BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 5
März 2025

Referentenentwurf des Bundesministeriums der Justiz eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts

Mitglieder des Strafrechtsausschusses (Strauda):

RAin Dr. Carolin Arnemann
RA Prof. Dr. Jan Bockemühl
RA Prof. Dr. Alfred Dierlamm
RA Prof. Dr. Björn Gercke
RA Dr. Mayeul Hiéramente (Berichterstatter)
RA Thomas C. Knierim
RA Dr. Daniel M. Krause
RAin Theres Kraußlach
RA Prof. Dr. Holger Matt (Vorsitzender)
RA Prof. Dr. Ralf Neuhaus
RA Prof. Dr. Tido Park
RAin Dr. Hellen Schilling
RA Dr. Jens Schmidt
RAin Dr. Annette von Stetten

Prof. Dr. Dominik Brodowski (Berichterstatter)

RAin Leonora Holling, Schatzmeisterin, Bundesrechtsanwaltskammer

Verteiler:
Bundesministerium der Finanzen
Bundesministerium der Justiz
Bundesministerium des Innern und für Heimat
Justizministerien der Länder
Innenministerien der Länder
Rechtsausschuss des Deutschen Bundestages
Arbeitskreise Recht der Bundestagsfraktionen
Rechtsanwaltskammern
Der Generalbundesanwalt beim BGH
Bundesgerichtshof
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Deutscher Steuerberaterverband
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer
Deutscher Anwaltverein
Deutscher Notarverein
Deutscher Richterbund
Deutscher Juristinnenbund
Bundesvorstand Neue Richtervereinigung
Strafverteidigervereinigungen
Deutsche Strafverteidiger e.V.
Neue Richtervereinigung e.V.
Bund Deutscher Kriminalbeamter
Redaktionen der NJW,
Beck Verlag, Deubner Verlag, Jurion, Juris, LexisNexis,
Otto Schmidt Verlag,
Strafverteidiger,
Neue Zeitschrift für Strafrecht,
ZAP Verlag,
Zeitschrift für höchstrichterliche Rechtsprechung im Strafrecht,
Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht,
wistra - Zeitschrift für Wirtschafts- und Steuerstrafrecht,
Zeitschrift HRR-Strafrecht,
Kriminalpolitische Zeitschrift
FAZ, Süddeutsche Zeitung, Die Welt, Handelsblatt, Tagesspiegel, LTO, Der Spiegel, Focus, Die ZEIT

Die Bundesrechtsanwaltskammer (BRAK) ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten[1] gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

I. Einführung

Die Bundesrechtsanwaltskammer begrüßt den vom Bundesministerium der Justiz am 04.11.2024 als Referentenentwurf vorgelegten „Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrechts“. Wesentliche Zielsetzung des Entwurfes ist es, für die IT-Sicherheitsforschung bestehende Strafbarkeitsrisiken zu reduzieren und damit einer überschießenden Kriminalisierung von gesellschaftlich erwünschtem Verhalten entgegenzuwirken (II.).[2] Daneben soll für besonders schwere Fälle des Ausspähens und Abfangens von Daten ein erhöhter Strafrahmen gelten (III.).

II. Teilweise Reduzierung von Strafbarkeitsrisiken für die IT-Sicherheitsforschung

1. Überschießende Kriminalisierung der IT-Sicherheitsforschung als Problem

Die IT-Sicherheitsforschung muss sich, um Sicherheitslücken in informationstechnischen Systemen aufzuspüren und sodann auf deren Behebung hinwirken zu können, nicht selten derselben Methoden bedienen, die auch Straftäterinnen und Straftäter anwenden.[3] Diese Herangehensweise unterliegt nicht selten einer Strafbarkeit nach § 202a Abs. 1 StGB (Ausspähen von Daten), nach § 202b StGB (Abfangen von Daten) oder § 303a Abs. 1 StGB (Datenveränderung). Dies liegt an den geringen tatbestandlichen Voraussetzungen, aber auch an der extensiven Auslegung, die diese Strafvorschriften durch den BGH erhalten hat und an der praktischen Schwierigkeit, ein Einverständnis aller Berechtigten einzuholen. In Verbindung mit dem strafprozessualen Legalitätsprinzip führt dies zu einem erheblichen Risiko für IT-Sicherheitsforschende, sich strafbar zu machen oder sich zumindest schwerwiegenden strafprozessualen Ermittlungsmaßnahmen ausgesetzt zu sehen.[4] Das wiederum hemmt IT-Sicherheitsforschung, die zum gesellschaftlichen Nutzen gereicht, und stellt im europäischen und internationalen Vergleich einen Standortnachteil für die IT-Sicherheitsforschung dar.

---

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden gewählte männliche Form schließt alle Geschlechter gleichberechtigt ein.

[2] Zur Problemstellung siehe *Balaban u.a.*, Whitepaper zur Rechtslage der IT-Sicherheitsforschung, 2021, abrufbar unter: https://sec4research.de/assets/Whitepaper.pdf; Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht, 2023, abrufbar unter https://doi.org/10.1628/978-3-16-162184-0; *Valerius*, NSW 2024, 303 ff.

[3] *Freiling*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 21 ff.

[4] *Brodowski*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 3 (7 ff.); *Golla*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 3 (7 ff.); *Bao/Zech*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 131 (132 ff.); *Valerius*, NSW 2024, 303 (305 ff.).

Dieses Problem adressiert der vorliegende Referentenentwurf. Er schlägt vor, den Tatbestand des § 202a Abs. 1 StGB durch einen neuen Abs. 3 einzuengen, wenn die Tathandlung erstens „in der Absicht erfolgt, eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems […] festzustellen“ (Nr. 1 Hs. 1), zweitens die Absicht besteht, eine aufgefundene Sicherheitslücke dem „für das informationstechnische System Verantwortlichen, de[m] betreibenden Dienstleister des jeweiligen Systems, de[m] Hersteller der betroffenen IT-Anwendung oder [dem] Bundesamt für Sicherheit in der Informationstechnik“ zu melden (Nr. 1 Hs. 2), und drittens die Vornahme der Tathandlung „zur Feststellung der Sicherheitslücke erforderlich ist“ (Nr. 2). Durch Verweisungen soll dieser Tatbestandsausschluss auch für die Tatbestände des Abfangens von Daten (§ 202b Abs. 2 Alt. 1 StGB-E) und der Datenveränderung (§ 303a Abs. 4 StGB-E) greifen.

2. Zum gewählten Regelungsmodell

Die Bundesrechtsanwaltskammer begrüßt das Ziel einer Entkriminalisierung der IT-Sicherheitsforschung mit großem Nachdruck. Sie schafft zumindest für §§ 202a Abs. 1, 202b und 303a Abs. 1 StGB Rechtssicherheit für Forschende, die durch ihren tatkräftigen Einsatz für die Resilienz von IT-Systemen gegen Angriffe Dritter – einschließlich staatlicher Akteure – einen erheblichen gesellschaftlichen Nutzen leisten. Die Bundesrechtsanwaltskammer gibt allerdings zu bedenken, dass auch bei der Verabschiedung des vorgelegten Entwurfs für die IT-Sicherheitsforschung insbesondere im Urheberstrafrecht erhebliche Strafbarkeitsrisiken verbleiben,[5] die Strafvorschrift des § 202c StGB enger gefasst werden könnte und dass auch zivilrechtliche Ansprüche dringend gebotene IT-Sicherheitsforschung hemmen können.[6]

Anders als alternative Regelungsmodelle (etwa das einer nachträglichen Straffreistellung, wenn eine Sicherheitslücke über einen bestimmten Meldeweg gemeldet wird) bietet der vom Bundesministerium der Justiz vorgeschlagene Tatbestandsausschluss die nötige Rechtssicherheit für die IT-Sicherheitsforschung und erweitert daher z.B. Möglichkeiten, auch an staatlichen oder staatlich geförderten Einrichtungen rechtssicher IT-Sicherheitsforschung zu betreiben.[7] Wie der Referentenentwurf überzeugend begründet, entstehen selbst in atypischen Konstellationen – etwa einem nachträglichen Wegfall der privilegierenden Absicht (siehe sogleich) – „keine unvertretbaren Strafbarkeitsdefizite“.[8]

3. Nachbesserungsbedarf im Detail

In der konkreten Ausgestaltung des § 202a Abs. 3 StGB-E sieht die Bundesrechtsanwaltskammer indessen noch geringfügigen Nachbesserungsbedarf.

---

[5] *Kuschel/Rostam*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 83 ff.; zu weiteren Problembereichen siehe insbesondere *Wörner/Blocher*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 57 ff.; *Nolde*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 107 ff. sowie *Balaban u.a.*, Whitepaper zur Rechtslage der IT-Sicherheitsforschung (Fn. 1), S. 9 ff.

[6] Vgl. *Freiling*, in: Golla/Brodowski (Hrsg.), IT-Sicherheitsforschung und IT-Strafrecht (Fn. 1), S. 21 (25 ff.).

[7] *Balaban u.a.*, Whitepaper zur Rechtslage der IT-Sicherheitsforschung (Fn. 1), S. 45 f.; siehe auch RefE, S. 17.

[8] RefE, S. 12 f.

In Nr. 1 sollte präzisiert werden, dass die auf die Feststellung, Meldung und Beseitigung der Sicherheitslücke gerichtete Absicht handlungsleitend sein muss. Das erscheint erforderlich, um legitime IT-Sicherheitsforschung z.B. von Ransomware-Angriffen rechtssicher zu differenzieren: Auch bei diesen wird eine Sicherheitslücke aufgefunden und der Verantwortliche hierüber informiert; allerdings ist dann dies nicht handlungsleitend, sondern die Absicht, dies zu einer Erpressung auszunutzen. Der vorgenannten handlungsleitenden Absicht steht hingegen nicht entgegen, wenn IT-Sicherheitsforschende durch Auffinden der Sicherheitslücke wissenschaftliche Reputationsgewinne erzielen oder z.B. im Rahmen eines Bug Bounty-Programms finanziell profitieren möchten.

Bezüglich Nr. 2 begegnet das Merkmal der Erforderlichkeit „zur Feststellung der Sicherheitslücke“ Bedenken, selbst wenn man dieses Merkmal nach Maßstäben der IT-Sicherheitsforschung in einer ex ante-Perspektive bestimmt. Da diese Forschung notwendigerweise unter Bedingungen von Ungewissheit agiert, droht eine weitreichende Tatsachenunsicherheit und daraus folgende Rechtsunsicherheit, ob dieselbe Sicherheitslücke nicht auch auf alternativen Pfaden hätte erforscht werden können. Mit einer solchen Rechtsunsicherheit gäbe man der IT-Sicherheitsforschung Steine statt Brot.

III. Einführung besonders schwerer Fälle des Ausspähens und Abfangens von Daten

Flankierend sieht der Referentenentwurf mit § 202a Abs. 4 Satz 1 StGB-E vor, den Strafrahmen für Taten des Ausspähens von Daten (§ 202a Abs. 1 StGB, Freiheitsstrafe bis zu drei Jahren oder Geldstrafe) bei besonders schweren Fällen maßvoll auf eine Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu erhöhen. Als Regelbeispiele für besonders schwere Fälle benennt § 202a Abs. 4 Satz 2 StGB-E die Herbeiführung eines Vermögensverlusts großen Ausmaßes (Nr. 1), das Handeln aus Gewinnsucht, die gewerbsmäßige oder bandenmäßige Begehung (Nr. 2) sowie die Beeinträchtigung einer kritischen Infrastruktur oder der Sicherheit Deutschlands oder eines seiner Länder (Nr. 3). Durch Verweisung in § 202b Abs. 2 Alt. 2 StGB-E soll dieser erhöhte Strafrahmen auch bei Taten des Abfangens von Daten (§ 202b StGB) greifen.

Die zunehmende Datafizierung unserer Gesellschaft hat zu einer weitreichenden Abhängigkeit von IT-Infrastrukturen geführt. Dies erstreckt sich insbesondere auf die Vertraulichkeit von Daten, die es vor Angriffen Dritter zu schützen gilt. Angesichts dessen tritt die Bundesrechtsanwaltskammer der Einführung dieses besonders schweren Falles und der vorgesehenen Regelbeispiele nicht entgegen. Sie gibt allerdings zu bedenken, dass kriminologisch nicht nachgewiesen ist, dass eine Erhöhung des Strafrahmens potenzielle Täterinnen und Täter stärker abschrecken würde. Auch reichte es bei § 202a Abs. 4 Nr. 3 StGB-E aus, an die „Vertraulichkeit einer kritischen Infrastruktur“ anzuknüpfen, dass Taten des § 202a Abs. 1 StGB stets die Vertraulichkeit eines informationstechnischen Systems verletzen und die weiteren in Nr. 3 StGB angesprochenen Schutzziele („Verfügbarkeit, Funktionsfähigkeit, Integrität, Authentizität“) daher allenfalls mittelbar betroffen sein können.

- - -