Entscheidung des Monats – März 2025

LG Aachen, Urt. v. 04.11.2024, Az. 74 NBs 34/24

I. Leitsätze des Verfassers

1. Für die Frage, ob Daten „nicht für den Täter bestimmt" sind, ist der Wille des Dispositionsbefugten maßgeblich. Eine beschränkte Nutzungsberechtigung für bestimmte Daten umfasst nicht automatisch den Zugriff auf den gesamten Datenbestand.

2. Das Tatbestandsmerkmal „besonders gesichert" im Sinne des § 202a Abs. 1 StGB ist auch dann erfüllt, wenn ein Passwort im Quellcode einer Software im Klartext hinterlegt ist, sofern dessen Auffinden und Auslesen spezielle IT-Kenntnisse erfordert und dies nicht für jedermann ohne weiteres möglich ist.

3. Eine Rechtfertigung nach § 34 StGB für das Handeln von sogenannten Grey-Hat-Hackern kommt nur in Betracht, wenn die Sicherheitslücke bereits vor dem Eindringen in das System bekannt war. Ein verdachtsmäßiges Eindringen ist nicht gerechtfertigt.

II. Sachverhalt

Das *Amtsgericht Jülich* verurteilte den Angeklagten wegen des Ausspähens von Daten (§ 202a Abs. 1 StGB) zu einer Geldstrafe von 50 Tagessätzen zu je 60,00 Euro.[1] Das *Landgericht Aachen* verwarf die durch den Angeklagten eingelegte Berufung als unbegründet. Es traf im Rahmen der Berufungshauptverhandlung die folgenden Feststellungen:

Bei der R. F. GmbH & Co KG (R. F.) handelt es sich um ein Unternehmen, das eine eCommerce-Lösung hostete und sie großen Online-Marktplätzen gegen Entgelt über eine Schnittstelle zur Verfügung stellte. Dadurch verwaltete sie auf ihrem Server persönliche Daten von ca. 600.000-700.000 Endkunden.

---

[1] Der Verfahrenslauf stellte sich bis dato wie folgt dar: Antrag der *Staatsanwaltschaft Köln* vom 13.02.2023 auf Erlass eines Strafbefehls; Beschluss des *Amtsgerichts Jülich* vom 10.05.2023, mit der der Antrag der *Staatsanwaltschaft Köln* auf Erlass des Strafbefehls aus rechtlichen Gründen abgelehnt wurde; sofortige Beschwerde der *Staatsanwaltschaft Köln* vom 22.05.2023 gegen die Entscheidung des *Amtsgerichts Jülich*; Entscheidung des *Landgerichts Aachen* vom 27.07.2024 - 60 Qs 16/23 (AG Jülich) = MMR 2023, 866 mit der auf die sofortige Beschwerde der *Staatsanwaltschaft Köln* der angegriffene Beschluss aufgehoben und die Sache zur erneuten Entscheidung über den Strafbefehlsantrag an das *Amtsgericht Jülich* zurückverwiesen wurde; Urteil des *Amtsgerichts Jülich* vom 17.01.2024 - 17 Cs-230 Js 99/21-55/23 = MMR 2024, 363.

Einer der Kunden von R. F. bat den Angeklagten, der von Beruf Programmierer ist und seinerzeit ein Dienstleistungsunternehmen für Onlinehändler betrieb, um Unterstützung. Konkret sollte der Angeklagte die Homepage des Kunden auf Fehler untersuchen. Bei dieser Untersuchung wurde der Angeklagte im Quellcode der von seinem Kunden genutzten Software der R. F. auf ein dort unverschlüsselt hinterlegtes Passwort aufmerksam.

Nachdem der Angeklagte Kenntnis von dem Passwort erlangt hatte, gab er dieses in die Kundendatenbank ein. Spätestens zu diesem Zeitpunkt wurde ihm bewusst, dass er nun Zugriff auf alle Endkundendaten von R. F. hatte, einschließlich jener, die ihm und seinem Kunden nicht zugänglich sein sollten. Trotz dieses Wissens entschied sich der Angeklagte dazu, Screenshots von den in der Datenbank der R. F. gespeicherten Kundendaten anzufertigen.

Sodann richtete der Angeklagte eine neue E-Mail-Adresse ein und schickte unter dem Pseudonym „Anonym“ eine E-Mail mit dem Betreff „NR.“ an die R. F. In dieser E-Mail berichtete er von einem entdeckten Sicherheitsproblem. Die E-Mail war in einem sachlichen, aber aufforderndem Ton verfasst und enthielt technische Details, die seine Behauptungen untermauern sollten. Eine Belohnung forderte der Angeklagte nicht. Die R. F. erstattete daraufhin Strafanzeige.

III. Entscheidungsgründe

Nach Auffassung des *Landgerichts Aachen* hat sich der Angeklagte wegen Ausspähens von Daten gem. § 202a Abs. 1 StGB schuldig gemacht. Er habe sich unter Überwindung der Zugangssicherung unbefugt Zugang zu der Datenbank der R. F. verschafft, obwohl die enthaltenen Daten nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert waren.

Bei den in der Datenbank enthaltenen Informationen handele es sich um solche, die nicht für den Angeklagten bestimmt waren. Es komme bei dieser Frage auf den Willen des Dispositionsbefugten, hier der R. F., an. Nach ihrem Willen habe weder der Angeklagte noch sein Auftraggeber Zugang zu der vollständigen Datenbank erhalten sollen. Obwohl der Auftraggeber des Angeklagten Kunde der R. F. gewesen sei und als solcher auch über eine Nutzungsberechtigung der Software verfügt habe, habe seine Dispositionsbefugnis nicht die verfahrensgegenständlichen Endkundendaten umfasst. Dass der Auftraggeber von R. F. ein umfassend Zugriffsrecht gewährt bekommen habe, sei unwahrscheinlich. Selbst bei Bestehen eines solchen Zugriffsrecht wäre dieses auf den notwendigen Geschäftsbetrieb beschränkt gewesen. Das Anfertigen von Screenshots fremder Kundendaten sei davon jedenfalls nicht umfasst. Für diese Nutzung habe weder ein Einverständnis vorgelegen, noch seien die Daten für den Angeklagten bestimmt gewesen.

Der Angeklagte habe sich die Daten auch verschafft, indem er sie zum einen zur Kenntnis genommen und zum anderen auch Screenshots davon gefertigt habe.

Die Daten seien gegen unberechtigten Zugang besonders gesichert gewesen und der Angeklagte habe diese Zugangssicherung auch überwunden. Eine besondere Sicherung sei anzunehmen, wenn der Zugang Unbefugter zu den Daten verhindert oder wenigstens erheblich erschwert wird. Durch die Sicherung müsse der Berechtigte sein spezielles Geheimhaltungsinteresse dokumentieren. Die konkrete Art der Sicherung sei gesetzlich nicht vorgegeben. Es kämen sowohl physische Schutzmaßnahmen als auch systemimmanente Sicherungen auf Hard- oder Software-Ebene in Betracht. Eine Passwortsicherung reiche grundsätzlich aus. Diese auch hier eingerichtete Passwortsicherung habe der Angeklagte durch die Auslesung des Quellcodes der Software und die anschließende Passworteingabe überwunden. Es sei nicht entscheidend, ob es zuvor einer sog. Dekompilierung[2] des Quellcodes bedurfte. Denn Ansatzpunkt des strafbaren Verhaltens sei vorliegend der Zugriff auf die Endkundendaten in der passwortgesicherten Datenbank von R. F.

Auch der Umstand, dass das Passwort möglicherweise durch die Darstellung als Klartext im Objektcode der Datei nachlässig gesichert war, führe nicht zu einem Ausschluss des Tatbestandes. Denn es komme für das Vorliegen einer Zugangssicherung nur auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter an. Es sei nicht maßgeblich, ob auch Eingeweihte oder Experten leicht auf die Daten zugreifen können. Ebenso sei unerheblich, ob die Sicherung gerade gegenüber dem Täter wirke. Zwar müsse die Überwindung der Zugangssicherung einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordern. Aber dabei komme es nur darauf an, dass dies typischerweise so sei, also unabhängig von den besonderen Fähigkeiten und Kenntnisse des Täters. Das sei etwa der Fall, wenn eine Passwortabfrage einfach umgangen werden könne oder das Passwort in Rechnernähe für jeden ersichtlich notiert sei. Indes solle eine Strafbarkeit nicht daran scheitern, dass zu hohe Anforderungen an den Passwortschutz gesetzt werden. Auch einfache Passwörter seien ausreichend, da auch dadurch das Geheimhaltungsinteresse dokumentiert werde. Vor diesem Hintergrund stelle die hier erfolgte Sicherung der Endkundendaten durch ein im Quellcode hinterlegtes Passwort eine Zugangssicherung dar, die eine deutliche Schranke setzte und deren Überwindung kriminelle Energie manifestierte. Denn ein Auslesen des Passworts habe jedenfalls spezielle IT-Kenntnisse (des Angeklagten) erfordert. Das Auffinden des Passwortes und die Überwindung des damit verbundenen Schutzes sei gerade nicht für jedermann ohne weiteres möglich gewesen, sondern habe die Kenntnis und Anwendung einer bestimmten Software sowie zumindest Grundkenntnisse über die

---

[2] Ein Computerprogramm, welches ursprünglich in Form eines „Quellcodes“ in einer verständlichen Programmiersprache abgefasst ist, wird mittels eines als „Compiler“ bezeichneten speziellen Programms in eine für den Computer ausführbare Form, d.h. den „Objektcode“, umgewandelt. Der Vorgang der Umwandlung des Quellcodes in den Objektcode wird „Kompilierung“ genannt.

Bedeutung und Funktion von Datenbanksprachen bedingt, über die ein technischer Laie nicht verfüge.

Die Tat des Angeklagten sei auch nicht gerechtfertigt. Der rechtfertigende Notstand des § 34 StGB sei nicht einschlägig. Durch die seinerzeitige Reformierung des § 202a StGB habe man manifestieren wollen, dass böswillig handelnde Hacker (sog. Black Hats) generell strafbar und solche, die im Auftrag des Verfügungsberechtigten (hier R. F.) tätig sind (sog. White Hats), straffrei sein sollen. Bei dem Angeklagten handele es sich hingegen um einen Grey-Hat-Hacker. Dieser handele nicht böswillig, könne sich aber auch nicht auf die Einwilligung des Verfügungsberechtigten berufen. Grey-Hat-Hacker würden nur dann gem. § 34 StGB gerechtfertigt handeln, wenn die Sicherheitslücke schon vor dem Eindringen in das System bekannt sei. Ein verdachtsmäßiges Eindringen sei indes nicht nach § 34 StGB gerechtfertigt. Darauf komme es vorliegend aber nicht an, weil dem Angeklagten jedenfalls mildere Mittel als die Anfertigung von Screenshots zur Verfügung gestanden hätten.

IV. Verteidigungsrelevanz

Die Entscheidung des *Landgerichts Aachen* verdeutlicht eindrucksvoll den bestehenden Reformbedarf im Bereich des Cyberstrafrechts, insbesondere in Bezug auf die Hacking-Straftatbestände der §§ 202a ff. StGB. Der Fall zeigt die Komplexität der rechtlichen Beurteilung von IT-Sicherheitsforschung und unterstreicht die Notwendigkeit klarer gesetzlicher Vorgaben für Forschende, Penetrationstestende und sonstige – nicht böswillige handelnde – Hacker im Bereich der Informationssicherheit.[3] Denn diese erfüllen in Zeiten hybrider Kriegsführung und wachsenden IT-Sicherheitsrisiken für Unternehmen eine wichtige Aufgabe, indem sie im gesamtgesellschaftlichen Interesse Sicherheitslücken aufdecken und schließen.

Auch vor diesem Hintergrund erarbeitete das Bundesministerium der Justiz im Jahr 2024 einen Referentenentwurf „*Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches – Modernisierung des Computerstrafrecht*“, um eine „*klare gesetzliche Abgrenzung von nicht zu missbilligendem Handeln der IT-Sicherheitsforschung von strafwürdigem Verhalten*“ zu erreichen.[4] Kern des Referentenentwurfs war die Anpassung des Straftatbestandes des Ausspähens von Daten gem. § 202a StGB. In einem neuen 3. Absatz waren drei kumulative Voraussetzungen enthalten, deren Vorliegen das Tatbestandsmerkmal „unbefugt“ ausschließen würde: Der Täter muss in der Absicht handeln, eine Sicherheitslücke eines informationstechnischen Systems festzustellen

---

[3] Siehe auch *Kipker/Rockstroh*, Anm. zu LG Aachen, Entsch. vom 27.07.2023 - 60 Qs 16/23 (AG Jülich) = MMR 2023, 866 (868).

[4] Abrufbar unter (zuletzt abgerufen am 26.03.2025): https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/RefE_ComputerStrafR.pdf?__blob=publicationFile&v=3

und die Information hierüber an eine verantwortliche Stelle weiterzugeben, die die Lücke selbst schließen oder die Schließung veranlassen kann (Feststellungs- und Unterrichtungsabsicht).

Eine Feststellungsabsicht sollte gem. der Begründung nur dann anzunehmen sein, wenn es dem Täter gerade darum ging, eine Sicherheitslücke festzustellen und zu schließen. Ein mutwilliges Ausprobieren, ob Systeme „knackbar" sind oder ein Hacking aus persönlichen Motiven sei weiterhin strafbar. Nach § 202a Abs. 3 Nr. 1 StGB-E sind die für das informationstechnische System Verantwortlichen, die betreibenden Dienstleister des jeweiligen Systems, die Hersteller der betroffenen IT-Anwendung oder das Bundesamt für Sicherheit in der Informationstechnik die tauglichen Adressaten der Meldung. Eine verbindliche Meldemethode sah der Gesetzesentwurf indes nicht vor. Durch das weitere Merkmal der Erforderlichkeit sollte sichergestellt werden, dass sich derjenige weiterhin strafbar macht, wer auf mehr oder andere Daten zugreift, als dies für die Feststellung der Sicherheitslücke erforderlich ist oder wer im Vorfeld die Erlaubnis des Berechtigten hätte einholen können.

Da auch dieses Gesetzesvorhaben der Diskontinuität zum Opfer gefallen ist, müssen sich sowohl die „Hacker" als auch Strafverteidiger und präventiv beratende Rechtsanwälte mit der bestehenden Rechtslage arrangieren.

Konkret bedeutet dies, die Auslegung der Tatbestandsmerkmale durch die erkennenden Gerichte zu kennen und bei der Verteidigungsstrategie bzw. der Compliance-Beratung im Vorfeld von Penetrationstest zu berücksichtigen. Gerade eine saubere Aufarbeitung des technischen Sachverhalts ist von besonderer Bedeutung, da kleine Nuancen hierbei erhebliche Auswirkungen auf die strafrechtliche Würdigung haben können.[5]

Zunächst ist freilich zu eruieren, ob der sich der Beschuldigte überhaupt Zugang zu Daten verschafft hat. Das wäre bei dem vorliegenden Sachverhalt etwa dann nicht der Fall gewesen, wenn der Angeklagte lediglich durch die Dekompilierung des Quellcodes den Objektcode der Software erlangt und die dort hinterlegten Passwörter zur Kenntnis genommen, jedoch die erlangten Informationen nicht zum Eindringen in die Datenbank genutzt hätte.[6]

Sodann ist zu prüfen, ob der hinsichtlich der Dispositionsbefugte im Vorfeld der Zugangsverschaffung hierzu seine Einwilligung erteilt hat. Dann wäre der Zugriff im Grundsatz nicht tatbestandsmäßig, was insbesondere für im Vorfeld von dem entsprechenden Unternehmen beauftragte White-Hat-Hacker von Bedeutung ist.[7] Ein

---

5 *Leffer*, Anm. zu AG Jülich, Urt. v. 17.01.2024 – 17 Cs-230 Js 99/21-55/23 = MMR 2024, 363 (366).

6 *Klaas*, MMR 2022, 187 (189).

7 *Klaas*, MMR 2022, 187 (188).

nachträgliches Einverständnis gegenüber zunächst eigeninitiativ handelnden Hackern führt hingehen nicht zum Tatbestandsausschluss, kann jedoch auf Ebene der Strafzumessung Berücksichtigung finden oder dazu führen, dass kein Strafantrag gestellt wird.[8]

Hinsichtlich des Tatbestandsmerkmals der „besonderen Zugangssicherung" stehen der Verteidigung insbesondere zwei Verteidigungslinien offen. Zum einen sollte sie kritisch hinterfragen, ob der Verfügungsberechtigte überhaupt ein Passwort eingerichtet, er also *„Vorkehrungen getroffen hat, um den allgemeinen Zugriff auf …* [die Daten] *auszuschließen oder wenigstens nicht unerheblich zu erschweren"*[9]. Sollte dies der Fall sein, ist zu prüfen, ob begründet werden kann, dass der Verfügungsberechtigte den Zugriff des Täters auf die Daten überhaupt erst durch seinen nachlässigen Umgang mit dem von ihm gesetzten Passwort ermöglicht hat. Indes wird durch die Entscheidung des *Landgerichts Aachen*, die insoweit im Einklang mit der Rechtsprechung des *Bundesgerichtshofes* steht,[10] abermals deutlich, dass die Gerichte nur sehr geringe Anforderungen an die Qualität der Passwortsicherung[11] stellen und nur in besonderen Konstellationen aufgrund des nachlässigen Umgangs die besondere Sicherung ablehnen. Sofern ein – auch noch so einfaches – Passwort eingerichtet ist, die Passwortabfrage nicht vollständig umgangen werden kann oder das Passwort nicht in Rechnernähe notiert ist und auch noch spezielle IT-Kenntnisse des Täters erforderlich sind, um das Passwort auszulesen, reicht dies aktuell aus, um eine besondere Zugangssicherung und damit erhebliche Strafbarkeitsrisiken für Personen aus dem Bereich der IT-Sicherheitsforschung zu begründen. Zwar könnte man – aus Verteidigersicht zutreffend – argumentieren, dass etwa die Ablage eines Passworts als Klartext des Quellcodes einer Notiz im Nahbereich eines Computers entspricht,[12] jedoch zeigt die Entscheidung des *Landgerichts Aachen*, dass diese Verteidigungsstrategie auf wackeligen Beinen steht.[13]

Sollte eine Verteidigung auf Tatbestandsebene nicht erfolgsversprechend sein, kommt der Weg über die Rechtfertigungsebene in Betracht. So kann die Ermittlung von

---

8 *Klaas*, in: Klaas/Momsen/Wybitul, Datenschutzsanktionenrecht, 1. Aufl. 2023, § 11 Rn. 39

9 BGH, Beschl. v. 13.05.2020 - 5 StR 614/19 (LG Berlin) = MMR 2021, 411 (412).

10 Vgl. nur BGH, Beschl. v. 13.5.2020 - 5 StR 614/19 (LG Berlin) = MMR 2021, 411.

11 Siehe zu der Frage, ob das Kompilieren des Quellcodes in den Objektcode eine besondere Sicherung i. S. d. § 202a StGB darstellt (quod non), die zutreffenden Ausführungen von *Kipker/Rockstroh*, Anm. zu LG Aachen, Entsch. vom 27.7.2023 - 60 Qs 16/23 (AG Jülich) = MMR 2023, 866 (868) sowie *Leffer*, Anm. zu AG Jülich, Urt. v. 17.1.2024 - 17 Cs-230 Js 99/21-55/23 = MMR 2024, 363 (366).

12 So auch *Leffer*, Anm. zu AG Jülich, Urt. v. 17.1.2024 - 17 Cs-230 Js 99/21-55/23 = MMR 2024, 363 (366).

13 Sollte einem technischen Laien, der es mehr oder wenig zufällig geschafft hat, einen eingerichteten Passwortschutz zu umgehen, eine Strafbarkeit gem. § 202a StGB verstoßen zu haben, dürfte bezüglich dieses Tatbestandsmerkmals unter Verweis auf die mangelnde technische Expertise Verteidigungspotenzial bestehen.

Sicherheitslücken über den rechtfertigenden Notstand gem. § 34 StGB zur Straffreiheit führen. [14] Bestehende Sicherheitslücken in IT-Systemen können gegenwärtige (Dauer-)Gefahren für diverse Individualrechtsgüter sowie Rechtsgüter der Allgemeinheit darstellen. [15] Neben dieser Notstandslage muss auch eine Notstandshandlung vorliegen. Die handelnde Person muss zielgerichtet die Daten vor unberechtigtem Zugriff schützen bzw. die Funktionsfähigkeit des Systems gewährleisten.[16] Eine Rechtfertigung kommt indes nur in Betracht, wenn die ergriffenen Maßnahmen erforderlich, also geeignet und das relativ mildeste Mittel sind. [17] Außerdem muss die Interessenabwägung zugunsten des Schutzes der gefährdeten Rechtsgüter dem Interesse des Verfügungsberechtigten an der formellen Geheimhaltung wesentlich überwiegen.[18]

Geeignet ist eine Maßnahme nur, wenn die entdeckte Sicherheitslücke auch einer zur Abhilfe berechtigten und fähigen Stelle (etwa dem Verfügungsberechtigten oder dem BSI) berichtet wird.[19] Sollte von Seiten der Ermittlungsbehörden vorgebracht werden, eine Maßnahme war nicht das relativ mildeste Mittel, weil erlangte Informationen, die eine Überwindung von IT-Sicherheitsmechanismen ermöglicht haben, nicht direkt gemeldet, sondern ausgenutzt wurden, muss die Verteidigung darlegen, dass gerade das Ausnutzen der Informationen zur Zielerreichung tatsächlich erforderlich war.[20] Bei der Interessenabwägung sind etwa der Intensitätsgrad der drohenden Gefahren für die geschützten und beeinträchtigten Rechtsgüter sowie die Wahrscheinlichkeit des Gefahreneintritts und des Rechtsgüterschutzes von Bedeutung.[21]

Abschließend ist festzuhalten, dass sich insbesondere eigeninitiativ handelnde White-Hat(oder Grey-Hat)-Hacker nach der aktuellen Rechtslage einem nicht zu unterschätzenden Strafbarkeitsrisiko aussetzen. Zwar stehen sowohl auf Tatbestands-

---

14 *Klaas*, MMR 2022, 187 (189).

15 *Klaas*, MMR 2022, 187 (189); nach *Mansdörfer* soll eine Rechtfertigung nur dann in Betracht kommen, wenn die die Sicherheitslücke schon vor dem Eindringen in das System bekannt ist, *Mansdörfer*, in: BeckOK-IT-Recht, 17. Ed. 01.01.2025, StGB § 202a Rn. 31. Hintergrund dieser Annahme dürfte sein, dass als subjektives Rechtfertigungselement die Kenntnis der Notstandslage erforderlich ist, vgl. *Momsen/Savić*, in: BeckOK-StGB, 64. Ed. 01.02.2025, § 34 Rn. 20.

16 *Klaas*, MMR 2022, 187 (189).

17 *Kipker/Rockstroh*, Anm. zu LG Aachen, Entsch. vom 27.7.2023 - 60 Qs 16/23 (AG Jülich) = MMR 2023, 866 (869)

18 *Klaas*, MMR 2022, 187 (189).

19 *Klaas*, MMR 2022, 187 (190); *Klaas*, in: Klaas/Momsen/Wybitul, Datenschutzsanktionenrecht, 1. Aufl. 2023, § 11 Rn. 64 ff.

20 *Klaas*, MMR 2022, 187 (190); *Klaas*, in: Klaas/Momsen/Wybitul, Datenschutzsanktionenrecht, 1. Aufl. 2023, § 11 Rn. 70 ff.

21 *Klaas*, in: Klaas/Momsen/Wybitul, Datenschutzsanktionenrecht, 1. Aufl. 2023, § 11 Rn. 73 ff. mit weiteren Beispielen.

als auch auf Rechtfertigungsebene Verteidigungsargumente zur Verfügung, jedoch besteht eine gewisse Unsicherheit, wie tragfähig diese Argumente im jeweiligen Einzelfall sind. Die angedachte Anpassung des § 202a StGB wäre sicherlich ein erster Schritt gewesen, um mehr Rechtsklarheit herbeizuführen und die neue Bundesregierung sollte sich – im Interesse der Allgemeinheit – dieser Thematik vor dem Hintergrund der steigenden Bedrohungslage schnellstmöglich annehmen. Die Diskussionen dürften jedoch auch nach einer – wie auch immer gearteten – Anpassung des Straftatbestandes nicht abebben.

Rechtsanwalt und Fachanwalt für Strafrecht Dr. Marius Haak,
PARK | Wirtschaftsstrafrecht, Dortmund.