Kommunikation & Recht

K&R
4 | April 2024
27. Jahrgang
Seiten 229 - 300

www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

tions- und Unterhaltungsangebote, sondern bereiten die jeweiligen Inhalte auch in anwenderfreundlichen Übersichten auf. Ihre auf den ersten Blick naheliegende Einordnung als regulierungsbedürftige Medienplattformen bzw. Benutzeroberflächen ist bei näherer Betrachtung zu relativieren. Insbesondere die Anzeige analog und digital verbreiteter Radiosender als Kernstück sämtlicher Infotainmentsysteme ist jedenfalls bei einer an Systematik und Schutzzweck orientierten Würdigung der medienrechtlichen Vorschriften grundsätzlich nicht vom Anwendungsbereich der Benutzeroberflächenregulierung erfasst.

Auch eine abweichende Rechtsauffassung unterstellt, wären die resultierenden Regulierungspflichten der dann verantwortlichen Fahrzeughersteller nicht uferlos. So ist im Einzelfall zu untersuchen, inwieweit aufgrund unverhältnismäßiger Umsetzungserfordernisse und eingeschränkter Absatzzahlen des betroffenen Infotainmentsystems der Pflichtenkanon der §§ 78 ff. MStV überhaupt zur Anwendung gelangt. Jedenfalls im EU-Ausland ansässige Fahrzeughersteller dürften mit Blick auf die jüngste EuGH-Rechtsprechung von deutschen Regulierungsvorschriften vollständig befreit sein.

Dr. Tobias Bosch

ist Partner in den Bereichen Telekommunikation sowie IT, Outsourcing und Datenschutz der Kanzlei Noerr PartmbB in Berlin. Er studierte Rechtswissenschaften in Heidelberg und in Stanford. Er ist seit 1999 als Rechtsanwalt in führenden internationalen Sozietäten in Frankfurt und Berlin tätig, seit 2008 als Partner.

Luise Lautenbach

ist Rechtsanwältin im Bereich Data, Tech & Telecom der Kanzlei Noerr Partnerschaftsgesellschaft mbB in Berlin. Sie studierte Rechtswissenschaften in Göttingen und Frankfurt (Oder) und promoviert derzeit an der Freien Universität bei Prof. Dr. Momsen.

Dr. Jan Weismantel

studierte Rechtswissenschaften in Würzburg. Er ist Senior Associate der Kanzlei Noerr PartmbB, wo er seit 2019 an den Standorten München und Berlin schwerpunktmäßig im Bereich des privaten und öffentlichen Medienrechts tätig ist.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Update IT-Sicherheitsrecht 2022/2023 – Teil 2

Kurz und Knapp

Die Autoren stellen anschließend an ihr Update aus den Vorjahren in K&R 2021, 689 ff. und K&R 2022, 794 ff. die Entwicklung des IT-Sicherheitsrechts im Zeitraum 2022/23 dar. Während Teil 1 in Abschnitt I und II über die Gesetzgebung berichtet hat (K&R 2024, 169 ff.), widmet sich der vorliegende Teil 2 mit Abschnitt III der Rechtsprechung und zieht in Abschnitt IV ein Fazit.

III. Rechtsprechung

Folgende gerichtliche Entscheidungen im Berichtszeitraum sind für die IT-Sicherheit relevant:

1. EuGH zur Darlegungs- und Beweislast bei Verletzungen von Art. 32 DSGVO

Infolge eines Cyberangriffs hatte ein Täter unbefugten Zugang zu personenbezogenen (Finanz-) Daten bei einer bulgarischen Behörde. Betroffene stehen regelmäßig vor dem Problem, dass sie zwar Kenntnis von derartigen Vorfällen erhalten, aber nicht von ihren näheren Umständen. Dies erschwert die Geltendmachung von Schadensersatzansprüchen. Dazu hat der EuGH im Urteil vom 14. 12. 2023 (C-340/21)[1] zu Art. 32 DSGVO folgende Aussagen getroffen:

Allein die unbefugte Offenlegung personenbezogener Daten, das heißt der erfolgreiche Cyberangriff bzw. ungeplante Datenabfluss, sei kein Indiz für ungeeignete Sicherheitsmaßnahmen und einen Verstoß gegen Art. 32 DSGVO (Rn. 22 - 39 des Urteils). Aus technischer Sicht stellt sich allerdings die Frage, welche Kriterien der EuGH für ein Indiz sonst erwartet – ein Autofahrer, der auf Glatteis ins Schleudern kommt, sieht sich auch dem Vorwurf der nicht angepassten Geschwindigkeit ausgesetzt. Das simple Argument: Wäre sie angepasst gewesen, wäre er nicht geschleudert. Diese Argumentation muss konsequenterweise auch für IT-Sicherheit gelten.

Dem Betroffenen muss ein wirksamer Rechtsbehelf gegen den Verantwortlichen zur Verfügung stehen. Deshalb muss der Verantwortliche den Inhalt, die Art und Weise sowie die praktischen Auswirkungen der von ihm getroffenen Schutzmaßnahmen darlegen und nachweisen (Rn. 40 - 47 des Urteils).

Dabei trägt der Verantwortliche gemäß den Artt. 5 Abs. 2, 24 DSGVO die Beweislast dafür, dass seine Maßnahmen geeignet waren, um den Datenabfluss infolge des Cyberangriffs zu verhindern. Für diesen Nachweis ist indes nicht in jedem Fall ein Sachverständigengutachten erforderlich, der Nachweis kann auch durch andere Beweismittel erbracht werden (Rn. 48 - 64 des Urteils).

In Rn. 65 bis 74 stellt der EuGH fest, dass der Verantwortliche für unterlassene oder ungeeignete Sicherheitsmaßnahmen auch dann haftbar bleibt, wenn ein Dritter diese Lücken ausgenutzt hat. Selbst das kriminelle Handeln des Dritten unterbricht die Zurechnung zu Lasten des Verantwortlichen nicht.

Schließlich stellt das Gericht in Rn. 86 des Urteils fest: Allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, dass ihre personenbezo-

* Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 22. 2. 2024.

1 K&R 2024, 104 - 109.

genen Daten durch Dritte missbräuchlich verwendet werden könnten, kann einen „immateriellen Schaden“ im Sinne dieser Bestimmung darstellen. Allerdings reicht ein pauschaler Vortrag dazu nicht aus; die betroffene Person muss einen immateriellen Schaden auch nachweisen. Dies dürfte zumindest einen konkreten Vortrag verlangen, welche Folgen im Einzelnen der Betroffene aufgrund des Datenlecks befürchtet und wie sich diese auf ihn auswirken. Dabei beruft sich das Gericht ausdrücklich auf sein Urteil vom 4. 5. 2023.[2]

2. EuGH und „Deutsche Wohnen“

Für die Verhängung von DSGVO-Bußgeldern in Deutschland ist das EuGH-Urteil „Deutsche Wohnen“ ein Paukenschlag: Unternehmen haften nicht nur für Verstöße ihrer Vertreter, Leiter oder Geschäftsführer, sondern auch für Verstöße, die von jeder anderen Person begangen wurden, die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser juristischen Personen handelt. Zwar muss für ein Bußgeld ein vorsätzlicher oder fahrlässiger Verstoß nachgewiesen sein, aber ein Bußgeld gemäß Art. 83 DSGVO setzt nicht einmal eine Kenntnis eines Leitungsorgans des Verantwortlichen voraus (Rn. 44 und 77 des Urteils). Mit Beschluss vom 22. 1. 2024 hat das KG Berlin das Verfahren an das LG Berlin zurückverwiesen, welches in der Sache zu entscheiden hat.[3] Mit dieser Rechtsprechung kann auch ein Verstoß gegen die IT-Sicherheitspflichten des Art. 32 DSGVO durch ein Bußgeld geahndet werden, z. B. bei fahrlässig unterlassenen Maßnahmen.

3. Werkstattzugang zu OBD-Systemen in Kfz

Ein On-Board-Diagnosesystem (OBD-System) ist ein System, das sich in einem Fahrzeug befindet oder an einen Motor angeschlossen und in der Lage ist, eine Fehlfunktion festzustellen, anzuzeigen und mithilfe rechnergespeicherter Informationen den wahrscheinlichen Bereich von Fehlfunktionen anzuzeigen sowie diese Informationen nach außen zu übermitteln (Art. 3 Nr. 49 VO (EU) 2018/858). Die Reparatur eines Kfz ist ohne Zugang zum OBD-System erschwert. Deshalb verpflichtet Art. 61 VO (EU) 2018/858 die Kfz-Hersteller dazu, unabhängigen Werkstätten den Zugang zum OBD-System zu gewähren.

Der Fiat-Chrysler-Konzern machte den Zugang von einem kostenpflichtigen Abonnement abhängig. Die Mitarbeiter in den Werkstätten sollten sich persönlich auf einem Server registrieren und darüber Zugang zum OBD-System des betreffenden Kfz erhalten, welches ebenfalls mit dem Server verbunden war. Der Autokonzern bezeichnete dies als „Secure Gateway System“ und gab als Grund für dieses Vorgehen „Anforderungen der Cybersicherheit“ an.[4] Unklar bleibt, worin das „Cybersecurity“-Problem bestehen sollte und welche technische Funktion der genannte Server haben sollte: Für den standardisierten ODB2-Stecker gibt es auch für Privatkunden unter anderem zahllose Bluetooth-Dongles, damit der Fahrzeugbesitzer im laufenden Betrieb jederzeit Daten aus den Steuergeräten auslesen kann und auch den Fehlerspeicher prüfen kann. Welche „Cyber-Sicherheit“ betroffen sein soll, wenn man die (mit etwas Suche auch im Internet frei verfügbaren) Fehlercodes direkt in Reparatur-Hinweise übersetzen lassen kann, erschließt sich den Autoren nicht. Genauso wenig ist aus technischer Sicht für die Diagnose das Erfordernis eines Serverzugangs ersichtlich.

Selbst wenn man dem (falschen) Cybersicherheit-Argument folgen würde: Ein kostenpflichtiges Abonnement ist dafür nicht notwendig, wie der EuGH nunmehr bestätigt hat.[5] Laut Rn. 37 des Urteils ist die Sicherheit im Stadium der Entwicklung, der Konstruktion und des Zusammenbaus zu gewährleisten, aber nicht zum Nachteil anderer Marktteilnehmer. Zur Sicherheit des Datenaustauschs legt Anhang X Ziffer 6.2 bis 6.4 der VO (EU) 2018/858 unter Berufung auf den „Stand der Technik“ detaillierte Vorgaben fest. Diese sind auch ohne kostenpflichtiges Abonnement umsetzbar.

Gesmann-Nuissl weist dazu auf den Data Act hin, der als horizontale Regelung einen entsprechenden Datenzugang zu vernetzen Produkten vorgibt. Dazu müsse ein Gleichlauf mit der sektorspezifischen VO (EU) 2018/858 hergestellt werden.[6] Insofern sind die Hersteller verpflichtet, entsprechende Sicherheitsvorkehrungen für den Datenaustausch zu treffen, wenngleich dies im Data Act nur rudimentär geregelt ist.[7]

4. Unzulässige Demonstration einer Sicherheitslücke

Der BGH hatte folgende Konstellation über die Zulässigkeit des „Vorführens“ einer Sicherheitslücke zu entscheiden:[8] Beide Parteien sind Mobilfunkanbieter, die Beklagte erbringt u. a. Dienste im mTAN-Verfahren für Banken zur Legitimation von Online-Überweisungen. Sie entdeckte im Sommer 2014 eine Schwachstelle im Mobilfunknetz der Klägerin und demonstrierte diese im November 2014 ohne Wissen der Klägerin einem ihrer Kunden; zu diesem Zeitpunkt war die Lücke der Klägerin bereits bekannt (Rn. 45 d. Urteils). Dazu nutzte die Beklagte Zugangsdaten in Form sog. Global Titles (GT) von Roaming-Partnern der Klägerin, um Daten in das Netz der Klägerin einzuleiten, auszulesen und zu verändern. Der BGH bejahte den Anspruch der Klägerin aus § 1004 BGB, die Vorführung der Sicherheitslücke wie dargestellt zu unterlassen. Die Anlagen für den Betrieb des Mobilfunknetzes sind Sachen im Eigentum der Klägerin. Durch die Einleitung von Daten in das Netz hat die Beklagte in das Eigentum der Klägerin eingegriffen (Rn. 20 des Urteils), insbesondere durch die Vorführung der Lücke bei Dritten. Der Eingriff sei nicht gerechtfertigt, weder aufgrund einer Einwilligung der Klägerin (Rn. 27 ff. des Urteils) noch durch berechtigte Interessen (Rn. 45 des Urteils) oder durch Art. 32 DSGVO und auch nicht durch § 5 GeschGehG (Rn. 48 des Urteils).[9]

Mit der Praxis von IT-Sicherheitsforschern zum „Responsible Disclosure“ scheint die Entscheidung kompatibel: Dabei ist es üblich, dass Entdecker einer Sicherheitslücke sie zunächst dem Hersteller melden, ihm eine angemessene Gelegenheit zum Bereitstellen eines Patches geben und sie dann erst publizieren, auch, um die Öffentlichkeit zu warnen und die

2 EuGH, 4. 5. 2023 – C-300/21, K&R 2023, 416 ff.; dem folgend die Instanzrechtsprechung zu den sogenannten „Scraping“-Fällen, in denen zahlreiche Social-Media-Nutzer Forderungen an die Social-Media-Anbieter stellten, weil Dritte Daten aus ihren veröffentlichten Profilen ausgelesen haben („Scraping“), was die Social-Media-Anbieter durch technische Maßnahmen hätten verhindern können, z. B. LG Freiburg (Breisgau), 15. 9. 2023 – 8 O 21/23, juris; LG Freiburg (Breisgau), 15. 9. 2023 – 8 O 184/22, juris; LG Heidelberg, 31. 3. 2023 – 7 O 9/22, juris; LG Bonn, 23. 2. 2023 – 10 O 142/22, juris; LG Frankfurt a. M., 27. 1. 2023 – 2-27 O 158/22, juris; LG Lüneburg, 24. 1. 2023 – 3 O 81/22, juris.

3 EuGH, 5. 12. 2023 – C-807/21, K&R 2024, 30-35 (m. Anm. *Grosmann/Hansen*); dazu *Grages/Strassemeyer*, CR 2024, 10-18; zur Vorlage des LG Berlin *Deusch/Eggendorfer*, K&R 2022, 794, 799; KG Berlin, 22. 1. 2024 – 3 Ws 250/21, 161 AR 84/21, 3 Ws 250/21 – 161 AR 84/21.

4 EuGH, 5. 10. 2023 – C-296/22, WRP 2023, 1442, Rn. 15.

5 EuGH, 5. 10. 2023 – C-296/22, WRP 2023, 1442.

6 *Gesmann-Nuissl*, InTeR 2023, 185, 197 (ab S. 198 ist das EuGH-Urteil wiedergegeben).

7 Siehe *Deusch/Eggendorfer*, K&R 2024, 169, 172, Abschnitt I Ziffer 1 lit. d.

8 BGH, 13. 5. 2022 – V ZR 7/21 – WRP 2022, 1140.

9 BGH, 13. 5. 2022 – V ZR 7/21, WRP 2022, 1140; unter dem Aspekt des Art. 32 DSGVO *Grages*, in: Plath, DSGVO/BDSG/TTDSG, 3. Aufl. 2023, Art. 32 DSGVO Rn. 1.

Gefahr zu beseitigen. Das Publizieren ist unter IT-Sicherheitsforschern aber erst dann vorgesehen, wenn der Hersteller die Sicherheitslücke verleugnet oder überhaupt nicht reagiert.[10] Vorliegend ist nicht feststellgestellt, ob die „Publikation" erfolgte, bevor der Hersteller reagieren konnte. Jedoch hat der BGH in Rn. 45 des Urteils ausgeführt, dass die Präsentation der Lücke bei einem einzigen Kunden keine geeignete Maßnahme ist, um die Netzsicherheit wieder herzustellen. Die Demonstration der Lücke kann somit auch nicht als Responsible Disclosure gewertet werden.

5. E-Mail-Kommunikation ausgespäht, doppelt bezahlt: OLG Karlsruhe

Ein Autohändler hatte seine Rechnung als PDF-Datei mit unverschlüsselter E-Mail an den Käufer übermittelt.[11] Eine Minute später erhielt der Käufer eine weitere E-Mail mit einer manipulierten zweiten PDF-Rechnung, die eine andere Bankverbindung auswies (mit einer bislang unbekannten natürlichen Person als Kontoinhaber und dem – für Kfz-Geschäfte unverständlichen – Satz „Bitte senden Sie uns nach der Herstellung der Decke eine Kopie nach der Banküberweisung"). Der Käufer zahlte an die Bankverbindung aus der zweiten E-Mail, weshalb der Verkäufer ihn auf Zahlung verklagte.

Das OLG Karlsruhe gab der Klage statt. Der Käufer habe an eine falsche Bankverbindung gezahlt und seine Kaufpreisschuld nicht erfüllt. Er habe auch keinen Schadensersatzanspruch gegen den Verkäufer aufgrund unterlassener IT-Sicherheitsmaßnahmen, die das Ausspähen und die Manipulation der E-Mail-Kommunikation verhindert hätten. Insbesondere gebe es bei dem Kaufvertrag keine vertragliche Nebenpflicht aus den §§ 280 Abs. 1, 241 Abs. 2 BGB, die PDF-Datei zu verschlüsseln oder für die E-Mail-Transportverschlüsselung oder Ende-zu-Ende-Verschlüsselung anzuwenden. Die Orientierungshilfe des Arbeitskreises Technische und organisatorische Datenschutzfragen[12] empfehle zwar eine Ende-zu-Ende-Verschlüsselung für E-Mails, diese sei zwischen den Parteien aber nicht anwendbar, weil es sich um juristische Personen handle und deshalb keine personenbezogenen Daten betroffen seien.[13] Unklar ist aber, ob tatsächlich keine personenbezogenen Daten in den Rechnungen enthalten waren. Viele Rechnungen enthalten z. B. den Namen des zuständigen Mitarbeiters beim Käufer oder Verkäufer, aber auch die Pflichtangaben zum Namen des Geschäftsführers. Bereits dies sind personenbezogene Daten. Insoweit scheint die Formulierung des Gerichts unglücklich: Die DSGVO ist für die streitgegenständliche E-Mail-Kommunikation sehr wohl anwendbar, fraglich ist lediglich, ob die Parteien des Rechtsstreits sich auf die Schutzwirkungen der DSGVO berufen können, obwohl sie juristische und keine natürlichen Personen sind.

Das Gericht hatte sich zudem mit dem Argument des Käufers auseinanderzusetzen, der Verkäufer habe es unterlassen, beim Versand seiner E-Mail das Sender Policy Framework (SPF) zu verwenden. Dieses Argument ist technisch betrachtet kaum nachzuvollziehen: Das SPF entstand 2006 mit dem Ziel, unerwünschte Werbe-E-Mails (SPAM) zu reduzieren.[14] Dabei nutzten die Spammer häufig E-Mail-Adressen Dritter für ihren Versand, verschickten also z. B. Aktienspam unter der Domain kommunikationundrecht.de. Technisch ist das auch heute noch möglich, weil das für den E-Mail-Versand verwendete Protokoll SMTP keine verpflichtende Authentifizierung vorsieht. Somit ist es trivial, eine beliebige Absenderadresse anzugeben, also E-Mails zu fälschen. SPF erlaubt es nun, dass der Empfänger prüft, ob die IP-Adresse des versendenden Servers zu einer im DNS-Eintrag der Domain angegebenen Liste von zulässigen Mailservern gehört. Damit lässt sich die SPAM-Wahrscheinlichkeit erkennen. Allerdings nutzen nicht alle Absender SPF, teilweise auch nicht korrekt konfiguriert, durchaus auch bei großen Konzernen und Behörden,[15] weshalb SPF keine verlässliche Erkennung erlaubt. Weiter verhindert SPF eine automatische E-Mail-Weiterleitung von user@example.com an nutzer@beispiel.de, denn die Weiterleitung erfolgt durch den Mailserver von example.com, der nicht für die Domain des Original-Absenders gelistet ist. Ähnliche Probleme können bei Mailinglisten auftreten. Besonders in der Anfangszeit von SPF waren Spammer die Hauptnutzer, sie registrierten sich Domains für ihre Spam-Kampagnen und richteten SPF ein, damit sie mit SPF-Bonus besser an Spam-Filtern vorbeikamen. Daher nutzt die Praxis SPF zwar häufig als Indikator, aber nicht als verlässliches Erkennungsmerkmal für SPAM (oder andere modifizierte Mails). Aus SPF auf die Echtheit einer Mail schließen zu wollen, ist aber falsch. Das technische Mittel dafür ist die digitale Signatur.[16]

Das Urteil ist in der Literatur teilweise mit der Begründung begrüßt worden, man könne bei der E-Mail-Kommunikation „aufgrund des erheblichen Aufwands" keine Ende-zu-Ende-Verschlüsselung erwarten.[17] Dem ist einerseits entgegenzuhalten: Ende-Zu-Ende-Verschlüsselung ist nicht das Mittel der Wahl, um eine Manipulation zu verhindern, dazu dienen Signaturen. Denn auch ein verschlüsselter Text kann – wenn auch blind – modifiziert werden. Die Signatur sichert Integrität und Authentizität. Andererseits hätte in dem Fall voraussichtlich Ende-Zu-Ende-Verschlüsselung den Schaden des Käufers verhindert, denn der Angreifer hätte es kaum geschafft, ohne Zugriff auf die IT des Absenders eine authentisch aussehende Rechnung in eine verschlüsselte Kommunikation einzuschleusen.[18] Sowohl E-Mail-Signaturen mit GPG[19] und S/MIME als auch Ende-zu-Ende-Verschlüsselung von E-Mails sind Stand der Technik und müssen maßgeblich sein für die gemäß § 276 BGB geschuldete Sorgfalt in der E-Mail-Kommunikation.[20] Nicht nachvollziehbar ist, dass das OLG Karlsruhe stattdessen von „berechtigten Sicherheitserwartungen des Verkehrs" ausgeht (Ziffer 2 a), dd) der Urteilsgründe). Zu hinterfragen ist zudem, dass der Senat die Empfehlungen der Datenschutzbehörden zur Verschlüsselung verwirft, weil die DSGVO zwi-

10 Siehe zum Responsible Disclosure auch *Deusch/Eggendorfer*, K&R 2023, 649, 655 f. sowie unten zu AG Jülich.

11 Ob der Rechnungsadressat diese E-Mail erhalten hat, ist der Entscheidung nicht zweifelsfrei zu entnehmen; die Formulierung der Entscheidungsgründe sprechen jedoch für einen Erhalt.

12 Zur Empfehlung der Datenschutzbehörden: https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf.

13 OLG Karlsruhe, 27. 7. 2023 – 19 U 83/22, K&R 2023, 607, 610.

14 https://datatracker.ietf.org/doc/html/rfc4408; https://de.wikipedia.org/wiki/Sender_Policy_Framework; *Eggendorfer*, No Spam. Besser vorbeugen als heilen, 2005; *Eggendorfer*, Methoden der Spambekämpfung und -vermeidung, 2007.

15 Wer IT-Sicherheit im Hochschul-Umfeld lehrt, SPF in der Vorlesung erklärt und fleißige Studierende hat, die direkt prüfen, ob die Hochschule ihre Konfiguration auch ordentlich umgesetzt hat, kann sich das schallende Gelächter im Hörsaal vorstellen…

16 Mehr dazu unten und in *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 38. Ergänzung 2023, Kap. 50.1 Rn. 199 sowie *dieselben*, Beauftragte für IT-Sicherheit und Informationssicherheit, 2024, Ziffer 2.3.1.4.

17 *Diehm*, BB 2023, 2644; *Ziegler/Schröder*, MMR 2023, 765 f.

18 Im Gegensatz zur ebenfalls angesprochenen „Transportverschlüsselung", siehe dazu *Deusch/Eggendorfer*, K&R 2022, 577, 579 und *Deusch/Eggendorfer*, Beauftragte für IT-Sicherheit und Informationssicherheit, 2024, Ziffer 2.3.1.7.1.

19 PGP (Pretty Good Privacy) war das Originalverfahren von Phil Zimmermann, das später kommerzialisiert wurde. Die OpenSource-Implementierung mit gleicher Funktionalität und Logik heißt GnuPG bzw. kurz GPG.

20 *Deusch/Eggendorfer*, K&R 2015, 11, 13, 16 f. und *Deusch/Eggendorfer*, (Fn. 18), Ziffer 2.3.1.7.1.

schen den Parteien nicht anwendbar sei. Die Empfehlung der Datenschutzbehörden gibt – ähnlich wie eine technische Norm – den Stand der Technik für die E-Mail-Kommunikation wieder. Wer jedoch den Stand der Technik nicht einhält, indiziert einen Sorgfaltsverstoß, und zwar auch außerhalb der DSGVO.[21] Wie der entstandene Schaden beweist, sind die betroffenen Daten des Käufers nicht weniger schutzwürdig als personenbezogene Daten.

In diesem Zusammenhang ist auch der Beschluss des VG Frankfurt a. M., 15. 7. 2022 – 5 L 1281/22.F zu kritisieren, wonach kein Anspruch auf Transportverschlüsselung bei elektronischer Kommunikation wegen elektronischem Kriegswaffenbuch bestehen soll. Zum einen ist nur die Ende-zu-Ende-Verschlüsselung diejenige Maßnahme, die nach dem Stand der Technik effektiven Schutz der Vertraulichkeit einer E-Mail gewährleistet; dies ist bei anderen diskutierten Maßnahmen wie z. B. der „Transportverschlüsselung" gerade nicht der Fall. Zum anderen ist nicht nachvollziehbar, weshalb es dem Betroffenen versagt bleiben soll, eine elektronische Kommunikation mit der Behörde nach dem Stand der Technik zu verlangen. Derartige Entscheidungen sind fast schon eine Einladung an Cyberkriminelle, die Kommunikation auszuspähen.

Zu folgen ist dem OLG Karlsruhe dagegen im entscheidungserheblichen Punkt: Der Käufer hat nicht vorgetragen, dass er selbst in der Lage war, Ende-zu-Ende-verschlüsselt zu kommunizieren. Wer Verschlüsselung einfordert, muss auch einen Schlüssel bereitstellen. Der technische Aufwand für eine Ende-zu-Ende-Verschlüsselung ist entgegen mancher Unkenrufe minimal im Vergleich zu den Kosten anderer Security-„Lösungen". Weiter bleibt ein erhebliches Mitverschulden, weil der Käufer aufgrund des Inhalts der E-Mail die Manipulation hätte erkennen können. Es bleibt auch unklar, ob und wie in dem vorliegenden Fall die E-Mail-Manipulation erfolgte, was allerdings für die rechtliche Beurteilung relevant sein dürfte.

6. OLG Karlsruhe und LG Köln zu Schäden infolge von Cyberangriffen

Zum Schadensersatz Betroffener infolge von Cyberangriffen kommen das OLG Karlsruhe und das LG Köln zu unterschiedlichen Ergebnissen:[22]

In beiden Fällen wurden die verantwortlichen Unternehmen durch die kriminelle Ausnutzung von Sicherheitslücken Opfer von Cyberangriffen, in deren Folge personenbezogene Daten Betroffener an Unbefugte abgeflossen sind. In beiden Fällen geht es um Schadensersatzansprüche der Betroffenen gegen die angegriffenen Unternehmen, mit dem Vorwurf, deren Sicherheitsvorkehrungen seien nicht ausreichend gewesen. Während das OLG Karlsruhe dem Betroffenen immateriellen Schadensersatz versagte, weil er einen Schaden nicht ausreichend dargelegt habe und sich das beklagte Unternehmen zudem durch Sicherheitsmaßnahmen gemäß Art. 82 Abs. 3 DSGVO entlastet habe, hat das LG Köln aufgrund eines Verstoßes gegen Art. 32 DSGVO einen immateriellen Schadensersatzanspruch i. H. v. € 1200,00 zugesprochen. Wenngleich die Fallgestaltungen im Einzelnen unterschiedlich sind, fällt auf, dass der klägerische Vortrag vor dem LG Köln zu den befürchteten Nachteilen infolge des Datenabflusses erheblich substantiierter ist als im Fall des OLG Karlsruhe. Maßgeblich waren für das LG Köln die Befürchtung des Klägers, zur Preisgabe weiterer Daten und zu Zahlungen veranlasst zu werden sowie die Gefahr des Identitätsmissbrauchs. Dies dürfte sich in die Anforderungen des EuGH zum Vortrag bei immateriellen Schadensersatzansprüchen zu Art. 82 DSGVO (siehe oben Ziffer 1) fügen.

Wichtig für die anwaltliche Beratung: Im Gegensatz zum Verfahren beim LG Köln beantragte der Kläger vor dem OLG Karlsruhe richtigerweise die Feststellung, dass die Beklagte verpflichtet ist, künftigen Schaden aus dem Datenabfluss zu ersetzen. Ein solcher Antrag ist wichtig, um die Position des Klägers abzusichern, falls sich im weiteren Verlauf Schäden ergeben, die zum Zeitpunkt der Klage nicht vollständig absehbar sind. Das OLG Karlsruhe lehnte den Feststellungsantrag zwar als unzulässig ab, da es „die Möglichkeit eines Schadenseintritts für theoretisch" hielt (Rn. 32 des Urteils), ob diese Beurteilung zutrifft, kann zumindest hinterfragt werden, wie der Vortrag beim LG Köln und die Praxis zeigt: Auch die Autoren erhalten regelmäßig Phishing- und Malware-E-Mails, die ersichtlich auf Data-Breaches zurückzuführen sind. Das spricht deutlich gegen ein rein theoretisches Risiko, sondern für eine sehr reale Gefahr. Genau zu dem Zweck stellen Angreifer erbeutete Daten zum Verkauf ins Netz, und genau deswegen sind sie den Käufern auch Geld wert. Ein Feststellungsantrag (zumindest die Aufklärung des Mandanten dazu) dürfe jedoch bei der Beratung von Betroffenen in Cyberschadensfällen zum anwaltlichen Pflichtrepertoire gehören.

7. Leistungen aus Cyberversicherung (LG Tübingen)

Der Versicherungsnehmer, selbst ein Versicherungsunternehmen, war Opfer eines Ransomware-Angriffs. Er hatte für die Windows-Betriebssysteme seiner Server nicht in allen Fällen aktuelle Sicherheitsupdates installiert.[23] Nach den Feststellungen des Gerichts wäre der Schaden aber auch eingetreten, wenn die Updates installiert worden wären. Einfallstor für die Täter und schadensursächlich war die Gestaltung der Administratorenrechte im Betriebssystem. Die Täter hatten solche Admin-Rechte erbeutet und hierüber die Schadsoftware installiert (Ziffer 3 a. aa. der Urteilsgründe). In der Folge verschlüsselten die Täter die Daten des Versicherungsnehmers. Dieser gab der Lösegeldforderung der Täter für die Entschlüsselung nicht nach, sondern stellte den Zustand des Systems anhand von Datensicherungen wieder her. Dafür verlangte er von der beklagten Cyberversicherung den Ersatz des Betriebsunterbrechungsschadens sowie die Kosten für das Wiederherstellen des Systems in Höhe von insgesamt ca. € 3,77 Mio.; davon sprach das Gericht dem Versicherungsnehmer ca. € 2,86 Mio. zu.[24] Dabei stritten die Parteien um folgende Punkte:

- Die fehlenden Updates waren für das Gericht kein Grund, den Anspruch zu versagen. Ob die Klägerin dazu vor Vertragsschluss angegeben habe, sie unterziehe alle ihre Systeme aktuellen Sicherheitsupdates (was nicht zutraf), war für den Schaden nicht relevant, da dieser unabhängig davon eintrat. Aus demselben Grund führt das unterlassene Updating auch nicht zu einer Gefahrerhöhung.
- Der Sachverständige hat festgestellt, dass der Schaden verhindert oder reduziert eingetreten wäre, wenn der Versicherungsnehmer weitere Sicherheitsmaßnahmen, wie z. B. Multi-Faktor-Authentifizierung eingesetzt hätte. Auch dies war für das Gericht kein Grund zur Anspruchsreduktion, denn der beklagte Versicherer habe nach derartigen weiteren Maßnahmen vor Abschluss der Versicherung nicht gefragt. Auch technisch ist fraglich, ob eine Multi-Faktor-

21 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 16), Kap. 50.1, Rn. 489 m. w. N.
22 OLG Karlsruhe, 7. 11. 2023 – 19 U 23/23, juris; LG Köln, 18. 5. 2022 – 28 O 328/21, juris.
23 Wie das Beispiel in der Einleitung (oben Abschnitt I) zeigt, sind auch Sicherheitsupdates selbst beim Hersteller Microsoft nicht ausreichend, um vollständigen Schutz zu erlangen.
24 LG Tübingen, 26. 5. 2023 – 4 O 193/21, BB 2023, 1858 (Leitsatz) = NJW-RR 2023, 1194 - 1201.

Authentifizierung überhaupt sinnvoll ist: Angreifer können zwar irgendwoher das Administrator-Passwort erlangen und einzusetzen versuchen (in diesem Fall scheitern die Angreifer, wenn sie nicht im Besitz des „zweiten Faktors" sind), in der Regel nutzen sie jedoch Sicherheitslücken in der Software aus, um auf ein System zu gelangen. Dort nutzen sie dann weitere Lücken für eine sogenannte Privilege Escalation. Dabei findet nie eine Authentifizierung statt, eine Multi-Faktor-Authentifizierung würde also auch nicht getriggert. Ein Allheilmittel ist sie jedenfalls nicht, oft sogar eher eine trügerische Sicherheit.[25]
Aus Sicht des LG Tübingen stelle die Multi-Faktor-Authentifizierung dagegen eine zusätzliche Sicherheitsmaßnahme dar. Der Versicherer könne keine zusätzlichen Sicherheitsmaßnahmen verlangen, die für ihn zum Zeitpunkt des Schadensfalls eine bessere Risikolage darstelle als bei Abschluss der Police. Abweichendes kann indes gelten, wenn gesetzliche Sicherheitspflichten erst nach der Policierung in Kraft getreten sind. Sie sind von den Versicherungsnehmern zu befolgen und könnten bei Verstoß auch anspruchsreduzierend wirken.[26] Versicherungsnehmer, die z. B. nach der NIS-2-RL neue Sicherheitspflichten zu erfüllen haben, müssen damit rechnen, dass Verstöße hiergegen den Versicherungsschutz auch dann gefährden, wenn die Police bereits vor Inkrafttreten der NIS-2-RL (bzw. dem nationalen Umsetzungsgesetz) ausgefertigt war.
- Der Fall zeigt zudem die Relevanz einer sorgfältigen Dokumentation und Darlegung der Schadenshöhe auf. Insofern wird auf Ziffer 4 der Urteilsgründe verwiesen.

Hinweise für die Beratungspraxis:

- Bei einer Cyberversicherung sind die Antragsunterlagen und die vorvertraglichen Auskünfte penibelst zu prüfen.
- Im eingetretenen Schadensfall ist die Feststellung der Ursachen relevant. Nicht jeder Sicherheitsverstoß wirkt schadensursächlich und somit anspruchsreduzierend. Auch die Schadenshöhe ist sorgfältig zu dokumentieren.
- In diesem Zusammenhang ist auch der Vorschlag von *Hörl* relevant, in Zulieferverträgen betreffend IT-Leistungen die Behandlung von Cyberschäden zu regeln.[27]

8. Geschäftsführerhaftung

Im Berichtszeitraum geben zwei Gerichtsentscheidungen Anlass zu Ausführungen über die zivil- und strafrechtliche Verantwortung von Geschäftsführern:

a) OLG Zweibrücken zur Geschäftsführerhaftung für Phishing und CEO-Fraud

Die klagende GmbH stand in Geschäftsbeziehung mit dem Unternehmen S, deren E-Mail-Adresse sales@w…*film*.com lautet. Sie hatte von kriminellen Tätern mehrere (Phishing-) E-Mails mit der Adresse sales@w…*flim*.com erhalten und zahlte aufgrund der darin enthaltenen Täuschungen zur Erfüllung vermeintlicher Forderungen von S insgesamt 137 828,13 US-Dollar sowie einen weiteren Betrag in Höhe von € 91 230,39. Die Überweisungen hat die Beklagte vorgenommen, welche seinerzeit (Mit-) Geschäftsführerin der Klägerin war. Das OLG Zweibrücken lehnte die Schadensersatzforderung der GmbH mit erstaunlicher Begründung ab. Das Tätigen von Überweisungen gehöre nicht zu den spezifischen Organpflichten, für die ein Geschäftsführer mit der nach § 43 GmbHG geschuldeten Sorgfalt verantwortlich sei (Ziffer 1 der Entscheidungsgründe). Auch eine Haftung aufgrund des Geschäftsführer-Anstellungsvertrags komme nicht in Betracht. Denn die beklagte Geschäftsführerin sei durch den weiteren (Mit-)Geschäftsführer und Gesellschafter derart in ihrer Entscheidungsbefugnis begrenzt, dass sie mit einem Arbeitnehmer vergleichbar sei und für leichte Fahrlässigkeit nicht hafte. Diese liege hier vor, da alle weiteren Inhalte der Phishing-E-Mails außer der fehlerhaften E-Mail-Adresse plausibel gewesen seien. Zudem nimmt das Gericht den weiteren Geschäftsführer in die Verantwortung, da dieser die gesamte E-Mail-Kommunikation „im cc" erhalten und den Überweisungen nicht widersprochen habe.[28]

An der Entscheidung fällt auf, dass der Senat in Ziffer 1 lit. c, bb) der Entscheidungsgründe zwar von einer allgemeinen Überwachungspflicht und einer daraus abgeleiteten Compliance-Pflicht der Geschäftsführung ausgeht, Gesetzesverstöße von Unternehmensangehörigen schon im Vorfeld durch geeignete und zumutbare Schutzvorkehrungen zu verhindern. Ob die beklagte Geschäftsführerin diese Pflicht erfüllt oder hiergegen verstoßen hat, behandelt das Urteil aber nicht; die Entscheidung gibt auch keine Hinweise auf einen entsprechenden Vortrag der Klägerin. Dies verwundert, zumal nach dem Stand der Technik Schutzvorkehrungen gegen Phishing existieren. Die Verwendung fortgeschrittener digitaler Signaturen (Art. 3 Nr. 11 VO (EU) Nr. 910/2014 – eIDAS-VO) in den E-Mails mit dem Unternehmen S zum Beispiel hätte dem Betrug entgegengewirkt.[29]

Hinweis: In Phishing-Fällen zum Online-Banking, in denen die Opfer aufgrund betrügerischer E-Mails oder Webseiten Passwörter oder TANs preisgeben, nimmt die Rechtsprechung regelmäßig grobe Fahrlässigkeit der Opfer an; dies führt dazu, dass die Opfer die betrügerischen Überweisungen nicht rückgängig machen können und auf dem Schaden sitzen bleiben.[30]

b) Strafrechtliche Haftung bei der Vertuschung von Sicherheitsvorfällen

Adler/Hötzel weisen auf die Entscheidung eines US-Gerichts vom 5. 10. 2022[31] zur strafrechtlichen Haftung eines Chief Security Officer hin, der zur Aufklärung eines Ransomware-Vorfalls im Unternehmen Uber beauftragt war. Statt einer Aufklärung veranlasste der Angeklagte die Zahlung des Lösegelds und wies die Mitarbeiter zum Stillschweigen über den Vorfall an. Nach deutschem Recht könnte dieses Verhalten als Strafvereitelung (§ 258 StGB), Betrug bzw. Untreue (§§ 263, 266 StGB) strafbar sein. Falschaussage (§ 153 StGB) kommt in Betracht, wenn in Verfahren bei Aufsichtsbehörden (etwa bei der Aufbereitung eines Data Breach nach einer Meldung gemäß Art. 33 DSGVO) falsche Angaben gemacht werden.[32]

9. Kryptohandys/Encrochat

Französische Ermittlungsbehörden haben im Frühjahr 2020 umfangreiche Daten aus verschlüsselter elektronischer Kommunikation sichergestellt, die aus der Nutzung von Smartphones mit der Bezeichnung „Encrochat" stammte. Da die

25 Siehe dazu auch *Deusch/Eggendorfer* (Fn. 18), Ziffer 2.3.4.5.
26 Dazu: *Gesmann-Nuissl*, InTeR 2023, 137, 153.
27 *Hörl*, ITRB 2023, 268 ff.
28 OLG Zweibrücken, 18. 8. 2022 – 4 U 198/21 – juris = NJW 2023, 1589-1592, dazu *Ferner*, jurisPR-ITR 23/2023 Anm. 6.
29 *Deusch/Eggendorfer* (Fn. 18), Ziffer 2.3.1.4.3.2 (Signaturen); weitere Hinweise z. B. auf der Website des österreichischen Finanzministeriums https://www.onlinesicherheit.gv.at/Services/Technologie-Schwerpunkte/Phishing-und-Cybercrime/Praeventionsmassnahmen-gegen-Phishing.html.
30 Formal liegt eine Online-Überweisung vor, die das Opfer nicht beauftragt hat und von der Bank gemäß § 675u S. 2 BGB zu erstatten wäre; dem steht aber ein Schadensersatzanspruch der Bank gemäß § 675v Abs. 3 Nr. 2 lit. b BGB entgegen, siehe z. B. LG Lübeck, 3. 1. 2024 – 3 O 83/23, juris.
31 USA v. Sullivan, Case No. 20-cr-00337-WHO-1.
32 *Adler/Hötzel*, PinG 2023, 60-62.

Daten auch Straftaten in Deutschland betreffen, mussten die hiesigen Gerichte darüber entscheiden, ob sie die in Frankreich ermittelten Daten ihren strafrechtlichen Verurteilungen zugrunde legen können. Nach mehreren Oberlandesgerichten bejahte dies am 2. 3. 2022 auch der BGH, unter anderem mit der Begründung, dass allein die Nutzung eines „Encrochat-Smartphones" einen ausreichenden Verdacht bilde, um die rechtsstaatlichen Mindesterfordernisse (ordre public) für die Infiltration von Smartphones und Server durch die französischen Behörden zu rechtfertigen. Aus Sicht der Autoren stellt sich dazu die Frage, ob die vom BGH herangezogenen Kriterien geeignet sind, tatverdächtiges Verhalten abzugrenzen von der unverdächtigen (gemäß Art. 32 DSGVO gewollten) Nutzung von Verschlüsselung.[33]

Das BVerfG hat dazu in einem Fall eine Verfassungsbeschwerde nicht zur Entscheidung angenommen; fünf weitere Verfassungsbeschwerden sind jedoch noch nicht entschieden.[34]

Der EuGH hat dazu ein Vorabentscheidungsersuchen des LG Berlin zu entscheiden; dazu liegen seit dem 26. 10. 2023 die Schlussanträge der Generalanwältin *Ćapeta* vor. Hiernach haben die deutschen Gerichte die in Frankreich getroffenen richterlichen Genehmigungen zu den Ermittlungen (das heißt die Infiltration von Smartphones und Server) zu akzeptieren. Die Generalanwältin betont aber auch, dass der Zugang der deutschen Strafbehörden zu den französischen Ermittlungsergebnissen gemäß Art. 6 Abs. 1 der RL 2014/41/EU („EEA-Richtlinie") nur zulässig ist, wenn dies unter Berücksichtigung der Rechte der betroffenen Personen verhältnismäßig und notwendig ist. Der Zugang der nationalen Behörden zu den französischen Ermittlungsergebnissen sei ein schwerwiegender Eingriff in das Privatleben der betroffenen Personen. Er könne nur durch ein gewichtiges öffentliches Interesse an der Aufklärung und Verfolgung von Straftaten aufgewogen werden (Abschnitt IV Rn. 132 der Anträge). Dazu führt die Generalanwältin in Rn. 82 ihrer Anträge aus, dass der EuGH nicht zur Entscheidung über die Frage berufen ist, „ob es unverhältnismäßig ist, die Übermittlung der Daten aller Encrochat-Nutzer in Deutschland anzuordnen, wenn keine konkreten Anhaltspunkte für die begangenen Straftaten vorlagen."[35]

Es bleibt daher eine Aufgabe von Rechtsprechung und Wissenschaft, herauszuarbeiten, unter welchen Voraussetzungen elektronische Daten als Beweismittel gewonnen, ausgewertet und verwertet werden können.[36]

10. Strafbarkeit von IT-Sicherheitsforschern und Pentestern/Responsible Disclosure

Mit der Frage, wann Daten „besonders gesichert" im Sinne des § 202a StGB sind, hatten sich das AG Jülich und das LG Aachen zu befassen. Ein IT-Experte sollte im Auftrag seines Kunden ein webbasiertes Warenwirtschaftssystem „MS" in Betrieb nehmen. Dabei stellte er eine Sicherheitslücke fest, die mit der Möglichkeit verbunden war, auf die passwortgeschützte Datenbank von MS mit den Daten aller weiteren Kunden zuzugreifen. Das AG lehnte zunächst den Strafbefehlsantrag der Staatsanwaltschaft ab, weil es die Datenbank nicht als „besonders gesichert" ansah; das LG Aachen beurteilte dies anders und hob den Beschluss zur Ablehnung des Strafbefehls auf. Das Verfahren wirft grundsätzliche Fragen dazu auf, welche strafrechtlichen Risiken IT-Sicherheitsforscher und Penetrationstester tragen und welche rechtliche Relevanz das in der Szene übliche „Responsible Disclosure-Verfahren" hat.[37] Zwischenzeitlich liegt eine Entscheidung des AG Jülich in der Hauptsache vor.[38] Nach Auskunft des AG Jülich ist hiergegen Berufung eingelegt worden.

Das AG Jülich hielt den IT-Dienstleister für strafbar, eine Rechtsauffassung die die Autoren aus diversen Gründen nicht teilen.[39] Bereits die technischen Feststellungen im Urteil sind dünn: Der Einsatz von Datenbanktools wie PHPMyAdmin soll Hacking sein, obwohl das Tool üblicherweise Anfängern die Bedienung der Datenbank erleichtern soll. Außerdem wertet das Gericht den Einsatz einfacher Texteditoren als „Überwinden einer Sicherung". Der Anbieter habe zwar fahrlässig gehandelt, weil er das Passwort in den Programmcode fest (im Klartext!) einprogrammiert hat, dies wirke sich aber allenfalls strafmildernd und nicht strafbefreiend aus. Straffrei sei das Auslesen eines Passworts nur dann, wenn es sich um ein „werksseitiges, standardisiertes" Passwort handle. Diese Formulierung ist aus mehrfachen Gründen unpassend: „Standardisiert" im eigentlichen Sinn ist etwas, das einem Standard im Sinne einer technischen Norm entspricht. Dies liegt hier aber gerade nicht vor, die Begriffswahl des Gerichts ist insoweit irreführend. Das Gericht bezieht sich dabei auf die Kommentierung von *Eisele*,[40] der mit einem „werksseitig standardisiertem Passwort" den Fall meint, dass ein Gerät mit dem – änderbaren – Passwort „0000" an den Nutzer ausgeliefert wird. Wenn der Nutzer ein solches „werksseitiges, standardisiertes" Passwort nicht ändert, liegt nach *Eisele* beim Nutzer keine „besondere Sicherung" i. S. d. § 202a StGB vor. Beim AG Jülich liegt der Fall aber anders: Der Hersteller hat werksseitig ein festes Passwort vergeben, das im Programmcode im Klartext enthalten, für alle Nutzer gleich und unveränderbar ist. Das Abgrenzungskriterium „werksseitig standardisiert" ist damit für den vorliegenden Fall nicht tauglich. Eine Sicherung liegt nur vor, wenn sie „objektiv geeignet" ist (BT-Drs. 16/3656, S. 10). Ein Passwort an sich mag zwar ein Sicherungsmittel sein, doch muss es dafür geheim sein und bleiben. Steht es im Klartext in einer Datei, die – wie hier – an alle Kunden gleichermaßen ausgeliefert wird, ist es das nicht mehr.

Offen ist auch, wie ein so schwerwiegender Kunstfehler wie das feste, unveränderliche Hinterlegen eines Passwortes in einem Programm vom Gericht nur als fahrlässig eingestuft wird. Ein solches Vorgehen ist seit den 1980er Jahren nicht mehr Stand der Technik, verpönt und nach Auffassung der Autoren mindestens grob fahrlässig oder schlechterdings Pfusch.

33 BGH, 2. 3. 2022 – 5 StR 457/21, K&R 2022, 433 (bestätigt durch BGH, 8. 8. 2023 – 6 StR 243/23); dazu *Deusch/Eggendorfer*, K&R 2022, 404 ff.; Nach wie vor finden aufgrund der Encrochat-Datenlage Ermittlungen statt, z. B. am 10. 1. 2024 in Berlin: https://www.berlin.de/polizei/polizeimeldungen/2024/pressemitteilung.1403694.php.

34 BVerfG, 9. 8. 2023 – 2 BvR 558/22 (zu BGH 6 StR 639/21); offen dagegen noch 2 BvR 684/22 (zu BGH 5 StR 457/21, K&R 2022, 433 ff.) und 2 BvR 684/22, 2 BvR 1832/22, 2 BvR 2143/22, 2 BvR 64/23 und 2 BvR 1008/23.

35 Schlussanträge der Generalanwältin *Ćapeta* vom 26. 10. 2023 zum EuGH-Verfahren C-670/22 (https://curia.europa.eu/juris/document/document.jsf;jsessionid=EEF3F45D476085A9ADBA8A86C66FF78D?text=&docid=279144&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=100225).

36 Dazu auch mit interdisziplinären Aspekten zum Encrochat-Komplex sowie mit Angaben zum Stand der Rechtsprechung die Tagungsbeiträge in *Pfeffer* (Hrsg.), Policing Crime Chat Networks, Lessons Learned from the Encrochat-Operation, Schriftenreihe der Forschungsstelle Europäisches und Deutsches Sicherheitsrecht (FEDS), Band 6, erscheint März 2024; in diesem Zusammenhang ist auch die Feststellung von *Rückert/Meyer-Wegener/Safferling/Freiling*, JR 2023, 366 ff. bemerkenswert, wonach bislang die Sicherung und Auswertung derartiger elektronischer Daten durch die Strafverfolgungsbehörden ungeregelt ist. Dabei geht es insbesondere um die Frage, wie es sichergestellt ist, dass die Daten, die in einer Ermittlungsmaßnahme gewonnen werden, unter Wahrung der Authentizität und der Integrität in eine Verwendung im Strafprozess überführt werden können.

37 LG Aachen, 27. 7. 2023 – 60 Qs 16/23, K&R 2023, 693; dazu *Deusch/Eggendorfer*, K&R 2023, 649 ff.

38 AG Jülich, 17. 1. 2024 – 17 Cs-230 Js 99/21-55/23, K&R 2024, 298 ff.

39 *Deusch/Eggendorfer*, K&R 2023, 649 ff.

40 *Schönke/Schröder*, StGB, Kommentar, 30. Aufl. 2019, § 202a Rn. 14.

Das Gericht kommt damit im Widerspruch zu relevanten Teilen der Literatur[41] (allerdings unter Berufung auf das LG Aachen und den BGH) in Abschnitt IV der Urteilsgründe zum Ergebnis, dass nur der erkennbare Geheimhaltungswille des Anbieters zähle, nicht aber die Effektivität der Maßnahmen zur Geheimhaltung. Fraglich ist aus Sicht der Autoren allerdings, ob ein objektiv erkennbarer Geheimhaltungswille überhaupt bestehen kann, wenn Daten im Klartext in einem an jedermann übermittelten und mit einfachsten Mitteln auszulesenden Programmcode eingetragen werden. Nicht nachvollziehbar ist daher die Annahme des Gerichts, auch die Anwendung des Texteditors verwirkliche den Tatbestand des § 202a StGB.[42]

Im vorletzten Textabsatz von Abschnitt IV der Urteilsgründe bringt das Gericht dann technische Sachverhalte durcheinander: Das Gericht wirft dem Angeklagten vor, er habe mit dem „Tool N" eine Software eingesetzt, mit der man sowohl Texte editieren als auch SQL-Datenbanken verwalten könne. Mit dem „Tool N" als Texteditor habe er das Passwort aus dem Programmcode ausgelesen. Dann habe er das Passwort genutzt, um die betroffenen Daten aus der MySQL-Datenbank des Anbieters „MS" auszulesen. Deshalb sei das Auffinden des Passwortes und die Überwindung des damit verbundenen Schutzes aber nicht „für jedermann ohne weiteres möglich", sondern erfordere eine spezielle Software und zumindest Grundkenntnisse über die Bedeutung und Funktion von Datenbanksprachen, über die ein technischer Laie nicht verfüge.

Genau diese Schlussfolgerung ist allerdings zu kritisieren. Der Angeklagte hat den kompilierten Programmcode der lokalen Software-Komponente von „MS" schlicht in dem Texteditor „N" geöffnet. Hierfür sind keine SQL-Kenntnisse notwendig. Damit hat der Angeklagte das Programm weder dekompiliert noch Spezialsoftware genutzt. Er hat lediglich auf seinem PC den Befehl „Öffnen mit" ausgewählt. Dann hat er eine Zeichenfolge gesehen, die sich – weil Klartext – von der übrigen Darstellung des Programmcodes abgehoben hat – wie die späteren Versuche des Angeklagten zeigten, handelte es sich dabei um das Passwort. Auch dazu ist keine SQL-Kenntnis und keine Spezialsoftware notwendig. Die im Texteditor gelesene Zeichenfolge hat der Angeklagte dann testweise beim Einloggen in die MySQL-Datenbank des „MS" eingegeben. Dabei hat er festgestellt, dass dieses Passwort nicht nur Zugriff auf die Kunden seines Auftraggebers vermittelt. Den Autoren erschließt sich nicht, welche Spezialkenntnisse dazu notwendig waren, insbesondere welche „Grundkenntnisse über die Bedeutung und Funktion von Datenbanksprachen" dazu relevant waren. Insbesondere das Bildschirmfoto im Blogbeitrag zeigt, dass der Angeklagte grafische Tools eingesetzt hat, die Kenntnisse von Datenbanksprachen unnötig machen sollen[43]. Das Urteil offenbart auch nicht, ob das Gericht zu dieser Frage einen Sachverständigen hinzugezogen hat, was sinnvoll gewesen wäre, zumal die Urteilsgründe die Funktionen eines Texteditors und einer SQL-Datenbank nicht zutreffend einordnen.

Aus Sicht der Autoren stünde der Gedanken an einen Geheimhaltungswillen erst dann im Raum, wenn der Entwickler wenigstens mit untauglichen Methoden, wie z. B. XOR, ROT13 oder einem einfachen Cäsar-Chiffre, verschlüsselt hätte. Die wären zwar nach heutigen kryptographischen Standards völlig unsicher, könnten aber möglicherweise ein (schwaches) Indiz für einen Geheimhaltungswillen darstellen.

Interessant ist, dass das Gericht ein Vorgehen nach dem „Responsible Disclosure" für strafmildernd hielt, vorliegend aber feststellt, dass der Angeklagte sich nicht an die maßgeblichen Regelungen gehalten habe, da er vor dem Anbieter den Blogger unterrichtet habe, der über die Lücke berichtet habe. Unbewertet lässt das Gericht, dass die Veröffentlichung durch den Blogger erst stattfand, nachdem der Anbieter es gegenüber dem Angeklagten ablehnte, die Lücke zu beheben. Nach der Praxis des „Responsible Disclosure" führt das zur Veröffentlichung der Lücke. Bei richtiger Anwendung kann das „Responsible Disclosure"-Verfahren sogar eine rechtfertigende Nothilfe begründen, die einer Strafbarkeit entgegensteht.[44]

Das Ergebnis des Verfahrens ist geradezu grotesk: Der Anbieter hat mit dem Klartext-Passwort eine Gefährdung geschaffen und hat keine rechtlichen Konsequenzen zu tragen. Der Angeklagte, der dem Anbieter die Lücke gemeldet hat, wird dagegen bestraft. Die Praxis zeigt leider allzu oft, dass derartige Lücken gerade nicht gemeldet, sondern im Darknet zu kriminellen Zwecken verkauft und dann gegen unzählige IT-Nutzer eingesetzt werden.

Auch deshalb ist die Reform der sogenannten „Hackerparagrafen" (§§ 202a ff. StGB) notwendig, die das Bundesjustizministerium (BMJ) für die erste Jahreshälfte 2024 angekündigt hat. Dabei hat das BMJ auf den aktuellen Koalitionsvertrag verwiesen, wonach das Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren legal durchführbar sein soll.[45] Damit dürfte das „Responsible Disclosure"-Verfahren gemeint sein.

IV. Fazit und Blick in die Zukunft

Das Recht der IT-Sicherheit ist in höchstem Maße volatil. Bislang lassen sich nur schwer konsequente Linien in der Gesetzgebung und Rechtsprechung skizzieren. In der Rechtsanwendung und IT-Nutzung sind die legislativen und judikativen Entscheidungen gleichwohl hoch relevant, denn sie sind dafür maßgeblich, welche IT-Sicherheitsmaßnahmen getroffen werden müssen, welche aufgrund rechtlicher Grenzen unzulässig sind und wer die Risiken in Schadensfällen trägt. Wünschenswert wäre dabei, dass technische Sachverhalte in den Verfahren genauer ergründet werden, damit die Entscheidungen die technischen Rahmenbedingungen besser berücksichtigen.

Dr. Florian Deusch

ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter in Ravensburg. Er ist zudem als Datenschutzbeauftragter tätig.

Prof. Dr. Tobias Eggendorfer

ist Professor für Sicherheit in verteilten Anwendungen an der TH Ingolstadt, davor war er als Abteilungsleiter „Sichere Systeme" an der Agentur für Innovation in der Cybersicherheit für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT-Berater und Datenschutzbeauftragter tätig.

41 *Kipker*, MMR 2023, 866, 868.

42 Im Beitrag *Deusch/Eggendorfer*, K&R 2023, 64 ff. zeigen die Autoren mit konkreten Beispielen, wie einfach das Auslesen ohne Zusatzwerkzeuge möglich ist.

43 https://wortfilter.de/warnung-datenleck-beim-jtl-partner-modern-solution-gmbh-co-kg/.

44 *Deusch/Eggendorfer*, K&R 2023, 649, 655.

45 Abschnitt III des Eckpunktepapiers des Bundesministeriums der Justiz zur Modernisierung des Strafrechts vom November 2023 (https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2023_Modernisierung_Strafgesetzbuch.html?nn=110490); lesenswert dazu auch *Schneider*, Kriminalistik 2023, 433 ff.