Hörnle (2006), 950, 956: „Das Unwerturteil hat nicht nur den Täter zu tadeln, sondern auch die Einbußen, die das Opfer erlitten hat, anzuerkennen und sich mit ihm zu solidarisieren."

166 Vgl. insb. Duff (1986), 235 ff.; Günther K. (2002), 205, 207 ff.; Hassemer (2001), 1001, 1112 ff.; Hörnle (1999), 112 ff.; Kühl (2005), 149; Zürcher (2014), 127 ff.; neuerdings Frisch (2019), 537, 547 ff.; Hirsch (2021).

167 Vgl. Nettesheim (2022), 93, 102 ff., insb. S. 108: „Es geht vielmehr darum, dass die (in einer Gesellschaft von Menschen unweigerlich eintretende) Verletzung einer Verhaltensnorm in einem besonderen institutionellen ‚setting' gegenüber dem Verletzer, aber vor den Augen der Öffentlichkeit behandelt wird. Eine Präventionswirkung ist nicht das Ziel staatlichen Strafens, sondern *eine faktische Folge des gerechten staatlichen Strafens mit Öffentlichkeitswirkung*." (Hervorhebungen im Original).

168 Diese Annahme gründet auf der möglichen Konzeption von Kollektivbeleidigungen, die nach herrschenden Ansicht nur dann vorliegen, wenn die beleidigte Personengemeinschaft einen rechtlich anerkannten Zweck erfüllen und einen einheitlichen Willen bilden kann, s. Kühl (2018), N 5; nach a.A. sind Kollektive überhaupt nicht beleidigungsfähig, einen Überblick zum Meinungsstand gibt Kargl (2023) N 71 ff m.w.N.; in der Schweiz kommet es entscheidend darauf an, inwiefern erkennbar Einzelne betroffen sind, s. Trechsel/Lehmkuhl (2021), N 14; wenn also Kollektive nur unter eingeschränkten Voraussetzungen beleidigbar sind, ist auch eine Solidarisierung durch Strafausspruch nur eingeschränkt möglich.

Nachteile strafrechtlicher Regulierung

Welches Rechtsgut?

Die Rechtsgüterdiskussion stellt für die (deutschen) Strafrechtswissenschaften einen wichtigen Baustein zur kritisch-konstruktiven Bewertung von Strafnormen dar.[169] Deshalb hat ein strafrechtliches Regulierungsanliegen, wie etwa die Kriminalisierung einfacher politischer Desinformation, das durch die zu schaffende Norm geschützte Rechtsgut offenzulegen.[170] Anders gewendet bildet das Rechtsgut den Dreh- und Angelpunkt für die strafrechtswissenschaftliche Diskussion über die Legitimität eines neu zu schaffenden Straftatbestandes,[171] denn es identifiziert die mit Strafnormen zu schützenden Interessen und ermöglicht deshalb eine – für den Kontext des Untersuchungsgegenstand wichtige – kritische Auseinandersetzung mit der konkreten Tatbestandsformulierung.[172]

Bei einer Bestrafung von einfacher politischer Desinformation stellt sich die Frage, was überhaupt das zugrundeliegende Rechtsgut ist, welches man zu schützen intendiert. Antworten wie «Wahrheit», «Demokratie» oder «Wählerwillen» mögen zwar naheliegend sein, doch sind derartige Begriffe als Rechtsgüter kaum tauglich, weil sie als Schutzobjekt einerseits weitgehend konturlos und andererseits überaus wertungsanfällig sind.[173] Erstens besteht dann die Gefahr, dass bereits die blosse Verbreitung falscher Tatsachenbehauptung (und insofern das einfache Lügen) strafbar ist, was aus guten Gründen abzulehnen ist.[174] Zweitens steigt durch den Fokus auf derartige Rechtsgüter das potenzielle Instrumentalisierungs- und Rechtsmissbrauchsrisiko strafrechtlicher Normen erheblich.

Vor diesem Hintergrund sind die Bemühungen einiger Autoren zu verstehen, die angesichts der existentiellen Bedrohung von demokratischen Ordnungen durch einfache politische Desinformation strafrechtliche Ver-

169 Statt vieler s. Hörnle (2003), 268 mwN; zu den modernen Aufgaben einer kritischen Strafrechtswissenschaft s. Oberholzer (2002), 221, 226 ff.; Vest (2017), 256 ff.; Coca-Vila (2023), 79 ff.

170 Vgl. auch Gkountis (2010), 176 ff.

171 Vgl. die Beiträge in Hefendehl/Von Hirsch/Wohlers (2003) sowie, statt vieler, Kubiciel (2018), 143, 151 ff. und Roxin/Greco (2020), § 2 N 7 ff. m.w.N.

172 S. Kubiciel/Weigend (2019), 35 ff.

173 Cavaliere (2022), 481 ff.; Lammich (2022) 121 f.; Roseneck (2023), 61, 70 ff.

174 In der Literatur wurde dies überzeugend ausgeführt, s. Becker (1948), 1 ff.; Köhler (1985), 2389; zuletzt etwa Hoven (2017), 718, 739 f.

botsnormen in Stellung bringen möchten und argumentieren, dass es nicht um die Kriminalisierung von Lüge als solche geht, «sondern nur die Verletzung eines schutzwürdigen Interesses *durch die Lüge*»[175]. Dieses schutzwürdige Interesse, das durch Desinformation angegriffen wird, könnte im menschenrechtlichen Anspruch auf Information im politischen Bereich verortet werden.[176] Das Anliegen dieser Autorenschaft verdient grundsätzlich Beifall. Gleichwohl erscheint es aber fraglich, ob durch diese Konstruktion die vorher unter N 78 vorgetragenen Bedenken ausgeräumt werden können. Denn die Lüge bleibt weiterhin Bestandteil der Rechtsgutsidentifikation, wenngleich lediglich ihre instrumentalen Ausprägung stärker betont wird. Letztlich setzt der Vorschlag wiederum auf konturarme Begriffe, was die oben beschriebenen Gefahren nicht zu entkräften vermag.

Geht man zutreffend davon aus, dass die strafrechtsdogmatische Kategorie des Rechtsguts dazu dient, das legitime strafrechtliche Schutzobjekt analytisch zu identifizieren, so erscheint der strafrechtliche Schutz angesichts der mangelnden Konkretheit des Wahrheitsbegriffs[177] überzogen. Letztlich mag eine einzelfall-bezogene topisch-begründete Rechtsanwendung im Zivil- oder Verwaltungsrecht tolerabel sein und politische Desinformation mit derartigen rechtlichen Möglichkeiten eingehegt werden; im Strafrecht hingegen, welches die Verantwortung der Normadressaten für die Verletzung geltenden Rechts symbolisch markiert und auf eine Tat mit einer Übelszufügung reagiert, sind wachsweichen Grenzziehungen nicht tolerabel.

Vollzugsdefizit mit Ansage

Eine Kriminalisierung von einfacher politischer Desinformation würde erwartbar zu einer hohen zusätzlichen Arbeitsbelastung der Strafjustiz führen. Denn einerseits erfährt das Phänomen in vielfältigen Spielarten eine grosse Verbreitung auf den sozialen Medien. Andererseits sind die mit knappen finanziellen und personellen Ressourcen ausgestatteten Polizeikräfte und Staatsanwaltschaften bereits durch den Schwung der Digita-

175 Schünemann (2019), 621 (Hervorhebung im Original), 627; neuerdings auch Soares (2023), 179, 181 ff.

176 Schünemann (2019), 637; wohl zustimmend Kusche (2020), 421, 430 f.

177 Zu den unterschiedlichen Bedeutungen von Wahrheit im Kontext der Philosophie s. Hügli/Lübcke/Bafandi (2013), 935 ff.

lisierung[178], insb. durch Cybercrime und Hasskriminalität, an Kapazitätsgrenzen gestossen.[179] Die Implementierung eines neuen Straftatbestandes, der primär auf die digitale Welt abzielt, würde die Arbeitsbelastung weiter steigern und einen erheblichen zusätzlichen öffentlichen Finanzierungsbedarf generieren.[180]

Natürlich liesse sich dieser Einwand durch grosszügigere finanzielle Ausstattung von Strafverfolgungsbehörden zumindest teilweise entkräften. Dann stellt sich aber die Frage, ob die erhöhte Kapazität von Strafverfolgungsbehörden tatsächlich zielführend ist, um einfache politische Desinformation durch die Strafverfolgung fernzuhalten. Denn nicht wenige Akteure, die politische Desinformation etwa als Element hybrider Kriegsführung[181] betreiben, agieren aus dem Ausland und entziehen sich damit dem Zugriff der inländischen Strafverfolgungsbehörden. Nationalen Verfolgungsbehörden würden dann an die Grenzen ihrer Zuständigkeit gelangen, weshalb letztlich der Effekt einer besseren finanziellen Ausstattung der Strafverfolger verpufft.

Über die Rechtshilfe in Strafsachen wird sich dieses Problem angesichts zur Heterogenität der Debatte zur Kriminalisierung von politischer Desinformation kaum lösen lassen. Denn dann scheitern Rechtshilfegesuche etwa an elementaren Erfordernissen wie der beidseitigen Strafbarkeit und Gegenseitigkeit,[182] oder auch an anderen rechtshilferechtlichen Hürden, wie etwa das Verfolgungshindernis politischer Straftaten in Art. 3 IRSG oder das Auslieferungsverbot eigener Staatsangehöriger, drohende Grund- und Menschenrechtsverletzungen (insb. hinsichtlich Art. 10 EMRK) sowie Verhältnismässigkeitsüberlegungen[183]. Abhilfe schaffen könnte hier allenfalls ein internationales Abkommen (etwa im Kontext des Europarates), das entsprechende Kriminalisierungs-, Kooperations- und Tätigkeitspflichten für die Vertragsstaaten vorsehen würde. Ob ein derartiges Unterfangen auf internationaler oder europäischer Bühne angesichts der oben unter N 78 angesprochenen Rechtsmissbrauchsanfälligkeit überhaupt politisch konsensfähig ist, ist fraglich. Letztlich erscheint das Vorhaben der Kriminalisierung politischer Desinformation eher als ein strafrechtliches Vollzugsdefizit mit Ansage.

178 Zum Begriff s. Staffler/Ebersberger (2024), 3 ff.
179 Vgl. in diesem Zusammenhang die Studie von Höffler/Festerling (2022), 161, 164 ff.
180 Ähnlich schon Preuß (2021), 172 f.
181 Rotte (2022), 69 ff.
182 Gless (2021), 113 ff. m.w.N.
183 Überblicksweise bei Gless (2021), 125 ff. m.w.N.

Strafrechtlicher Überpaternalisierung

Die strafrechtliche Regulierung von politischer Desinformation, die darauf abzielt, die Stimmbürgerinnen und -bürger zu schützen, weist einen entscheidenden strafrechtsdogmatischen Konstruktionsfehler auf: Der Grundgedanke des modernen Strafrechts liegt in der Autonomie des Rechtsgutsinhabers und dessen freie Entscheidungsgewalt. Zwar artikuliert der Strafgesetzgeber verschiedene strafbewährte Regeln des sozialen Zusammenlebens, doch die letzte Entscheidung, ob ein Rechtsgut tatsächlich verletzt ist, liegt in der Kernkompetenz des Rechtsgutsinhabers selbst. So stellt etwa der Hausfriedensbruch nach Art. 186 StGB kein allgemeines Verbot dar, andere Menschen zu besuchen: Vielmehr ist es für den Tatbestand von entscheidender Bedeutung, ob das Einverständnis des Berechtigten zum Betreten des Hauses vorliegt.[184] Entsprechende Normkonstellationen finden sich zum Medizinstrafrecht (Schutz der Patientenautonomie)[185] oder zum Sexualstrafrecht[186]. In vielen strafrechtlichen Bereichen liegt also ein Autonomieschutz vor, sodass der Rechtsgutinhaber die massgeblichen materiellen Regelungen selbst bestimmen darf. Kriminalisierung politischer Desinformation würde diesem Kerngedanken des Strafrechts wegen Überpaternalisierung der Rechtsgutinhaber zuwiderlaufen.[187]

Legitimationstheoretische Überpaternalisierung

Die vorher vorgetragene Kritik wegen strafrechtlicher Überpaternalisierung hat eine weitere, legitimationstheoretische Ausprägung. Denn die Kriminalisierung einfacher Desinformation würde einen weiteren Nebeneffekt nach sich ziehen, der sich erst auf den zweiten Blick auf das konkrete Schutzanliegen eröffnet. Durch die Implementierung einer entsprechenden Strafvorschrift sollen die Bürgerinnen und Bürger in ihrem politischen Willensbildungsprozess materiell geschützt werden. Das Anliegen mag auf

184 Delnon/Rüdy (2018), N 5, 12; BGE 112 IV 31, 33, E. 3: „Geschütztes Rechtsgut ist das Hausrecht, worunter die Befugnis zu verstehen ist, über die bestimmten Räume ungestört zu herrschen und darin den eigenen Willen frei zu betätigen. Träger dieses Rechts ist derjenige, dem die Verfügungsgewalt über die Räume zusteht, gleichgültig, ob jene auf einem dinglichen oder obligatorischen Recht oder auf einem öffentlichrechtlichen Verhältnis beruht".

185 Ege (2018), 89, 107; Geth (2021) N 6a.

186 Scheidegger (2018), 3 ff., 34 ff.

187 Zum Ganzen vgl. auch Mahlmann (2023), 9, 38 ff.

den ersten Blick valide sein, weil es auf die für eine demokratische Willensbildung notwendige Informationsgrundlage abzielt: Nur wenn die Wählerschaft eine hinreichend qualitative Informationsgrundlage erhält, welche frei von Desinformation ist, kann sie genuin ihren Willen bilden.

Auf den zweiten Blick stellt sich allerdings die Frage, welches Menschenbild ein derartiger Strafgesetzgeber von seinen eigenen wahlberechtigten Bürgerinnen und Bürgern hat.[188] Geht der (Straf-)Gesetzgeber tatsächlich davon aus, dass seine Wählerschaft nicht in der Lage ist, einfache politische Desinformation von genuin-wahrhaftiger Information zu unterscheiden? Gerade in normativer Hinsicht ist hier mit besonderer Vorsicht zu agieren. Denn in diesem Kontext stellt sich die Frage, ob Kriminalisierung einfacher politischer Desinformation nicht implizit eine Resignation zum Leitbild einer selbstverantwortlichen und mündigen Wählerschaft darstellt, die nicht mehr allein in der Lage ist, Desinformation von wahrhaftiger Information zu unterscheiden und deshalb staatliche Hilfe benötigt, um die Entscheidungsfindung im demokratischen Willensbildungsprozess vornehmen zu können.

Man mag mit empirischer Evidenz gegen das normative Leitbild eines selbstverantwortlichen und kritisch-mündigen Bürgers[189] dagegenhalten und den tatsächlichen Bedarf offenlegen, wonach Bürgerinnen und Bürger zur Resilienz gegen einfache Desinformation staatliche Unterstützung benötigen, zumal politische Desinformation durch hochprofessionelle und teilweise staatliche Akteure lanciert wird. Ferner vermag der durchschnittliche Wahlberechtigte zwar politische Meinungen und Äusserungen als solche erkennen, bei erfundenen Fakten treten jedoch Schwierigkeiten auf, gerade wenn diese von gewissen Akteuren (etwa Personen in amtlicher Funktion) oder innerhalb gewisser Institutionen formuliert werden, denen man grundsätzlich mit einem Vertrauensvorschuss begegnet.[190]

Insgesamt ist der Kriminalisierungsanspruch gegenüber einfacher politischer Desinformation, der sich auf diese Befunde stützt, dennoch gefährlich, gerade wenn als Konsequenz das normative Bild der mündigen und verantwortungsbewussten Wählerschaft aufgegeben wird. Denn dann

188 Zum strafrechtlichen Menschenbild des *homo autonomus et inspiratus* s. Papathanasiou (2019), 151 ff.; zum demokratietheoretischen Menschenbild des Bürgers s. Petersen (2019), 93 ff. (insb. mit Fokus auf direktdemokratische Elemente: S. 101 ff.).

189 Siehe allgemein Kühler (2022), 77, 84 ff. m.w.N.

190 Instruktiv Sutter (2020), passim (insb. im Hinblick auf die Rolle des Strafrechts: S. 448 f.).

besteht die Gefahr der durch Kriminalisierung von Desinformation vorgenommenen Wählerbevormundung.[191] Tatsächlich spitzt sich bei der strafrechtlichen Verfolgung von politischer Desinformation die Frage zu, wo die Grenzen des paternalistischen Eingriffs eines Staates gegenüber seinem eigenen Legitimationssubjekt liegen. Dieser Gedanke soll im Folgenden näher entwickelt werden.

Als Ausgangspunkt dient die Feststellung, dass staatliche Herrschaftsmacht durch demokratische Wahlen in einem Verantwortungszusammenhang mit den einzelnen Bürgerinnen und Bürger gebracht wird. Die Legitimation staatlichen Handelns speist sich aus dem Wahlakt der Bürgerinnen und Bürger, denn in einer Demokratie ist der freie Bürger «Mitherrscher, nicht Beherrschter».[192] Vor diesem Hintergrund ist es in einer liberalen Demokratie[193] gefährlich, wenn die zu legitimierende Herrschaft (Staat) mit paternalistischen Regelungen (wie etwa einem Straftatbestand politischer Desinformation), deren Entfaltung in dessen Machtbereich selbst liegen, in die legitimierende Willensbildung und in den Willensbildungsprozess seiner Bürgerinnen und Bürger eingreift.[194] Das gilt gerade und insbesondere, wenn der Staat in diesem Willensbildungsprozess sein schärfstes Schwert zückt, nämlich das Strafrecht. Anders ausgedrückt: Für eine liberale Demokratie ist es gefährlich, wenn der staatliche Machtapparat in die informativen Grundlagen eines öffentlichen Willensbildungsprozesses zu weitreichend eingreift. Natürlich darf und soll er dafür Sorge tragen, dass Informationen bereitstehen und Desinformationen als solche grundsätzlich erkannt werden. Wenn er jedoch «moderierend» in diese Tätigkeit eingreift und dies gerade mit den repressivsten staatlichen Mitteln vornimmt, wird es gefährlich. Denn dann ist nämlich fraglich, ob der demokratische Legitimationsprozess durch Wahlen tatsächlich von einer genuin freien Willens-

191 Gkountis (2010), 207 ff.; Rigopoulou (2013), 115 ff.; Sutter/Maasen (2010), 318 ff.
192 Kirchhof (2009), 1009, 1011.
193 Vgl. Rigopoulou (2013), 47 ff.
194 Insofern gehen diese Ausführungen in dieselbe Richtung wie der Code of Conduct on Disinformation der Europäischen Kommission von 2018, der Internetnutzenden grundsätzlich keine nennenswerte Rolle bei der Verhinderung von Desinformation zuschreibt, abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (zuletzt abgerufen am 5.10.2022); zudem erfährt dieses Anliegen Unterstützung durch Dubber (2022), der die massiv wachsende Strafgewalt von Staaten im Namen eines Projektes westlich-liberaler Demokratien deshalb kritisiert, weil letztlich eine derartig ausgeübte Strafgewalt genau jene Personen objektiviert, deren Autonomie und Rechtssubjektivität eigentlich als Legitimationsspender staatlicher Macht gelten soll.

bildung der Wählerschaft begleitet ist und der Wahlvorgang selbst frei und fair war.

Als Kontrollüberlegungen zu den in N 88 dargelegten Ausführungen dient das Imaginieren von *worst-case* Szenarien. Natürlich kann sich eine gemässigte und liberale Mehrheit im demokratisch-rechtsstaatlichen Prozess mit besten Intentionen dafür entscheiden, einfache politische Desinformation zu kriminalisieren und einen entsprechenden Straftatbestand schaffen. Entsprechende Vorzüge strafrechtlicher Regulierung wurden oben dargelegt. Doch weil der demokratische Rechtsstaat nach dem berühmtem Böckenförde'schem Diktum von Voraussetzungen lebt, die er selbst nicht garantieren kann,[195] ist die demokratische Staatsform jene, die populistischen, radikalen und letztlich auch autoritativen Politikströmungen die legitime Möglichkeit gibt, die Macht zu ergreifen.[196] Was tatsächlich passiert, wenn die Idee des offenen Meinungsaustausches und demokratischen Meinungswettbewerbs selbst angegriffen wird, zeigt die toxische Situation in den USA[197] und der «gelebte» demokratische Diskurs in autoritären Demokratien. So verwundert es nicht, dass gerade populistische und autokratische Machthaber ihre Gegner mit den Mitteln des Strafrechts bekämpfen.[198]

Vor diesem Hintergrund sind strafrechtliche Mittel aufgrund ihres inhärenten Missbrauchspotentials auch in ihrer Schädlichkeit für den demokratischen Diskurs zu sehen. Das mag zwar bereits auf die nächsten, weiter unten angesprochenen Punkte überleiten, die weitere Argumente gegen den strafrechtlichen Einsatz bereithalten. Wichtig erscheint hier jedoch die Betonung des normativen Leitbildes von mündigen und selbstverantwort-

195 Böckenförde (2006), 112 f.: „Der freiheitliche, säkularisierte Staat lebt von Voraussetzungen, die er selbst nicht garantieren kann. Das ist das große Wagnis, das er, um der Freiheit willen, eingegangen ist. Als freiheitlicher Staat kann er einerseits nur bestehen, wenn sich die Freiheit, die er seinen Bürgern gewährt, von innen heraus, aus der moralischen Substanz des einzelnen und der Homogenität der Gesellschaft, reguliert. Andererseits kann er diese inneren Regulierungskräfte nicht von sich aus, das heißt mit den Mitteln des Rechtszwanges und autoritativem Gebots zu garantieren suchen, ohne seine Freiheitlichkeit aufzugeben und – auf säkularer Ebene – in jenen Totalitätsanspruch zurückfallen, aus dem er in den konfessionellen Bürgerkriegen herausgeführt hat."

196 Treffend beschreiben Levitsky/Ziblatt (2018), dass Demokratien nie von Generälen, sondern durch demokratische Institutionen selbst zugrunde gehen.

197 Eingehende Analyse bei Levitsky/Ziblatt (2018), 171 ff.

198 Instruktiv Hoven (2020), 101, 103 ff.; vgl. ferner auch die Warnung von Pieth (2014), 264, 269, wonach kollektive Ängste und primitiver Populismus Politiker, selbst jene der Mitte, dermassen unter Druck setzen, dass sie die Geschichte des Strafrechts vollkommen verdrängen.

lichen Bürgerinnen und Bürgern, das demokratischen Verfassungsstaaten immanent ist. Die Kriminalisierung von einfacher politischer Desinformation enthält also die Gefahr, in überpaternalisierender Wirkung dieses für den demokratischen Rechtsstaat fundamentale Leitbild infrage zu stellen. Denn die Kriminalisierung von Desinformation enthält das implizite Potential, die Wählerschaft zu entmündigen, weil ein derartiger Straftatbestand letztlich unterstellt, dass Bürgerinnen und Bürger eben nicht die Fähigkeit haben, einfache (und somit nicht technisch erzeugte) politische Desinformation im politischen Diskurs richtig einzuordnen, sodass es des strafrechtlichen Schutzes bedarf, um Desinformation aus dem politischen Diskurs (nicht nur sichtbar zu machen, sondern) zu entfernen. Vom normativen Leitbild mündiger und selbstverantwortlicher Bürgerinnen und Bürger sollte selbst angesichts der Gefahren von einfacher politischer Desinformation nicht abgekehrt werden!

Letztlich ist eine unmittelbare Kriminalisierung politischer Desinformation durch Schaffung eines eigenen Straftatbestands wegen der damit einhergehenden Überpaternalisierung der Stimmbürgerinnen und Stimmbürger nicht zielführend. Um den tatsächlich vorherrschenden Schutzbedarf dennoch zu realisieren, wären eher strafrechtlich-bewährte Transparenzpflicht[199] zielführender, die die politische Information begleiten: Die kommunizierenden Akteure und Institutionen sollen die Faktenbasis, auf der sie argumentieren, transparent und insofern überprüfbar machen. Wenn dank zivilgesellschaftlicher Kräfte (z.B. NGOs oder politische Wettbewerber) aufgedeckt wird, dass die vermeintliche Faktenbasis letztlich erfunden wurde, dann wird sich die Wählerschaft davon ein Bild machen können. Damit dieser Mechanismus aber funktioniert, bedarf es Transparenzpflichten – und allenfalls diese sollten mit strafrechtlichen Mitteln bewährt werden.[200]

Silencing bzw. Chilling Effects

Sollte tatsächlich eine Strafnorm zur Kriminalisierung von einfacher politischer Desinformation implementiert werden, so könnte dies für den politischen Diskurs in einer Demokratie wegen der sog. «*silencing* bzw. *chilling effects*» schädlich sein.[201] Diese Begriffe beschreiben die Situation,

199 Siehe im kriminalpolitischen Kontext Hoven (2020), 101, 112 f.

200 Zum Schweizerischen Modell nach Art. 76b ff. BPR siehe oben unter I.1.1.

201 Der Begriff des *chilling effect* geht auf die Rechtsprechung des EGMR zurück, vgl. EGMR (GK), Urt. v. 27.3.1996, 17488/90, Goodwin/The United Kingdom, § 39:

wonach angesichts des Bedrohungspotentials massiver juristischen Konsequenzen, wie dies typischerweise dem Strafrecht inhärent ist,[202] Teilnehmende am öffentlichen Diskurs davor abgeschreckt würden, ihre Meinung kund zu tun.[203] Mit anderen Worten: Steht eine mögliche Bedrohung durch Strafverfolgung wegen politischer Desinformation im Raum, werden sich (gerade nicht-professionelle) Teilnehmende des öffentlich-politischen Diskurses lieber zurückziehen als sich dem Risiko strafrechtlicher Verfolgung auszusetzen. Matthias Hong bezeichnet dies treffend als «Verstummungsschäden»[204].

Nun mag diese Konsequenz hinsichtlich der Desinformation willkommen sein, wenn nämlich von Desinformationskampagnen aus Angst vor juristischen Konsequenzen Abstand genommen wird. Dennoch könnte sich die abschreckende Wirkung auf sämtliche Diskursteilnehmenden erstrecken, weil sich die Strafnorm zwar gegen Desinformation richtet, aber das Konzept von Desinformation nur schwer konturierbar erscheint und daher in vielfältigen Kontexten angewendet werden könnte.

In diesem Zusammenhang stellt sich deshalb die Frage, ob mit dem Einsatz von Strafrecht dann nicht über das eigentliche Ziel hinausgeschossen wird. Oben unter N 78 wurde bereits dargelegt, wie schwierig es ist, das Phänomen von Desinformation aus der Sicht des Strafgesetzgebers hinreichend klar zu erfassen. Insofern besteht die Gefahr, dass die Grenzziehungen eines potentiellen Straftatbestandes nicht scharf und insofern auch nicht öffentlichkeitswirksam kommunizierbar sind. Der *silencing* bzw.

„Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms [...] without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest."

202 Statt vieler s. Staffler (2024), N. 5.

203 Insofern gebracht der EGMR den „*chilling effect*"-Begriff beispielsweise im Kontext der Strafverfolgung von Whistleblower, s. EGMR (GK), Urt. v. 12.2.2008, 14277/04, §§ 95 f.

204 Hong (2022), 126, 142; ausführlich Schreiber/Joss (2020), 523 ff. sowie Zanger (2017), 89 ff. und passim.

chilling effect würde durch das scharfe Instrument des Strafrechts daher nicht nur Desinformationskampagnen treffen. Wie vorher dargelegt ist zu befürchten, dass vielfältige Diskursteilnehmende – vom einfachen Wählenden über vielfältige politische Interessensvertretungen bis hin zu den Parteien und ihren Vertretern selbst – das Strafbarkeitsrisiko scheuen und gar nicht mehr am politischen Diskurs partizipieren.[205] Denn wenn der Aufwand der Diskurspartizipation mit strafrechtlichen Risiken verknüpft ist, die sich wohl nur durch einen nicht unerheblichen, präventiv-organisatorischen Aufwand (z.B. durch Einholen rechtlichen Rats) minimieren lassen, besteht das grosse Gefahrenpotential, dass lieber auf das eigene Einbringen in den Diskurs verzichtet wird. Dieses Abschreckungspotential, auf das gerade der Europäische Gerichtshof für Menschenrechte in seiner Rolle als demokratischer Diskurswächter[206] immer wieder im Zusammenhang mit Strafverfahren gegen Journalisten aufmerksam macht, hängt mit einem weiteren Gefahrenmoment zusammen, der sogleich näher erörtert wird: dem sog. SLAPP.

SLAPP

Eine besondere Gefahr als Folgeerscheinung von Kriminalisierung der politischen Desinformation stellt die strategische Prozessführung dar.[207] Bei dieser Art von Prozessführung geht es darum, das Potenzial von Gerichtsverfahren strafrechtlicher (oder auch zivilrechtlicher) Natur für den öffentlichen bzw. politischen Diskurs zu instrumentalisieren, um Gegner mit Gerichtsverfahren zu überziehen, Ressourcen finanzieller, zeitlicher und auch persönlicher Art dieser Gegner zu binden und durch die Wahl des Schauplatzes (den Gerichtssaal) dessen angsteinflössendes Potential zu nutzen.[208] Die strategische Prozessführung betrifft zwar unmittelbar die Interessen einer bestimmten Prozesspartei, hat aber darüber hinaus die Gerichtsöffentlichkeit und allenfalls auch politische Auswirkungen des Gerichtsverfahrens und des Gerichtsurteils im Blick.

205 Zum chilling effect im Strafrecht s. Schreiber/Joss (2020), 523, 534 f. sowie BGE 143 I 147, E. 3.3.; vgl. ferner. Fehling/Leymann (2020), 110 f.; Iben (2021), 412; Hoven (2017), 718, 744 mit Blick auf Satire.

206 Baade (2017), 305 ff. und passim.

207 Instruktiv zum Phänomen der strategischen Prozessführung Meier (2021), 17 ff.; Strobel (2022), 261 ff.

208 Vgl Bowie (2021), 160, 174, der im Kontext der US-amerikanischen Rechtsordnung den US-Supreme Court als die primäre Quelle von „Antidemokratie" identifiziert.

Eine Ausprägung strategischer Prozessführung ist das sog. SLAPP, also «*strategic litigation against public participation*».[209] Die phonetische Nähe zum englischen Begriff der Ohrfeige («*slap*») erscheint kaum zufällig.[210] Das Phänomen ist insbesondere im Zusammenhang mit kritischem Journalismus und NGOs bekannt, kann aber grundsätzlich gegen jede Person gerichtet sein, die im öffentlichen Diskurs als Gegner angegriffen werden soll. Durch SLAPP wirft ein (regelmässig einflussreicher und finanziell potenter) Kläger durch Ingangsetzung von gerichtlichen Verfahren zivilrechtlicher oder strafrechtlicher Natur einem Akteur des öffentlichen Meinungsbildungsprozesses Diffamation vor.[211] Damit soll die öffentliche Äusserung retrospektiv unterdrückt (gelöscht) bzw. prospektiv verhindert werden. Gleichzeitig soll mittels Klage(n) finanzieller Druck geschaffen werden, nämlich unmittelbar durch Anwalts- und Gerichtskosten und mittelbar/prospektiv durch hohe Schadensersatzforderungen und/oder beim Vorhandensein einschlägiger Straftatbestände die Forderung einer (hohen) Bestrafung. Da Gerichtsverfahren durchaus relevante zeitliche und finanzielle Ressourcen beanspruchen, gleichzeitig die betroffenen Personen auch angesichts des finanziellen Drucks einer Zivilklage oder der strafrechtlichen Drohung emotionalen Belastungen ausgesetzt sind, wird durch strategische Klagen sprichwörtlich ein Stein ins Rollen gebracht, der sich speziell gegen Menschen mit knappen Ressourcen richtet, um diese im Gerichtsverfahren zu verwickeln und mit entsprechenden Belastungen des Verfahrens einzudecken. Die Präferenz zwischen zivilrechtlichen oder strafrechtlichen Wegen erfolgt nach strategischen Gesichtspunkten. Eine strafrechtliche Klage kann durch die Aussicht auf Freiheitsentzug oder öffentliche Strafprozesse zu erheblichen psychischen Belastungen führen, bedarf allerdings eines entsprechenden strafrechtlichen Anknüpfungspunktes, während Zivilklagen gerade durch drohende immense Schadenssummen und entsprechenden Zahlungsverpflichtungen psychische Einschüchterung beabsichtigen.

209 Instruktiv (und namensgebend) Pring (1989), 3, 4 ff.

210 Mann (2022), 1358.

211 Siehe ErW 15–17 der RL (EU) 2024/1069 vom 11.4.2024 über den Schutz von Personen, die sich öffentlich beteiligen, vor offensichtlich unbegründeten Klagen oder missbräuchlichen Gerichtsverfahren („strategische Klagen gegen öffentliche Beteiligung").

SLAPP ist inhärent mit Rechtsmissbrauch verwandt[212] und hat gleichzeitig eine enorm schädliche Wirkung für den öffentlichen Diskurs. Deshalb erscheint es merkwürdig, dass die Befassung mit dem Phänomen rechtsmissbräuchlicher Klagen, die vor allem aus dem US-Kontext bekannt sind,[213] in der kontinental-europäischen (Straf-)Rechtswissenschaft noch nicht breitflächig thematisiert wurde – soweit ersichtlich, finden sich bislang nur im Kontext von umweltrechtlicher Prozessführung einige Studien.[214] Immerhin zeichnet sich ab, dass sich ein potenter legislativer Akteur in Kontinentaleuropa dem Problem annimmt: Angesichts der Werte und Zielsetzungen, für die die EU in ihren Gründungsverträgen (insb. Art 2 und 3 EUV) eintritt, verwundert es kaum, dass der EU-Gesetzgeber eine Anti-SLAPP-Regulative lanciert hat,[215] im Übrigen auch mit Auswirkungen für Drittstaaten wie der Schweiz.[216] Allerdings ist der Weg dieses Regulativprojektes steinig, weil die konkrete Ausgestaltung durchaus weitgehende Eingriffe in etablierte Rechtspraktiken der EU-Mitgliedstaaten vorsieht, was Verfassungsgerichte auf den Plan rufen könnte.

Die hier vertretene These lautet nun, dass mit der Kriminalisierung von einfacher politischer Desinformation ein SLAPP-tauglicher Straftatbestand geschaffen werden würde, der sich gerade für solche strategischen Prozessführungen aufdrängt. Kommt man politischen Opponenten nicht mit inhaltsstarken Gegenargumenten bei, so erscheint selbst eine – rein zu den Erfolgschancen aussichtslose – Instrumentalisierung des Gerichtswegs ein «probates» Mittel. Denn bereits die öffentliche Mitteilung zur Erhebung einer Strafanzeige gegen den politischen Gegner kann diesen in den Augen der Öffentlichkeit in den Kontext von Unlauterkeit oder Illegalität rücken. Der nächste logische Schritt ist dann nicht weit, nämlich anstelle der Bekämpfung von Desinformation eine Bekämpfung von non-konformen Politikbestrebungen mit den Mitteln des Strafrechts zu

212 Vgl. Pieth (2016), 3, der gerade mit Blick auf das Strafprozessrecht vor der inhärenten Missbrauchsgefahr staatlicher Hoheitsgewalt warnt.

213 Vgl. nur https://anti-slapp.org/your-states-free-speech-protection (zuletzt abgerufen am 01.01.2025).

214 Vgl. die Forschungsergebnisse der University of Amsterdam und Greenpeace International, abrufbar unter https://www.umweltinstitut.org/fileadmin/Mediapool/Downloads/01_Themen/05_Landwirtschaft/Pestizide/Suedtirol/University_of_Amsterdam_GPI_Research_SLAPPs_.pdf (zuletzt abgerufen am 01.01.2025).

215 RL (EU) 2024/1069 vom 11.4.2024; vgl. die Empfehlung der EU-Kommission, COM(2022) 2428 final; vgl. insb. Wagner (2022), 1861, 1862 sowie ausführlich Wiepen (2022), 149 ff.

216 Siehe Art. 16 und 17 RL (EU) 2024/1069 vom 11.4.2024.

bezwecken.[217] Dass ein derartiges Szenario keineswegs akademisches Elfenbein-Geklüngel darstellt, zeigen die jüngsten Entwicklungen auf Ebene des Europarates gegenüber der Türkei im Zusammenhang mit dem dortigen Desinformations-Strafgesetz: Im Mai 2022 lancierte die Türkei einen Gesetzgebungsprozess zur Bekämpfung von Desinformation, der nicht nur in das Presse- und Internetrecht im weitesten Sinne mit neuen Haftungs- und Verantwortungsmodellen eingriff, sondern auch ausdrücklich einen neuen Straftatbestand gegen Desinformation in Art. 217a türkStGB («*public dissemination of information misleading the public*») schuf.[218] Das türkische Gesetz, das am 13. Oktober 2022 verabschiedet wurde und – binnen kürzester Zeit – schon am 18. Oktober 2022 in Kraft trat, reiht sich in die unrühmliche Serie von neuen Typologien von Straftatbeständen ein, die eine Kriminalisierung von «Panikmache» (gerade auch im Zusammenhang mit der Covid-Pandemie) beabsichtigen.[219] Diese Initiative aus der Türkei ist vor dem Hintergrund der dortigen Entwicklung seit dem 15. Juli 2016 gescheiterten Putschversuch[220] und der für den aktuellen Machthaber ungünstigen Wahlprognosen mit Blick auf die türkischen Parlamentswahlen 2023 zu sehen, die er letztlich knapp in einer Stichwahl für sich entscheiden konnte. Ob und inwiefern der neue Straftatbestand zum Wahlerfolg des Machthabers beitrug, lässt sich mangels einschlägiger Studien nicht belegen – eine entsprechende Annahme, wonach regierungsgetreue Desinformationskampagnen weite Verbreitung erfuhren, liegt jedoch mit Blick auf die wissenschaftliche Literatur nahe.[221]

Letztlich kann das Strafrecht durch strafrechtliche SLAPP-Klagen für politische Agenden instrumentalisiert werden, indem eine Art Kriegsführung mit den Mitteln des Rechts gegen politisch Andersdenkende oder *public watchdogs* geführt wird. Strafrechtliche SLAPP sind daher im Kontext von «*lawfare*» zu sehen.[222] Hinter dem «*lawfare*»-Begriff schimmert jedoch

217 Louban et al. (2022), 265, 276 f.

218 Siehe etwa Schüller (2022), 820, 822; der Normwortlaut (*rectius*: die möglichen Wortlaute – offenbar divergieren die Informationen zum Wortlaut der Strafnorm des parlamentarischen Vorschlages und die Mitteilungen der Türkei gegenüber dem Europarat) ist im Bericht der Venedig-Kommission vom 7. Oktober 2022, CDL-Pl(2022)032, S. 4 abgedruckt.

219 Mit Blick auf das ungarische Pendant siehe Györy (2020) sowie Nagy (2020), 199 ff.

220 Nach Öktem (2017), 134, 135, 147 f. markiert dieses Event eine beginnende Eskalation in der Innenpolitik; vgl. auch Rohländer (2017), 81, 85 f.

221 Siehe etwa Akser/Baybars (2023), 159 ff.

222 Der Begriff „Lawfare" ist vom Begriff „Warfare" abgeleitet; s. Kennedy (2012), 158, 162 ff.; Kittrie (2016), 4 ff.; Ziolkowski (2010), 112.

gerade durch den strafrechtlichen Kontext ein bekannter strafrechtswissenschaftlicher Diskursgegenstand durch, der gerade in den frühen 2000er Jahre für viel Diskussionsstoff gesorgt hat: das sog. Feindstrafrecht[223]. Es mag zwar drastisch klingen, wenn man SLAPP-Klagen in den Kontext feindstrafrechtlicher Tendenzen stellt.[224] Die Realität zeigt aber, dass SLAPP insbesondere in autoritären Regimen dazu genutzt werden, politische Opponenten mundtot zu machen, indem diese hinter Gittern verschwinden. Kaum ein anderer Fall wie jener von Alexei Nawalny vermag dies deutlicher zu zeigen.[225]

Fazit und Ausblick

Nach Abwägung der Argumente wird hier die Position vertreten, dass politische Desinformation nicht durch einen eigenen Straftatbestand kriminalisiert werden soll. Dies stützt sich auf jüngere Studien ab, wonach es keine empirischen Nachweise dafür gibt, dass Desinformation auf demokratische Prozesse einen direkten Einfluss hat, sondern vielmehr die mediale und politische Thematisierung von Desinformation das Misstrauen schürt und gesellschaftliche Prozesse stabilisiert.[226] Im Folgenden werden kriminalpolitische Schlussfolgerungen kurz vorgestellt.

Keine direkte Kriminalisierung

Die kriminalpolitische Beantwortung der Frage, inwiefern die Kriminalisierung von einfacher politischer Desinformation vor- oder nachteilig ist, hat in dieser Untersuchung offengelegt, dass es letztlich auf das gesellschaft-

223 Die Konzeption des Feindstrafrecht geht bekanntermassen auf Beiträge von Günther Jakobs zurück, s. Jakobs (1985), 751 ff.; Jakobs (2000), 47 ff.; Jakobs (2004), 88 ff.; instruktiv zum Jakobs'schen Verständnis von Feindstrafrecht bei Greco (2010), 13 ff. sowie Ambos (2006), 1, 12 ff.

224 Insofern würde hier Feindstrafrecht als denunziatorisch-kritischer Begriff gebraucht, vgl. Greco (2010), 56 ff.; sowie Greco (2006), 96, 110 ff.; vgl. Ambos (2006), 1, 10 ff.; Koch (2012), 12 ff.; Fleckenstein (2017), 241 ff.

225 Vgl. hierzu EGMR (GK), Urt. vom 15. November 2018, 29580/12 u.a., Navalnyy/Russland.

226 Mansell et a. (2025); die Studie verdeutlicht aber auch die Notwendigkeit von Moderationssysteme in Online-Plattformen, um für den gesellschaftlichen Zusammenhalt schädliche Inhalte einzudämmen.

liche Verständnis ankommt, welche Aufgabe dem Strafrecht zukommt. Diesbezüglich hat Thomas Weigend zwei anschauliche Bilder gezeichnet: Strafrecht könnte, dem Bildnis eines strengen Vaters gleich, grundsätzlich die Freiheit zur Lebensgestaltung einräumen, aber einzelne schwere Verletzungen massiv ahnden; es könnte aber, dem Bildnis einer fürsorglichen Mutter gleich, ständiger und mahnender Begleiter der Menschen sein.[227] Befürworter einer Kriminalisierung von Desinformation scheinen in dieser Frage tendenziell dem Bildnis der fürsorglichen Mutter zugeneigt. Rhetorisch stellt sich die Frage, was aber mit einem derartigen Straftatbestand passiert, wenn die Dominanz einer überfürsorglichen Mutter überhand nimmt.[228]

Aus der Darlegung von Vor- und Nachteilen strafrechtlicher Regulierung und entgegen einem instrumentellen Rechtsverständnis[229] wird hier die Schlussfolgerung gezogen, dass eine strafrechtliche Normschaffung zur Bekämpfung von einfacher politischer Desinformation wesentlich mehr Schadenspotential aufweist, als ihr Nutzen verheisst. Die direkte Kriminalisierung von einfacher politischer Desinformation erscheint daher aus den oben dargelegten Gründen nicht vertretbar.[230]

Das soeben genannte Ergebnis ist hinsichtlich zweier Perspektiven zu präzisieren. Erstens impliziert die Ablehnung klassischer Straftatbestände gegen Straftatbestände nicht die Ablehnung von Regulativen prozeduralen Strafrechts.[231] Gemeint sind damit Bestimmungen wie Transparenz- oder Berichtspflichten, deren Einhaltung durch Strafrecht sanktionsbewährt werden. Ein derartiger Beitrag strafrechtlicher Normen zur Bekämpfung

227 Weigend (2013), 17, 32.

228 Die rhetorische Frage ist Neumann (2020), 91, 99 f. entlehnt.

229 Siehe insb. Albrecht (2013), 385, 406 ff.

230 Ähnlich auch Baade (2022), 201, 205; Rückert (2018), 167, 177 ff.; Iben (2021), 410 ff.; sowie wohl auch Fahl (2016), 735, 736 der keinen Anlass für einen Straftatbestand des „Missbrauchs des Internets" sieht.

231 Instruktiv zum prozeduralen Strafrecht Eicker/Fisch (2015), 591, 593: „Den vielfältigen Prozeduralisierungstheorien und -modellen, die im Schrifttum diskutiert werden, lässt sich als gemeinsamer Grundgedanke entnehmen, dass prozedurales (Straf-)Recht, ebenso wie herkömmliches materielles (Straf-)Recht, bestimmte Regelungsziele (z.B. Rechtsgüterschutz und Rechtfertigung von nicht strafwürdigem Verhalten) zu erreichen sucht, dies jedoch mittels eines eher ungewohnten Instrumentariums. Während gewohntes materielles Strafrecht direkt durch die Bereitstellung inhaltlicher Detailvorgaben Verhalten steuern will, verfolgt prozedurales Recht definierte Zielvorgaben indirekter, indem es durch ins materielle Recht integrierte Verfahren und eine reduzierte Rahmenregelung mehr Raum für eine ganzheitliche Einzelfallbetrachtung lässt und eine Strafbarkeitsbeurteilung ex ante ermöglicht."

von Desinformation scheint verhältnismässig und vertretbar. Zweitens ist das Untersuchungsergebnis auf die einfache politische Desinformation bezogen. Neue Möglichkeiten von qualifizierter Desinformation, die durch technische Videomanipulationen (Deep-Fakes) in naher Zukunft realisierbar sind, sind angesichts eines erhöhten Gefährdungspotentials anders zu bewerten. Während man Stimmbürgerinnen und Stimmbürgern zutrauen kann, einfache politische Desinformation zu identifizieren, sind etwa technisch erstellte Fake-Videos per se kaum von richtigen Videos zu unterscheiden und damit im politischen Kontext kaum als Desinformation identifizierbar. Daher liegt hinsichtlich qualifizierter politischer Desinformation ein anderer Schutzbedarf vor, der in dieser Untersuchung nicht thematisiert wurde.

Rolle von Zivilgesellschaft und sozialen Medien

Die zentralen Abwehrkräfte gegen einfache politische Desinformation sind nach der hier vertretenen Auffassung innerhalb der Zivilgesellschaft aufzubauen und zu stärken – mit anderen Worten: die Wählerschaft muss Resilienz gegen derartige Desinformation entwickeln.[232] Um das «Grundrecht auf Öffentlichkeitsinformation»[233] zu entfalten[234] und die Zivilgesellschaft selbst resilient gegen Desinformation zu machen, erscheinen als drängendste Massnahmen die Stärkung von Medienvielfalt einerseits und die Medienkompetenz der Bevölkerung andererseits.[235] Zudem ist auch bei den Social-Media-Plattformen selbst anzusetzen. Diese Plattformen sind nicht nur für die Zivilgesellschaft, sondern letztlich auch für die Akteure von politischer Desinformation der zentrale Ort für Informations- bzw. Desinformationsweitergabe. Die sozialen Medien selbst sollten nicht Propagandisten und Desinformationskampagnen überlassen werden. Weil

232 So auch Levitzsky/Ziblatt (2018), 256 ff.

233 Wegweisend EGMR, Khurshid Mustafa u. Tarzibachi/Turkey, 23883/06 (2008), § 44.

234 Vgl. De Gregorio (2022), insb. 157 ff. und passim sowie Siapera/Kirk (2022), 119 ff.; in einzelnen US-Bundesstaaten werden tatsächlich Online-Plattformen als grundrechtsgebundene Akteure angesehen; inwiefern allerdings diese Grundrechtsbindung nicht durch eine bestimmte, politische Agenda vereinnahmt wird, liegt angesichts der konkreten Regeln auf der Hand: s. Texas H.B. 20 (2021) und Florida S.B. 7072 (2021). Insofern ist auch hier Vorsicht bei der Normierung geboten.

235 Iben (2021), 407 f.; Preuß (2021), 142 ff.; Rotte (2022), 69, 78 f.

soziale Medien durch ihre kostenlose Nutzung ein grosses Potential an möglichen Nutzerinnen und Nutzern haben, müssen dort auch qualitativ hochwertige Informationsquellen amtlicher oder journalistischer Natur Präsenz zeigen.[236] Natürlich würden auch grossflächige Transparenz- und Kennzeichnungsmöglichkeiten (z.B. für politische Spenden)[237] helfen, die nicht nur Social-Bots[238] oder Deepfakes,[239] sondern generell bezahlte politische Werbung als solche erkennbar machen.[240] Letztlich braucht es sichtbares soziales Engagement gegen Akteure der Desinformation; Würdigung von Aktionen gegen Desinformation durch die Zivilgesellschaft; Aufbau von frei zugänglichen und verlässlichen Informationsarchiven ohne Geo-Blocking und ohne zeitliche Limitierung;[241] eigenverantwortliches Engagement von Bürgerinnen und Bürgern bei der Konsultation dieser Informationenplattformen[242]; eigenverantwortliche Gestaltung von Parteipolitik durch die Parteien im Bewusstsein ihrer Gatekeeper-Rolle;[243] verantwortungsbewusste Gestaltung von Unternehmenspolitik grosser digitaler Gatekeeper; institutionalisierte[244] und effektive Kontrollen von Parteien[245] und Unternehmen, die den politischen Meinungsbildungsprozess wesentlich beeinflussen, durch Berichtspflichten[246] und Transparenzpflichten sowie Forschungszugang zu verwendeten Algorithmen durch die wissenschaftliche Gemeinschaft[247].

---

236 Zur Praxis sozialer Medien als Quellen von solider Information s. Preuß (2021), 81 f. mit statistischen Erhebungen.

237 Vorbildlich etwa die US-Plattform opensecrets, abrufbar unter: https://www.opensecrets.org/donor-lookup

238 So etwa die Forderung von Schefer (2020), 1433, 1448; instruktiv Dürr (2024).

239 Preuß (2021), 88 ff.; Löber (2022), 289, 305 ff.; Von Ungern-Sternberg (2022), 94 ff.

240 Siehe auch Think Tank European Parliament, Towards new rules on transparency and targeting of political advertising vom 8.7.2022, abrufbar unter https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733592 (zuletzt abgerufen am 24.10.2022).

241 Zur Rolle von Wikipedia s. Schroeder (2022).

242 In diese Richtung argumentiert auch Bernhard Pörksen mit seiner Forderung, Bürgerinnen und Bürger zur Medienmündigkeit zu erziehen, damit sie selbst journalistische Gatekeeper werden können („Utopie einer redaktionellen Gesellschaft): Pörksen (2018).

243 Levitzsky/Ziblatt (2018), 42 ff.

244 Zur Bedeutung von Kontrollinstitutionen Schulz (2022), 237 ff.

245 Gerade bei den finanziellen Transparenzpflichten hat die Schweiz einen Aufholbedarf, s. Moeckli (2020), 487, 498 f.

246 Iben (2021), 385 f.

247 Iben (2021), 388 ff.

Prozedurales Strafrecht

Das Strafrecht kann hier einen Beitrag leisten, indem es Kooperations-, Berichts- und Transparenzpflichten strafrechtlich bewehrt: Desinformation ist nämlich kein technisches Problem, sondern ein Verantwortungsproblem. Werden entsprechende technische Facetten implementiert und von klaren Verantwortungszuweisungen (auch strafrechtlicher Natur) flankiert, können unterschiedliche Facetten von Desinformation (und den dahinterstehenden Akteuren) für die Zivilgesellschaft sichtbar gemacht werden.

Der Einsatz prozeduralen Strafrechts[248] könnte jedenfalls dazu beitragen, wesentliche Voraussetzungen zu schaffen, damit die Zivilgesellschaft ihre Resilienzen gegen Desinformation auf- und ausbaut. Die wichtigsten Kontrollmechanismen zur Bekämpfung von Desinformation sollten unmittelbare Kräfte aus der vollen Bandbreite der Zivilgesellschaft sein, nämlich in erster Linie NGOs, Journalisten und Forschende[249], welche Missstände einer gegen Desinformation resilienten Wählerschaft präsentieren könnten. Flankierende Massnahmen könnten etwa Oversight-Boards[250] darstellen, die unabhängig und ausserhalb des jeweiligen Unternehmens mit eigener Entscheidungsautorität eingerichtet werden und dessen Entscheidungen das Unternehmen als verbindlich anerkennt. Nicht zu vernachlässigen ist dabei der Whistleblower-Schutz, weil Missstände häufig erst durch diese Berichtskanäle an die breite Öffentlichkeit gelangen. Insofern erscheint die sekundäre Kriminalisierung von einfacher politischer Desinformation (zur Absicherung oben genannter Primärverpflichtungen unterschiedlicher Akteure) vertretbar. Eine unmittelbare Kriminalisierung von Desinformation hingegen erscheint für liberale Demokratien konzeptionell zu riskant.

248 Instruktiv Eicker (2010), 237 ff. und passim, sowie Schweiger (2018), 66 ff.; jeweils m.w.N.

249 Nach eigener Ansicht ist der Datenzugang hinsichtlich der grossen Plattformen für Forschende von essentieller Bedeutung, nämlich nicht nur im Hinblick auf die Wahrnehmung von Missbrauchskontrolle, sondern weit darüber hinaus: Während nämlich kommerzielle Plattformen allein die Maximierung ihres Erlöses von Werbung intendieren und daher das Potential der Datensätze grösstenteils ungenutzt lassen, könnte dieser Datenschatz für die Zivilgesellschaft und insb. für die sozialwissenschftliche Forschung von enormer Bedeutung sein.

250 So hat der Facebook-Konzern ein entsprechendes Oversight Board eingerichtet, s. Staffler (2022), 83 m.w.N.

Literatur

Aeschimann L./Schaub L. (2023), Die neuen Transparenzvorschriften des BPR, LeGes 34, 1.

Akser M./Baybars B. (2023), Repressed media and illiberal politics in Turkey: the persistence of fear, Southeast European and Black Sea Studies, vol. 23, n. 1, 159.

Albrecht P. (2013), Strafrecht ohne Recht?, ZStrR, vol. 131, 385,

Allcott H./Gentzkow M. (2017), Social Media and Fake News in the 2016 Election, Journal of Economic Perspectives, vol. 31, 211.

Allgaier J. (2022), Fake News und Verschwörungen in digitalen Medien, in: Eleftheriadi-Zacharaki/Hebing/Manstetten/Paganini (Hrsg.), Vom Umgang mit Fake News, Lüge und Verschwörung, Nomos, 83,

Al-Rawi A./Celestini C./Steward N./Worku N. (2022), How Google Autocomplete Algorithms about Conspiracy Theorists Mislead the Public, M/C Journal, vol. 25, https://doi.org/10.5204/mcj.2852

Ambos K. (2019), Nationalsozialistisches Strafrecht, Nomos,

Ambos K. (2006), Feindstrafrecht, ZStrR, vol. 124, n. 1, 1.

Arendt H. (1972), Wahrheit und Lüge in der Politik, Zwei Essays, Piper.

Baade B. (2023), Wahrheit und Recht, Mohr Siebeck.

Baade B. (2022), Der Kampf gegen Desinformation, Vereinte Nationen 70, n. 5, 201;

Baade B. (2017), Der Europäische Gerichtshof für Menschenrechte als Diskurswächter, Springer.

Bader K./Jansen C./Rinsdorf L. (2020), Jenseits der Fakten: Deutschsprachige Fake News aus Sicht der Journalistik, in: Steinebach/Bader/Rinsdorf/Krämer/Roßnagel (Hrsg.), Desinformation aufdecken und bekämpfen, Nomos, 33,

Baker P./Potts A. (2013), Why Do White People Have Thin Lips? Google and the Perpetuation of Stereotypes via Auto-Complete Search Forms, Critical Discourse Studies, vol. 10, 187

Bakir V. (2020), Psychological operations in digital political campaigns : Assessing Cambridge Analytica's psychographic profiling and targeting, Frontiers in Communication, vol. 8, 1.

Bale T./Wager A.J. (2015), The United Kingdom Independence Party: Insurgency or Splinter, in: Decker/Henningsen/Jakobsen (Hrsg.), Rechtspopulismus und Rechtsextermismus in Europa, Nomos, 217.

Balkin J. M. (2018), Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, University of California Davis Law Review, vol. 51, 1149

Balkin J. M. (2014), Old-School/New-School Speech Regulation, Harvard Law Review, vol. 127, 2296.

Baurmann M. (2022), Wir haben die Duldung der Demokratie mit ihrer Akzeptanz verwechselt, Verfassungsblog vom 30. Juni 2022, abrufbar unter https://verfassungsblog.de/duldung-akzeptanz/ (zuletzt abgerufen am 01.01.2025).

Becker W.G. (1948), Der Tatbestand der Lüge: Ein Beitrag zur Abstimmung von Recht und Ethik, Recht und Staat in Geschichte und Gegenwart, vol. 134/135, 1

Benson T.W. (2011), The Rhetoric of Civility: Power, Authenticity, and Democracy, Journal of Contemporary Rhetoric, vol. 1, n. 1, 22.

Bimber B. (2014), Digital Media in the Obama Campaigns of 2008 and 2012, Journal of Information Technology & Politics, vol. 11, 130.

Böckenförde E.-W. (2006), Recht, Staat, Freiheit, Suhrkamp.

Böller F./Haas C./Hagemann S./Sirakov D./Wagner S. (2020), Reign of Chaos? Die USA unter Donald J. Trump, in: dies. (Hrsg.), Donald Trump und die Politik in den USA. Eine Zwischenbilanz, Nomos, 7.

Borgi E./Bleyer-Simon K. (2021), Disinformation in the Perspective of Media Pluralism in Europe – the role of platforms, in: Bayer/Holznagel/Korpisaari/Woods (Hrsg.), Perspectives on Platform Regulation, Nomos, 531,

Bowie N. (2021), Antidemocracy, Harvard Law Review, vol. 135, 160.

Briant E.L. (2022), Propaganda Machine: Inside Cambridge Analytica and the Digital Influence Industrie, Bloomsbury.

Brown N. I. (2020), Deepfakes and the Weaponization of Disinformation, Virginia Journal of Law & Technology, vol. 23, n. 1, 1.

Cadwalladr C./Graham-Harrison E.G. (2018), Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian v. 17.3.2018, abrufbar unter https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (zuletzt abgerufen am 01.01.2025).

Canova G./Giardini T. (2023), Zum Einfluss der direkten Demokratie auf das Strafrecht, in: Staffler et al. (Hrsg.), Strafrecht und Demokratie, 2023, Nomos, 57.

Cantador I./Fernandez-Tobias I./Bellogin A./Kosinski M. (2013), Relating Personality Types with User Preferences in Multiple Entertainment Domains, CEUR Workshop Proceedings, 997.

Caroll D. R. (2021), Cambridge Analytica, in: Rawnsley/Ma/Pothong (Hrsg.), Research Handbook on Political Propaganda, Edward Elgar Publishing Limited, 41.

Cavaliere P. (2022), The Truth in Fake News: How Disinformation Laws Are Reframing the concepts of Truth and Accuracy on Digital Platforms, European Convention on Human Rights Law Review, n. 3, 481

Chaslot G. (2021), Google Autocomplete Pushed Civil War narrative, Covid Disinfo, and Global Warming Denial, Medium, 9.2.2021, abrufbar unter: https://guillaumechaslot.medium.com/google-autocomplete-pushed-civil-war-narrative-covid-disinfo-and-global-warming-denial-c1e7769ab191 (zuletzt abgerufen am 01.01.2025).

Coca-Vila I. (2023), Demokratisierung des Strafrechts? Zur Rolle der Strafrechtswissenschaft in der Gesetzgebung, in: Staffler et al. (Hrsg.), Strafrecht und Demokratie, Nomos, 79.

Coeni R. (2019), Falsche und irreführende Informationen im Verfassungsrecht der Schweiz, ex ante, n. 1, 3,

Costa P.T. /McCrae R.R. (1992), Revised NEO Personality Inventory (NEO PI-R) and NEO Five-Factor Inventory (NEO-FFI), professional manual. Odessa, FL: Psychological Assessment Resources.

De Gregorio G. (2022), Digital Constitutionalism in Europe, Cambridge University Press.

Degischer D./Wallnöfer M. (2024), Digitale Geschäftsmodelle, in: Staffler/Ebersberger/Jobin, Digitalwirtschaft, Springer, 87.

Delnon V./Rüdy B. (2018), Kommentar zu Art. 186, in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar zum Strafrecht, 4. Aufl., Helbing Lichtenhahn Verlag.

Demmelhuber T./Paul A./Reinkowski M. (2017), Arabellion. Vom Aufbruch zum Zerfall einer Region?, Leviathan Sonderband 31, Nomos.

Diamond L. (2015), Facing Up to the Democratic Recession, Journal of Democracy, vol. 26, n. 1, 141,

Drexl J. (2019), Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics. In: Gerard D, Lianos I, eds. Reconciling Efficiency and Equity: A Global Challenge for Competition Policy. Global Competition Law and Economics Policy. Cambridge University Press, 242.

Dubber M.D. (2022) Der doppelte Strafstaat. Die Krise des modernen Strafrechts in vergleichend-historischer Perspektive, Duncker & Humblot.

Duff R.A. (1986), Trials and Punishments, Cambridge University Press,

Dürr P. (2024), Social Bots. Digitale Manipulation und Verfassungsrecht, MohrSiebeck.

Ebersberger B./Dachs B. (2024), Die Ökonomik digitaler multinationaler Unternehmen, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, Springer, 69.

Eder-Rieder M. (2019), Kommentierung zu § 264, in Triffterer/Rosbaud/Hinterhofer (Hrsg.), Salzburger Kommentar zum StGB, 41. Lfg. Lexisnexis.

Ege G.A. (2018), Die Rechtfertigung der indirekt aktiven Sterbehilfe. Einwilligung in eine nicht einwilligungsfähige Handlung?, in: Schwarzenegger/Ida (Hrsg.), Autonomie am Lebensende – Kultur und Recht, Dike Verlag, 89.

Frischhut M (2024), Ethische Dimensionen der Digitalwirtschaft, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, Springer, 109

Eicker A. (2010), Die Prozeduralisierung des Strafrechts, Stämpfli/Nomos,

Eicker A./Fisch S. (2015), Zur prozeduralen Rechtfertigung von Suizidhilfe im. Strafrecht, AJP, 591,

Entman R.M./Usher N. (2018), Framing in a Fractured Democracy: Impacts of Digital Technology on Ideology, Power and Cascading Network Activation, Journal of Communication, vol. 68, 298.

Entman R.M. (1993), Framing: Towards Clarification of a Fractured Paradigm, Journal of Communication, vol. 43, 51.

Fahl C. (2016), Zur Strafbarkeit der Falschmeldung im Internet über den Tod eines Asylsuchenden, Jura, 735,

Fehling M./Leymann M. (2020), Der neue Strukturwandel der Öffentlichkeit: Wie lassen sich die sozialen Medien regulieren?, AfP, n. 2, 110.

Fichter C., Die Psychologie der Empörungsökonomie, Psychoscope, vol. 4, 26.

Fleckenstein F. (2017), Kampf den Feinden oder Schutz der Minderheiten?, Peter Lang Verlag.

Fleischmann G. (2023), Message Control. Was Sie schon immer über Politik und Medien wissen wollten, edition a Verlag.

Frattolillo A. (2021), La censure sur les réseaux sociaux, AJP, n. 2, 214.

Frenkel S./Kang C. (2021), Inside Facebook, Die hässliche Wahrheit, S. Fischer.

Frisch W. (2019), Zum Begründungshintergrund von Übel und Tadel in der Theorie der Strafe, Goltdammer's Archiv, 537,

Fuhrer C./Ronc P. (2020a), Kommentar zu Art. 279, in: Graf (Hrsg.), StGB Annotierter Kommentar, Stämpfli Verlag.

Fuhrer C./Ronc P. (2020b), Kommentar zu Art. 282, in: Graf (Hrsg.), StGB Annotierter Kommentar, Stämpfli Verlag.

Gerlant U. (2021), Die Einen vernichten, die Anderen einschüchtern. Disziplinieren durch Strafen in der späten Sowjetunion, in: Baberowski/Kindler/Donth (Hrsg.), Disziplinieren und Strafen, Campus Verlag, 271

Geth C. (2021), Vorbemerkungen zu Art. 111, in: Trechsel/Pieth (Hrsg.), Praxiskommentar Schweizerisches Strafrecht, 4. Aufl., Helbing Lichtenhahn Verlag.

Gille F./Papadopoulos K./Sedlakova J./Zavattaro F./Brall C. (2024), Vertrauen. Welche Rolle spielt Vertrauen in der Digitalwirtschaft?, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, Springer, 129.

Gkountis I. (2010), Autonomie und strafrechtlicher Paternalismus, Duncker & Humblot.

Gless S. (2021), Internationales Strafrecht, 3. Aufl., Helbing Lichtenhahn Verlag,

Golumbia D. (2024), Cyberlibertarianism. The Right-Wing Politics of Digital Technology, Columbia Academic Publ.

Greco L. (2010), Feindstrafrecht, Nomos,

Greco L. (2006), Über das sogenannte Feindstrafrecht, Goltdammer's Archiv, 96.

Güldenzopf R./Voigt M. (2016), Donald Trump – ein Wahlkampf der neuen Regeln?, Zeitschrift für Politikberatung, vol. 8, n. 1, 24.

Gunjic I. (2020), Die schweizerische Demokratie und „Fake News", in: Meyer/Zurkinden/Staffler (Hrsg.), Innovation und Recht, Dike Verlag, 179.

Günther K. (2002), Die symbolisch-expressive Bedeutung der Strafe – Eine neue Straftheorie jenseits von Vergeltung und Prävention?, in: Prittwitz/Baurmann/Günther/Kuhlen/Merkel/Nestler /Schulz (Hrsg.), FS für Klaus Lüderssen zum 70. Geburtstag, Nomos, 205,

Günther H.-L. (1983), Strafrechtswidrigkeit und Strafunrechtsausschluss, Studien zur Rechtswidrigkeit als Straftatmerkmal und zur Funktion der Rechtfertigungsgründe im Strafrecht, C. Heymann,

Györy C. (2020), Fighting Fake News or Fighting Inconvenient Truths?, Verfassungsblog vom 11.4.2020, abrufbar unter https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/ (zuletzt abgerufen am 01.01.2025).

Iben A. (2021), Staatlicher Schutz vor Meinungsrobotern, Nomos,

Haberman M. (2022), Täuschung: Der Aufstieg Donald Trumps und der Untergang Amerikas, Siedler Verlag.

Habermas J. (2022), Ein neuer Strukturwandel der Öffentlichkeit und die deliberative Politik, Suhrkamp Verlag,

Habermas J. (2021), Überlegungen und Hypothesen zu einem erneuten Strukturwandel der politischen Öffentlichkeit, in: Seeliger/Sevignani (Hrsg.), Ein neuer Strukturwandel der Öffentlichkeit?, Leviathan Sonderband 37, Nomos, 470,

Hao K. (2021), How Facebook and Google fund global misinformation v. 20.11.2021, abrufbar unter: https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/ (zuletzt abgerufen am 01.01.2025).

Hartmann A. (2019), Fake News, Wahrheit und Regulierung, in: Dal Molin-Kränzlin/Schneuwly/Stojanovic (Hrsg.), Digitalisierung – Gesellschaft – Recht, Dike Verlag, 81,

Hassemer W. (2001), Das Symbolische am symbolischen Strafrecht, in: Schpnemann/Achenbach/Bottke/Haffke/Rudolphi (Hrsg.), FS für Claus Roxin zum 70. Geburtstag, Walter de Gruyter Verlag, 1001,

Hassemer W./Reemtsma J.P. (2002), Verbrechensopfer: Gesetz und Gerechtigkeit, C.H. Beck.,

Hefendehl R./Von Hirsch A./Wohlers W. (eds.) (2003), Die Rechtsgutstheorie. Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel, Nomos.

Hirsch P.A. (2021), Das Verbrechen als Rechtsverletzung. Subjektive Rechte im Strafrecht, Duncker & Humblot.

Höffler K./Festerling T.N. (2022) In der Krise: Kriminalpolitik-Paradoxon zwischen Twitter und Aktendeckel, in: Pohlreich/Beck/Meier/Stefanopoulou/Ziemann (Hrsg.), Strafrecht in der Krise, Nomos, 161,

Högden B./Krämer N./Meinert J./Schaewitz L. (2020), Desinformation aus medienpsychologischer Sicht, in: Steinebach/Bader/Rinsdorf/Krämer/Roßnagel (Hrsg.), Desinformation aufdecken und bekämpfen, Nomos, 77.

Hohlfeld R. (2020), Wahr oder falsch? Eine empirische Untersuchung zur Wahrnehmung von „Fake News" und echten Nachrichten in der politischen Kommunikation, in: Hohlfeld/Harnischmacher/Heinke/Lehner/Sengl (Hrsg.), Fake News und Desinformation, Nomos, 179.

Hong M. (2022), Hassrede und Desinformation als Gefahr für die Demokratie – und die Meinungsfreiheit als gleiche und positive Freiheit im Zeitalter der Digitalisierung, RW Rechtswissenschaft, 126.

Hörnle T. (2006), Die Rolle des Opfers in der Straftheorie und im materiellen Strafrecht, JZ, vol. 61, 950.

Hörnle T. (2003), Der Schutz von Gefühlen im StGB, in: Hefendehl/von Hirsch/Wohlers (Hrsg.), Die Rechtsgutstheorie, Nomos, 268

Hörnle T. (1999), Tatproportionale Strafzumessung, Duncker & Humblot,

Horst P. (2009), Die Wahl Barack Obamas zum 44. Präsidenten der USA, Zeitschrift für Politikwissenschaft, vol. 19, n. 1, 107,

Hoven E. (2020), Populismus und Strafrecht, in: Hoven/Kubiciel (Hrsg.), Zukunftsperspektiven des Strafrechts. Symposium zum 70. Geburtstag von Thomas Weigend, Nomos, 101,

Hoven E. (2017), Zur Strafbarkeit von Fake News – de lege lata und de lege ferenda, ZStW, vol. 129, n. 3, 718.

Hügli A./Lübcke P./Bafandi S. (2013), Philosophielexikon, Erweiterte und vollständig revidierte Ausgabe, rowohit.

Hueso L. C. (2021), The danger of disinformation for democracy and the constitutional risks of its regulation, in: Iliopoulos-Strangas/Levits/Poctas/Ziller (Hrsg.), Die Herausforderungen der digitalen Kommunikation für den Staat und seine demokratischen Staatsformen, Nomos, 121 ff.

Jakobs G. (2004), Bürgerstrafrecht und Feindstrafrecht, HRRS, 88.

Jakobs G. (2000), Kommentar, in: Eser/Hassemer/Burkhardt (Hrsg.), Die deutsche Strafrechtswissenschaft vor der Jahrtausendwende, C.H. Beck, 47

Jakobs G. (1985), Kriminalisierung im Vorfeld einer Rechtsgutsverletzung, ZStW, vol. 97, n. 4, 751.

Jungherr A. (2016), Datengestützte Verfahren im Wahlkampf, Zeitschrift für Politikberatung, vol. 8, n. 1, 3.

Kadelbach S. (2019), Brexit And What it Means, Nomos.

Kaiser B. (2020), Die Datendiktatur. Wie Wahlen manipuliert werden, HarperCollins.

Kargl W. (2023) Vorbemerkungen zu §§ 185 ff, in: Kindhäuser/Neumann/Paeffgen (Hrsg.), Nomos Kommentar StGB, 6. Aufl., Nomos,

Keil J.-G. (2022), Verschwörungserzählungen aus der Sicht der Kriminalpsychologie und ihre besondere Rolle im Milieu von „Reichsbürgern", „Impfgegnern" und „QAnon-Anhängern", in: Lüttig/Lehmann (Hrsg.), Verschwörungstheorien. Ursprung – Anhänger – Bewältigung, Nomos, 13,

Kelsen H. (1929), Vom Wesen und Wert der Demokratie, J.C.B. Mohr.

Kennedy D. (2012), Lawfare and warfare, in: Crawford/Koskenniemi (eds.), The Cambridge Companion to International Law, Cambridge University Press, 158.

Khan L.M./Pozen D.E. (2019), A Skeptical View of Information Fiduciaries, Harvard Law Review, vol. 133, 497.

Kirchhof P. (2009), Der europäische Staatenverbund, in: von Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht. Theoretische und dogmatische Grundzüge, 2. Aufl., Springer, 1009,

Kittrie O. F. (2016), Lawfare. Law as a Weapon of War, Oxford University Press.

Klein E. (2020), Der tiefe Graben. Die Geschichte der gespaltenen Staaten von Amerika, Hofmann und Campe Verlag,

Kley, A. (2020), Eigenheiten des schweizerischen Verfassungsrechts, in: Diggelmann/Hertig Randall/Schindler (Hrsg.), Verfassungsrecht der Schweiz, Bd. I, Schulthess, 85.

Knüppel K.-N. (2022), Datenfinanzierte Apps als Gegenstand des Datenschutzrechts, Duncker & Humblot.

Koch A. (2012), Wider ein Feindstrafrecht, Juristische Kritik am Hexereiverfahren, Erich Schmidt Verlag,

Köhler M. (1985), Zur Frage der Strafbarkeit des Leugnens von Völkermordtaten, NJW, 2389.

König H. (2022), Lüge und Täuschung in der Politik, in: Eleftheriadi-Zacharaki/Hebing/Manstetten/Paganini (Hrsg.), Vom Umgang mit Fake News, Lüge und Verschwörung, Nomos, 121,

Konzett E./Klenk F./Staudinger M./Tóth B., Das Geständnis des Thomas Schmid, Falter.at v. 19.10.2022, abrufbar unter https://www.falter.at/zeitung/20221025/das-gestaendnis-des-thomas-schmid (zuletzt abgerufen am 01.01.2025)..

Kornelius B. (2009), Obamas Zeitenwende: Der Sieg allein ist nicht der Wechsel. Die US-Präsidentschaftswahl vom 4. November 2008, Zeitschrift für Parlamentsfragen, vol. 40, n. 2, 296.

Kosinski M. (2021), Facial recognition technology can expose political orientation from naturalistic facial images, Scientific Reports, vol. 11, abrufbar unter https://www.nature.com/articles/s41598-020-79310-1 (zuletzt abgerufen am 01.01.2025).

Kosinski M./Stillwell D./Graepel T. (2013), Private traits and attributes are predictable from digital records of human behavior, Proceedings of the National Academy of Science, vol. 110, n. 15, 5802.

Krzywon A. (2021), Summary Judicial Proceedings as a Measure for Electoral Disinformation: Defining the European Standard, German Law Journal, vol. 22, n. 4, 673.

Kubiciel M. (2020), Die Veränderung des Strafrechts durch die Digitalisierung der Lebenswelt, in: Hoven/Kubiciel (Hrsg.) Zukunftsperspektiven des Strafrechts. Symposium zum 70. Geburtstag von Thomas Weigend, Nomos, 159.

Kubiciel M. (2018), Die Strafrechtswissenschaft als kritische Wissenschaft, in: Barton/Eschelbach/Hettinger/Kempf/Krehl/Salditt (Hrsg.), FS Fischer, Nomos, 143,

Kubiciel M./Weigend T. (2019), Maßstäbe wissenschaftlicher Strafgesetzgebungskritik, KriPoZ, 35

Kühl K. (2018), Vorbemerkungen zu§ 185 StGB, in: Lackner/Kühl, StGB, 29. Aufl., C.H. Beck,

Kühl K. (2005), Zum Missbilligungscharakter der Strafe, in: Arnold/Burkhardt/Gropp/Heine/Koch/Lagodny/Perron/Walther (Hrsg.), FS für Albin Eser zum 70. Geburtstag, C.H. Beck, 149.

Kühler A. (2022), Würde, Autonomie und Selbstzweckhaftigkeit. Zur Kontroverse um ein kantisches Verständnis der Menschenwürde als Verfassungsbegriff, ZSR I, 77.

Kumkar L. K./Rapp J. P. (2022), Deepfakes – Eine Herausforderung für die Rechtsordnung, Zeitschrift für die Digitalisierung des Rechts, n. 3, 199.

Kusche C. (2020), „Fake News" – ein Fall für den Strafgesetzgeber?, in: Beck/Kusche/Valerius (Hrsg.), Digitalisierung, Automatisierung, KI und Recht, Nomos, 421,

Lammich T. (2022), Fake News als Herausforderungen des deutschen Strafrechts, Duncker & Humblot.

Landesanstalt für Medien NRW (2020), Was ist Desinformation? Betrachtungen aus sechs wissenschaftlichen Perspektiven, abrufbar unter https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Themen/Desinformation/WasIstDesinformation_Paper_LFMNRW.pdf (zuletzt abgerufen am 01.01.2025).

Lantwin T. (2020), Strafrechtliche Bekämpfung missbräuchlicher Deep Fakes, MMR Zeitschrift für IT-Recht und Recht der Digitalisierung, n. 2, 78.

Laux J. (2024), AdTech, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, Springer, 335.

Levitsky S./Ziblatt D. (2018), Wie Demokratien sterben, DVA.

Löber L. I. (2022), KI-Lösungen gegen digitale Desinformation: Rechtspflichten und -befugnisse von Anbietern von Social Networks, in: Friedewald/Rooßnagel/Heesen/Krämer/Lamla (hrsg.), Künstliche Intelligenz, Demokratie und Privatheit, Nomos, 289,

Lohsse S./Schulze R./Saudenmayer D. (eds.)(2020), Data as Counter-Performance – Contract Law 2.0?, Nomos.

Louban A./Tahraoui M./Aden H./Fährmann J./Krätzer C./Dittmann J. (2022)., Das Phänomen Deepfakes. Künstliche Intelligenz als Element politischer Einflussnahme und Perspektive einer Echtheitsprüfung, in: Friedewald/Rooßnagel/Heesen/Krämer/Lamla (Hrsg.), Künstliche Intelligenz, Demokratie und Privatheit, Nomos, 265,

Lubishtani K./Flattet M (2019), La démocratie directe face à la manipulation de l'information par des particuliers, AJP, n. 7, 710.

Mafi-Gudarzi N. (2019), Desinformation: Herausforderung für die wehrhafte Demokratie, ZRP, 65.

Mahlmann M. (2023), Strafrecht und Demokratie, in: Staffler et al. (Hrsg.), Strafrecht und Demokratie, Nomos, 9,

Mann R. (2022), Initiativen gegen missbräuchliche „SLAPP-Klagen", NJW, 1358

Mansell R./Durach F./Kettemann M./Lenoir T./Procter R./Tripathi G./Tucker E. (2025), Information Ecosystems and Troubled Democracy. A Global Synthesis of the State of Knowledge on News Media, AI and Data Governance, January 2025, abrufbar unter https://observatory.informationdemocracy.org/wp-content/uploads/2024/12/rapport_forum_information_democracy_2025.pdf

Martin C.J. (2016), Negotiating Political Agreements, in: Mansbridge/Martin (ed.), Political Negotiation. A Handbook, Brookings Institution Press, 7.

Matz S./Chan Y. W./Kosinski M. (2016), Models of Personality, in: Tkalcic/De Carolis/De Gemmis/Odic/Kosir (eds.), Emotions and Personality in Personalized Services, Springer, 35.

Mayer-Schönberger V. (2001), Informationsrecht für die Informationsgesellschaft, Schweizerische Juristenzeitung, vol. 97, 383.

McAdams D.P. (1992), The Five-Factor Model In Personality: A Critical Appraisal, Journal of Personality, vol. 60, n. 2, 329.

McCrae R.R./John O.P. (1992), An introduction to the five-factor model and its applications, Journal of Personality vol. 60, n. 2, 175,

Meier J. (2021), Gleichstellung der Geschlechter vor Gericht – strategische Prozessführung und die schweizerische Verfassungsordnung, in: Hussmann/Nickerson/Sang Bastian/Wujohktsang (Hrsg.), Unter Gleichen, sui generis Verlag, 17

Mérték, The Hungarian government media disseminates Kremlin propaganda v. 3.3.2022, abrufbar unter https://mertek.atlatszo.hu/the-hungarian-government-media-disseminates-kremlin-propaganda/ (zuletzt abgerufen am 01.01.2025).

Mirschel M. (2021), Gefühlte Repressionen. »Keine Nachsicht mit Verrätern«, in: Baberowski/Kindler/Donth (Hrsg.), Disziplinieren und Strafen, Campus Verlag, 69.

Moeckli S. (2020), Politische Willensbildung in der Schweiz, in: Diggelmann/Hertig Randall/Schindler (Hrsg.), Verfassungsrecht der Schweiz, Bd. I, Schulthess, 487.

Nagy F. (2020), Populistische Züge im ungarischen Strafensystem, in: Sinn/Hauck/Nagel/Wörner (Hrsg.), Populismus und alternative Fakten – (Straf-)Rechtswissenschaft in der Krise?, MohrSiebeck, 199.

Nassehi A. (2019), Muster. Theorie der digitalen Gesellschaft, Beck.

Nettesheim M. (2022), Verfassungsrechtliche Kriminalisierungspflichten und -grenzen, in: Bäcker/Burchard (Hrsg.), Strafverfassungsrecht, MohrSiebeck, 93,

Neumann U. (2020), Die Rolle des Strafrechts in der Gesellschaft, in: Hoven/Kubiciel (Hrsg.) Zukunftsperspektiven des Strafrechts. Symposium zum 70. Geburtstag von Thomas Weigend, Nomos, 91,

Oberholzer N. (2002), Die Rolle des modernen Strafrechts: Kriminalisierung als Mittel für jeden Zweck?, recht, 221,

Öktem K. (2017), Türkisches Zwischenspiel im Nahen Osten. Neo-imperialer Islamismus und die AKP zwischen Farce und Tragödie, in: Demmelhuber/Paul/Reinkowski (Hrsg.), Arabellion. Vom Aufbruch zum Zerfall einer Region?, Leviathan Sonderband, vol. 31, 134,

Oswald M. (2020), „Fake News Media": Der Begriff „Fake News" als rhetorisches Mittel des Framings in der politischen Kommunikation, in: Hohlfeld/Harnischmacher/Heinke/Lehner/Sengl (Hrsg.), Fake News und Desinformation, Nomos, 61.

Paal B. P. (2018), Vielfaltssicherung bei Intermediären, MMR Zeitschrift für IT-Recht und Recht der Digitalisierung, 567.

Papathanasiou K. (2019), Eigenverantwortung, Neuronensteuerung oder Habitus? Der homo autonomus et inspiratus als strafrechtliches Menschenbild, in: Funke/Schmolke (Hrsg.), Menschenbilder im Recht, MohrSiebeck, 151.

Pawlik M. (2008), Der Terrorist und sein Recht, C.H. Beck,

Pernice I./Guerra Martins A.M. (eds.) (2019), Brexit and the Future of EU Politics, Nomos.

Petersen N. (2019), Das Bild des Bürgers in der Demokratietheorie, in: Funke/Schmolke (Hrsg.), Menschenbilder im Recht, MohrSiebeck, 93.

Pieth M. (2016), Schweizerisches Strafprozessrecht, 3. Aufl., Helbing Lichtenhahn,

Pieth M. (2014), Die Wiederentdeckung des Punitivismus, ZStrR, vol. 132, n. 3, 264.

Pörksen B. (2018), Die große Gereiztheit. Wege aus der kollektiven Erregung, Hanser Verlag.

Prentoulis M. (2022), From Austerity to Brexit: The Failed Populist Moment, in: Eder-Ramsauer/Kim/Knott/Prentoulis (eds.), Populism, Protests, and New Forms of Political Organisation, Nomos, 55.

Preuß T. (2021), Fake News. Eine phänomenologische, kriminologische und strafrechtliche Untersuchung, Nomos.

Priester K. (2019), Umrisse des populistischen Narrativs als Identitätspolitik, in: Müller/Precht (Hrsg.), Narrative des Populismus, Springer, 11,

Pring G.W. (1989), SLAPPs: Strategic Lawsuits against Public Participation, Peace Environmental Law Review, vol. 7, 3,

Reimann N. (2023), Foreign Electoral Interference, Normative Implications in Light of International Law, Human Rights, and Democratic Theory, DOI: 10.38107/037,

Rigopoulou M. (2013), Grenzen des Paternalismus im Strafrecht, Duncker & Humblot,

Robinson N.J., The Truth Is Paywalled But The Lies Are Free, Current Affaires v. 02.08.2020, abrufbar unter https://www.currentaffairs.org/2020/08/the-truth-is-paywalled-but-the-lies-are-free/ (zuletzt abgerufen am 01.01.2025.

Rohländer J. (2017), EU-Türkei-Erklärung – Saubere Lösung oder schmutziger Deal?, Kritische Justiz, vol. 50, n. 1, 81,

Roseneck M. (2023), Zum Zusammenhang zwischen Wahrheit und Demokratie, in: Fröhlich (Hrsg.), Sprache und Politik, Nomos, 61,

Rostalski F. (2017), "Fake News" und die "Lügenpresse" – ein (neuer) Fall für das Straf- und Ordnungswidrigkeitenrecht?, RW Rechtswissenschaften, n. 4, 436.

Rotte R. (2022), Gezielte Desinformation als Element hybrider Konflikte, in: Eleftheriadi-Zacharaki/Hebing/Manstetten/Paganini (Hrsg.), Vom Umgang mit Fake News, Lüge und Verschwörung, Nomos, 69.

Roxin C./Greco L. (2020), Strafrecht Allgemeiner Teil I, 5. Aufl., C.H. Beck

Roy S./Ayalon L. (2020), Age and Gender Stereotypes Reflected in Google's „Autocomplete" Function: The Portrayal and Possible Spread of Societal Stereotypes, The Gerontologist, vol. 60, 1020.

Rückert C. (2018), Fake News und Social Bots – Demokratieschutz durch Strafrecht?, in: Albrecht/Geneuss/Giraud/Pohlreich (Hrsg.), Strafrecht und Politik, Nomos, 167,

Rudl T. (2021), Die Virenschleuder Amazon, netzpolitik.org v. 22.11.2021, abrufbar unter https://netzpolitik.org/2021/desinformation-im-netz-die-virenschleuder-amazon/ (zuletzt abgerufen am 01.01.2025).

Sadoghi A. (2022), Kommentar zu § 264, in: Höpfel/Ratz (Hrsg.), Wiener Kommentar zum Strafgesetzbuch, 2. Aufl., Manz.

Sängerlaub A./Meier M./Ruhl W.-D. (2018), Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestageswahlkampf 2017, abrufbar unter https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf (zuletzt abgerufen am 01.01.2025).

Sauer H. (2021), Öffentliches Reaktionsrecht. Theorie und Dogmatik der Folgen hoheitlicher Rechtsverletzungen, MohrSiebeck,

Saxer U. (2020), Medien- und Kommunikationsverfassung, in: Diggelmann/Hertig Randall/Schindler (Hrsg.), Verfassungsrecht der Schweiz Bd. III, Schulthess, 2371.

Schefer M. (2020), Kommunikationsgrundrechte, in: Diggelmann/Hertig Randall/Schindler (Hrsg.), Verfassungsrecht der Schweiz Bd. II, Schulthess, 1433.

Scheidegger N. (2018), Das Sexualstrafrecht der Schweiz. Grundlagen und Reformbedarf, Stämpfli,

Schemmel J. (2018), Soziale Netzwerke in der Demokratie des Grundgesetzes, Der Staat, vol. 57, 501,

Schick N. (2020), Deepfakes and the Coming Infocalypse, Twelve Verlag.,

Schmitz B./Buschuew E. (2022), (Be-)Zahlen mit Daten, MMR Zeitschrift für IT-Recht und Recht der Digitalisierung, 171

Schreiber M. (2022), Strafbarkeit politischer Fake News, Zugleich eine Untersuchung zum materiell-rechtlichen Umgang mit der Informationswahrheit in Zeiten demokratiegefährdender Postfaktizität, Duncker & Humblot.

Schreiber M./Joss M. (2020), Der „Chilling Effect" auf die Grundrechtsausübung, ZBl, n. 10., 523

Schroeder R., Can the Internet Advance the Social Good? Mapping the Landscape, Report v. Oktober 2022, abrufbar unter https://www.oii.ox.ac.uk/wp-content/uploads/2022/10/Can-the-Internet-Advance-the-Social-Good.pdf

Schubert K./Schwiertz H. (2021), Konstruktivistische Identitätspolitik, Zeitschrift für Politikwissenschaften, vol. 31, 565,

Schüller G.U. (2022), Länderreport Türkei, RIW, n. 12, 820,

Schulz W. (2022), Changing the Normative Order of Social Media from Within: Supervisory Bodies, in: Celeste/Heldt/Keller (Hrsg.), Constitutionalising Social Media, Hart Publishing, 237.

Schünemann B. (2019), Gefährden Fake News die Demokratie, wächst aber im Strafrecht das Rettende auch?, Goltdammer's Archiv für Strafrecht, vol. 166, n. 10, 620.

Schweiger T (2018), Prozedurales Strafrecht, Zur Bedeutung von Verfahren und Form im Strafrecht, Nomos,

Segalin C./ Lepri B./Cristani M./Celli F./Polonio L./Kosinski M./Stillwell D./Sebe N. (2017). What your Facebook Profile Picture Reveals about your Personality.

Shaw D. (2016), Assessing the Impact of Campaigning in the 2016 U.S. Presidential Election, Zeitschrift für Politikberatung, vol. 8, 15.

Siapera E./Kirk N. (2022), Social Media, Electoral Campaigns and Regulation of Hybrid Political Communication: Rethinking Communication Rights, in: Celeste/Heldt/Keller (Hrsg.), Constitutionalising Social Media, Hart Publishing, 119

Sirakov D. (2017), Beispiellos? Der Auftakt der Präsidentschaft von Donald J. Trump, Atlantische Themen, n. 1,

Shipman T. (2016), All Out War, The Full Story of How Brexit Sank Britain's Political Class, HarperCollins Publisher.

Snyder T. (2018), Der Weg in die Unfreiheit. Russland, Europa, Amerika, C.H. Beck.

Soares H. (2023), Strafrechtliche Bekämpfung von Fake News? Zum Umgang der Kriminalisierungstheorie mit der Wahrheit, in: Staffler et al. (Hrsg.), Strafrecht und Demokratie, Nomos, 179.

Staffler L. (2025), DORA, MiCAR und AI Act, in: Splechtna/Kojic (Hrsg.), Praxiskompendium Bankwissen, 3. Aufl., FCH Verlag.

Staffler L. (2024), Kommentar zu Art. 32 BV, in: Schlegel/Ammann (Hrsg.), Onlinekommentar zur Bundesverfassung, abrufbar unter https://onlinekommentar.ch/de/kommentare/bv32 (zuletzt abgerufen am 01.01.2025).

Staffler L. (2022), Business Criminal Law, Springer.

Staffler L. (2021), Der strafrechtliche Schutz vor industrieller Produktpiraterie im Lichte nationaler, europäischer und internationaler Vorgaben, in: Laimer/Perathoner (Hrsg.), Italienisches, europäisches und internationales Immaterialgüterrecht, Springer, 217.

Staffler L. (2020), Opferschutz und Verjährung im Spiegel der EGMR-Judikatur: Überlegungen zu den opferbezogenen Schutzpflichten im staatlichen Strafrechtssystem, in: Abraham/Bublitz/Geneuss/Krell/Wegner (Hrsg.), Verletzte im Strafrecht, Nomos, 53.

Staffler L. (2018), Industrie 4.0 und wirtschaftlicher Geheimnisschutz, Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt), Nr. 4, 269.

Staffler L. (2017), Gesetzesinitiative gegen Fake News made in Italy, MMR-Aktuell, n. 387090.

Staffler L./Ebersberger B. (2024), Digitalwirtschaft, in: Staffler/Ebersberger/Jobin (Hrsg.), Digitalwirtschaft, Springer, 1.

Stark H./Zimmermann F. (2023), Zeit Online vom 16. Februar 2023, abrufbar unter https://www.zeit.de/2023/08/desinformation-team-jorge-social-media-storykillers (zuletzt abgerufen am 01.01.2025).

Stehliková J. (2020), Disinformation and the European Union, in: European Horizons (Hrsg.), How Can Digital Technologies Build a More Integrated Europe?, Nomos, 49,

Steinbicker J. (2011), Zur Theorie der Informationsgesellschaft, 2. Aufl., VS Verlag für Sozialwissenschaften,

Steinmann G. (1996), Interventionen des Gemeinwesens im Wahl- und Abstimmungskampf, AJP, n. 3, 255.

Steinmann G./Besson S. (2023), Kommentar zu Art. 34, in: Ehrenzeller/Egli/Hettich/Hongler/Schindler/Schmid/Schweizer (Hrsg.), Die schweizerische Bundesverfassung St. Galler Kommentar, 4. Aufl., Schulthess,

Sterne J. (2017), Artificial Intelligence for Marketing, John Wiley & Sons.

Streinz R. (2020), Das Brexit Referendum: Hintergründe, Streitthemen, Reversibilität, in: Ludwigs/Schmahl (Hrsg.), Die EU zwischen Niedergang und Neugründung, Nomos, 95,

Strobel V. (2022), Strategic Litigation and International Internet Law, in: Golia/Kettemann/Kunz (Hrsg.), Digital Transformation in Public International Law, Nomos, 261.

Strobl N. (2018), Radikalisierter Konservativismus. Eine Analyse, Suhrkamp.

Sturm R. (2016), Brexit – das Vereinigte Königreich im Ausnahmezustand?, Zeitschrift für Parlamentsfragen, vol. 47, n. 4, 878.

Sutter K. (2020), Vertrauen im Recht. Eine Theorie für den demokratischen Verfassungsstaat, Dike & Nomos Verlag.

Sutter B./Maasen S. (2010), „Bürgergesellschaft". Der verdeckte Paternalismus eines politischen Programms, in: Fateh-Moghadam (Hrsg.), Grenzen des Paternalismus, Kohlhammer,

Terchechte J.P. (2020), Strukturen und Probleme des Brexit-Abkommens, NJW, n. 7, 425.

Thelen S. (2020), Wahlkampf gleich Schlammschlacht?, Eine Analyse des Negative Campaigning der Parteien zur Bundestagswahl, Nomos.

Thiel T. (2022), Der digitale Strukturwandel von Öffentlichkeit: Demokratietheoretische Anmerkungen, in: Spiecker gen. Döhmann/Westland/Campos (Hrsg.), Demokratie und Öffentlichkeit im 21. Jahrhundert – zur Macht des Digitalen, Nomos, 41,

Thiele A. (2022), Die lädierte Demokratie, RW Rechtswissenschaft, vol. 13, n. 1, 1.

Thieltges A./Serrano J.C.M. (2021), Politische Werbung und Microtargeting auf Facebook, Zeitschrift für Politik, vol. 68, n. 1, 3,

Towfigh E.V./Luckey J. (2022), Zielgruppenbasierte Ansprache von Wahlbeteiligten durch politische Parteien. Zur rechtlichen Zulässigkeit politischen Online-Microtargetings in Deutschland, RW Rechtswissenschaft, n. 1, 61.

Töndury A. (2011), Intervention oder Teilnahme? Möglichkeiten und Grenzen staatlicher Kommunikation im Vorfeld von Volksabstimmungen, ZBl, vol. 112, n. 7, 341.

Trechsel S./Lehmkuhl J. (2021), Vorbemerkungen zu Art. 173, in: Trechsel/Pieth (Hrsg.), Praxiskommentar Schweizerisches Strafgesetzbuch, 4. Aufl., Dike Verlag.

Trechsel S./Vest H. (2021), Vorbemerkungen zu Art. 279, in: Trechsel/Pieth (Hrsg.), Praxiskommentar Schweizerisches Strafgesetzbuch, 4. Aufl., Dike Verlag.

Tschannen P. (2015), Kommentar zu Art. 34, in: Waldmann/Belser/Epiney (Hrsg.), Basler Kommentar zur Bundesverfassung, Helbing Lichtenhahn Verlag.

Tufekci Z. (2015), Algorithmic Harms beyond Facebook and Google: Emergent Challenges of Computational Agency, Colo. Tech. L.J., vol. 13, 203.

Tufekci Z. (2012), Beware the Smart Campaign, The New York Times v. 17.11.2012, abrufbar unter https://www.nytimes.com/2012/11/17/opinion/beware-the-big-data-campaign.html (zuletzt abgerufen am 01.01.2025).

Uhle A. (2018), Information und Einflussnahme. Gefährdungen der Offenheit des demokratischen Willensbildungsprozesses, Duncker & Humblot.

Uhle A./Friehe M. (eds.) (2022), Polarisierung des Politischen, Gesellschaftliche Herausforderungen und institutionelle Konsequenzen, Duncker & Humblot.

Venturini T./Rogers R. (2019), „API-based research" or how can digital sociology and journalism studies learn from Facebook and Cambridge Analytica data breach, Digital Journalism, vol. 7, 532.

Vest H. (2017), Zum Verhältnis von Strafrechtswissenschaft und Strafrechtspraxis, ZStrR, n. 3, 256

Von Bogdandy A. (2022), Strukturwandel des öffentlichen Rechts, Suhrkamp,

Von Ungern-Sternberg A. (2022), Mehr Lauterkeit für Onlinekommunikation, RW Rechtswissenschaft, 94.

Vorberg, L. (2023): The (Dis)informed Citizen: Anachronismen in der Debatte um Demokratiegefährdungen durch Desinformation in den sozialen Medien, in: Paul/Vormann (Hrsg.), Die USA – eine liberale Demokratie und ihre Anachronismen, Nomos, 103.

Wagner R. (2022), Aktuelle Entwicklungen in der justiziellen Zusammenarbeit in Zivilsachen, NJW, 1861,

Weigend T. (2013), Wohin bewegt sich das Strafrecht? Probleme und Entwicklungstendenzen im 21. Jahrhundert, in: Freund/Murmann/Bloy/Perron (Hrsg.), FS Frisch, Duncker & Humblot, 17.

Weiss C. (2008), Der US-Präsident als Inszenierung, Nomos.

Wehrle S. (2018a), Vorbemerkungen zu Art. 279, in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar zum Strafrecht, 4. Aufl. Helbing Lichtenhahn Verlag,

Wehrle S. (2018b), Kommentar zu Art. 282, in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar zum Strafrecht, 4. Aufl., Helbing Lichtenhahn Verlag,

Wehrle S. (2018c), Kommentar zu Art. 282bis in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar zum Strafrecht, 4. Aufl., Helbing Lichtenhahn Verlag,

Wiepen M. (2022), Anti-SLAPP-Richtlinie und deutscher Umsetzungsbedarf, ZRP, 149.

Wiggins J. S. (ed.) (1996), The Five-Factor Model of Personality. Theoretical Perspectives, The Guilford Press.

Winkelmann T./Griebel T. (eds.) (2018.), Der Brexit und die Krise der europäischen Integration, Nomos.

Wittner F. N. (2022), Verantwortlichkeit in komplexen Daten-Ökosystemen, MohrSiebeck.

Wolff C. (2013), Das Web 2.0 in Ägypten: Über das Twittern im Arabischen Frühling, in: Albrecht/Demmelhuber (Hrsg.), Revolution und Regimewandel in Ägypten, Nomos, 163.

Wong J.C. (2019), Document relveals how Facebook downplayed early Cambridge Analytica concerns v. 23.8.2019, abrufbar unter https://www.theguardian.com/technology/2019/aug/23/cambridge-analytica-facebook-response-internal-document (zuletzt abgerufen am 01.01.2025).

Wylie C. (2019), Mindf*ck: Inside Cambridge Analytica's Plot to Break the World, Profile Books,

Zabel M. (2017), Euroskeptizismus. Ursprünge und Ausdrucksformen im Verlauf des europäischen Integrationsprozesses, Nomos, 275.

Zanger J. (2017), Freiheit vor Furcht. Zur grundrechtsdogmatischen Bedeutung von Einschüchterungseffekten, Duncker & Humblot.

Zerback T./Töpfl F. (2022), Forged Examples as Desinformation: The Biasing Effects of Political Astroturfing Comments on Public Opinion Perceptions and how to Prevent Them, Political Psychology, vol. 43, 399.

Zimmermann F./Kohring M.(2018), „Fake News" als aktuelle Desinformation. Systematische Bestimmung eines heterogenen Begriffs, Medien & Kommunikationswissenschaft, vol. 66, n. 4, 526,

Ziolkowski K. (2010), "Lawfare" – die Theorie von der Fortsetzung des Krieges mit „rechtlichen Mitteln", Humanitäres Völkerrecht Informationsschriften. Journal of International Law of Peace and Armed Conflict, vol. 23, 112.

Zuckerberg M. (2018), A Blueprint for Content Governance and Enforcement, abrufbar unter https://m.facebook.com/nt/screen/?params=%7B%22note_id%22%3A751449002072082%7D&path=%2Fnotes%2Fnote%2F&refsrc=deprecated&_rdr (zuletzt abgerufen am 01.01.2025).

Zürcher T. (2014), Legitimation von Strafe, Die expressiv-kommunikative Straftheorie zur moralischen Rechtfertigung von Strafe, MohrSiebeck,

Lösegeldzahlungen bei Cyber-Angriffen

Christoph Skoupil, Eike Bicker, Christoph Ehrke und Felix Wrocklage

A. Begriff und Erscheinungsformen

Cyberangriffe und Lösegelderpressungen mittels Schadprogrammen (sog. Ransomware) sind im digitalen Zeitalter eine allgegenwärtige Bedrohung für Unternehmen. Das Bundeskriminalamt (BKA) stuft Ransomware Angriffe bereits seit Jahren als die primäre Bedrohung im Bereich der Cyberkriminalität ein.[1] Diese Bedrohungslage hat auch die deutsche Wirtschaft längst erreicht. In einer Studie des Branchenverbandes Bitkom aus dem Jahr 2024 gaben 80 % der befragten Unternehmen an, dass Cyberangriffe in den vergangenen zwölf Monaten stark oder eher zugenommen haben; der dadurch entstandene Gesamtschaden beläuft sich auf ca. EUR 178,6 Mrd.[2] Insbesondere der Einsatz von Ransomware bei Cyberangriffen steigt dabei rasant an: Während die befragten Unternehmen im Jahr 2022 angaben, dass 12 Prozent der entstandenen Schäden auf Ransomware zurückzuführen waren, hat sich dieser Wert im Jahr 2024 auf 31 Prozent mehr als verdoppelt.[3]

Cyberangriffe können jedes Unternehmen treffen. Während nach wie vor umsatzstarke Großunternehmen zum Opfer von Cyberangriffen werden (sog. „big game hunting"), rücken immer mehr kleine und mittelständische Unternehmen (KMU) in den Fokus von Cyberkriminellen. Diese gelten oftmals als „Weg des geringsten Widerstandes".[4] Während in großen Unternehmen das Verständnis für die Bedrohungslage und die notwendigen Investitionen derzeit schnell wächst, mangelt es in vielen KMU an

1 BKA, Bundeslagebild Cybercrime 2023 (im Folgenden: „Bundeslagebild Cybercrime 2023"), S. 18.

2 Bitkom e.V., Studie „Wirtschaftsschutz 2024" v. 28.8.2024 (im Folgenden: „Studie Wirtschaftsschutz 2024"), S. 12 und 13.

3 Studie Wirtschaftsschutz 2024, S. 15.

4 BSI, Die Lage der IT-Sicherheit in Deutschland 2024 (im Folgenden: „Lagebericht IT-Sicherheit 2024"), S. 61; Europol, Internet Organised Crime Threat Assessment 2024, S. 18.

ausreichender Kenntnis über das eigene Risikoprofil.[5] Erheblichen Risiken sind auch Betreiber kritischer Infrastrukturen (KRITIS) ausgesetzt, deren Störungen sich auf die Versorgung der Bevölkerung mit kritischen Dienstleistungen auswirken können.[6] Insbesondere die Zunahme von IT-Supply-Chains macht IT-Dienstleister zu einem „attraktiven" Angriffsziel, da die Täter mit einzelnen Attacken eine Vielzahl von Unternehmen und Behörden gleichzeitig treffen können.[7] Als Beispiel sei hier der Angriff auf einen kommunalen IT-Dienstleister Ende 2023 genannt, der über 70 Städte und Gemeinden in Nordrhein-Westfalen betraf und deren IT-Infrastruktur weitgehend lahmlegte.[8]

Als Unterfall sog. Malware bezeichnet Ransomware Schadprogramme, die den Zugriff auf Daten und Systeme einschränken bzw. verhindern. Zur Freigabe dieser Daten verlangen die Täter sodann Lösegeldzahlungen (engl. ransom).[9] Regelmäßig bedienen sich die Täter bei dieser Form der digitalen Erpressung des sog. Double Extortion-Modells: Zunächst versuchen die Täter ihre Opfer durch die Verschlüsselung ihrer Daten zu einer Lösegeldzahlung zu bewegen; weigern sich die Angegriffenen, drohen die Täter mit der Veröffentlichung der ausgespähten Daten.[10] Da Unternehmen vermehrt ihre Daten über Backups sichern und durch eine Verschlüsselung allein weniger erpressbar sind, gewinnt die Drohung einer Veröffentlichung an Bedeutung.[11] Um der Forderung Nachdruck zu verleihen, wird die Verschlüsselung und Exfiltration der Daten zudem teilweise mit einem sog. DDoS-Angriff kombiniert, um zudem die bestehende IT-Infrastruktur zu überlasten und dem Angriff Nachdruck zu verleihen.[12] Zur Verschleierung der Zahlungsempfänger der Lösegelder bedienen sich die Täter in der Regel anonymen Zahlungsmitteln wie Kryptowährungen oder anonymen Bezahlkarten, um einen direkten Geldtransfer ohne Einschaltung von Mittelsmännern zu ermöglichen.[13]

---

5 Lagebericht IT-Sicherheit 2024, S. 69.
6 Lagebericht IT-Sicherheit 2024, S. 62.
7 Bundeslagebild Cybercrime 2023, S. 26.
8 Hackerangriff stellt NRW-Kommunen weiter vor große Probleme, 2.11.2023, abrufbar unter https://www1.wdr.de/ (zuletzt abgerufen am 6.1.2025).
9 BSI, Ransomware Bedrohungslage 2022, S. 4.
10 Lagebericht IT-Sicherheit, S. 47; König/NZWiSt 2023, 167 (167).
11 Bundeslagebild Cybercrime 2023, S. 22 f.; Europol, Internet Organised Crime Threat Assessment 2024, S. 20.
12 Sog. Triple Extortion, vgl. Brodowski/Schmid/Scholzen/Zoller NStZ 2023, 385 (386).
13 BSI, Ransomware Bedrohungslage 2022, S. 4; Heinrichs/Neumeier CB 2022, 14 (15).

Eine Identifizierung der Täter ist oft schwierig. Die aktuelle Aufklärungsquote liegt bei etwa 30 %.[14] Die größte Motivation der Täter im Bereich der Ransomware Angriffe ist der dadurch erhoffte finanzielle Gewinn.[15] Hier ist eine seit Jahren zunehmende Professionalisierung zu erkennen. Die Entwicklung von Ransomware ist zu einem Massengeschäftsmodell geworden (sog. Ransomware-as-a-Service, RaaS).[16] Die Organisationsstruktur der kriminellen Organisationen zeichnet sich dabei durch Internationalität und eine hohe Dynamik aus, die auf nicht klar abgrenzbare Gruppierungen und eine Arbeitsteilung zwischen Entwicklung der Ransomware und Ausführung der Angriffe zurückzuführen ist.[17] Teilweise werden die Täter auch allein zu Sabotagezwecken tätig, sodass die Opfer keine Möglichkeit haben, die Daten zu entschlüsseln.[18] Die Hintergründe dieser Attacken können politischer oder wirtschaftlicher Natur sein, teilweise lassen sie sich auch staatlichen Akteuren zuordnen.[19] Vereinzelt agieren die Täter auch, um sich in der Hacker-Szene einen Namen zu machen oder als sog. Hacktivisten auf gesellschaftliche Problemfelder aufmerksam zu machen.[20]

Angesichts des Zeitdrucks, der mit einem Ransomware Angriff einhergeht, sehen sich betroffene Unternehmen häufig zu einer raschen Entscheidung gezwungen, die wegen der drohenden Konsequenzen für Arbeitnehmer, Kunden und Geschäftspartner oft zugunsten einer Lösegeldzahlung ausfällt.[21] Sicherheitsbehörden raten dagegen von einer Zahlung ab, da es keine Garantie dafür gibt, dass die verschlüsselten Daten tatsächlich wieder freigegeben und gestohlene Daten tatsächlich gelöscht werden.[22] Zudem besteht das Risiko, dass durch die Zahlung Angriffe auf Dritte – oder erneut auf das eigene Unternehmen – finanziert werden.[23] Da die Zahlung des Lösegeldes bei der Wahl zwischen einer Geschäftseinstellung oder der Forderungserfüllung der Erpresser jedoch eine gelebte Praxis darstellt, müssen

14 BKA, Polizeiliche Kriminalstatistik 2023, S. 26.
15 BSI, Ransomware Bedrohungslage 2022, S. 8.
16 BSI, Ransomware Bedrohungslage 2022, S. 14.
17 Bundeslagebild Cybercrime 2023, S. 20.
18 BSI, Ransomware Bedrohungslage 2022, S. 9.
19 3 Jahre NotPetya: Der Erpressungstrojaner, der keiner war, 27.6.2020, abrufbar unter www.heise.de (zuletzt abgerufen am 6.1.2025).
20 BSI, Ransomware Bedrohungslage, S. 9.
21 So betrug die weltweit durchschnittlich gezahlte Lösegeldsumme 2023 621.868 US-Dollar, vgl. Bundeslagebild Cybercrime 2023, S. 18.
22 Lagebericht IT-Sicherheit 2023, S. 19.
23 BSI, Arbeitspapier „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall", S. 15.

sich die Entscheidungsträger der betroffenen Unternehmen auch die potentiellen rechtlichen Risiken dessen vor Augen führen.

Bei der Entscheidung, ob einer Lösegeldforderung nachgekommen werden soll oder nicht, ist zu bedenken, dass stets das Risiko besteht, dass die Erpresser im Falle einer Zahlung ihre Versprechungen, wie z.B. die Entschlüsselung der Daten, nicht einhalten. Auch unter Zeitdruck sollte daher eine sorgfältige Prüfung und Abwägung aller Interessen erfolgen und ggf. externer Rat eingeholt werden. Nach Möglichkeit sollten auch die Ermittlungsbehörden einbezogen und informiert werden.

B. Strafrechtliche Risiken im Falle einer Lösegeldzahlung

I. Der Einsatz von Ransomware als Straftat

Nach Auffassung der höchstrichterlichen Rechtsprechung und der einschlägigen Literatur erfüllt den Tatbestand der Erpressung gem. § 253 StGB, wer Daten auf einem IT-System mit einer Schadsoftware verschlüsselt und die betroffenen Personen zur Zahlung eines Geldbetrags nötigt, um die Zugriffs- und Nutzungssperrungen von IT-Equipment abzuwenden. Die Infektion von Computern und Netzwerken mit entsprechender Schadsoftware und die Installation eines Sperrbildschirms kann überdies eine Datenveränderung nach 303a Abs. 1 Nr. 1 StGB sowie eine (schwere) Computersabotage nach § 303b Abs. 1 Nr. 1 und Abs. 2 StGB sein.[24] Daneben kann eine Strafbarkeit wegen der Bildung einer kriminellen oder terroristischen Vereinigung nach den §§ 129, 129a StGB in Betracht kommen.[25] Plant der Täter die Ransomware von Beginn an so einzusetzen, dass die Daten auch nach erfolgter Zahlung nicht entschlüsselt werden, kommt zudem eine Strafbarkeit wegen (gewerbsmäßigen) Betrugs gem. § 263 StGB in Betracht.[26]

24 BGH Beschl. v. 8.4.2021 – 1 StR 78/21 = NJW 2021, 2301 Rn. 11 ff.; zustimmend Brodowoski/Schmid/Scholzen/Zoller NStZ 2023, 385 (387); M. Gercke ZUM 2021, 921 (930); Neuhöfer/Schefer jurisPR-Compl 5/2021, Anm. 3; Dittrich/Erdogan ZWH 2022, 13 (15 f.); Eisele JZ 2021, 1067 (1067). So auch jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; Vogelgesang/Möllers jM 2016, 381 (383 f.).

25 Siehe hierzu Brodowski/Schmid/Scholzen NStZ 2023, 385 (387).

26 JurisPK-Internetrecht/Heckmann, Kap. 8 Rn. 165; Vogelgesang/Möllers jM 2016, 381 (384). Grundsätzlich auch Eisele JZ 2021, 1067 (1067), nach dem aber der Betrug

II. Strafbarkeitsrisiken für die Geschäftsleitung nach deutschem Recht

1. Straftatbestände

Aus Sicht der von einem Ransomware-Angriff betroffenen Geschäftsleitung tritt (insbesondere wenn die betroffenen Daten nicht mittels Backup oder Unterstützung eines IT-Dienstleisters wiederhergestellt werden können) die Überlegung in den Fokus, eingefordertes Lösegeld zu zahlen, um die Freigabe verschlüsselter Daten zu erreichen. Es bestehen jedoch weiterhin nicht abschließend geklärte Strafbarkeitsrisiken, wenn Geschäftsleiter Zahlungsaufforderungen von Erpressern nachkommen. Auch wenn das Unternehmen in erster Linie Opfer von Cyberattacke und anschließender Erpressung ist, wird kontrovers diskutiert, ob Lösegeldzahlungen eine strafbare Unterstützung einer kriminellen oder terroristischen Vereinigung nach §§ 129, 129a StGB darstellen können.[27] Daneben kommen Verstöße gegen das Finanzsanktionsregime der EU (§ 18 AWG i.V.m. Art. 2 Abs. 2, 2a VO (EU) 881/2002) oder gegen weitere Finanzierungsverbote außereuropäischen Rechts in Betracht.[28] Die mitunter erörterte Gefahr der Terrorismusfinanzierung nach § 89c Abs. 1 Var. 3 StGB[29] wird sich in den Fällen einer Lösegeldzahlung regelmäßig nicht verwirklichen, da der Zahlende (als Täter) dafür mit dem Wissen – bedingter Vorsatz genügt nicht – oder sogar in der Absicht handeln müsste, dass das Lösegeld zur Begehung einer Katalogtat im Sinne des § 89c StGB verwendet werden soll.[30] Eine entsprechende positive Kenntnis eines solchen Verwendungszwecks wird im Zeitpunkt der Lösegeldzahlung regelmäßig fehlen. Die bloße Berichterstattung über die konkreten Täter der Cyberattacke und deren sonstige

---

im Wege der Konkurrenz verdrängt wird oder zumindest an einem eigenständigen Schaden Zweifel bestehen.

27 S. Salomon MMR 2016, 575 (575 ff.); Habbe/Gergen CCZ 2020, 281 (286); Fuhlrott/Schröder NZA-RR 2017, 625 (629); Gabel/Heinrich/Kiefner Rechtshandbuch Cyber-Security/Xylander/Gans Kap. 11 Rn. 21; jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; Scheurer AnwZert ITR 6/2017 Anm. 2; Rückert GWuR 2021, 103 (105).

28 Vgl. Brodowski/Schmid/Scholzen NStZ 2023, 385 (387); Fuhlrott/Schröder NZA-RR 2017, 625 (629); Rückert GWuR 2021, 103 (105). Zur Sanktionierung von Verstößen gegen das unionsrechtliche Außenwirtschafts- und Sanktionsrecht s. Spoerr/Gäde CCZ 2016, 77 (77 ff.).

29 So abstrakt Fuhlrott/Schröder NZA-RR 2017, 625 (629), für die Tatvariante des „zur Verfügung Stellens" von Vermögenswerten.

30 So auch Rückert GWuR 2021, 103 (105). Zu den hohen Anforderungen im subjektiven Tatbestand vgl. BGH Urt. v. 12.11.2020 – 3 StR 31/20 = NStZ 2021, 671 (673) Rn. 27; MünchKomm. StGB/Schäfer/Anstötz StGB § 89c Rn. 15.

kriminelle Aktivitäten reichen grundsätzlich nicht aus, um Anforderungen an den subjektiven Tatbestand zu erfüllen.[31] Abhängig von den Umständen des jeweiligen Einzelfalls kann aber eine Strafbarkeit wegen Urkundenfälschung (§ 267 StGB), Untreue (§ 266 StGB), Steuerhinterziehung (§ 370 AO) und unrichtiger Darstellung (§ 331 HGB) in Betracht kommen, wenn die Geschäftsleitung die wahren Hintergründe der Zahlung verschleiert.[32]

Den Schwerpunkt der strafrechtlichen Diskussion bildet die Frage nach einer Strafbarkeit gemäß den §§ 129, 129a StGB. Der objektive Tatbestand des § 129 StGB verlangt dabei eine Zahlung an eine kriminelle oder terroristische Vereinigung. Hierunter ist ein auf längere Dauer angelegter, organisierter Zusammenschluss von mehr als zwei Personen zur Verfolgung eines übergeordneten gemeinsamen Interesses zu verstehen, dessen Zweck oder Tätigkeit auf die Begehung von bestimmten schweren Straftaten[33] gerichtet ist.[34] Auch wenn die Struktur hinter den Tätern von Ransomware-Angriffen regelmäßig schwer zu ermitteln sein wird, liegt die Annahme einer kriminellen Vereinigung jedenfalls in den Fällen nahe, in denen Hacker-Gruppen den Ransomware-Angriff verüben.[35]

Unter einem Unterstützen im Sinne des § 129 StGB ist grundsätzlich jedes Tätigwerden zu verstehen, das durch ein Nichtmitglied der Vereinigung deren innere Organisation und ihren Zusammenhalt unmittelbar fördert, die Realisierung der von ihr geplanten Straftaten – wenn auch nicht zwingend maßgeblich – erleichtert oder das sich sonst auf deren Handlungsmöglichkeiten oder Zwecksetzung in irgendeiner Weise positiv auswirkt und damit die ihr eigene Gefährlichkeit festigt.[36] Hierfür reicht es aus, dass die Hilfe für die Bestrebungen der Vereinigung in irgendeiner Weise objektiv nützlich und vorteilhaft ist.[37] Der Tatbestand setzt dagegen

31 Rückert GWuR 2021, 103 (105), der für die Bejahung des Vorsatzes eine „glaubhafte, konkrete Information über den Verwendungszweck des gezahlten Lösegeldes (z.B. durch Behörden)" für notwendig hält, die im Regelfall nicht existiert.

32 Vgl. Fuhlrott/Schröder NZA-RR 2017, 625 (629) (Fn. 54).

33 Für die kriminelle Vereinigung auf die Begehung von Straftaten, die im Höchstmaß mit Freiheitsstrafe von mindestens zwei Jahren bedroht sind, und für die terroristische Vereinigung auf die in § 129a StGB aufgeführten Katalogtaten.

34 Vgl. nur Schönke/Schröder/Sternberg-Lieben/Schittenhelm StGB § 129 Rn. 4 f.

35 Brodowski/Schmid/Scholzen NStZ 2023, 385 (387).

36 BGH Urt. v. 19.4.2018 – 3 StR 286/17 = NJW 2018, 2425 (2426); LK-StGB/Krauß StGB § 129 Rn. 120; Schönke/Schröder/Sternberg-Lieben/Schittenhelm StGB § 129 Rn. 15; Lackner/Kühl/Heger StGB § 129 Rn. 6.

37 BGH Urt. v. 25.1.1984 – 3 StR 526/83 (S), juris-Rn. 5 = BGHSt 32, 243 (244); BeckOK StGB/von Heintschel-Heinegg StGB § 129 Rn. 13.

nicht voraus, dass der Vorteil von der Vereinigung konkret genutzt wird oder dass hierdurch eine konkrete, aus der Organisation heraus begangene Straftat oder auch nur eine organisationsbezogene Handlung geprägt wird.[38] Die Zahlung von Geldern an eine entsprechende Organisation ist ein typischer Fall der Unterstützung[39], so dass auch die (erpresste) Auskehr eines Lösegelds als Unterstützungshandlung anzusehen ist.[40] Die Geschäftsleitung muss es für eine Verwirklichung des vollständigen Tatbestands im Zeitpunkt der Lösegeldzahlung zumindest für möglich halten und billigend in Kauf nehmen, dass durch die Zahlung eine kriminelle Organisation unterstützt wird.[41] Ob dies der Fall ist, richtet sich nach den Umständen des Einzelfalls. Ob durch die Zahlung die Ziele der Organisation befürwortet werden oder der Erfolgseintritt an sich unerwünscht ist, ist für den Vorsatz nicht relevant.[42] Verkennt die Geschäftsleitung, dass die von der kriminellen Vereinigung begangenen oder geplanten Maßnahmen strafrechtlich relevant sind, oder hält sie entsprechende Verhaltensweisen mangels genauerer Kenntnis als von untergeordneter Bedeutung (vgl. § 129 Abs. 3 Nr. 2 StGB), handelt sie grundsätzlich (irrtumsbedingt) nicht vorsätzlich.[43]

Mit der Herausforderung für die Geschäftsleitung einerseits, in Ungewissheit über die Täter der Erpressung mit dem Cyber-Angriff konfrontiert zu sein, geht zugleich die Feststellung einher, dass der Nachweis eines festen, organisierten Zusammenschlusses von mindestens drei Personen mit gemeinsamem übergeordnetem Ziel als Täter der Erpressung in der Praxis oftmals nur schwierig zu führen sein wird. Geben sich die Täter nicht zu erkennen, wird häufig weder von der Geschäftsleitung noch von

38 Vgl. LK-StGB/Krauß StGB § 129 Rn. 123 m.w.N.; MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 112.

39 König NZWiSt 2023, 167 (168); LK-StGB/Krauß StGB § 129 Rn. 127.

40 Salomon MMR 2016, 575 (576); Rückert GWuR 2021, 103 (105); wohl auch Fuhlrott/Schröder NZA-RR, 2017, 625 (629).

41 So die h.M., vgl. nur BGH Urt. v. 3.10.1979 – 3 StR 264/79 = NJW 1980, 64; Brodowski/Schmid/Scholzen NStZ 2023, 385 (388);LK-StGB/Krauß StGB § 129 Rn. 147; König NZWiSt 2023, 167 (168 f.); Fischer StGB § 129 Rn. 48; Meyer/Biermann MMR 2022, 940 (943); jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; a.A. NK-StGB/Ostendorf StGB § 129 Rn. 25, der unter Verweis auf BGH bei Schmidt MDR 1991, 186 direkten Vorsatz fordert.

42 Salomon MMR 2016, 575 (576); Schönke/Schröder/Sternberg-Lieben/Schuster StGB § 15 Rn. 8.

43 Vgl. BGH Urt. v. 27.9.1956 – 6 StR 23/56 = LM Nr. 6 zu § 129 StGB; MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 123, 125;LK-StGB/Krauß StGB § 129 Rn. 147.

den Ermittlungsbehörden zu klären sein, ob sich hinter den (anonymen) Erpressern eine kriminelle oder terroristische Vereinigung verbirgt.[44] Auch wenn sich statistisch betrachtet eine Vielzahl solcher Vereinigungen aus der Erpressung von Lösegeldern im Zusammenhang mit Cyber-Angriffen finanziert,[45] kann hieraus nicht geschlossen werden, dass jeder anonyme Erpresser einer kriminellen oder terroristischen Vereinigung angehört, die von einer Lösegeldzahlung profitieren würde.[46] Dies gilt auch, wenn man versucht vorsätzliches Handeln von (hier nicht strafbaren) fahrlässigen Verhaltensweisen abzugrenzen, wenn unklar ist, wer hinter der Erpressung steht da sich der Eventualvorsatz auf eine konkrete Vereinigung beziehen muss. Es reicht also nicht aus, dass der Täter damit rechnet, dass er das Geld an eine „beliebige" kriminelle Vereinigung zahlt.[47] Bloße Vermutungen oder Spekulationen über eine konkrete Vereinigung reichen ebenfalls nicht aus.[48]

Dabei handelt es sich insgesamt um faktische Probleme der Beweisermittlung und des Tatnachweises durch Ermittlungsbehörden. Die Geschäftsleitung darf bei der Einschätzung, ob eine Zahlung strafrechtlich und gesellschaftsrechtlich zulässig ist, zwar berücksichtigen, ob für sie überhaupt Anhaltspunkte vorliegen, dass die Zahlung einen Straftatbestand erfüllen könnte. Ist dies der Fall, dürfen Erwägungen über eine faktische Verfolgung oder Nachweisschwierigkeiten durch die Ermittlungsbehörden bei der Entscheidung über eine Zahlung aber keine Rolle spielen.

2. Straflosigkeit durch Rechtfertigungsgründe?

Unabhängig von den tatsächlichen (Beweis-)Schwierigkeiten bei der Ermittlung der tatbestandlichen Voraussetzungen kann eine Lösegeldzahlung

44 So auch Rückert GWuR 2021, 103 (105); Hilgendorf/Kudlich/Valerius Handbuch des Strafrechts Bd. 6/Eisele § 63 Rn. 145; Nadeborn/Dittrich International Cybersecurity Law Review 3 (2022), 147 (157 f.).

45 Nach Salomon MMR 2016, 575 (576) sei es „bekannt, dass gerade auch Gruppierungen Erpressungstrojaner als Geschäftsmodell entdeckt haben".

46 So aber ohne tiefere Begründung Salomon MMR 2016, 575 (576). Für die Bejahung eines hinreichenden Tatverdachts müsste die Qualifikation als Vereinigung jedenfalls feststehen, da sonst eine Verurteilung gem. §§ 129, 129a StGB nicht möglich wäre, ohne gegen den *in dubio pro reo*-Grundsatz zu verstoßen. Zu dessen Anwendung auf tatbestandsbegründende Umstände vgl. nur KK-StPO/Ott StPO § 261 Rn. 6 m.w.N.

47 Rückert GWuR 2021, 103 (105).

48 Vgl. Rückert GWuR 2021, 103 (105).

wegen der besonderen Erpressungssituation gerechtfertigt sein. Dies wird vor dem Hintergrund der Notstandsregeln diskutiert.[49] Geht man davon aus, dass die Lösegeldzahlung den Tatbestand der §§ 129 ff. StGB erfüllt, läge ein sogenannter Nötigungsnotstand vor. Die Notstandslage ergibt sich aus der der Nötigung der Geschäftsleitung durch den Erpresser; die Geschäftsleitung würde durch Lösegeldzahlungen in die Rechtsgüter der inneren öffentlichen Sicherheit und staatlichen Ordnung einschließlich des öffentlichen Friedens[50] eingreifen, die von den §§ 129 ff. StGB geschützt werden.[51]

Bei einer unter Druck erfolgten Zahlung von Schutz- bzw. Lösegeld soll nach teilweise vertretener Auffassung ein rechtfertigender Notstand nach § 34 StGB regelmäßig ausscheiden.[52] Nach dieser Ansicht kann die Rechtsordnung keine Verhaltensweisen billigen, durch die sich der Notstandstäter zur Abwendung eines ihm angedrohten Übels zum Werkzeug eines rechtswidrig handelnden Dritten machen lässt[53] und insoweit selbst auf die Seite des Unrechts tritt.[54] Straffreiheit könne der Nötigungstäter allenfalls unter den Voraussetzungen des entschuldigenden Notstands nach § 35 StGB (analog) erlangen.[55] Dieses Verständnis dehnt ein mögliches Strafbarkeitsrisiko von Geschäftsleitern bei Ransomware-Angriffen zu weit aus, da in der Regel die für eine Entschuldigung nach § 35 StGB (analog) erforderliche Gefahr für Leben, Leib oder Freiheit[56] nicht vorliegen und ein Schuldausschluss damit in den meisten Fällen ausscheiden wird.[57] Häufig wird der zu erwartende Nachteil weder den Handelnden selbst noch eine von § 35 Abs. 1 StGB genannte Person treffen, weshalb zusätzlich ein

49 Vgl. allgemein Arzt/Weber/Heinrich/Hilgendorf Strafrecht BT/Hilgendorf § 44 Rn. 17 und § 10 Rn. 10; jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165; SK-StGB/Stein/Greco StGB § 129 Rn. 53.

50 S. MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 1.

51 Vgl. Salomon MMR 2016, 575 (576) m.w.N.; Rückert GWuR 2021, 103 (106).

52 MünchKomm. StGB/Schäfer/Anstötz StGB § 129 StGB Rn. 126; Schönke/Schröder/Sternberg-Lieben/Schittenhelm StGB § 129 StGB Rn. 17; Fischer StGB § 129 Rn. 41; SSW-StGB/Lohse StGB § 129 Rn. 53.

53 Vgl. Schönke/Schröder/Perron StGB § 34 StGB Rn. 41b.

54 Ausführlich Schönke/Schröder/Perron StGB § 34 Rn. 41b; im Ergebnis auch Arzt JZ 2001, 1052 (1054 ff.).

55 MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 126; Schönke/Schröder/Perron StGB § 43 Rn. 41b; Fischer StGB § 129 Rn. 41.

56 Siehe hierzu MünchKomm. StGB/Müssig StGB § 35 Rn. 12 ff.

57 König NZWiSt 2023, 167 (169); Brodowski/Schmid/Scholzen NStZ 2023, 385 (388); Meyer/Biermann MMR 2022, 940 (942).

übergesetzlicher entschuldigender Notstand zu erwägen ist.[58] Etwas anderes wird man insbesondere bei Attacken auf kritische Infrastrukturen, wie Krankenhäuser, annehmen müssen, bei denen eine Gefahr für Leib und Leben in den Vordergrund tritt.[59] Auch ein Schuldausschluss nach § 17 StGB dürfte regelmäßig ausscheiden. Ransomware-Angriffe haben inzwischen keinen Seltenheitswert mehr.[60] Durch den Anstieg der Ransomware-Angriffe und der damit verbundenen Bedrohungslage für Unternehmen könnten Ermittlungsbehörden davon ausgehen, dass betroffene Geschäftsleitungen es jedenfalls für möglich halten werden, mit Lösegeldzahlungen eine kriminelle Vereinigung zu unterstützen und sich dem Risiko einer Strafbarkeit nach § 129 StGB auszusetzen.[61] In einem solchen Fall würde ein Verbotsirrtum nach § 17 StGB ausscheiden.[62] Durch die Möglichkeit, im Falle eines Ransomware-Angriffs Rechtsrat einzuholen, würde ein etwaiger Irrtum von Ermittlungsbehörden voraussichtlich zudem als vermeidbar angesehen sein und insoweit allenfalls eine Milderung nach § 17 S. 2 StGB in Betracht kommen.[63]

Überzeugender ist es deshalb im Fall von Lösegeldzahlungen die Regeln des rechtfertigenden Notstands gemäß § 34 StGB anzuwenden. Anders als der entschuldigende Notstand (gem. § 35 StGB) sieht der offenere Wortlaut des § 34 StGB keine Restriktionen hinsichtlich des Ursprungs der Gefahr vor. Auch beim Nötigungsnotstand verdient der unter dem Nötigungsdruck handelnde Täter die Solidarität der Rechtsordnung.[64] Der in Zwangslage handelnde (Nötigungs-)Täter tritt auch nicht freiwillig auf die Seite des Unrechts, sondern wird vom Erpresser auf diese Seite gedrängt[65]. Möglicherweise beeinträchtigte Interessen Dritter können im Rahmen der Interessenabwägung angemessen berücksichtigt werden.[66]. Die Anwendung von

58 Vgl. Salomon MMR 2016, 575 (577). Dazu Bechtel JuS 2021, 401 (401 ff.).
59 So Meyer/Biermann MMR 2022, 940 (942); wohl auch Salomon MMR 2016, 575 (576); Dittrich/Erdogan ZWH 2022, 13 (17).
60 BSI, Ransomware Bedrohungslage 2022, S. 4 f.
61 König NZWiSt 2023, 167 (169).
62 BGH, Beschl. v. 24.2.2011 – 5 StR 514/09 = NJW 2011, 1236 (1239); Fischer StGB, § 17 Rn. 2.
63 König NZWiSt 2023, 167 (169); vgl. Graf/Jäger/Wittig Wirtschafts- und Steuerstrafrecht/Sackreuther StGB § 17 Rn. 16 ff.
64 MünchKomm. StGB/Erb StGB § 34 Rn. 192 ff. m.w.N. zu beiden Ansichten. Zustimmend Salomon MMR 2016, 575 (577). Wohl auch jurisPK-Internetrecht/Heckmann Kap. 8 Rn. 165. Ausführlich auch Brand/Lenk JuS 2013, 883 (883 ff.).
65 Brand/Lenk JuS 2013, 883 (884).
66 MünchKomm. StGB/Erb StGB § 34 Rn. 194.

§ 34 StGB auf Fälle der durch einen Ransomware-Angriff hervorgerufenen Notstandshandlung, ermöglicht danach sachgerechte Ergebnisse im jeweiligen Einzelfall.[67]

Bei Zahlung eines Lösegeldes muss daher stets eine Interessenabwägung zwischen dem bedrohten Rechtsgut (hier des Erpressungsopfers) und dem Rechtsgut, in das durch die abgenötigte Straftat eingegriffen wird, erfolgen. Eine solche Abwägung wird regelmäßig zur Rechtfertigung der Zahlung führen[68], auch wenn in der Literatur teilweise ein deutliches Überwiegen der Interessen des Genötigten gefordert wird:[69]

Durch die Zahlung wird in keine Individualrechtsgüter, wie Leib, Leben oder persönliche Freiheit einer anderen Person, eingegriffen sodass auch keine problematischen Duldungspflichten auf Seiten anderer Individuen bestehen.[70] Es gibt hier kein konkretes Notstandsopfer, da die §§ 129 ff. StGB ausschließlich abstrakte Allgemeinrechtsgüter schützen, d.h. insbesondere die innere öffentliche Sicherheit und die staatliche Ordnung einschließlich des öffentlichen Friedens.[71] Die Schwere der durch die Lösegeldzahlung tatbestandlich verwirklichten Notstandstat ist abstrakt als sehr gering zu bewerten. Auch unter Berücksichtigung des jeweiligen Einzelfalls wird durch die Zahlung des Lösegelds die innere öffentliche Sicherheit und die staatliche Ordnung allenfalls gering konkret betroffen sein.[72]

Selbst wenn das angegriffene Unternehmen keine schwerwiegenden Rechtsgutsbeeinträchtigungen (wie z.B. die Gefährdung von Menschen) zu befürchten hat, werden im Rahmen der Interessenabwägung die Beeinträchtigung des Eigentums und der Berufsausübungsfreiheit regelmäßig überwiegen. Eine entsprechende Beeinträchtigung liegt bei einem Ransomware-Angriff regelmäßig vor, da die Erpresser regelmäßig den Zugriff auf die Unternehmensdaten verhindern und diese löschen oder veröffentlichen können.[73] Das Unternehmen hat ein Interesse an der Vermeidung

67 So auch König NZWiSt 2023, 167 (169).
68 So auch König NZWiSt 2023, 167 (169); Rückert GWuR 2021, 103 (106); Salomon MMR 2016, 575 (577); SK-StGB/Stein/Greco StGB § 129 Rn. 53, die offenlassen, ob Rechtfertigung oder Entschuldigung einschlägig ist.
69 So MünchKomm. StGB/Erb StGB § 34 Rn. 194; BeckOK StGB/Momsen/Savić StGB § 34 Rn. 17; Meyer/Biermann MMR 2022, 940 (942).
70 Vgl. Rückert GWuR 2021, 103 (106); Salomon MMR 2016, 575 (577).
71 Vgl. hierzu MünchKomm. StGB/Schäfer/Anstötz StGB § 129 Rn. 1.
72 So auch Salomon MMR 2016, 575 (578); Rückert GWuR 2021, 103 (106).
73 Vgl. Salomon MMR 2016, 575 (577 f.); vgl. auch Brodowski/Schmid/Scholzen/Zoller NStZ 2023, 385 (388).

erheblicher wirtschaftlicher Schäden, der Wiedererlangung der häufig für den Geschäftsbetrieb unverzichtbaren Daten und der Vermeidung eines drohenden Reputationsverlusts. Auch kann die wirtschaftliche Existenz des Unternehmens durch den Ransomware-Angriff und der damit einhergehenden Folgen gefährdet sein. Dies (sowie die Cyber-Attacke selbst) haben auch Auswirkungen auf Beschäftigte die bspw. freigestellt werden müssen, solange kein Zugriff auf wichtige Daten besteht, da hierdurch die Funktionsfähigkeit des gesamten Unternehmens eingeschränkt sein kann. Bei Angriffen auf kritische Infrastrukturen, wie Krankenhäuser, treten weitere Rechtsgüter auf Seiten der Erpressten in die Abwägung ein (z.B. die Aufrechterhaltung der öffentlichen Gesundheitsvorsorge).[74]

Für ein Überwiegen der Interessen des angegriffenen Unternehmens spricht auch, dass die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) im Jahr 2017 eine Ransomware-Versicherung in Cyber-Versicherungspolicen genehmigt hat (siehe hierzu auch Rz. 34.151).[75] Der Genehmigung der BaFin kommt zwar keine rechtsverbindliche Wirkung zu, sie entfaltet jedoch eine starke Indizwirkung gegen eine Strafbarkeit von Lösegeldzahlungen nach deutschem Recht. Andernfalls hätte die BaFin eine solche Genehmigung voraussichtlich nicht erteilt. Es gebietet daher der Gedanke der Einheit der Rechtsordnung, die als rechtlich legitimen Versicherungsgegenstand anzusehende Lösegeldzahlung auch als strafrechtlich möglich/gerechtfertigt anzusehen. Dem stehen auch die Ausführungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und BKA zu Lösegeldzahlungen bei Ransomware-Angriffen nicht entgegen:[76] So führen BSI und BKA zwar aus, dass auf eine Erpressung nicht eingegangen und ein Lösegeld nicht bezahlt werden sollte. Zur Begründung weisen sie jedoch insbesondere darauf hin, dass eine Zahlung die Gefahr möglicher weiterer Angriffe berge und selbst bei Zahlung keine Garantie bestünde, dass der kriminelle „Verhandlungspartner" die Verschlüsselung nach der Lösegeld-

74 So auch insg. Rückert GWuR 2021, 103 (106).

75 BaFin Mitteilung vom 15. September 2017, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (zuletzt abgerufen am 6.1.2025).

76 Vgl. BSI, Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Arbeitspapier – Version 1.2 (7. Oktober 2022), S. 15; BKA, Ransomware – Unternehmen und Institutionen als Zielscheibe, S. 10 f.; auch im Bundeslagebild Cybercrime 2021 führt das BKA zu einer Strafbarkeit von Lösegeldzahlungen nicht aus, vgl. Bundeslagebild Cybercrime 2023, S. 25 f.; auf eine kleine Anfrage der AfD-Fraktion ist die Bundesregierung den Ausführungen von BSI und BKA nicht entgegengetreten, vgl. BT-Drs. 20/2926, S. 3.

zahlung tatsächlich aufhebe. Eine mögliche Strafbarkeit einer Lösegeldzahlung wird zur Begründung dagegen nicht herangezogen. Vielmehr weist das BKA ausdrücklich darauf hin, dass im Einzelfall eine Zahlung in Betracht gezogen werden kann, wenn das Unternehmen vor der Wahl steht, den Geschäftsbetrieb einzustellen oder Lösegeld zu zahlen.[77]

Um etwaige strafrechtliche Risiken weiter zu reduzieren, sollten frühzeitig (spätestens jedoch) bei Eingang einer konkreten Lösegeldforderung die Ermittlungsbehörden (und dort zunächst die zuständige Spezialstelle des Landeskriminalamtes) informiert und eine mögliche Lösegeldzahlung im Vorfeld mit den Ermittlungsbehörden (auch der zuständigen Staatsanwaltschaft) abgestimmt werden. Zusätzlich sollte in diesem Fall eine detaillierte Prüfung der hier skizzierten Risiken anhand des konkreten Einzelfalls stattfinden.

Die Möglichkeit einer Rechtfertigung der Lösegeldzahlung nach § 34 StGB unter Abwägung der widerstreitenden Interessen kommt auch für weitere Straftatbestände in Betracht. So schützen die Verbotstatbestände des § 18 Abs. 1 Nr. 1 und 2 AWG die abstrakten Rechtsgüter der Sicherheit der Bundesrepublik und des Völkerfriedens[78]. Erfolgt eine Lösegeldzahlung, muss diese im Unternehmen und der Buchhaltung korrekt und transparent dargestellt werden, so dass die oben angesprochenen Tatbestände der Urkundenfälschung (§ 267 StGB), Untreue (§ 266 StGB), Steuerhinterziehung (§ 370 AO) und unrichtiger Darstellung (§ 331 HGB) nicht drohen verwirklicht zu werden.

III. Sanktionsrisiken nach US-amerikanischem Recht (insbesondere „civil monetary penalties")

Sofern die vom Cyberangriff betroffene Gesellschaft Geschäfte mit einem Bezug zur US-Jurisdiktion betreibt, sind zudem erhebliche Risiken mit Blick auf die dortigen Sanktionsvorschriften zu beachten.[79] In seinen unverbindlichen Leitlinien aus September 2021 weist das *U.S. Department of the Treasury's Office of Foreign Assets Control* (*OFAC*) insofern darauf hin, dass sich Gesellschaften in zivilrechtlicher Hinsicht („*civil monetary*

77 Vgl. BKA, Ransomware – Unternehmen und Institutionen als Zielscheibe, S. 10.

78 Vgl. MünchKomm. StGB/Wagner AWG § 18 Rn. 11.

79 Rückert GWuR 2021, 103 (104); vgl. auch: *U.S. Department of the Treasury's Office of Foreign Assets Control* (OFAC), Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments v. 21.9.2021.

penalty") einer „*strict liability*", d.h. einer von der Bösgläubigkeit ihrer Geschäftsleiter unabhängigen Haftung, ausgesetzt sähen.

C. Gesellschaftsrechtliche Haftungsrisiken

I. Ransomware-Angriffe als Haftungsfall?

Sofern und soweit die Zahlung von Lösegeld im Falle eines Cyberangriffs nach der hier vertretenen Auffassung gerechtfertigt ist (und zudem kein Verstoß gegen EU- oder US-Sanktionsregelungen vorliegt), liegt eine unternehmerische Entscheidung vor. Die Geschäftsleitung hat dann eine Interessenabwägung vorzunehmen, bei der sämtliche der Geschäftsleitung bekannten Kriterien einzubeziehen sind. Nach den Grundsätzen der Business Judgement Rule hat die Geschäftsleitung allerdings das Unternehmenswohl stärker zu berücksichtigen als bei der Abwägung im Rahmen des § 34 StGB. Es ist im Einzelfall abzuwägen, ob die Zahlung eines Lösegeldes zum Wohle des Unternehmens das bessere Mittel darstellt oder ob es vorzugswürdig ist, zunächst abzuwarten und die Daten durch die eigene IT-Abteilung oder externe Experten wiederherstellen zu lassen bzw. dies zu versuchen.

Bei einem erfolgreichen Ransomware-Angriff wird spätestens bei der nachträglichen Aufarbeitung auch die Haftung des Vorstands wegen eines etwaigen Organisationsversagens zu prüfen sein, unabhängig davon, ob Lösegeld gezahlt wurde oder nicht. Denn die Risikovorsorge ist – auch in der Informationssicherheit – originäre Aufgabe des Managements. Der Vorstand muss daher ausreichende Schutzvorkehrungen zur Vermeidung eines erpresserischen Cyber-Angriffs treffen.[80] Wird dies in einem Organhaftungsprozess angezweifelt, bestehen für die an sich darlegungs- und beweisbelastete Gesellschaft nach der Rechtsprechung Beweiserleichterungen für den Nachweis eines kausalen Schadens. Für den Ursachenzusammenhang zwischen Zahlung einer Beraterleistung und Schaden hat etwa das LG München I in seiner „Siemens/Neubürger"-Entscheidung § 287 ZPO herangezogen.[81] Danach muss die Gesellschaft nur Tatsachen vortra-

80 Vgl. zu den denkbaren (präventiven) Maßnahmen Heinrichs/Neumeier CB 2022, 14 (17 f.). Zur drohenden gesellschaftsrechtlichen Haftung der Geschäftsleiter in diesem Kontext vgl. u.a. Mehrbrey/Schreibauer MMR 2016, 75 (79 f.); Daghles DB 2018, 2289; Grieger WM 2021, 8 (11 ff.); Schmidt-Versteyl NJW 2019, 1637 (1638 f.).

81 LG München I Urt. v. 10.12.2013 – 5 HK O 1387/10 = AG 2014, 33. Vgl. hierzu auch Scholz ZZP 133 (2020), 491 (506 f.).

gen und unter Beweis stellen, die für eine Beurteilung nach § 287 ZPO ausreichend greifbare Anhaltspunkte bieten. Das beklagte Organmitglied hat demgegenüber darzulegen und erforderlichenfalls zu beweisen, dass es seinen Sorgfaltspflichten nachgekommen ist oder es kein Verschulden trifft oder dass der Schaden auch bei pflichtgemäßem Alternativverhalten eingetreten wäre. Andere wollen die Regelungen über den Anscheinsbeweis anwenden.[82]

Nach einem erfolgten Cyberangriff sind in jedem Fall unverzüglich die erforderlichen Maßnahmen zu ergreifen, um das Schadensrisiko zu begrenzen sowie den Sachverhalt aufzuklären, mögliche Verstöße abzustellen und festgestelltes Fehlverhalten zu sanktionieren (Aufklärung, Abstellung, Ahndung). Dazu gehört auch, die IT-Systeme einer Prüfung zu unterziehen und Schwachstellen zu identifizieren und zu beseitigen. Darüber hinaus ist die bestehende IT-Compliance-Organisation und -Infrastruktur kritisch zu hinterfragen und auf Basis der gewonnenen Erkenntnisse und Erfahrungen weiterzuentwickeln.

II. Erweiterte Pflichten und Haftung nach der NIS-2-Richtlinie

Am 16. Januar 2023 ist die NIS-2-Richtlinie in Kraft getreten.[83] Sie erweitert den Anwendungsbereich der gesetzlichen Cybersicherheitspflichten, die bisher vor allem für Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste galten, auf weite Teile der Wirtschaft und verschärft das Sanktionsregime bei Verstößen erheblich. Die Mitgliedsstaaten der Europäischen Union (EU) hätten die NIS-2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen müssen. In Deutschland ist dies bislang nicht geschehen.

Durch die NIS-2-Richtlinie und die geplante nationale Umsetzung werden öffentliche und private Stellen zur Einhaltung eines hohen Cybersicherheitsniveaus verpflichtet. Dabei ist nicht nur der Anwendungsbereich der Regelungen deutlich weiter als bei der Vorgängerrichtlinie – viele Unternehmen werden erstmals von konkreten Cybersicherheitspflichten

82 KölnKomm. AktG/Cahn AktG § 93 Rn. 142.

83 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148.

betroffen sein. Die Regelungen gehen auch inhaltlich weiter, als dies bisher der Fall war.[84] Das Umsetzungsgesetz sieht insbesondere eine Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG) vor (folgend „BSIG-E").

§ 28 BSIG-E definiert die besonders wichtigen Einrichtungen und die Betreiber kritischer Anlagen, die in den Anwendungsbereich fallen. Neben dem Datenschutz gelten weitergehende Cybersicherheitsanforderungen bislang nur für bestimmte Unternehmen, insbesondere im Bereich kritischer Infrastrukturen und digitaler Dienste. Mit der NIS2-Richtlinie und dem BSIG-E wird die Liste der Sektoren, für die verbindliche Cybersicherheitspflichten gelten sollen, deutlich erweitert. Ausweislich der Gesetzesbegründung ist nunmehr davon auszugehen, dass ca. 8.250 Unternehmen als besonders wichtige und rund 21.600 Unternehmen als wichtige Einrichtungen klassifiziert werden.[85] Nach Angaben des BSI waren bisher nur ca. 1.100 kritische Infrastrukturen mit ca. 2.000 kritischen Anlagen von der KRITIS-Regulierung erfasst.[86]

Nach § 30 des BSIG-E müssen besonders wichtige und wichtige Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Betroffene Unternehmen müssen u.a. ein Risikomanagementsystem zum Schutz ihrer IT-Strukturen einrichten und dokumentieren und Sicherheitsvorfälle müssen innerhalb von 24 Stunden gemeldet werden (§ 32 BSIG-E).[87] Pflichtverstöße können Geldbußen von bis zu EUR 10 Mio oder 2 % des Jahresumsatzes nach sich ziehen (§ 65 BSIG-E). Die Geschäftsleitung trägt die Verantwortung für die Umsetzung und Überwachung dieser Maßnahmen und kann bei Pflichtverletzungen haftbar gemacht werden. Die Geschäftsleitungen besonders wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der

84 Schmidt RDi 2024, 550 (550) Rn 2.
85 BT-Drs. 20/13184, S. 102.
86 Vgl. Schmidt RDi 2024, 550 (551) Rn 4.
87 Dazu Kipker/Dittrich MMR 2023, 481 (483).

Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können (§ 38 BSIG-E).[88]

III. Absicherung durch Cyberversicherungen

Um das Risiko von Schäden nach einem Cyber-Angriff zu reduzieren, werden mittlerweile häufig, entsprechende Cyber-Versicherungen abgeschlossen, die auch die Zahlung von Lösegeld einschließen können.[89] Lösegeldversicherungen waren zwar früher verboten, wurden aber schon durch die Vorgängerbehörde der BaFin für zulässig erklärt[90] und dürfen nun auch gebündelt mit einer Cyber-Versicherung abgeschlossen werden, wobei die Lösegeldversicherung selbst nicht beworben werden darf.[91] Je nach Risikolage des Unternehmens, etwa bei Geschäftsfeldern, die oft ins Visier von Cyber-Attacken geraten, müssen Vorstand und Aufsichtsrat abwägen, ob der Abschluss einer solchen Versicherung im Interesse des Unternehmens liegt, was zumindest bei größeren Unternehmen der Fall sein dürfte.[92]

Um aufgrund der sicher erscheinenden Auszahlung keine zusätzlichen Anreize für Erpresser zu schaffen, müssen Cyber-Versicherungen nach den Versicherungsbedingungen geheim gehalten werden.[93] Aus diesem Grund stehen Versicherungen für Lösegeldzahlungen auch in der Kritik, da damit das Geschäftsmodell Cyber-Erpressung nicht „ausgetrocknet" wird, sondern weiter attraktiv bleibt.[94] Ein Verbot wurde von der Bundesregierung jedoch als nicht notwendig und nicht zielführend erachtet, da die

88 Kipker/Dittrich MMR 2023, 481 (485); Schmidt RDi 2024, 550 (554 f.) Rn. 22 ff.

89 Zur Möglichkeit der Versicherung Veith/Gräfe Der Versicherungsprozess/Gebert/Klapper § 24 Rn. 96; Fortmann r+s 2019, 429 (434 f.); Gabel/Heinrich/Kiefner Rechtshandbuch Cyber-Security/Wirth Kap. 12 Rn. 67 ff.; Wirth BB 2018, 200 (204); Prölss/Martin VVG/Klimke A1_17 A1–17 AVB Cyber Rn. 23; Notthoff r+s 2022, 61 (65); vgl. aber noch die Regelung A1–17.7 der AVB Cyber (Stand: April 2017), die inzwischen durch die Praxis überholt wurde.

90 Bundesaufsichtsamt für das Versicherungswesen (BAV): Rundschreiben 3/1998 (VA).

91 BaFin, BaFin Journal, September 2017, S. 4 f., abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (zuletzt abgerufen am 6.1.2025).

92 Kiefner/Happ BB 2020, 2051 (2055); Daghles DB 2018, 2289 (2292).

93 BaFin, BaFin Journal, September 2017, S. 4 f.; vgl. dazu auch Fortmann r+s 2019, 429 (435).

94 Dittrich/Erdogan ZWH 2022, 13 (17); Stellungnahme der Gesellschaft für Informatik et al. aus Juni 2022, abrufbar unter: https://gi.de/offener-brief-zu-loesegeldzahlu

Unternehmen auch ohne Versicherung nicht davon abgehalten würden, ein Lösegeld (selbst) zu zahlen.[95]

ngen-bei-ransomware-angriffen-ein-geostrategisches-risiko (zuletzt abgerufen am 6.1.2025).

95 BT-Drs. 20/2926, S. 6.

Die Verstrafrechtlichung des Schweizer Wirtschaftsrechts – Verwaltungssanktionen vs. Verwaltungsstrafen anhand der Beispiele Datenschutzgesetz und Wettbewerbsrecht

Oliver Jany, Lukas Staub[*1]

1. Einleitung

Aus Sicht der Akteure einer liberalen Marktwirtschaft ist es entscheidend zu wissen, welche Regeln für sie gelten und welche Sanktionen drohen, sollten sie gegen die Regeln verstossen. In dieser Hinsicht beklagen Lehre[2] und Praxis[3] sowohl in der Schweiz als auch in Deutschland schon seit einiger Zeit eine zunehmende „Verstrafrechtlichung" des Wirtschaftsrechts, das heisst die Tendenz des Gesetzgebers, Regeln des Wirtschaftsrechts durch die Androhung strafrechtlicher Sanktionen im Falle ihrer Verletzung durchzusetzen.

Anders als das Schlagwort der Verstrafrechtlichung vielleicht indizieren mag, ist diese Verknüpfung der zwei grundsätzlich unterschiedlichen Rechtsgebiete des Wirtschaftsrechts einerseits und des Strafrechts andererseits freilich nicht neu. So sind beispielsweise die Konkursdelikte in Art. 163 ff. des Strafgesetzbuchs („**StGB**") oder die Strafbestimmungen im Bankengesetz einschliesslich des Bankkundengeheimnisses für wahr keine Erfindungen der jüngeren Vergangenheit.

Dennoch scheint sich der Eindruck zu verfestigen, dass sich der Schweizer Gesetzgeber in den letzten gut drei Jahrzehnten zunehmend strafrechtlicher Mechanismen zur Durchsetzung wirtschaftsrechtlicher Regelungen bedient. Wesentliche Meilensteine bei der Einführung strafrechtlicher Sanktionen im Bereich der Wirtschaft – einschliesslich entsprechender

---

* Dr. iur. Oliver Jany, Rechtsanwalt bei Prager Dreifuss, Zürich; Lukas Staub, Rechtsanwalt bei Lenz & Staehelin, Zürich, und Dozent an der Fernfachhochschule Schweiz (FFHS).

1 Die Autoren danken MLaw Julia Schorer für die Zusammenstellung und Aufarbeitung von Quellen und Materialien.

2 So bereits vor rund 20 Jahren Strasser, S. 752; siehe zudem auch Bohrer, S.127.

3 Gaberthuel, „Verstrafrechtlichung" der Wirtschaft, FUW Nr. 23/2016, S. 13.

Zuständigkeit der Strafbehörden im Strafverfahren – waren beispielsweise die Einführung der Insiderstrafnorm 1988[4], der Geldwäschereistrafnorm 1990[5], der Kursmanipulation 1995[6] und der Privatbestechung 2016[7].

Demgegenüber hat sich der Schweizer Gesetzgeber der Verwaltungssanktionen – namentlich durch Verwaltungsbehörden zu verhängende Sanktionen ausserhalb des Straf- bzw. Nebenstrafrechts – nur sehr zurückhaltend bedient.[8] Von praktischer Bedeutung sind in der Schweiz primär die kartellrechtlichen Sanktionen sowie, mit weit weniger praktischer Bedeutung, die Sanktionsmöglichkeiten im Fernmelde- und Landwirtschaftsbereich. Der Bundesrat veröffentlichte 2022 einen umfassenden Bericht zu den pekuniären Verwaltungssanktionen, der den damaligen Status quo darlegt.[9]

Aus Sicht der Digitalwirtschaft, die ganz wesentlich auf der Nutzung von Daten, auch Personendaten aufbaut, sind die Regeln des Datenschutzrechts von besonderer Bedeutung. Das einschlägige totalrevidierte Datenschutzgesetz („**DSG**“) ist erst kürzlich, per 1. September 2023, in Kraft getreten. Dabei hat sich der Schweizer Gesetzgeber – obwohl er sich beim neuen DSG in weiten Teilen stark an der EU-Datenschutzgrundverordnung („**DSGVO**“) orientiert hat – im Bereich der Sanktionen bewusst gegen den Weg der Verwaltungssanktionen entschieden und stattdessen erneut das Strafrecht zur Durchsetzung gewählt. Der Gesetzgeber hat sich damit erneut für eine „Verstrafrechtlichung“ des Wirtschaftsrechts entschieden und zahlreiche Verstösse gegen das DSG dem (Neben-)Strafrecht unterstellt. Somit unterstehen nun auch weite Teile der Regeln zum Datenschutz bei Verstössen einer potentiellen Strafdrohung, wobei deren Abschreckungswirkungen – wie noch zu zeigen sein wird – nicht in jeder Hinsicht zu überzeugen vermag.

---

4 Die Strafbarkeit von Insidergeschäften wurde am 18. Dezember 1987 beschlossen und trat am 1. Juli 1988 in Kraft, im Jahr 2016 ins neue Finanzmarktinfrastrukturgesetz („**FinfraG**“) aufgenommen.

5 Eingefügt durch Ziff. I des Bundesgesetzes [„**BG**“] vom 23. März 1990, in Kraft seit 1. August 1990 (Amtliche Sammlung [„**AS**“] 1990 1077; Bundesblatt [„**BBl**“] 1989 II 1061).

6 Eingefügt durch Art. 46 des Börsengesetzes vom 24. März 1995 (AS 1997 68; BBl 1993 I 1369). Aufgehoben durch Ziff. II 3 des BG vom 28. September 2012, mit Wirkung seit 1. Mai 2013 (AS 2013 1103; BBl 2011 6873), im Jahr 2016 ins FinfraG übertragen.

7 Gemäss Ziff. I des BG vom 25. September 2015 (Korruptionsstrafrecht), in Kraft seit 1. Juli 2016 (AS 2016 1287; BBl 2014 3591).

8 Bericht Verwaltungssanktionen, S. 2, S. 22.

9 Vgl. Bericht Verwaltungssanktionen.

Vor diesem Hintergrund stellt der vorliegende Beitrag die Modelle der Verwaltungssanktionen und der Verwaltungsstrafen anhand zweier praktischer Beispiele – die Verwaltungssanktionen im Kartellrecht und die neuen Strafnormen im DSG – gegenüber, wobei besonders auf die Bedeutung für die Digitalwirtschaft eingegangen wird.

2. Das Modell Verwaltungssanktionen

Verwaltungssanktionen bilden komplementär zu den Verwaltungsstrafen das alternative Modell zur Sanktionierung im Wirtschaftsbereich. Der Prototyp der Verwaltungssanktion ist die Kartellbusse. Sie war die erste repressive Sanktionsform gegen Unternehmen.[10] Konsequenterweise haben sich viele sanktions- und verfahrensrechtliche Fragen des Verwaltungssanktionsverfahrens erstmals im Bereich des Kartellrechts gestellt. Hierzu zählt etwa die Frage, welche (strafrechtlichen) Verfahrensrechte den im Kartellverfahren beschuldigten Unternehmen zukommen.[11] Das Kartellsanktionsrecht gilt aus diesem Grund als das am weitesten entwickelte Verwaltungssanktionsrecht und dient in der EU daher als Blaupause auch für neuere Sanktionsverfahren, etwa der bereits erwähnten DSGVO, dem Digital Service Act („**DSA**"). oder dem Digital Markets Act („**DMA**"). Die Bedeutung der Kartellsanktion ist deshalb kaum zu überschätzen und legt nahe, sie zur Betrachtung des Verwaltungssanktionsmodells heranzuziehen.

Es wird sich allerdings zeigen, dass das Kartellsanktionsrecht bislang keinesfalls stets stringente Lösungen für die komplexe Differenzierung zwischen Verwaltungs- und Kriminalstrafrecht bereithält.

a. Kartellsanktionen als Verwaltungssanktionen

Sowohl in der Schweiz als auch in der Europäischen Union können gegen Unternehmen, die wettbewerbsrechtliche Zuwiderhandlungen – wie unmittelbare Preisabsprachen oder Marktaufteilungen – begehen, Kartellsanktionen von bis zu 10 % des erzielten Gesamtumsatzes der letzten drei Geschäftsjahre (Schweiz) bzw. des im vorausgegangenen Geschäftsjahrs

10 In der Europäischen Union ergingen erste Entscheidungen zur Kartellsanktion bereits ab 1969, vgl. EuGH, Urt. v. 13.2.1969 Walt Wilhelm, ECLI:EU:C:1969:4.

11 Jany, Legitimationsdefizite, S. 34ff.

erzielten Gesamtumsatzes (EU) verhängt werden.[12] Die Kartellsanktionen sind in beiden Rechtsordnungen formell als Verwaltungssanktionen ausgestaltet.

Verwaltungssanktionen sind behördliche Massnahmen zur Ahndung verwaltungsrechtlicher Pflichtverletzungen. Sie richten sich gegen Unternehmen,[13] nicht aber gegen die für das Unternehmen handelnden Personen (Organe, Mitarbeitende), und sehen als Rechtsfolge zum Teil hohe finanzielle Bussen vor. Obwohl sich Verwaltungssanktionen[14] in der Schweiz sektoriell als Instrument des Wirtschaftsaufsichtsrechts[15] etabliert haben, sind sie nach wie vor die Ausnahme.[16] Wie strafrechtliche Sanktionen, haben Verwaltungssanktionen eine präventive und repressive Straffunktion.[17] Das Bundesgericht hält fest, dass pekuniären Verwaltungssanktionen ein präventiver, gleichzeitig aber auch ein pönaler und repressiver Charakter zukommt.[18] Kartellsanktionen werden daher als „quasi-strafrechtlich" oder „strafrechtliche Sanktionen im weiteren Sinne" bezeichnet.[19] Die (Verwaltungs-)Sanktion unterscheidet sich jedoch von der Kriminalstrafe im Umfang des staatlichen Vorwurfs für die Zuwiderhandlung, dem Sanktionsorgan sowie bei der Anwendung prozessualer Verfahrensgarantien.

---

12 Nach Art. 49a Abs. 1 Schweizerisches Kartellgesetz (**„KG"**) können Unternehmen, die kartellrechtlich unzulässig handeln, mit einem mit einem Betrag bis zu 10 Prozent des in den letzten drei Geschäftsjahren in der Schweiz erzielten Umsatzes belastet werden. Für Deutschland ergibt sich dies aus § 81c Abs. 2 Gesetz gegen Wettbewerbsbeschränkungen („**GWB**") für Zuwiderhandlungen nach § 81 Abs. 2 Nr. 1 GWB, Art. 1 GWB. Für die EU ergibt sich die Sanktion aus Art. 101 Abs 1 Vertrag über die Arbeitsweise der Europäischen Union („**AEUV**") i.V.m. Art. 103 Abs. 2 lit. a AEUV iVm. Art. 23 Abs. 2 VO 1/2003.

13 Abhängig vom Geltungsbereich eines Sacherlasses können auch natürliche Personen erfasst sein, die einer regulierten Tätigkeit nachgehen, vgl. beispielsweise Art. 60 des Fernmeldegesetzes (FMG). Organe einer juristischen Person und Mitarbeitende von Unternehmen sind hingegen nicht von pekuniären Verwaltungssanktionen erfasst, vgl. Bericht Verwaltungssanktionen, S. 16.

14 Anmerkung: Der Begriff der „pekuniären Verwaltungssanktion" wird im Bundesrecht der Schweiz nicht explizit verwendet, die Sacherlasse sprechen Verwaltungssanktion (z.B. Art. 100 und 109 Bundesgesetz über Geldspiele [BGS]), „verwaltungsrechtliche" Sanktion (Art. 23 Nationalbankgesetz [NBG]), oder von „administrative" Sanktion (Art. 122 Ausländer und Integrationsgesetz [AIG]).

15 Bericht Verwaltungssanktionen, S. 2.

16 Botschaft DSG, 7098.

17 Das Schweizerische Bundesgericht betont den abschreckenden wie vergeltenden Charakter des Art. 49 a KG, vgl. BGE 139 I 72, S. 79.

18 BGE 139 I 72 E. 2 – Publigroupe – (betreffend das Kartellrecht).

19 Das Bundesgericht spricht von einem strafrechtsähnlichen Charakter, vgl. BGE 139 I 72 S. 79.

b. Kartellsanktionen ohne sozial-ethischen Tadel

Im Hinblick auf den staatlichen Vorwurf sanktioniert die Verwaltungssanktion eine verwaltungsrechtliche Pflichtverletzung. Anders als die Strafe, setzt die Sanktion keine Schuld im Sinne einer individuellen Vorwerfbarkeit voraus (vgl. Art. 47 Abs. 1 S. 1 u. Abs. 2 StGB). Der Verwaltungssanktion soll im Gegensatz zur Strafe kein sittlich-ethischer oder moralischer staatlicher Tadel immanent sein. Zwar ist die subjektive Zurechenbarkeit zum Unternehmen (im Sinne der Vorwerfbarkeit) für das Bundesgericht und das Bundesverwaltungsgericht eine notwendige Voraussetzung für die kartellrechtliche Sanktionierung;[20] das strafgesetzliche Schuldprinzip und die allgemeinen Bestimmungen des Strafgesetzbuchs (vgl. Art. 47, Art. 333 Abs. 1 und 7 StGB) seien aber auf Kartellsanktionen nicht anwendbar.[21] Für die Vorwerfbarkeit und damit die Verantwortlichkeit für kartellrechtliche Zuwiderhandlungen des Unternehmens i.S.v. Art. 49a KG reicht der Nachweis eines Organmangels (sog. Organisationsverschulden, objektiver Sorgfaltsmangel) seitens des Unternehmens oder eines zurechenbaren Verhaltens eines Mitarbeiters aus.[22] Ein vorsätzliches Verhalten der natürlichen Person ist dabei nicht erforderlich.[23] Das Bundesgericht geht davon aus, dass „in aller Regel die objektive Sorgfaltspflicht verletzt ist", wenn ein „nachweisbares wettbewerbswidriges Verhalten" vorliegt.[24] Compliance Programme dienen insoweit nicht der Exkulpation, sondern können auf der Sanktionszumessungsebene sanktionsmindernd berücksichtigt werden.[25] Nach überwiegender Auffassung besteht darin kein Widerspruch zu den abwehrrechtlichen (Straf-)Verfahrensrechten im Kartellermittlungs-

20 BGE 143 II 297 E. 9.6.1 f., mit Verweis auf BGer 29. Juni 2012, 2C_484/2010 E. 12.2.1. f. (nicht publ. in: BGE 139 I 72) – Publigroupe; BGE 146 II 217 E. 8.5.2 – Swisscom ADSL; Urteil des Bundesverwaltungsgerichts („**BVGer**") B-7633/2009 vom 14. September 2015 E. 654 ff., 674 – Swisscom ADSL, bestätigt mit Urteil des BVGer B-581/2012 vom 16. September 2016 E. 8.2.2 – Nikon.

21 Urteil des BVGer B-7633/2009 vom 14. September 2015 E. 651 – Swisscom ADSL, bestätigt in BGE 146 II 217 E. 8.5.3 – Swisscom ADSL.

22 Bericht Verwaltungssanktionen, S. 40; vgl. BGer 4.2.2021, 2C_149/2018 E. 8.4. – Hors Liste Medikamente; ausführlich Urteil des BVGer vom 18.12.2018, B-831/2011E. 1488 ff. – SIX/DCC.

23 BGE 146 II 217 E. 8.5.2 – Swisscom ADSL; bestätigt in BGE 147 II 72 E. 8.4.2; Bericht Verwaltungssanktionen, S. 41.

24 BGE 146 II 217 E. 8.5.2 m.w.H. – Swisscom ADSL.

25 Bericht Verwaltungssanktionen, S. 41.

verfahren, da die Garantien der Konvention zum Schutze der Menschenrechte und Grundfreiheiten („**EMRK**") Anwendung finden.[26]

c. Kartellsanktionen von Wettbewerbsbehörden

Dass es sich bei Kartellverwaltungssanktionen nicht um Kriminalstrafen handeln soll, hat zur Folge, dass Verwaltungssanktionen nicht zwingend von einem Gericht zu verhängen sind. Während über eine „strafrechtliche Anklage" nach Art. 6 Abs. 1 S. 1 EMRK (vgl. Art. 30 Abs. 1 Bundesverfassung) zwingend ein unabhängiges und unparteiisches, auf Gesetz beruhendes Gericht zu entscheiden hat, werden Verwaltungssanktionen von Behörden wie der Schweizerischen Wettbewerbskommission („**WEKO**") oder der Europäischen Kommission verhängt. Ebenso obliegt die Durchführung des verwaltungsrechtlichen Kartellverfahrens den Wettbewerbsbehörden.

In der Schweiz und der Europäischen Union werden das Kartell*ermittlungs-* und das Kartell*sanktions*verfahren formell-institutionell getrennt geführt. Während die Ermittlung dem Sekretariat (Art. 23 Abs. 1 KG) bzw. der Generaldirektion Wettbewerb obliegen, entscheidet die Wettbewerbskommission (Art. 18 Abs. 3 KG) bzw. die Versammlung der Kommissare der Europäischen Union formell über die Kartellsanktion.

Die Sanktionierung von Kartellverstössen durch verwaltungsrechtliche Spezialbehörden hat Vor- und Nachteile. Der bereits überlasteten Staatsanwaltschaft fehlen oft die Ressourcen und das Know-how, um komplexe Wettbewerbsverstösse umfassend aufzuklären. Das flexiblere Verwaltungsverfahren erscheint hierzu besser geeignet als das starre und formale Strafverfahren. Eine Wettbewerbsbehörde kann zudem eher mit der allgemeinen Wirtschaftspolitik koordiniert werden, was einen gesamthaften und pragmatischeren Ansatz zur Wahrung öffentlicher Interessen ermöglicht.

---

26 Kartellrecht: Der EGMR hat im Urteil Menarini Diagnostics S.R.L. gegen Italien betreffend ein Kartellverfahren mit hohen Bussgeldern festgehalten, dass Artikel 6 EMRK grundsätzlich anwendbar ist. Das Bundesgericht ordnet die kartellrechtlichen Verwaltungssanktionen nach Artikel 49a KG ebenfalls dem Anwendungsbereich der strafprozessualen Garantien zu. (BGE 139 I 72 E. 2 – Publigroupe. Vgl. auch BGE 144 II 194 E. 5.1; 143 II 297, E. 9.1;
BGer 4.2.2021, 2C_149/2018 E. 8.2). Demnach haben kartellrechtliche Sanktionen nach Artikel 49a KG den Charakter einer strafrechtlichen Anklage im Sinn von Artikel 6 EMRK weshalb die entsprechenden Garantien von Artikel 6 und 7 EMRK und Artikel 32 der Bundesverfassung grundsätzlich anwendbar sind.

Auch im Verwaltungsverfahren sind die „strafrechtlichen" Verfahrensrechte der Unternehmen gewahrt, denen nach einer Sanktion zudem der Rechtsweg offensteht, was die Überprüfung der Einhaltung der Europäischen Menschenrechtskonvention durch die Wettbewerbsbehörden sicherstellen soll.[27]

In der Praxis bestehen zum Teil jedoch Zweifel daran, ob das Wettbewerbsverfahren tatsächlich konventionskonform umgesetzt wird. Kritisiert wird dabei insbesondere der Umfang der Geltung der strafrechtlichen Verfahrensrechte sowie die unzureichende – rein formale – Trennung zwischen Kartellermittlungs- und Kartellsanktionsbehörde. Nicht zuletzt kritisieren Praktiker teilweise die zu zurückhaltende gerichtliche Nachprüfung der Entscheidungen der Kartellbehörden sowie den zu weitreichenden Ermessenspielraum, den die Gerichte den Kartellbehörden einräumen.[28].

d. Strafrechtliche Verfahrensrechte

Zuletzt unterscheidet sich die Verwaltungssanktion im Geltungsumfang strafrechtlicher Verfahrensrechte. Während die Verfahrensrechte im Rahmen kriminalstrafrechtlicher Verfahren grundsätzlich vollständig zur Anwendung kommen, gilt dies nicht für die lediglich im weiteren Sinne strafrechtlichen Sanktionsverfahren nach Art. 6 Abs. 1 EMRK, zu denen nach überwiegender Ansicht auch Verwaltungssanktionsverfahren zählen. Dort kommen die strafrechtlichen Verfahrensrechte soweit die „Engel-Kriterien" der EMRK erfüllt sind zwar grundsätzlich zur Anwendung;[29] sie gelten jedoch „nicht notwendigerweise im vollem Umfang".[30]

---

27 EGMR, A. Menarini Diagnostics S.R.L. c. Italie, 43509/08, 27.11.2011, § 67.

28 BGE 139 II 185 E. 9.3; vgl. Jany, Legtimationsdefizite, S. 39ff.

29 EGMR, Urt. v. 8.6.1976 – Engel u.a. v. Niederlande – Rn. 82ff. Die Anwendbarkeit der strafrechtlichen Garantien des Art. 6 EMRK hängt von den drei Engel-Kriterien ab: 1. Die Zuordnung der Tat nach nationalem Recht 2. Die Natur des Vergehens und 3. Die Art und Schwere der Sanktion; vgl. Jany, Legitimationsdefizite, S. 186ff.

30 EGMR, Urt. v. 23.11.2006 – Jussila v. Finland – Rn. 43: „the criminal-head guarantees will not necessarily apply with their full stringency". Der EGMR hat mit diesem Urteil das Strafrecht in einen „engeren" und „weiteren" Bereich Fragmentiert. Das Kartellverfahren und die Kartellsanktion werden ihrer Rechtsnatur nach überwiegend dem Strafrecht im weiteren Sinne zugeordnet. Die Kartellsanktion ist daher eine „strafrechtliche Anklage" iSd. Art. 6 Abs. 1 EMRK. Gleichwohl finden strafrechtliche Verfahrensrechte nicht notwendig vollständige Anwendung. Der EuGH hat sich dieser Rechtsprechungslinie angeschlossen. Erstmals für das Recht eines Unternehmens,

Die Anwendung der strafrechtlichen Verfahrensgarantien des Art. 6 EMRK hängt davon ab, ob es sich bei der Kartellsanktion bzw. dem Kartellverfahren um eine „strafrechtliche Anklage" handelt. Eine „Anklage" („charge", „accusation pénale") liegt vor, wenn eine offizielle Benachrichtigung einer staatlichen Behörde vorliegt, in der diese behauptet, dass eine Straftat begangen wurde (*formelle* Anklage).[31] Es genügt auch eine *materielle* Anklage, die auch in jeder anderen Massnahme zu erblicken ist, die implizit eine solche Behauptung enthält und die Situation des beschuldigten Unternehmens gleichermassen beeinträchtigt.[32]

Ob die Mitteilung der Beschwerdepunkte auch eine „strafrechtliche" Anklage ist, bestimmt sich nach den Engel-Kriterien. Der EGMR prüft, ob 1. nach der Selbsteinordnung des nationalen Rechts der Vertragsparteien, 2. der Art der Zuwiderhandlung oder 3. der Schwere der abstrakten Sanktion eine Zuordnung der Sanktion zum Strafrecht erforderlich ist.[33] Auch wenn die EU und die nationalen Vertragsstaaten die Kartellsanktion nicht als „Strafe" einordnen, ist überwiegend anerkannt, dass Kartellsanktionen die anderen Engel-Kriterien erfüllen und damit die Verfahrensgarantien des Art. 6 EMRK grundsätzlich Anwendung finden.[34]

Aufgrund der Weite dieser Rechtsprechung haben EGMR und EuGH diese später teilweise relativiert. Mit der Jussila-Entscheidung unterscheidet der EGMR das Strafrecht im engeren und weiteren Sinne und macht deutlich, dass Strafsanktionen im weiteren Sinne – wozu er auch das Kartellrecht zählt – nicht notwendigerweise vollständig zur Anwendung kommen müssen.[35] Was dies im Einzelfall für die Anwendbarkeit von strafrechtlichen Verfahrensrechten bedeuten soll, lässt der EGMR jedoch offen.[36] Faktisch können sich Unternehmen im Kartellermittlungsverfahren

---

die Aussage zu verweigern, EuGH, Urt. v. 18.10.2989 – Orkem – EU:C:1989:387, Rn. 34, vgl. auch EuGH, Urt. v. 2.2.2021 – Consob – EU:C:2021:84, Rn. 43 für den Unterschied auch zu natürlichen Personen, Rn. 46.

31 EGMR, Urt. v. 27.02.1980 – Deweer/Belgien – Nr. 6903/75, Rn. 46: „official notification given to an individual by the competent authority of an allegation that he has committed a criminal offence".

32 EGMR, Urt. v. 21.02.1984 – Öztürk/Deutschland – Nr. 8544/79, Rn. 55.

33 EGMR, Urt. v. 8.6.1976 – Engel u.a. v. Niederlande – Rn. 82ff.

34 EGMR, Urt. v. 27.11.2011 – Menarini v. Italien – Rn. 44, vgl. auch Bericht Verwaltungssanktionen, S. 28.

35 EGMR, Urt. v. 23.11.2006 – Jussila v. Finnland – Rn. 43.

36 Dies bemängelt auch Richter Loucaides in seimem Sondervotum: EGMR, U. v. 23.11.2006 – Jussila/Finnland – Nr. 73053/01; „I find it difficult, in the context of a fair trial, to distinguish, as the majority do in this case, between criminal offences be-

aber z.B. nicht auf das Recht zu Schweigen berufen und auch der Öffentlichkeitsgrundsatz, die gerichtliche Kontrolle der Entscheidungen oder die Unschuldsvermutung sind nicht eindeutig in vollem Umfang kriminalstrafrechtlich ausgestaltet.

e. Faktische Pönalisierung

Brisanz erfährt diese Rechtsprechung vor dem Hintergrund, dass der zu Beginn des Aufsatzes dargestellte Kriminalisierungstrend auch vor dem Kartellrecht nicht Halt macht; dort jedoch mit divergierenden Stossrichtungen.

Einerseits beklagen Unternehmen seit Jahrzehnten zunehmend höhere Kartellsanktionen. Kartellsanktionen in Milliardenhöhe seien faktisch keine Verwaltungssanktionen sondern Kriminalstrafen.[37] Begründet wird dies mit den stetig steigenden Kartellbussen, ohne, dass es zu einer gesetzlichen Anpassung der Ermächtigungsgrundlage zur Verhängung von Kartellsanktionen gekommen wäre (sog. faktische Pönalisierung).[38] Derartig hohe Sanktionen, die zudem noch öffentlich publiziert werden, seien nicht mehr mit den üblichen Ordnungswidrigkeiten vergleichbar und zudem mit einem staatlichen sittlich-ethischen Tadel behaftet. Dies führe dazu, dass es sich bei den Kartellsanktionen zwar nicht formell aber doch materiell um Kriminalstrafen handle.

Andererseits wird eine Kriminalisierung insbesondere von hard-core Kartellsanktionen diskutiert, also die Kriminalisierung besonders schwerwiegender Verstösse gegen das Kartellrecht wie Preisabsprachen oder Marktaufteilungen.[39] Vorbild ist der US-amerikanische Sherman Act, der

---

longing to the ‚hard core of criminal law' and others which fall outside that category. Where does one draw the line?".

37 Die Europäische Kommission hatte Google für einen Verstoß gegen das EU-Kartellrecht eine Geldbusse in Höhe von 4.34 Milliarden Euro auferlegt. Google hatte laut der Kommission Herstellern von Android-Geräten und Betreibern von Mobilfunknetzen seit 2011 rechtswidrige Einschränkungen auferlegt, um seine beherrschende Stellung auf dem Markt für allgemeine Internet-Suchdienste zu festigen, vgl. https://ec.europa.eu/commission/presscorner/detail/de/ip_18_4581 (zuletzt abgerufen am 22.05.2025).

38 Vgl. Bericht der Europäischen Kommission über die Verhängung von Kartellbussen, abrufbar unter: https://competition-policy.ec.europa.eu/antitrust-and-cartels/cartels-cases-and-statistics_en / (zuletzt besucht am 22.05.2025).

39 Bericht Einführung von Strafsanktionen gegen natürliche Personen im Kartellrecht.

bei Kartellverstössen auch kriminalstrafrechtliche Sanktionen wie Gefängnisstrafen für natürliche Personen vorsieht. Eine in Europa bislang nicht vorgesehene strafrechtliche Verantwortlichkeit nicht des Unternehmens, sondern der für das Unternehmen handelnden natürlichen Personen, wird teilweise als erforderlich angesehen, um dem Kartellrecht zu einer besseren Wirksamkeit zu verhelfen. Andernfalls komme der Kartellsanktion auch aufgrund der nur geringen Aufdeckungswahrscheinlichkeit von ca. 20–30 %[40] keine hinreichend abschreckende Wirkung zu.[41]

f. Spill-over-Effekt für die Digitalwirtschaft

Vor dem Hintergrund der Funktion der Kartellsanktion als Prototyp der Verwaltungssanktionen, drohen diese Unsicherheiten, wie etwa der genaue Umfang der Anwendung strafrechtlicher Verfahrensrechte, auf neue Rechtsbereiche der Digitalwirtschaft übertragen zu werden (Spill-over-Effekt).

So sieht der DMA etwa für Zuwiderhandlungen nicht nur Geldbussen i. H. v. 10 % des weltweiten jährlichen Geschäftsumsatzes analog der Kartellbusse vor (Art. 30 Abs. 1 DMA), sondern – im Wiederholungsfall innerhalb von acht Jahren nach einer Entscheidung – sogar bis zu 20 % (Art. 30 Abs. 2 DMA). Damit nähert sich die Verwaltungsbusse noch mehr dem Strafverfahren an, sodass sich die Frage stellt, ob es sich hierbei um eine kriminalstrafrechtliche Sanktion handelt.

Auch der DSA sieht Geldbussen für die Nichteinhaltung einer in der Verordnung festgelegten Verpflichtung vor (Art. 52 Abs. 3 DSA), die allerdings höchstens 6 % des weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahres betragen.

Es bleibt abzuwarten, wie sich die Übertragung des Verwaltungssanktionsmodells auf die Digitalwirtschaft auswirken wird. Es ist zu hoffen, dass der Spill-over-effekt nicht nur die dargestellten Unklarheiten des Sanktionsmodells in das digitale Zeitalter überträgt, sondern dass die Digitalwirtschaft innovative Impulse für eine Modernisierung des Verwaltungssanktionsmodells generiert.

---

40 Wagner von Papp, WUW 60/2010, S. 268, S. 271; MüKo-EUWettbR- Engelsing/Schneider, Art. 23 VO 1/2003, Rn. 13 f.; Wils, Concurrences 2006, S. 1, 12.

41 Bericht Verwaltungssanktionen, S. 17 m.H. auf: Botschaft steuerliche Behandlung finanzieller Sanktionen, 8514; Bericht zur Reform der lebenslangen Freiheitsstrafe, S. 12 m.w.H.

3. Das verwaltungsstrafrechtliche Modell

a. Zum neuen DSG

Das totalrevidierte DSG bezweckt, die Vereinbarkeit mit dem europäischen Recht sicherzustellen und ermöglicht, die modernisierte Datenschutzkonvention 108 des Europarats zu ratifizieren. Dies ist für den Wirtschaftsstandort Schweiz wesentlich, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch in Zukunft ohne zusätzliche Anforderungen möglich bleibt.[42] Im Folgenden betrachten wir insbesondere die Strafbestimmungen in Art. 60 ff. DSG.

Zwar hatte bereits das alte Datenschutzgesetz vom 19. Juni 1992 („**aDSG**") gewisse Strafbestimmungen in Art. 34 und 35 vorgesehen. Die Tatbestände waren jedoch sehr eng formuliert, sodass nur sehr wenige Verstösse gegen das aDSG überhaupt erst potentiell erfasst waren. Da es sich zudem lediglich um Antragsdelikte handelte und einzig Vorsatz strafbar war, waren die Voraussetzungen für eine Strafverfolgung so hoch, dass in den meisten Jahren schweizweit nur eine einstellige Anzahl Strafverfahren geführt wurde.[43] Auch die abschreckende Wirkung von Bussen von maximal CHF 10'000 dürfte im Wirtschaftsbereich beschränkt geblieben sein. In der Literatur wurde das strafrechtliche Regime denn auch als „eher lasch" bezeichnet.[44]

Das totalrevidierte DSG stellt demgegenüber Verstösse gegen die meisten Pflichten unter Strafe: Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 60 DSG), Verletzung von Sorgfaltspflichten (Art. 61 DSG), Verletzung der beruflichen Schweigepflicht (Art. 62 DSG) und Missachten von Verfügungen (Art. 63 DSG). Zudem sind neu deutlich höhere Bussen von bis zu CHF 250'000 bei fehlbaren Personen möglich. Ebenfalls können Unternehmen bei Widerhandlungen in Geschäftsbetrieben in Anlehnung an Art. 7 des Verwaltungsstrafrechtsgesetzes – aber mit der

42 Kneifl, SJZ 118/2022. S. 1108, Die EU anerkennt das Datenschutzniveau der Schweiz seit dem Jahr 2000.

43 Bundesamt für Statistik, Polizeiliche Kriminalstatistik 2009–2012; BSK aDSG-Niggli/Maeder, Art. 34 N 4.

44 BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 5.

deutlich erhöhten Maximalbusse von CHF 50'000 – direkt sanktioniert werden.[45]

Nicht verändert hat sich demgegenüber, dass alle Delikte Antragsdelikte und nur deren vorsätzliche Begehung strafbar sind. Dies war im Vorentwurf des Bundesrates noch anders, wonach auch für fahrlässige Begehung Busse bis zu CHF 250'000 und für vorsätzliche Begehung Busse bis zu CHF 500'000 vorgesehen war.

Nach Auffassung des Bundesrates ist damit sowohl den „abschreckenden Sanktionen" nach Art. 10 des Datenschutzübereinkommens (SEV) 108 und Art. 57 der Schengen-relevanten Richtlinie (EU) 2016/680[46] als auch den Anforderungen für die Äquivalenzanerkennung nach der DSGVO Genüge getan.[47] Letzteres wurde durch die erneute Äquivalenzanerkennung durch die Europäische Kommission Anfangs 2024 bestätigt.[48]

b. Die Wahl der Verwaltungsstrafen im DSG

Wie bereits erwähnt, ist das verwaltungsstrafrechtliche Modell in der Schweiz die Norm zur Durchsetzung des Wirtschaftsrechts und Verwaltungssanktionen wurden nur punktuell eingeführt, namentlich im Kartellrecht.[49]

Entsprechend ist es nicht weiter erstaunlich, dass der Bundesrat das verwaltungsstrafrechtliche Modell auch bei der Revision des DSG vorgeschlagen hat. Nach Ansicht des Bundesrats wäre es „*nicht angemessen*", dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten („**EDÖB**") die Befugnis einzuräumen, Verwaltungssanktionen zu verhängen. Diese in anderen Ländern bestehende Möglichkeit widerspricht nach Meinung des Bundesrates der schweizerischen Rechtstradition.[50] Mit anderen Worten argumentiert der Bundesrat im Wesentlichen, dass man sich in der Vergangenheit mehrheitlich mit Verwaltungsstrafen beholfen hat und er am bisherigen Modell festhalten möchte.

45 BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 7.
46 Botschaft DSG, 7099.
47 BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 5; Botschaft DSG, 7100.
48 Vgl. Medienmitteilung des Bundesamt für Justiz vom 20.02.2024: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/angemessenheit-ch.html (zuletzt abgerufen am 22.5.2025).
49 Bericht Verwaltungssanktionen, S. 2; siehe hierzu auch Ziff. 2 oben.
50 Bericht Vorentwurf DSG, S. 15.

Als weiteres Argument führte der Bundesrat im Bericht zum Vernehmlassungsentwurf immerhin noch an, dass es vorteilhafter sei, Zuwiderhandlungen im Strafverfahren mit seinen strafprozessualen Garantien zu ahnden. Zudem hätte die Organisation des EDÖB erheblich angepasst und ausgebaut werden müssen, um die Verfahrensgarantien wahren zu können, was erhebliche Kosten verursacht hätte.[51] Gleichzeitig scheint der Bundesrat an der Wirksamkeit seines eigenen Konzept in der Durchsetzung zu zweifeln und bezeichnet es als Alternative zu den Verwaltungssanktionen gerade einmal als „*wirksam genug*".[52]

In der Vernehmlassung wurde der Ansatz des Bundesrates von „*sehr vielen*" Teilnehmern kritisiert, die mehrheitlich Verwaltungssanktionen analog der DSGVO forderten. Vorgebracht wurde hierzu insbesondere, dass die strafrechtlichen Sanktionen in erster Linie auf natürliche Personen ausgerichtet seien, während die Unternehmen, die vom DSG als Verantwortliche bzw. Beauftragte erfasst werden, dafür auch direkt strafbar sein müssten. Zudem wurde die mangelnde Kompatibilität mit dem EU-Recht kritisiert. Insbesondere von den Kantonen wurde zudem vorgebracht, dass die Staatsanwaltschaften zusätzliche Kompetenzen mit spezialisierten Mitarbeitern aufbauen müssten und ein schweizweit einheitlicher Vollzug erschwert werde.[53]

Nichtsdestotrotz hielt der Bundesrat in der Vernehmlassungsvorlage unverändert an seinem Konzept fest. Dabei verwies er im Wesentlichen auf dieselben Argumente wie bereits im Bericht zum Vorentwurf und betonte noch stärker das Argument der Verfahrensgarantien, namentlich auch aufgrund des Fehlens eines kodifizierten Prozessrechts für Verwaltungssanktionen mit pönalem Charakter. Während das Konzept unverändert blieb, wurden freilich die Maximalbussen halbiert und die fahrlässige Strafbarkeit gestrichen, was die Abschreckungswirkung, namentlich im Vergleich zur DSGVO, weiter reduzierte.[54]

Im Parlament führte das Sanktionskonzept erneut zu Diskussionen. Das Parlament hat sich letztlich zwar für den vom Bundesrat vorgeschlagenen verwaltungsstrafrechtlichen Weg entschieden[55], gleichzeitig aber den Bun-

51 Bericht Vorentwurf DSG, S. 83.
52 Bericht Vorentwurf DSG, S. 15.
53 Ergebnisbericht Vernehmlassung DSG, S. 50 f.
54 Botschaft DSG, 6973 f., 7098 f.
55 Vgl. Medienmitteilung der Staatspolitischen Kommission des Nationalrats („**SPK-N**") vom 16.08.2019: https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx (zuletzt abgerufen am 22.5.2025).

desrat beauftragt aufzuzeigen, wie ein allgemeines System von pekuniären Verwaltungssanktionen einschliesslich der erforderlichen Verfahrensgarantien im Schweizer Recht eingeführt werden könnte.[56] In diesem Zusammenhang sollte dann noch einmal geprüft werden, inwiefern für Zuwiderhandlungen gegen das DSG allenfalls doch pekuniäre Verwaltungssanktionen einzuführen seien.[57]

Der daraufhin vom Bundesrat veröffentlichte Bericht vom 23. Februar 2022 inventarisiert den aktuellen Bestand an pekuniären Verwaltungssanktionen im Schweizer Recht und analysiert die anwendbaren Garantien einschliesslich unter dem übergeordneten Recht detailliert.[58] Dieser stellt somit die Grundlage für eine etwaige künftige Einführung pekuniärer Verwaltungssanktionen im DSG dar, was in Lehre und Praxis weiterhin teilweise gefordert wird.[59] Der Bundesrat hat auf Grundlage des Berichts allerdings beschlossen, dass er derzeit keinen solchen Anpassungsbedarf im Schweizer Recht sieht.

c. Praktische Überlegungen zu den Verwaltungsstrafen im DSG

Vor diesem Hintergrund möchten wir nun ausgewählte praktische Auswirkungen der Wahl der Verwaltungssanktionen im DSG beleuchten, insbesondere mit Blick auf die Digitalwirtschaft.

i. Verfahrensgarantien

Wie bereits ausgeführt, liegt ein grosser Vorteil der Verwaltungsstrafen in der Wahrung der Verfahrensgarantien. Wie der Bundesrat in seinem Bericht von 2022 detailliert ausführt, sind diese für das Strafverfahren im Strafprozessrecht und in der zahlreichen Rechtsprechung abgesichert, während für das Verwaltungsverfahren mit pönalem Charakter kein eigent-

56 Postulat Nr. 18.4100 der SPK-N vom 01.11.2018: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184100 (zuletzt abgerufen am 22.5.2025).

57 Vgl. Medienmitteilung der SPK-N vom 16.08.2019: https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx (zuletzt abgerufen am 22.5.2025); Untersuchung EDÖB zu Art. 51 DSG N 1.

58 Vgl. Bericht Verwaltungssanktionen.

59 BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 19 f.; Untersuchung EDÖB zu Art. 51 DSG N 1.

liches kodifiziertes Prozessrecht existiert und sich die Rechtsprechung im Wesentlichen auf das Kartellgesetz beschränkt.[60] Gerade aus Sicht der Rechtsunterworfenen und letztlich auch für die Akzeptanz der Entscheide ist dies in einem Rechtsstaat entscheidend.

Auch in praktischer Hinsicht ist zudem zu berücksichtigen, dass die Einhaltung der strafprozessualen Garantien für die Strafbehörden zum Kern ihrer Tätigkeit, quasi zum „daily business" gehört. Demgegenüber sind Fachbehörden primär im Verwaltungsverfahren ohne pönalen Charakter, d.h. ohne entsprechende Anwendung strafprozessualer Garantien, unterwegs. Wie auch der Bundesrat für den EDÖB ausgeführt hat, müssten die entsprechenden Fähigkeiten und Kapazitäten unter entsprechenden Kostenfolgen erst aufgebaut werden.[61] Hinzu kommt noch die praktische Schwierigkeit, dass Verfahren mit und ohne pönalen Charakter strikt getrennt behandelt werden müssen, was im Verfahrensalltag durchaus Schwierigkeiten bereiten kann.

ii. Fachkompetenz & Spezialwissen

Geradezu umgekehrt zu den Verfahrensgarantien verhält es sich bei der Fachkompetenz und dem fachspezifischen Spezialwissen der Behörden. Hier sind Fachbehörden wie der EDÖB klar im Vorteil: Sie können ihre Fachkompetenz über alle Verfahren hinweg akkumulieren und ausspielen und sind so besser gerüstet, auch komplexe Sachverhalte der Digitalwirtschaft zu erfassen und korrekt zu beurteilen. Demgegenüber müssen diese Kompetenzen bei den Staatsanwaltschaften mit dem Inkrafttreten des DSG erst aufgebaut werden. Dass diese Kompetenzen kantonal aufgebaut werden müssen, erschwert dies zusätzlich – was denn auch einer der wesentlichen Kritikpunkte der Kantone in der Vernehmlassung war.[62]

Auch ist in praktischer Hinsicht fraglich, welche Bedeutung die kantonalen Staatsanwaltschaften den weiterhin nicht besonders zahlreichen Verfahren nach DSG im Verhältnis zu den jährlich über 38'000 Urteilen nach StGB und gar über 52'000 Urteilen nach Strassenverkehrsgesetz (SVG)[63] beimessen werden. Wenig ermutigend in dieser Hinsicht ist, dass viele Kan-

60 Bericht Verwaltungssanktionen, S. 113.
61 Botschaft DSG, 7099.
62 Botschaft DSG, 6977.
63 https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/strafjustiz.html (zuletzt abgerufen am 22.5.2025).

tone alle Bussenverfahren unabhängig von der Höhe der etwaigen Busse regelmässig an Sachbearbeiter delegieren, d.h. die DSG-Verfahren gar nicht erst durch Staatsanwälte beurteilt werden.[64]

Vor diesem Hintergrund erschiene es nach hier vertretener Auffassung sinnvoller, die Fachkompetenz zur Verfolgung von Zuwiderhandlungen gegen das DSG zentralisiert in einer Behörde aufzubauen, anstatt dies in 26 Kantonen zu tun. In einem Umfeld, wo sich neue Technologien und die Möglichkeiten der Bearbeitung von Personendaten rasend schnell entwickeln, derzeit z.B. unter dem Stichwort künstliche Intelligenz, dürfte dies auch die Nachteile überwiegen, dass wie dargelegt in dieser Behörde parallel die entsprechenden Kompetenzen im Bereich der Verfahrensabläufe aufgebaut werden müssten.

iii. Abschreckungswirkung

Schwierig zu beurteilen ist die abschreckende Wirkung von Sanktionen, obwohl gerade diese z.B. vom europäischen Datenschutzrecht ausdrücklich verlangt wird. Der Bundesrat weist in seinem Bericht von 2022 gar darauf hin, dass der Nachweis der abschreckenden Wirkung von Strafbestimmungen bis heute nicht erbracht sei.[65] Die strafrechtliche Literatur geht teilweise so weit zu sagen, dass es „als erwiesen gelte, dass härtere Strafen nicht zu weniger Kriminalität führen".[66] Demgegenüber dürfte die Wahrscheinlichkeit, dass es überhaupt zu einem Strafverfahren kommt, das heisst das vermutete Entdeckungsrisiko, mehr zur Prävention beitragen.[67] Zur Abschreckung sind daher sowohl die Wahrscheinlichkeit überhaupt bestraft zu werden, als auch die Höhe der potentiellen Strafe anzuschauen.

64 Vgl. anstatt vieler Art. 13 des Einführungsgesetzes zur Schweizerischen Straf- und Jugendstrafprozessordnung (EG-STPO) des Kantons St. Gallen.

65 Bericht Verwaltungssanktionen, S. 17 und Fn. 41.

66 BSK StGB-Wiprächtiger/Keller, Art. 47 N 82, 82c, m.H. auf: Niggli/Maeder, AJP 04/2011, S. 443, 448; Wiprächtiger, Anwaltsrevue 11/12I2014, S. 477, 483; Wiprächtiger/Spahni, Schnellfahren und Strafzumessung, S. 12, 19; Wiprächtiger/Spahni, forumpoenale 1/2017, S. 60 f.; s. dazu auch Alder, Diss., S. 25 ff. m. w. Hinw.; vgl. ferner das Votum Nationalrat Fluri, Amtliches Bulletin Nationalrat 2009, 1002: «Generell möchten wir aber davor warnen, sich der Illusion hinzugeben, dass härtere Strafen zu weniger Kriminalität führen. Diese Meinung ist empirisch ganz klar widerlegt».

67 Jositsch /Ege/Schwarzenegger, S 1, 18.

Die Wahrscheinlichkeit, für eine Zuwiderhandlung bestraft zu werden, setzt sich aus verschiedenen Faktoren zusammen, z.B. Fachkompetenz und Ressourcen der zuständigen Behörde, dem anwendbaren Prozessrecht etc., wobei wir namentlich die Fachkompetenz der zuständigen Behörde bereits analysiert haben. An dieser Stelle sei daher insbesondere noch auf die Frage des Verschuldens hingewiesen: Während Verwaltungssanktionen grundsätzlich verschuldensunabhängig sind und nach der Rechtsprechung eine blosse Vorwerfbarkeit genügt, ist für Verwaltungsstrafen immer ein Verschulden im Sinne des Strafrechts erforderlich. In der Folge ist die Hürde für eine Sanktion im Verwaltungsstrafrecht erheblich höher, zumal die Zurechenbarkeit der Verantwortlichkeit im Innenverhältnis in einem Unternehmenskontext, v.a. grossen, internationalen Unternehmen, erheblich erschwert ist.[68] Durch den Verzicht auf die Strafbarkeit der fahrlässigen Begehung im DSG nach der Vernehmlassung, wurde dabei innerhalb des Rahmens der Verwaltungsstrafen die Hürde für die Strafverfolgung noch einmal angehoben. Praktisch dürfte sich die Strafbarkeit nach DSG somit in einem sehr engen Rahmen bewegen. Gerade in grossen Organisationen mit teilweise unklaren Verantwortlichkeiten – bewusst oder unbewusst – dürfte es so kaum je gelingen, ein Verschulden im Sinne des Strafrechts nach strafprozessualen Grundsätzen nachweisen zu können. Die Fallzahlen unter den Straftatbeständen des aDSG blieben denn auch verschwindend gering[69] und unter Berücksichtigung aller Faktoren dürften diese unter dem neuen DSG auf niedrigem Niveau bleiben.[70] Dieüberaus hohe Hürde für eine Verurteilung wird auch von den ersten Gerichtsentscheiden unter dem neuen DSG gestützt, wobei auch die mangelnde Klarheit der Strafnormen als eine weitere Hürde bemängelt wird.[71] Die Aufklärungswahrscheinlichkeit dürfte somit noch einmal deutlich unter den für das Kartellrecht geschätzten 20–30 % liegen.

Das zweite Faktor ist, wie erwähnt, die Höhe der in Frage stehenden Busse. Diese erscheinen unter dem DSG mit maximal CHF 250 000 gegenüber der DSGVO mit Bussen bis zu € 20 Mio. bzw. im Fall eines Unternehmens bis zu 4 % des weltweiten Jahresumsatzes geradezu gering.[72] Während

68 Bericht Verwaltungssanktionen, Ziff. 4.3 ff. (S. 37 ff).
69 BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 9.
70 vgl. Rosenthal/Gubler, SZW/RSDA 01/2021, S. 52, 59; Rosenthal, Jusletter 11/ 2020, S. 70; BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG N 9.
71 Vgl. https://datenrecht.ch/cour-de-justice-ge-strafbarkeit-wegen-verletzung-der-datensicherheit-maximal-bei-offensichtlichen-faellen/.
72 Vgl. BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 15.

sich die strafrechtlichen Bussen nach DSG, unter Vorbehalt der sehr eingeschränkten Unternehmensstrafbarkeit, gegen die verantwortliche natürliche Person richten, zielen die verwaltungsrechtlichen Bussen unter der DSGVO auf das Unternehmen.[73] Teilweise wird in dieser Hinsicht eine höhere Abschreckungswirkung vermutet, da die (potentielle) Strafe direkt die natürliche Person trifft, einschliesslich Eintrag im Strafregister.[74] Ebenfalls wird darauf verwiesen, dass Bussen, gerade auch im Bereich Datenschutz, nach ständiger Rechtsprechung des Bundesgerichts höchstpersönlicher Natur sind und daher im Grundsatz weder vom Unternehmen übernommen noch versichert werden können, sodass sich ihre Abschreckungswirkung voll entfalte.[75]

Selbst wenn der präventive Charakter persönlicher Sanktionen höher sein mag, dürfte das Element der schwierigen Zurechenbarkeit und der daraus resultierenden erschwerten Verfolgbarkeit in den meisten Fällen – jedenfalls in grossen, internationalen Organisationen – überwiegen. Hinzu kommt, dass der rationale Verwaltungsrat oder CEO für nicht versicherbare Risiken eine höhere Risikoprämie – sprich Lohn – fordern müsste, was den präventiven Charakter von persönlichen pekuniären Sanktionen weiter in Frage stellt. Ohnehin stellt sich die grundsätzliche Frage, ob für Zuwiderhandlungen gegen auf Unternehmen anwendbare Regeln die regelmässig durch Gremien und Hierarchien und nicht durch einzelne verantwortliche Personen handeln, persönliche Sanktionen überhaupt der richtige Anknüpfungspunkt sind.

4. Schlussfolgerungen

Die Schweiz setzt für die Durchsetzung ihrer wirtschaftsrechtlichen Vorschriften – das Kartellrecht ausgenommen – grossmehrheitlich auf Verwaltungsstrafen. Die Vorteile liegen dabei klar auf der Hand: Das strafprozessuale Verfahren ist bekannt und erprobt und die Einhaltung der Verfahrensgarantien ist organisatorisch wie rechtlich sichergestellt. Ebenso klar sind aber die Nachteile: Für die Strafbehörden, die heute oft ausgelastet

73 BSK DSG-Mathys/Thomann, Vor Art. 60–66 DSG, N 14; Rosenthal/Gubler, SZW/RSDA 01/2021 S. 53.

74 Jedenfalls wenn die Busse CHF 5000 überschreitet, Art. 18 Abs. 1 lit. c Strafregistergesetz (StReG).

75 BSK DSG-Kunz, Art. 64 N 68; BGE 86 II 71; 134 III 59 E. 2.3.2; 115 II 72 E. 3b. Vgl. auch Mathys.

oder gar überlastet sind, sind die Fragestellungen komplexer Wirtschaftssachverhalte schwer zu bewältigen, was letztlich zu einer niedrigeren Entdeckungswahrscheinlichkeit führt, zumal die entsprechenden Fähigkeiten und Ressourcen noch kantonal aufgebaut werden müssen. Hinzu kommt die Schwierigkeit der Zurechenbarkeit, vor allem in komplexen, internationalen Organisationen, und damit die hohe Hürde bei der Beweisführung betreffend Vorsatz.

Die Nachteile manifestieren sich besonders im Datenschutzrecht, wo die kantonalen Staatsanwaltschaften Mühe bekunden die komplexen technischen Fragestellungen der Digitalwirtschaft, auch z.B. durch neue Technologien wie künstlicher Intelligenz, zu bewältigen. Ebenso stellt sich hier die Frage der Zurechenbarkeit in Anbetracht globaler Technologieunternehmen und zunehmend autonomer Systeme in zugespitzter Form. Die bloss unbesehene Übertragung des Verwaltungssanktionsmodells nach dem Vorbild des Schweizer oder EU Kartellrechts auf die Digitalwirtschaft (etwa den DMS oder DSA) riskiert die dogmatischen Unzulänglichkeiten des Modells als Altlast in das digitale Zeitalter zu übertragen.

Vor diesem Hintergrund ist auch interessant, dass die Diskussionen im Kartell- und im Datenschutzrecht teilweise in entgegengesetzte Richtungen laufen: Während im Kartellrecht zum Teil gefordert wird, zusätzlich auch ein strafrechtliches Element einzubauen, wird im Schweizer Datenschutzrecht gefordert, dem EDÖB die Kompetenz zu Verwaltungssanktionen zu erteilen. Dabei wird mit oft mit demselben Argument, der Abschreckungswirkung, gearbeitet, wobei im Datenschutzrecht auch weitere Argumente wie internationale Kompatibilität und Spezialwissen der Behörde eine Rolle spielen.

Die derzeit wohl interessanteste Debatte zur Einführung von Verwaltungssanktionen in der Schweiz findet jedoch im Finanzmarktrecht statt: Mit dem Zusammenbruch der Credit Suisse stellt sich der Schweizer Gesetzgeber einmal mehr die Frage, ob für die eidgenössische Finanzmarktaufsicht („**FINMA**") Verwaltungssanktionen eingeführt werden sollen. Bislang hatte der Gesetzgeber dies, analog zum Datenschutzrecht, immer wieder abgelehnt.[76] Ein von den Behörden bestelltes Rechtsgutachten empfiehlt die Einführung von Verwaltungssanktionen in Analogie zum Kartell-

76 Siehe z.B. das Postulat Nr. 13.4106 vom 09.12.2013, eingereicht von alt Ständerat Markus Stalder: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134106 (zuletzt abgerufen am 22.5.2025).

recht.[77] Die politische Debatte ist derzeit noch im vollen Gange, aber in Anbetracht des öffentliches Druckes auf der too-big-too-fail Problematik im Nachgang zum Untergang der Credit Suisse, dürften die Befürworter von Verwaltungssanktionen gute Chancen haben. Der Bundesrat hat denn auch kürzlich eine entsprechende Motion zur Annahme empfohlen[78], welche in der Folge auch vom Parlament angenommen wurde.

Im Rahmen der Arbeiten zur Einführung von Verwaltungssanktionen im Finanzmarktrecht sind die Fragen zum Verfahren und den entsprechenden Verfahrensgarantien zu klären. Damit wäre dann die Grundlage geschaffen, Verwaltungssanktionen auch in anderen Rechtsgebieten, namentlich im Datenschutzrecht, einzuführen, zumal wohl auch nicht mehr mit ihrer fehlenden Verbreitung im Schweizer Recht argumentiert werden könnte. Es scheint daher wahrscheinlich, dass eine etwaige Einführung von Verwaltungssanktionen im Finanzmarktrecht mittelfristig die Diskussion im Datenschutzrecht erneut aufbringt. Damit stellen sich dann aber neue bzw. alte Fragen: Treten Verwaltungssanktionen zu den Strafbestimmungen hinzu oder ersetzen sie diese? Wird dadurch auch die Diskussion um die Kumulation von Verwaltungssanktionen und Verwaltungsstrafen angeheizt? Die Zeiten bleiben spannend.

Literaturverzeichnis

Zitierweise: Die nachfolgenden Werke werden, wenn nichts anderes angegeben ist, mit Nachnamen des Autoren, der Autorin oder der Autoren sowie mit Seitenzahl oder Randnummer zitiert.

Alder Markus: Die Strafzumessungsrichtlinien der USA in ihrem Kontext mit Plea Bargaining, Dissertation, Frankfurt am Main 2001 (zit. Alder, Diss).

Blechta Gabor P./Vasella David (Hrsg.): Basler Kommentar („**BSK**“) Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Auflage, Basel 2024

(zit. BSK DSG-Bearbeiter/In, Art._N._).

Blechta Gabor/Maurer-Lambrou Urs (Hrsg.): Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Auflage, Basel 2014

(zit. BSK aDSG-Bearbeiter/In, Art._N._).

Bohrer Andreas: „Better Regulation im Wirtschaftsrecht, Anregungen an den Gesetzgeber in der Schweiz“, in: Das Aktienrecht im Wandel, Festschrift zum 50. Geburtstag von Prof. Dr. Hans-Ueli Vogt, Zürich 2020, S. 109 ff.

77 Rechtsgutachten pekuniäre Verwaltungssanktionen im Finanzmarktrecht.
78 Siehe Stellungnahme des Bundesrates zum Bericht der PUK CS, Motion Nr. 3, S. 34.

Gaberthuel Tino, „Verstrafrechtlichung" der Wirtschaft nimmt zu. Das verschärfte Korruptionsstrafrecht fordert Unternehmen und Verwaltungsräte, in: Finanz und Wirtschaft (**„FUW"**) vom 24. März 2016, Nr. 23, S. 13 abrufbar unter: https://www.fuw.ch/article/verstrafrechtlichung-der-wirtschaft-nimmt-zu/

(zuletzt abgerufen am 22.05.2025). (zit. Gaberthuel, „Verstrafrechtlichung" der Wirtschaft)

Jany Oliver, Legitimationsdefizite im europäischen Kartellermittlungsverfahren, Duncker & Humblot, Berlin, 2025 (zit. Jany, Legitimationsdefizite).

Jositsch Daniel/Ege Gian/Schwarzenegger Christian: Strafrecht II, Strafen und Massnahmen, in: Daniel Jositsch (Hrsg.), Zürcher Grundrisse des Strafrechts, Zürich 2018.

Mathys Roland: „DSGVO-Sanktionen – ein Fall für die Versicherung?", abrufbar unter https://www.swissict.ch/dsgvo-sanktionen-ein-fall-fuer-die-versicherung/?

(zuletzt abgerufen am 22.05.2025).

Montag Frank /Säcker Franz Jürgen/Bien Florian/Meier-Beck Peter (Hrsg.): Münchener Kommentar zum Europäischen und Deutschen Wettbewerbsrecht ("**MüKo-EU-WettbR**"), Band 1, München 2022, (zit. MüKo-EUWettbR- Bearbeiter/in, Art.__, Rn.__).

Niggli Marcel Alexander/Maeder Stefan: Was schützt eigentlich Strafrecht (und schützt es überhaupt etwas)?, in: Aktuelle Juristische Praxis (**„AJP"**), 04/2011, S. 442 ff.

Niggli Marcel Alexander /Wiprächtiger Hans (Hrsg.): Basler Kommentar Strafrecht I, Art. 1–110 StGB, 4. Aufl., Basel 2019 (zit. BSK StGB I-Bearbeiter/In Art._ N._)

Rosenthal David: Das neue Datenschutzgesetz, in: Jusletter vom 16. November 2020

Rosenthal David/Gubler Seraina: Die Strafbestimmungen des neuen DSG, in: Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht („**SZW/RSDA**") 01/2021, S. 52 ff.

Sherin Kneifl: Ab 1. September 2023 gilt ein neues Datenschutzrecht, in: Schweizerische Juristen-Zeitung (**„SJZ"**) 118/2022 S. 1108 ff.

Strasser Othmar, Strafrechtliche Verantwortung des Unternehmensjuristen einer Schweizer Bank, in: Monti Mario et al. (Hrsg.), Economic Law and Justice in Times of Globalisation, Festschrift for Carl Baudenbacher, Baden-Baden/Wien/Bern 2007, 749 ff.

Wagner -von Papp Florian: Kriminalisierung von Kartellen, in: Wirtschaft und Wettbewerb („**WuW**") 60/2010, S. 268 ff.

Wils Wouter P.J.: **Is criminalization of EU competition law the answer?, in:** *Concurrences*, Competition law review, Februar 2006.

Wiprächtiger Hans: Revisionen des Strafgesetzbuches - (insbesondere des Sanktionenrechts) unnötig, unwirksam, unübersichtlich, in: Anwaltsrevue/Revue de l'avocat, Heft Nr. 11/12/2014, S. 477 ff. (zit. Wiprächtiger, Anwaltsrevue 11/12I2014).

Wiprächtiger Hans/Spahni Sara: Schnellfahren, Fahren in angetrunkenem Zustand und Strafzumessung, in: Strassenverkehr, interdisziplinäre Zeitschrift 2017, S. 12 ff.

(zit. Wiprächtiger/Spahni, Schnellfahren und Strafzumessung).

Wiprächtiger Hans/Spahni Sara: Rezension Leitfaden Strafzumessung Hans Mathys, in: forumpoenale 1/2017, S. 60 ff (zit. Wiprächtiger/Spahni, forumpoenale 1/2017).

Materialienverzeichnis

Stellungnahme des Bundesrates zum Bericht der Parlamentarischen Untersuchungskommission („**PUK**") vom 17. Dezember 2024 bezüglich Geschäftsführung der Bundesbehörden im Kontext der CS-Krise, vom 20. Dezember 2024; BBl 2025 516 ff.

(zit. Stellungnahme des Bundesrates zum Bericht der PUK CS).

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (**„EDÖB"**), Untersuchung von Verstössen gegen Datenschutzvorschriften durch den EDÖB, Anwendung von Art. 49 – 53 des revidierten Datenschutzgesetzes vom 1. Oktober 2024

(zit. Untersuchung EDÖB zu Art._, N._).

Rechtsgutachten über pekuniäre Verwaltungssanktionen im Finanzmarktrecht von Prof. Dr. iur. Isabelle Häner, Rechtsanwältin, zu Handen des Staatssekretariat für Internationale Finanzfragen vom 10. November 2023, abrufbar unter:

https://www.bratschi.ch/assets/content/files/publikationen/Rechtsgutachten-pekuniaere-Verwaltungssanktionen.pdf (zuletzt abgerufen am 22.05.2025) (zit. Rechtsgutachten pekuniäre Verwaltungssanktionen im Finanzmarktrecht).

Änderung des Strafgesetzbuches (Reform der lebenslangen Freiheitsstrafe), Erläuternder Bericht des Bundesrates zur Eröffnung des Vernehmlassungsverfahrens vom 2. Juni 2023 (zit. Bericht zur Reform der lebenslangen Freiheitsstrafe).

Bericht des Bundesrates in Erfüllung des Postulates 18.4100 Staatspolitische Kommission des Nationalrats (**„SPK-N"**) vom 1. November 2018: Pekuniäre Verwaltungssanktionen vom 23. Februar 2022, BBl 2022 776 ff. (zit. Bericht Verwaltungssanktionen).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz (**„DSG"**) und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941ff. (zit. Botschaft DSG).

Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens vom 10. August 2017 (zit. Ergebnisbericht Vernehmlassung DSG).

Erläuternder Bericht des Bundesrats zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016 (zit. Bericht Vorentwurf DSG).

Botschaft zum Bundesgesetz über die steuerliche Behandlung finanzieller Sanktionen vom 16. November 2016, BBI 2016 8503 ff. (zit. Botschaft steuerliche Behandlung finanzieller Sanktionen).

Bericht des Eidgenössischen Volkswirtschaftsdepartements zuhanden der Kommission für Wirtschaft und Abgaben des Ständerats in Erfüllung des Ordnungsantrages Schweiger vom 21./22. Juni 2010: Einführung von Strafsanktionen gegen natürliche Personen im Kartellrecht vom 16. August 2010 (zit. Bericht Einführung von Strafsanktionen gegen natürliche Personen im Kartellrecht).