Jessica Kriegel, Jubin Dejam, Hanno Durth, Florian Franke, Wolfram Hemkens, Sebastian Rothweiler

Zur Strafbarkeit des Zugriffs auf passwortgeschützte Bilder

Simulationsstudie für mehr Rechtssicherheit in der Cybersicherheitsforschung

Das Cybersicherheitsrecht in Deutschland hat in den letzten Jahren einige Modernisierungen erfahren, bietet jedoch Cybersicherheitsforschenden weiterhin keine klaren Handlungsvorgaben. Forschende sehen sich mit erheblichen rechtlichen Unsicherheiten konfrontiert, was die Forschung einschränkt. Vor diesem Hintergrund führt das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE eine mehrjährige Simulationsstudie durch, um mehr Orientierungspunkte zur Rechts-konformität von Forschungsaktivitäten zu entwickeln.

Jessica Kriegel

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie und am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.
E-Mail: jessica.kriegel@sit.fraunhofer.de

Jubin Dejam

ist Staatsanwalt in der Staatsanwaltschaft Frankfurt am Main.

Hanno Durth

ist Rechtsanwalt in der Anwaltskanzlei Kipper Durth Schott PartGmbB in Darmstadt.

Florian Franke

ist Richter, derzeit am Oberlandesgericht Frankfurt am Main.

Wolfram Hemkens

ist Rechtsanwalt in der Anwaltskanzlei HEMKENS in Krefeld.

Sebastian Rothweiler

ist Richter am Amtsgericht Frankfurt am Main.

1 Hintergrund der Simulationsstudie[1]

Cyberangriffe in Deutschland nehmen stetig zu[2] und bedrohen die öffentliche Verwaltung, Unternehmen und die Zivilbevölkerung. Vor diesem Hintergrund wird es immer wichtiger, durch Cybersicherheitsforschung neuartige Cyberangriffsmethoden und Schwachstellen frühzeitig zu erkennen und Gegenmaßnahmen abzuleiten.

Bereits im Rahmen der ersten simulierten Gerichtsverhandlung, die am 17. September 2024 am Fraunhofer Institut für Sichere Informationstechnologie SIT in Darmstadt durchgeführt wurde, konnte aufgezeigt werden, dass sich Cybersicherheitsforschende regelmäßig in einem rechtlichen Graubereich bewegen, da das Risiko besteht, dass ihre Forschungsaktivitäten mit den Handlungen böswilliger Cyberkrimineller gleichgesetzt werden. Durch diesen rechtlichen Graubereich entsteht wiederum ein Spannungsfeld, in dem Forschende einerseits wissenschaftliche Erkenntnisse sammeln wollen, um für ein hohes Maß an Cybersicherheit in der Bevölkerung zu sorgen, andererseits aber fürchten müssen, für ihre Forschungsaktivitäten strafrechtlich belangt zu werden.[3]

An diesem Befund hat sich seitdem nichts geändert. Vor diesem Hintergrund haben es sich Rechtswissenschaftler des Nationalen Forschungszentrums für angewandte Cybersicherheitsforschung ATHENE auch in diesem Jahr zur Aufgabe gemacht, die

1 Die diesem Beitrag zugrundeliegenden Forschungsarbeiten wurden vom BMFTR und vom HMWK im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Der Beitrag gibt die persönliche Meinung der Autoren wieder.

2 *BSI*, Die Lage der IT-Sicherheit in Deutschland, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5.

3 Details hierzu vgl. Kriegel et al, DuD 2024, S. 769 f.

rechtlichen Rahmenbedingungen der Cybersicherheitsforschung genauer zu untersuchen, mögliche Rechtsunsicherheiten aufzuzeigen und diese im Rahmen von Simulationsstudien zu adressieren. Ziel ist es, durch ein weiteres Urteil des Simulationsgerichts entscheidende Wegweiser für Bereiche der Cybersicherheitsforschung zu geben, die mit besonders hoher Rechtsunsicherheit belastet sind.

2 Die zweite simulierte Gerichtsverhandlung im Überblick

Simulationsstudien sind simulierte Gerichtsverhandlungen mit echten Strafrichtern, Staatsanwälten, Strafverteidigern und Sachverständigen, die bezwecken, für einen fiktiven, aber realitätsnahen Fall ein simuliertes Gerichtsurteil zu erzielen. Die simulierte Gerichtsverhandlung selbst folgt einem realitätsgetreuen Ablauf, bei dem Komparsen die Rollen von Angeklagten und Zeugen übernehmen.[4]

Im Rahmen der ersten simulierten Gerichtsverhandlung wurde im Jahr 2024 über die rechtliche Zulässigkeit einer fiktiven Forschungsaktivität entschieden, im Rahmen derer es insbesondere um die Strafbarkeit von Datenfunden im Darknet ging.[5] Aufbauend auf dieser ersten simulierten Gerichtsverhandlung diskutierten im Rahmen der zweiten simulierten Gerichtsverhandlung, die am 27. August 2025 in den Räumlichkeiten des Fraunhofer-Instituts für Sichere Informationstechnologie SIT in Darmstadt durchgeführt wurde, ein Richter, ein Staatsanwalt und zwei Strafverteidiger (unter weiterer Beteiligung eines IT-Sachverständigen sowie von fünf Statisten als Angeklagte und weitere Zeugen) auf Basis einer fiktiven Forschungsaktivität darüber, welche Reaktionen von Cybersicherheitsforschenden zulässig sind, wenn sie den Verdacht haben, dass (sensible) personenbezogene Daten unzureichend vor Zugriffen geschützt sind.

2.1 Der fiktive Fall[6]

Am späten Nachmittag des 12. Mai 2024 wird der Bruder von Cybersicherheitsforscher A nach einem brutalen Überfall schwer im Gesicht verletzt. A begleitet seinen Bruder am nächsten Tag zu einer nahegelegenen Opferberatungsstelle, wo die Personalien des Bruders aufgenommen und Fotos von den Verletzungen angefertigt werden. Der Bruder von A erhält per E-Mail eine Nachricht von der Opferberatungsstelle, in der ihm vier individuelle Download-Links zur Verfügung gestellt werden, über die er die vier angefertigten Fotos abrufen kann. Um die Links öffnen zu können, muss er ein Passwort eingeben. Dieses Passwort wurde ihm von der Opferberatungsstelle mitgeteilt. Es basiert auf dem Datum der Fotoaufnahme und lautet: „42025031-opferSCHUTZorga“. Da der Bruder des A die Fotos nicht selbst einsehen möchte, bittet er A, die Fotos zu sichten. Dabei fällt A auf, dass die Links gewisse Regelmäßigkeiten aufweisen:

- https://simulations-opferschutzorga.de/134D8811,
- https://simulations-opferschutzorga.de/134D8812 (usw.)

A erkennt, dass das Datum der Aufnahme als Hexadezimalwert in jeder URL auftaucht und sich daran eine fortlaufende Zahl anzuschließen scheint. Das Passwort lässt sich dadurch mit geringem Aufwand aus der URL ableiten. Das erkennbare Muster könnte es ermöglichen, durch gezielte Variationen weitere gültige Links mitsamt den Passwörtern zu ermitteln und so unberechtigt auf Fotos anderer Betroffener zuzugreifen.

Um mit seinen Kollegen zu besprechen, ob es sich hierbei tatsächlich um eine cybersicherheitstechnisch relevante Angriffsstelle handeln könnte, leitet A die Mail mit Zustimmung seines Bruders an seine berufliche Mail-Adresse weiter.

Am nächsten Tag (14. Mai 2024) zeigt A die Links seinen Kollegen B und C am Y-Institut, einer Forschungseinrichtung für Cybersicherheit. B und C teilen die Einschätzung von A. B erachtet den Fund als so kritisch, dass sie ausprobieren möchte, ob sie tatsächlich Zugriff auf Fotos anderer Betroffener erhalten kann. Sie argumentiert, dass eine tatsächliche Überprüfung der möglichen Schwachstelle vorab erforderlich sei, um ihr volles Ausmaß zu verstehen und effektive Sicherheitsmaßnahmen empfehlen zu können. A schließt sich dem Vorschlag der B an. C beteiligt sich an der Diskussion nur zurückhaltend und äußert sich ab der Entscheidung von A und B, das Ausmaß der Schwachstelle zu testen, nicht mehr.

Am darauffolgenden Tag (15. Mai 2024) probieren A und B am Rechner der B aus, ob sie Zugriff auf Fotos anderer Gewaltopfer erhalten können. Beide Forscher wissen, dass sie ohne ausdrückliche Erlaubnis der Betroffenen oder der Beratungsstelle handeln und dass sie durch ihr Vorgehen unautorisiert auf personenbezogene Daten zugreifen, gehen aber davon aus, dass ihr Vorgehen im Rahmen legitimer Sicherheitsforschung gerechtfertigt sein sollte. C ist zwar ebenfalls anwesend, übernimmt aber keine aktive Rolle.

Es ist tatsächlich möglich, durch gezielte Variation der URL auf weitere „Fotoreihen“ von betreuten Opfern der Opferberatungsstelle zuzugreifen. Konkret gelingt A und B der Zugriff auf fünf Fotoreihen aus fünf aufeinanderfolgenden Jahren. Bei allen fünf Fällen ließ sich das Passwort direkt aus der jeweiligen URL ableiten (Datum in anderer Reihenfolge plus „-opferSCHUTZorga“). Um einschätzen zu können, wie groß der zugreifbare Datenbestand ist, entscheiden A und B gemeinsam darüber, weiterzusuchen. So gelingt es ihnen, auf fünf weitere „Fotoreihen“ zuzugreifen, bis sie insgesamt zehn Fotoreihen aus zehn verschiedenen Jahren gesichtet haben. A, der den Rechner bedient, lädt die Fotos aller gesichteten Fotoreihen herunter und legt sie nach gemeinschaftlicher Entscheidung mit B in eine Dateiablage ihres aktuellen Forschungsprojektes ab, um sie mit den Mitarbeitenden ihrer Forschungsgruppe (drei weitere Wissenschaftler) teilen zu können und zu diskutieren, wie sie mit diesem Fund umgehen sollen. Ihnen ist bewusst, dass es sich bei den Fotos um sehr sensibles Material handelt und dass die Speicherung in einem gemeinsamen Ordner kritisch sein könnte. C hält sich während der gesamten Zeit im Hintergrund und greift weder bestätigend noch abwehrend ein.

Im Rahmen der Diskussion mit den anderen Wissenschaftlern (am 21. Mai 2024) entscheiden alle Anwesenden (alle sechs Wissenschaftler der Forschungsgruppe), dass sie sich in einer Mail an die Opferberatungsstelle wenden, ihnen zum Beweis der Schwachstelle einen Screenshot der heruntergeladenen Fotos

4 Details zum Simulationsstudienablauf: Kriegel et al, DuD 2024, S. 769 f.

5 Details hierzu vgl. Kriegel et al, DuD 2024, S. 769 f.

6 Dieser Sachverhalt sowie die darin vorkommenden Personen sind frei erfunden. Er dient ausschließlich der Veranschaulichung der Herausforderungen, denen sich Cybersicherheitsforscher in ihrer Arbeit gegenübersehen, und dessen Entscheidung durch das simulierte Simulationsgericht soll eine erste, vorsichtige Einschätzung zur Rechtskonformität der beschriebenen Forschungsaktivitäten ermöglichen.

übersenden und Empfehlungen unterbreiten, wie sie die bisherigen betreuten Opfer nachträglich vor Angriffen auf die Fotodatenbank schützen und diese Angriffe für zukünftige Opfer vermeiden können. Die Nachricht verschickt A am 21. Mai 2024 per verschlüsselter E-Mail. In dieser setzt er seine Kollegin B in cc und beendet die Grußformel mit den Namen von B und ihm selbst. Da sich C nicht aktiv an der Suche nach weiteren Fotos beteiligt hat, wurde sie nicht in cc gesetzt.

Die Opferberatungsstelle nimmt die Meldung zur Kenntnis, wertet das über den Screenshot ersichtliche Herunterladen der Fotos jedoch als unbefugten Zugriff auf personenbezogene Daten. Nach interner Prüfung kommt sie zu dem Schluss, dass A und B möglicherweise eine Straftat begangen haben. Daher erstattet die Opferberatungsstelle Strafanzeige gegen A und B.

Die Polizei und die Staatsanwaltschaft überprüfen daraufhin die Handlungen von A und B im Detail. Nach Abschluss der Ermittlungen erhebt die Staatsanwaltschaft Anklage gegen A und B wegen gemeinschaftlich begangener Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen gemäß § 201a Abs. 1 Nr. 5 StGB i.V.m. § 25 Abs. 2 StGB sowie wegen gemeinschaftlich begangenen Ausspähens von Daten gemäß § 202a StGB i.V.m. § 25 Abs. 2 StGB. C hingegen wird nicht angeklagt.

2.2 Umfassende Prüfung

Ziel der Simulationsstudie war es, die Straffreiheit oder Strafbarkeit der fiktiven Angeklagten A und B nach dem StGB zu bestimmen.[7] Um einen möglichst umfassenden Überblick über die „Dos" and „Don´ts" der Cybersicherheitsforschung im Rahmen der Simulationsstudie zu erhalten, wurde das Simulationsgericht gebeten, neben der Frage der Strafbarkeit des Verhaltens der Angeklagten A und B und der Straffreiheit der C auch auf alle im Rahmen der Simulationsvorbereitung aufgeworfenen Rechtsfragen und Probleme einzugehen, die im Folgenden dargestellt werden.

3 Die simulierte Entscheidung

Das Gericht kam hinsichtlich des Zugriffs auf die Fotos des Bruders von A zu einem Freispruch der Forscher A und B aufgrund der Einwilligung des Bruders. Hinsichtlich des Zugriffs auf die Fotos fremder Betroffener der Opferschutzorganisation wurden die Forscher A und B vom Gericht unter Vorbehalt einer Geldstrafe von 30 Tagessätzen zu je 100 Euro verwarnt. Innerhalb eines Jahres müssen sie zudem jeweils 500 Euro an die Opferberatungsstelle zahlen. Bewähren sie sich in dieser Zeit und begehen keine weiteren Straftaten, bleibt es bei der Verwarnung.

In seiner Entscheidung ging das Gericht auf folgende Fragen ein:

1. Unter welchen Voraussetzungen sind „personalisierte", nicht öffentlich bekannte Links, die nur durch direkte Eingabe in den Browser zugänglich sind – vergleichbar mit Freigabelinks bei Cloud-Diensten wie OneDrive –, als Zugangssicherung im Sinne des § 202a StGB zu werten? Kann ein Passwort eine eigenständige Zugangssicherung im Sinne des § 202a StGB darstellen, wenn es aus dem Link selbst herausgelesen oder zumindest in ähnlicher Form abgeleitet werden kann? Wäre ein Passwort wie im Sachverhalt (ohne das „Zusatzkonstrukt Link") eine Zugangssicherung im Sinne des § 202a StGB?
2. Wie ist das Abspeichern von sensiblem oder potenziell verletzendem Material in einem gemeinsamen Projektordner rechtlich zu bewerten, wenn dadurch das Material weiteren Personen zugänglich gemacht wird? Wird hierdurch der § 201a Abs. 2 StGB erfüllt? Welche rechtlichen Leitplanken sind für die Handhabung von Materialien zu beachten, die möglicherweise Persönlichkeitsrechte verletzen oder Ansehensverlust verursachen könnten, insbesondere im Hinblick auf Darknet-Funde? Wie müssen Forschende mit Materialien (z.B. Bild- oder Videodateien) umgehen, die sie aus dem Darknet erhalten, um sicherzustellen, dass deren Speicherung den rechtlichen Vorgaben entspricht und die befugte Weitergabe oder Zugänglichmachung verhindert wird?
3. Welche Voraussetzungen müssen erfüllt sein, damit A und B als Mittäter im Sinne des § 25 Abs. 2 StGB anzusehen sind? Welche konkreten Handlungen und Absichten und welches Maß an Zusammenarbeit sind erforderlich, damit eine gemeinsame Tatbegehung angenommen werden kann? Welche rechtlichen Leitplanken sind für die Zurechnung einer strafbaren Handlung im Kontext der Forschung maßgeblich, insbesondere im Hinblick auf die gemeinsame Zielsetzung, arbeitsteiliges Vorgehen und den Austausch von Ressourcen oder Infrastruktur? In welchem Maße kann das Handeln des einen Forschers, das möglicherweise strafrechtlich relevant ist, dem anderen zugerechnet werden, wenn er z.B. nicht aktiv eingreift, aber an der Planung oder Durchführung des Projekts beteiligt war?
4. Kann die bloße Anwesenheit von C während der Tatbegehung als Beihilfe im Sinne des § 27 StGB gewertet werden? Inwiefern kann das Unterlassen eines Einschreitens als psychische Unterstützung und damit als strafbare Beihilfe ausgelegt werden?

3.1 Entscheidung zu Frage 1

Zwar könnte man nach einem ersten Blick auf die Vorschrift des § 202a Abs. 1 StGB zu dem Schluss kommen, dass „personalisierte Links" im vorgenannten Sinne keine besondere Zugangssicherung im Sinne dieser Vorschrift darstellen. Dem ist jedoch nicht so. Denn nach dem Sinn und Zweck der Vorschrift ist maßgeblich, ob es sich bei der Zugangssicherung um eine Vorkehrung handelt, die den Zugang Unbefugter zu den geschützten Daten *typischerweise* verhindert oder zumindest erheblich erschwert. Sie muss hierbei nicht allein und ausschließlich dem Schutz der Daten dienen.[8] Vielmehr muss der Berechtigte durch die Sicherung „sein spezielles Interesse an der Geheimhaltung dokumentieren".[9] Dies trifft auf personalisierte Links wie im hiesigen Fall zu:

Für unbeteiligte Dritte, das heißt insbesondere solche Personen, denen die genaue Link-Kennung nicht mitgeteilt worden ist, sind die unter der Link-Kennung eingestellten Daten *typischerweise* nicht zugänglich. Zugleich dokumentiert der Host des Link-Inhalts über die nicht ganz unerhebliche Komplexität der Link-Adresse auch sein *typisiertes* Geheimhaltungsinteresse an den dort abgelegten Daten. Hieran ändert auch nichts, dass diese Art der Zugangssicherung für Eingeweihte oder Experten leicht zu über-

7 Gegenstand der Simulationsverhandlung war die Strafbarkeit nach dem deutschen Strafgesetzbuch. Ggfs. auftretende datenschutzrechtliche Fragen, insbesondere zur DSGVO, blieben unberücksichtigt und waren kein Gegenstand der Simulationsverhandlung.

8 Graf in: MüKo StGB, 5. Auflage 2025, § 202a, Rn. 39 m.w.N.

9 BGH, Beschluss vom 13.05.2020 – 5 StR 614/19 in BeckRS 2020, 12264.

winden sein mag, da es diesen nur unter Einsatz ihrer besonderen Fähigkeiten und mit Blick auf den Querschnitt der Bevölkerung *ausnahmsweise* möglich ist.
Ein Passwort kann nicht nur im Einzelfall eine eigenständige Zugangssicherung im Sinne des § 202a StGB darstellen, sondern dürfte den Regelfall einer solchen Zugangssicherung abbilden. Dabei sind angesichts der gebotenen, vorgezeichneten „abstraktgenerellen Betrachtungsweise“[10] keine übermäßig hohen Anforderungen an die Stärke des Passworts zu stellen. In den Worten des Bundesgerichtshofs ist es „für das geschützte Rechtsgut […] unerheblich, ob die Sicherung von Daten vor unberechtigtem Zugang schnell oder langsam, mit viel oder wenig Aufwand überwunden wird.“ Allenfalls dann, wenn ein Passwort derart schwach ist, dass die Durchbrechung des Schutzes für jedermann ohne weiteres möglich wäre, mag die Grenze der Strafbarkeit erreicht sein. Dies ist hier in der vorliegenden Konstellation ersichtlich nicht der Fall:
Im vorliegenden Fall beruht die Ermittlung des Passwortes im Kern darauf, dass die Experten erkennen, dass das Datum der Aufnahme als Hexadezimalwert in jeder URL auftaucht. Hierbei handelt es sich um Fachwissen, welches sie durch ihre Ausbildung und ihren Beruf spezifisch erlernt haben und nicht um Allgemeinwissen, welches in breiten Bevölkerungsschichten bekannt ist.
Ein Passwort mit der hier dargestellten Komplexität („42025031-opferSCHUTZorga“), bestehend aus Zahlen, Buchstaben in Groß- und Kleinschreibung sowie Sonderzeichen, dürfte jedenfalls die *strafrechtliche* Grenze einer hinreichenden Zugangssicherung im Sinne des § 202a StGB deutlich überschreiten. Wobei dies nichts daran ändert, dass andere Regelungswerke, allen voran das Datenschutzrecht mit spezifischen Vorschriften zur Sicherheit der Verarbeitung wie etwa in Art. 32 DSGVO – insbesondere bei sensiblen Daten – engere Grenzen für eingesetzte Passwörter setzen könnten.

3.2 Entscheidung zu Frage 2

Die Frage, wie das Vorgehen von Cybersicherheitsforschenden zu bewerten ist, die auf sensibles Bildmaterial stoßen, insbesondere im Darknet, ist komplex. Eine Strafbarkeit kann sich insbesondere wegen Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen gemäß § 201a Abs. 1 und Abs. 2 StGB ergeben. Durch den Einbau von organisatorischen und technischen Leitplanken kann das Risiko einer Strafbarkeit aber verkleinert werden, wenngleich ein nicht unerhebliches Restrisiko verbleibt. § 201a Abs. 1 und Abs. 2 StGB schützt den Kernbereich des allgemeinen Persönlichkeitsrechts. § 201a Abs. 1 Nr. 1 schützt den höchstpersönlichen Lebensbereich und erfasst vor allem, aber nicht nur, die Bereiche Krankheit, Tod und Sexualität. § 201a Abs. 1 Nr. 2 StGB schützt hilflose Personen davor, durch Bildaufnahmen zur Schau gestellt zu werden. § 201a Abs. 1 Nr. 3 StGB schützt das Persönlichkeitsrecht Verstorbener. Auch das unbefugte Gebrauchen und Zugänglichmachen solcher Bildaufnahmen ist nach § 201a Abs. 1 Nr. 4 StGB strafbar. Unter „Gebrauchen“ fällt nach der Gesetzesbegründung auch das Speichern und Archivieren von unbefugt hergestellten Aufnahmen. Nach § 201a Abs. 1 Nr. 5 StGB ist es schließlich auch strafbar, wenn befugt hergestellte Bildaufnahmen der in den Nummern 1 bis 3 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich gemacht werden und dadurch der höchstpersönliche Lebensbereich der (lebenden) abgebildeten Personen verletzt wird.
Wichtig ist in allen Fällen, dass die abgebildete Person erkennbar sein muss. Es genügt aber, wenn das Opfer sich selbst anhand von Identifizierungsmerkmalen wiedererkennen kann. Das Handeln ist unbefugt, wenn die aufgenommene Person mit dem Herstellen oder Übertragen der Bildaufnahme nicht einverstanden ist. Das bloße Herunterladen der Bilder durch Cybersicherheitsforschende, etwa aus dem Darknet, stellt kein „Herstellen“ im Sinne des Gesetzes dar. Denn dafür wäre die Tatherrschaft über den primären Aufzeichnungsakt erforderlich. Das Herunterladen kann jedoch als „Gebrauchen“ der Bilder gewertet werden, denn nach der Gesetzesbegründung soll auch das Speichern und Archivieren umfasst sein. Da „Gebrauchen“ aber nur bei unbefugt hergestellten Aufnahmen strafbar ist (§ 201a Abs. 1 Nr. 4 StGB), war im vorliegenden Fall das reine Herunterladen noch nicht strafbar. Anders verhält es sich, wenn die Bilder auf einer Abteilungsablage gespeichert werden, auf die auch andere Kollegen Zugriff haben. Dies stellt ein „Zugänglichmachen“ dar, das sowohl bei befugt als auch bei unbefugt hergestellten Aufnahmen strafbar ist (§ 201a Abs. 1 Nr. 4, Nr. 5 StGB).
Zugänglichmachen ist das Verschaffen der Möglichkeit zur Kenntnisnahme durch mindestens einen Dritten. Eine tatsächliche Kenntnisnahme ist nicht erforderlich, ebenso wenig eine Möglichkeit zum „physischen Zugriff“ auf oder gar eine „eigene Verfügungsgewalt“ über die Aufnahme. Das Recht am eigenen Bild wird bereits dadurch verletzt, dass das Bild vor Dritten reproduziert wird. Nicht ausreichend ist hingegen, Dritte nur über die Aufnahme zu unterrichten. Sobald Dateien in Ordnern einer Organisation abgespeichert werden, auf die mindestens eine weitere Person Zugriff hat, liegt daher ein Zugänglichmachen vor. Sollte nur die Person, die die Datei gespeichert hat, Zugriff haben, läge kein Zugänglichmachen vor. Dies könnte zum Beispiel durch entsprechenden Passwortschutz gewährleistet werden.
Der für die Strafbarkeit erforderliche Eventualvorsatz war im Simulationsfall gegeben. Denn die Forschenden hielten es zumindest für möglich, dass sie die geschützten Bilder Dritten zugänglich machten, und nahmen dies billigend in Kauf. Die Forschenden wussten auch, dass die abgebildeten Personen dem Zugänglichmachen nicht zugestimmt hatten und handelten daher „wissentlich unbefugt“ im Sinne von § 201a Abs. 1 Nr. 5 StGB.
Eine Strafbarkeit kann gemäß § 201a Abs. 4 StGB ausgeschlossen sein, wenn die Handlungen in Wahrnehmung überwiegender berechtigter Interessen erfolgen. Dazu zählen Zwecke der Wissenschaft, Forschung oder der Berichterstattung. Forschung umfasst alle Handlungen, die auf dem ernsthaften, planmäßigen und nachprüfbaren Versuch beruhen, Erkenntnisse zu fördern und die Wahrheit zu ermitteln. Die Arbeit von Cybersicherheitsforschenden ist daher grundsätzlich als Forschung im Sinne des § 201a Abs. 4 StGB einzuordnen. Dieser Ausschluss greift aber nur dann, wenn es sich nicht um rein kommerzielle Zwecke handelt und die Verbreitung auf den Nutzungszweck beschränkt ist. Das allgemeine Persönlichkeitsrecht der Abgebildeten ist gegen das Forschungsinteresse abzuwägen. Letztendlich ist eine Einzelfallabwägung vorzunehmen. Wichtig ist jedoch, dass bei einer Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen von Personen, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befinden (§ 201a

10 BGH Beschl. v. 13.5.2020 – 5 StR 614/19, BeckRS 2020, 12264 Rn. 24.

Abs. 1 Nr. 1 auch in Verbindung mit Nr. 5 StGB), eine Abwägung mit der Wissenschaftsfreiheit nicht möglich ist. Ein Zugänglichmachen solcher Bildaufnahmen erfüllt daher selbst bei einem Forschungszweck den Tatbestand und ist damit strafbar.
Es dürfte sich in jedem Fall empfehlen zu dokumentieren, welche Dritten aus welchem Grund Zugang zu den Daten haben. Zugleich sollte dokumentiert werden, im Rahmen welches Forschungsprojekts die Daten erlangt wurden und weshalb eine Speicherung notwendig erscheint. Eine Zugänglichmachung für Dritte, die nicht konkret mit dem Forschungsgegenstand befasst sind, „dient" nicht der Forschung, selbst wenn es sich bei den Dritten auch um Cybersicherheitsforschende handelt. Ebenso dürfte reine wissenschaftliche „Neugier" kein ausreichender Grund für die Speicherung und Zugänglichmachung inkriminierter Dateien seien. Denn auch dann dienen die Handlungen nicht der Wahrnehmung „überwiegender" berechtigter Interessen.

Im Zweifelsfall sollte Rechtsrat eingeholt werden. Ein Ver-botsirrtum nach § 17 StGB, also eine Fehleinschätzung über die Rechtslage, ist nur dann ein Entschuldigungsgrund, wenn er unvermeidbar war. Im vorliegenden Fall hatten es die Sicherheitsforschenden unterlassen, Rechtsrat einzuholen, obwohl ihnen die „Brisanz" des Materials bewusst war. Ein (unvermeidbarer) Verbotsirrtum schied daher aus. Soweit möglich, sollte bereits vor der Speicherung (interner oder externer) Rechtsrat eingeholt werden. In größeren Organisationen dürfte es sich anbieten, vorab verbindliche Vorgehensweisen festzulegen, die die Forschenden dann im Einzelfall zu beachten haben.

In der simulierten Hauptverhandlung wurde lebhaft diskutiert, ob die Speicherung der Bilddateien auf der Abteilungsablage und die damit verbundenen Zugriffsmöglichkeiten noch vom speziellen Nutzungszweck der Cybersicherheitsforschenden umfasst war und ob es zur Zweckerreichung notwendig war, sämtliche Datenreihen auf der Abteilungsablage abzulegen. Wo konkret die Grenze für das berechtigte Interesse zu ziehen ist, lässt sich nur unter Berücksichtigung der jeweiligen Umstände des Einzelfalles entscheiden. Wenn die aufgenommene Person – wie im Falle des Bruders des Sicherheitsforschers – mit der Aufnahme und Verbreitung der Aufnahmen einverstanden ist, ist das Handeln nicht strafbar. Insoweit erfolgte daher am Ende der simulierten Hauptverhandlung ein Freispruch. Das Zugänglichmachen der Bilder von weiteren Tatopfern an andere Sicherheitsforscher im Institut wurde hingegen als strafbar angesehen.

3.3 Entscheidung zu Frage 3

Die Entscheidung des Simulationsgerichts widmete sich zudem der Frage, ob die Cybersicherheitsforscher als Mittäter im Sinne des § 25 Abs. 2 StGB zu qualifizieren sind. Mittäterschaft ist dann anzunehmen, wenn ein Beteiligter nicht bloß fremdes tatbestandsverwirklichendes Tun fördern will, sondern sein Beitrag Teil eines gleichgeordneten, arbeitsteiligen Vorgehens ist. Wesentlich hierfür ist, dass jeder Beteiligte das Tun des anderen als Ergänzung seiner eigenen Handlung begreift, sodass ein einheitliches deliktisches Gesamtgeschehen entsteht.[11] Im vorliegenden Fall hatten sich A und B darauf verständigt, eine mögliche Schwachstelle in einem geschützten Zugangssystem durch gezielte URL-Manipulation herauszufinden. Während A den Rechner bediente und die Bildaufnahmen herunterlud, war B auch maßgeblich an der Entscheidung zur Vorgehensweise, zum Umfang des Tests sowie zur Speicherung der sensiblen Daten beteiligt. Das Gericht wertete diese Rollenverteilung als arbeitsteilig im gleichgeordneten Sinn, da beide Forscher ihre Beiträge in gegenseitiger Ergänzung und in bewusstem Zusammenwirken leisteten. Der Grad des eigenen Interesses am Erfolg der Handlung, nämlich das Aufzeigen der Sicherheitslücke mit dem Ziel deren Beseitigung und deren Dokumentation innerhalb der Forschergruppe, war bei beiden hoch. B hatte nicht nur konkrete fachliche Impulse gegeben, sondern auch maßgeblich auf das Ob und Wie der Tatgestaltung Einfluss genommen. Damit lagen sämtliche Merkmale vor, die nach der Rechtsprechung eine Mittäterschaft annehmen lassen: einen gemeinsamen Tatplan bei arbeitsteiligem Vorgehen, welches von einem Willen zur Tatherrschaft sowie einer strukturprägenden Beteiligung an Planung und Durchführung getragen wird. Keine Rolle spielt auf dieser Ebene, welche Motivation das Handeln der Täter begründet; der vorliegende Fall zeigt die Problematik, dass auch „redliche" Überlegungen und Beweggründe zugunsten der Cybersicherheit eine Strafbarkeit begründen können. Dies ist allenfalls eine Frage der Strafzumessung.

Hervorzuheben ist, dass § 202a StGB ausdrücklich auch das Verschaffen eines Zugangs für einen anderen unter Strafe stellt und den Anwendungsbereich der Mittäterschaft insoweit erweitert: Wer im arbeitsteiligen Verschaffen eines Zugangs zu gesicherten Daten eine tragende Rolle übernimmt, verwirklicht den Tatbestand eigenständig, auch ohne Eigeninteresse am Zugang. Beihilfe kommt nach dieser Struktur nur für solche Beteiligte in Betracht, die nicht an der Verschaffungshandlung selbst beteiligt sind. Für § 201a StGB gilt dagegen, dass die Beteiligungsform nach den allgemeinen Regeln der §§ 25 ff. StGB zu bestimmen ist. Durch das willentliche Ablegen der Bilddateien in einem für weitere Forschende zugänglichen Ordner haben A und B jedenfalls ein bewusstes Zugänglichmachen i.S.d. § 201a Abs. 2 StGB verwirklicht. Die Entscheidung macht deutlich, dass eine Beteiligung in Form der aktiven Planung, Entscheidungsfindung oder Umsetzung eines Forschungsvorhabens, das objektiv tatbestandliches Verhalten beinhaltet, zur Übernahme strafrechtlicher Verantwortung führen kann – und zwar auch, wenn nicht sämtliche Beiträge von einem der (Mit-)täter ausgeführt werden. Die Zurechnung erfolgt nicht lediglich auf Grundlage von Ausführungshandlungen, sondern anhand einer wertenden Gesamtbetrachtung: Entscheidend ist, ob der Beteiligte Tatherrschaft anstrebt oder jedenfalls will, dass sein Beitrag als integraler Bestandteil des gemeinsamen Handelns wirkt. Auch die Mitwirkung in einem arbeitsteiligen Handeln, etwa durch ideengebende Einflussnahme, strukturelle Steuerung, Mitentscheidung über das „Ob" und „Wie" des Vorgehens, kann die Mittäterschaft begründen.

3.4 Entscheidung zu Frage 4

Objektive Voraussetzung für eine strafbare Beihilfe gemäß § 27 Abs. 1 StGB ist einerseits eine vorsätzliche und rechtswidrige Haupttat des Haupttäters und andererseits eine Hilfeleistung des Gehilfen. Der Gehilfe muss parallel hierzu subjektiv einerseits den wesentlichen Unrechtsgehalt der Haupttat erfassen und sich andererseits seiner Hilfeleistung bewusst sein (sog. doppelter Gehilfenvorsatz). Die Hilfe muss entweder die Haupttat ermöglichen oder die Verletzung des Rechtsguts vertiefen. Sie kann physisch

11 Vgl. BGH, Beschluss vom 26.03.2014 – 5 StR 91/14; BGH, Beschluss vom 12.8.2021 – 3 StR 441/20; MüKoStGB/Scheinfeld, 5. Aufl. 2024, StGB § 25 Rn. 2119 m.w.N.

oder psychisch erfolgen. Eine physische Beihilfe wäre etwa die Bedienung der Tastatur oder der Anschluss einer Festplatte zur Datensicherung. Beides ist durch C nicht erfolgt.

Die Bestimmung einer psychischen Beihilfe ist weniger eindeutig. Auch eine psychische Hilfeleistung kann durch aktives Tun oder durch Unterlassen erfolgen. Sie kann beispielsweise aktiv „durch technischen Rat" des Gehilfen oder Bestärkung des Tatentschlusses des Haupttäter erfolgen. Eine bloße Anwesenheit während der Tatbegehung der Haupttäter ist keine psychische Beihilfe durch aktives Tun. Dies gilt selbst bei Kenntnis einer Straftat und deren Billigung. Die Grenze zur Strafbarkeit wird erst überschritten, wenn der Gehilfe dem Haupttäter dies gegenüber vorsätzlich zum Ausdruck bringt, sodass dieser in seinem Tatentschluss bestärkt wird.

C äußert sich ab der Entscheidung des A und B nicht mehr. Sie widerspricht dem Vorhaben zwar nicht, hält sich jedoch im Hintergrund auf, sodass die Tat unabhängig von ihr ausgeführt wurde. Damit liegt keine Beihilfe durch aktives Tun vor.

Wenn die rechtliche Bewertung zu dem Ergebnis gelangt, dass keine strafbare Handlung vorliegt, trotz Anwesenheit des Beschuldigten am Tatort, kommt eine Strafbarkeit durch Unterlassen gemäß § 13 Abs. 1 StGB in Betracht.

Objektive Voraussetzung für eine Strafbarkeit durch Unterlassen ist zunächst eine Rechtspflicht zum Tätigwerden, eine sog. Garantenstellung. Diese liegt vor, wenn der Beschuldigte eine Obhutspflicht für die verletzten Rechtgüter innehat (Beschützergarant) oder eine Sicherungspflicht für bestimmte Gefahrenquellen (Überwachungsgarant).[12]

C hat keine Verbindung zu den Datenberechtigten, sodass sie keine Beschützergarantenstellung innehatte. Sie hatte auch keine Pflicht, A und B als Gefahrenquellen zu überwachen. Sie hörte sich lediglich die Pläne der beiden an, hierin liegt kein vorangegangenes pflichtwidriges Vorverhalten. Sie schaffte keine adäquate Gefahr für die später eingetretene Rechtsgutsverletzung.

Es kann außerdem keine der C mögliche und zumutbare Handlung hinzugedacht werden, sodass der tatbestandsmäßige Erfolg mit an Sicherheit grenzender Wahrscheinlichkeit entfiele. In Betracht käme lediglich eine Information an den Vorgesetzten. Ob dieser wiederum am Ende als Garant zum Handeln verpflichtet gewesen wäre, ist anhand des Sachverhalts nicht zu bestimmen.

C hat sich demnach nicht wegen Beihilfe durch Unterlassen gemäß §§ 202a Abs. 1, 27 Abs. 1, 13 Abs. 1 StGB strafbar gemacht, indem sie es unterließ, gegen A und B einzuschreiten.

12 Fischer, StGB, 71. Auflage 2024, § 13 Rn. 14f.

4 Fazit

Im Rahmen der Cybersicherheitsforschung besteht hohes Maß an Rechtsunsicherheit. Simulationsstudien können die Rechtssicherheit erhöhen, indem sie Forschungsaktivitäten durch ein Simulationsgericht mit Richtern, Staatsanwälten und Strafverteidigern bewerten lassen. Die diesjährige Simulationsstudie hat gezeigt, dass der Zugriff auf passwortgeschützte Bilder durch Cybersicherheitsforschende strafbar sein kann – insbesondere dann, wenn der Zugriff auf die Bilder auch weiteren Cybersicherheitsforschenden ermöglicht wird. Zugleich wurde deutlich, dass die rechtliche Bewertung stets vom Einzelfall abhängt. Insbesondere kann der Einbau von organisatorischen und technischen Leitplanken das Risiko einer Strafbarkeit verkleinern, nicht jedoch ausschließen. Die ATHENE-Simulationsstudie wird weitere Forschungsaktivitäten rechtlich bewerten. Cybersicherheitsforscher sind eingeladen, der Erstautorin Vorschläge über zu verhandelnde Aktivitäten zu unterbreiten.