BUNDESGERICHTSHOF

BESCHLUSS

5 StR 614/19

vom

13. Mai 2020

in der Strafsache

gegen

1.

2.

wegen Wohnungseinbruchdiebstahls u.a.

ECLI:DE:BGH:2020:130520B5STR614.19.0

Der 5. Strafsenat des Bundesgerichtshofs hat nach Anhörung des Generalbundesanwalts und der Beschwerdeführer am 13. Mai 2020 gemäß § 349 Abs. 2 und 4 sowie entsprechend § 354 Abs. 1 StPO beschlossen:

1. Die Revision des Angeklagten H. gegen das Urteil des Landgerichts Berlin vom 10. April 2019 wird mit der Maßgabe verworfen, dass die Einziehung des Wertes von Taterträgen ihm gegenüber auf 53.300 Euro reduziert wird.

   Der Beschwerdeführer hat die Kosten seines Rechtsmittels zu tragen.

2. Auf die Revision des Angeklagten B. wird das vorgenannte Urteil aufgehoben, soweit es ihn betrifft.

   Die weitergehende Revision wird verworfen.

   Im Umfang der Aufhebung wird die Sache zu neuer Entscheidung und Verhandlung, auch über die Kosten dieses Rechtsmittels, an eine andere Strafkammer des Landgerichts zurückverwiesen.

Gründe:

1 Das Landgericht hat den Angeklagten H. wegen Wohnungseinbruchdiebstahls, Ausspähens von Daten in zwei Fällen und Besitzes kinderpornographischer Schriften zu einer Gesamtfreiheitsstrafe von einem Jahr und elf Monaten verurteilt, deren Vollstreckung zur Bewährung ausgesetzt und fünf Monate der Strafe als vollstreckt erklärt; zudem hat es gegen ihn die Einziehung des Wertes von Taterträgen in Höhe von 70.900 Euro angeordnet. Den Angeklagten B. hat es wegen Ausspähens von Daten in zwei Fällen zu einer Gesamtgeldstrafe von 300 Tagessätzen zu jeweils 220 Euro verurteilt, von der 60 Tagessätze als vollstreckt gelten. Die jeweils mit Verfahrens- und der Sachrüge geführten Revisionen der Angeklagten führen beim Angeklagten H. zu einer Reduzierung des Einziehungsbetrages und bei dem Angeklagten B. zu einer Aufhebung des Schuldspruchs; im Übrigen sind sie im Sinne von § 349 Abs. 2 StPO unbegründet (vgl. Antragsschrift des Generalbundesanwalts).

A) Revision des Angeklagten H.

2 Das Urteil hält insbesondere rechtlicher Überprüfung stand, soweit das Landgericht den Angeklagten H. wegen Ausspähens von Daten (§ 202a Abs. 1 StGB) in zwei Fällen verurteilt hat.

I.

3 1. Das Landgericht hat insoweit Folgendes festgestellt:

4 Der Angeklagte B. lernte den Angeklagten H. kennen, als er im März 2006 dessen sexuelle Dienstleistungen als „Callboy“ in Anspruch nahm. In

der Folge kam es 2007 und 2008 zu mehreren solcher Treffen. Im Juli 2007 war B. Leiter der Stabsstelle des Apothekerlobbyverbandes A. geworden und betrieb daneben das Online-Informationsportal „a. –a. “. Auf diesem Portal wurden regelmäßig Hintergrundinformationen aus dem Bundesministerium für Gesundheit veröffentlicht, die in der Pharma- und Apothekerbranche auf große Aufmerksamkeit stießen. Im Ministerium gab es 2006 bis 2012 – wie auch schon zuvor – „undichte Stellen“, die unbefugt verwaltungsinterne Informationen weitergaben. Der Angeklagte H. wurde von seinem Arbeitgeber ab Juli 2008 als Systemadministrator am Berliner Standort des Ministeriums eingesetzt.

5 Beide Angeklagte kamen spätestens im Januar 2009 überein, dass H. B. mit internen Informationen aus dem Ministerium versorgen werde, die dieser für seine berufliche Tätigkeit nutzen wollte. Dem Angeklagten H. war es als Administrator möglich, nach Anmeldung mit seinem Passwort im zentralen Verzeichnis des Systems Zugriff auf alle darin elektronisch geführten Postfächer und auf den Inhalt gespeicherter E-Mails zu nehmen. Hierbei nutzte er für seine Administratorentätigkeit regelmäßig auch das für Schulungszwecke eingerichtete und in die Gruppe „E. D. S. “ eingetragene Benutzerprofil „p. “, dessen Kennwort unter den Administratoren des Ministeriums allgemein bekannt war.

6 Am 20. Juli 2009 änderte das Ministerium die Zugriffsrechte, nachdem die unbeschränkte Zugriffsmöglichkeit der Administratoren auf alle Postfächer als Sicherheitsmangel erkannt worden war. Die Administratoren waren nicht mehr in der Gruppe „E. D. S. “ im zentralen Verzeichnis des Systems eingetragen und konnten deshalb ohne weiteres nur noch auf die öffentlichen Postfächer der Abteilungen oder Referate zugreifen. Zunächst konnten sich die Administratoren – was ihnen allerdings verboten war – noch selbst

in die Gruppe „E. D. S. “ eintragen und dadurch ungehindert Zugriff auf die persönlichen Postfächer nehmen; auch diese Möglichkeit wurde Anfang Oktober 2009 aber beseitigt. Seitdem war für Administratoren der ungehinderte Zugriff eigentlich nur auf öffentliche Postfächer vorgesehen.

7 Allerdings ergab sich für die Administratoren zur Erfüllung einzelner Aufträge (etwa Wiederherstellung versehentlich gelöschter E-Mail-Nachrichten, Einrichtung neuer Postfächer für neue Mitarbeiter) verschiedentlich die Notwendigkeit, auf den Inhalt einzelner persönlicher Postfächer zugreifen zu müssen. Hierfür war ein kompliziertes Prozedere vorgesehen, wonach die Administratoren unter dem Blick des jeweiligen Ministeriumsbediensteten nach dessen Anmeldung mit seinem Kennwort im System entweder mit ihm vor Ort oder durch „Fernaufschalten“ auf dessen Arbeitsplatz agieren sollten. Wenn das Aufschalten nicht gelang oder – was häufiger geschah – Mitarbeiter darum baten, die Behebung einzelner Probleme in der Mittagspause oder in Zeiten sonstiger Abwesenheit vorzunehmen, kam das Einloggen des Administrators mittels eines zentral hinterlegten Notfallkennworts in Frage, was indes sehr aufwändig war. Deshalb äußerten mehrere Administratoren bald nach dem 20. Juli 2009 den Wunsch nach einer einfacheren Lösung.

8 Der leitende Systemadministrator des Ministeriums, der Zeuge P. , wies die Administratoren darauf hin, dass sie sich unter Umgehung der kurz zuvor eingeführten Einschränkungen mit wenig Aufwand selbst Zugriff auf einzelne persönliche Postfächer von Ministeriumsmitarbeitern verschaffen könnten. Hierfür mussten sich die Administratoren unter Aufruf des dienstlichen Profils der einzelnen Nutzer und Anklicken von „Allgemein“, „Eigenschaften“, „Exchange – Erweitert“ und dann „Postfachberechtigung“ selbst in die Liste der Zugriffsberechtigten eintragen, Optionen wie „Leseberechtigung“ oder „Vollständiger Postfachzugriff“ anklicken und diese Einstellungen über ein „OK-

Kästchen“ bestätigen. Anschließend konnten sie das Postfach des jeweiligen Mitarbeiters im Outlook-Programm aufrufen und hatten so die Möglichkeit zum Ausführen der notwendigen Operationen. Diese mit wenigen Mausklicks und in wenigen Minuten zu bewerkstelligenden Handlungen eröffneten anschließend die Möglichkeit, den Inhalt einzelner Ordner wie „Posteingang“ und „Gesendete Nachrichten“ zu kopieren.

9 Spätestens von Ende 2009 bis zum 6. November 2012 griff der Angeklagte H. in 33 Fällen auf öffentliche und jeweils auch private Postfächer zu, die ihm zuvor der Angeklagte B. bezeichnet hatte. Anschließend kopierte er E-Mail-Dateien, speicherte sie auf einer CD und übergab diese für 600 bzw. später 400 Euro an B. oder dessen Mitarbeiterin. Der Angeklagte H. ging dabei wie oben beschrieben vor, wobei er das Benutzerprofil „p. “ nutzte. Nach Kopieren der E-Mails löschte er „p. “ wieder aus der Liste der Zugriffsberechtigten. Dem Angeklagten B. war die Art und Weise des Zugriffs auf die von ihm begehrten Daten zwar nicht bekannt; er hielt es aber für möglich, dass der Angeklagte H. würde „tricksen“ müssen, um an die Daten zu kommen. B. war insbesondere an E-Mails der jeweiligen Minister, Staatssekretäre und von bestimmten Abteilungs- und Referatsleitern (Abteilung Gesundheitsversorgung, Krankenversicherung, Pflegeversicherung, Referate Arzneimittelversorgung sowie Grundsatzfragen, Apothekengesetz, Pharmaberufe) und der Leiterin des Leitungsstabes des Ministeriums interessiert und übermittelte H. die entsprechenden Namen.

10 Nach Teileinstellung gemäß § 154 Abs. 2 StPO sind insoweit noch die Anklagefälle 28 und 40 verfahrensgegenständlich. Im Fall 28 kopierte der Angeklagte H. wenige Tage vor dem 10. Februar 2012 bzw. an diesem Tag selbst zahlreiche E-Mails auf Bitten des Angeklagten B. aus den privaten

Postfächern des Ministers B. (55 Nachrichten), des Referatsleiters D. (634 Nachrichten), der Staatssekretärin F. (195 Nachrichten), der Leiterin des Leitungsstabes W. (699 Nachrichten), des Juristen O. (302 Nachrichten), des Referatsleiters M. (184 Nachrichten) und der Referatsleiterin M.
(167 Nachrichten). Anschließend brannte er die Daten auf eine CD und übergab sie am Abend gegen Zahlung von 600 Euro an B. . In den E-Mails ging es insbesondere um die Novellierung der Apothekenbetriebsordnung, den Entwurf eines auch Fragen der Apothekervergütung betreffenden Arzneimittelneuordnungsgesetzes und Ergebnisse vertraulicher Verhandlungen um die Höhe von Erstattungsbeiträgen für Arzneimittel mit neuen Wirkstoffen. Im Fall 40 kopierte der Angeklagte H. wenige Tage vor dem 6. November 2012 bzw. an diesem Tag selbst wiederum zahlreiche E-Mails der oben genannten Personen (insgesamt 2.378) aus dem Zeitraum Anfang Oktober bis 5. November 2012. Dabei ging es u.a. um aktuelle Honorarverhandlungen mit der Kassenärztlichen Bundesvereinigung und den gesetzlichen Krankenversicherungen („Bitte streng vertraulich behandeln“) und um eine Ministervorlage zur Einführung einer Pauschalvergütung für die Nacht- und Notdienste der Apotheken. Die CD mit den Daten übergab H. am Morgen des 6. November 2012 an B. gegen Bezahlung von 400 Euro.

11 B. wertete die ihm übergebenen Daten als Hintergrundinformationen für sein Online-Portal „a. –a. “ aus. Hierdurch wollte er möglichst hohe Besucherzahlen erreichen, um Kunden zur Buchung zahlungspflichtiger Anzeigen zu bewegen; damit erzielte das Portal seine Einnahmen. Der Angeklagte H. war in seinem Arbeitsvertrag mit seinem Arbeitgeber B. auf das Datengeheimnis verpflichtet worden, die Weitergabe von Betriebsinterna war ihm untersagt. Eine Verpflichtung nach dem Gesetz über die förmliche Verpflichtung

nichtbeamteter Personen erfolgte gegenüber dem Bundesministerium für Gesundheit nicht.

12 2. Das Landgericht hat die beiden Taten hinsichtlich der in privaten Postfächern gespeicherten E-Mails als gemeinschaftliches Ausspähen von Daten nach § 202a StGB gewertet. In der manuellen Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten hat es eine Überwindung der Zugangssicherung nach § 202a Abs. 1 StGB gesehen. Bei der Einziehungsentscheidung hat es auch die Einnahmen des Angeklagten H. aus den nach § 154 Abs. 2 StPO eingestellten Fällen eingerechnet.

II.

13 1. Die Revision des Angeklagten H. erzielt lediglich hinsichtlich der Einziehungsentscheidung einen Teilerfolg, ist aber im Übrigen unbegründet.

14 a) Verfahrenshindernisse bestehen nicht. Durch die Anklage der verfahrensgegenständlichen Taten nach § 202a StGB hat die Staatsanwaltschaft zumindest konkludent das besondere öffentliche Interesse an der Strafverfolgung im Sinne von § 205 Abs. 1 StGB bejaht (vgl. BGH, Beschluss vom 20. April 2017 – 2 StR 79/17, NStZ-RR 2017, 251, 252 mwN), so dass es auf die Frage der Wirksamkeit des Strafantrages vom 14. September 2012 nicht ankommt.

15 b) Die auf rechtsfehlerfreier Beweiswürdigung beruhenden Feststellungen tragen die Verurteilung des Angeklagten H. wegen Ausspähens von Daten in zwei Fällen.

16

Nach § 202a Abs. 1 StGB in der ab 11. August 2007 geltenden Fassung (BGBl. I 1786) macht sich strafbar, wer sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

17 aa) Indem der Angeklagte H. Zugriff auf die Inhalte der elektronisch gespeicherten E-Mails aus den persönlichen Postfächern der Ministeriumsmitarbeiter genommen und diese kopiert hat, hat er sich nicht nur den Zugang zu Daten (vgl. § 202a Abs. 2 StGB) verschafft, die nicht für ihn bestimmt waren, sondern sogar die Daten selbst. Dass die Daten nicht für den Angeklagten bestimmt waren, folgt aus seinen begrenzten Zugriffsrechten als Administrator. Diese umfassten gerade nicht das aufgabenunabhängige Lesen und Kopieren von E-Mails aus den persönlichen E-Mail-Postfächern der Behördenmitarbeiter, sondern sein Zugriffsrecht war auf rein technische Aufgaben zur Verwaltung des Netzwerks beschränkt (vgl. auch MüKo-StGB/Graf, 3. Aufl., § 202a Rn. 24 f.).

18 bb) Diese Daten waren gegen unberechtigten Zugang besonders gesichert.

19 (1) Dies ist der Fall, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Durch die Sicherung muss der Berechtigte sein spezielles Interesse an der Geheimhaltung dokumentieren (vgl. BT-Drucks. 16/3656 S. 10; BGH, Beschlüsse vom 27. Juli 2017 – 1 StR 412/16, NStZ 2018, 401, 403; vom 21. Juli 2015 – 1 StR 16/15, NStZ 2016, 339, 340; vom 6. Juli 2010 – 4 StR 555/09, NStZ 2011, 154, jeweils mwN).

20 (2) Im vorliegenden Fall war der Zugang zu dem jeweiligen EDV-Arbeitsplatz des einzelnen Behördenmitarbeiters und damit auch zu seinen nicht öffentlich zugänglichen persönlichen Dienst-E-Mails – wie allgemein üblich – durch Passwörter gesichert (vgl. UA S. 10, 49). Dies reicht als Zugangssicherung aus (vgl. Schönke/Schröder/Eisele, StGB, 30. Aufl., § 202a Rn. 14; Fischer, StGB, 67. Aufl., § 202a Rn. 9a; Graf, aaO Rn. 46).

21 Für das Vorliegen einer Zugangssicherung ist auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter abzustellen, nicht darauf, ob Eingeweihte oder Experten leicht auf die Daten zugreifen können (vgl. Valerius in Graf/Jäger/Wittig, Wirtschaftsstrafrecht, 2. Aufl., § 202a StGB Rn. 26). Es ist auch nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt (vgl. Valerius, aaO Rn. 27). Dass dem Angeklagten als Administrator der tatsächliche Zugriff auf die Daten möglich war, ist deshalb unerheblich (vgl. Graf, aaO Rn. 47; NK-StGB/Kargl, 5. Aufl., § 202a Rn. 11).

22 cc) Der Angeklagte H. hat sich den Zugang zu den Daten auch unter Überwindung dieser Zugangssicherung verschafft.

23 (1) Durch dieses Erfordernis sollen nach der Vorstellung des Gesetzgebers Handlungen aus dem Tatbestand ausgegrenzt werden, bei denen besonders gesicherte Daten auf andere Weise erlangt werden. Zum einen sollen damit Bagatellfälle aus dem Anwendungsbereich der Strafnorm ausgeschieden werden, zum anderen soll das Merkmal der Zugangssicherung dem Täter eine deutliche Schranke setzen, deren Überwindung die strafwürdige kriminelle Energie manifestiert. Es sollen Fälle erfasst sein, bei denen der Täter zu einer Zugangsart gezwungen ist, die der Verfügungsberechtigte erkennbar verhindern wollte; dies betrifft allerdings nicht die bloße Verletzung oder Umgehung

von organisatorischen Maßnahmen oder Registrierungspflichten (BT-Drucks. 16/3656, S. 10).

24 Soweit es in den Gesetzesmaterialien heißt, die Überwindung der Zugangssicherung müsse einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordern, weshalb vom Tatbestand solche Fälle nicht erfasst würden, in denen die Durchbrechung des Schutzes ohne weiteres möglich sei (aaO), versteht der Senat dies dahingehend, dass die Überwindung der Zugangssicherung typischerweise – also unabhängig von spezifischen Möglichkeiten oder Kenntnissen des konkreten Täters – einen nicht unerheblichen Aufwand erfordern muss. Unter Überwinden ist diejenige Handlung zu verstehen, die geeignet ist, die jeweilige Sicherung auszuschalten oder zu umgehen (vgl. Fischer, aaO Rn. 11a). Auch wenn eine Zugangssicherung aufgrund besonderer Kenntnisse, Fähigkeiten oder Möglichkeiten schnell und ohne besonderen Aufwand überwunden wird, ist der Tatbestand erfüllt. Für das geschützte Rechtsgut – das formelle Geheimhaltungsinteresse des Verfügungsberechtigten (BGH, Beschluss vom 27. Juli 2017 – 1 StR 412/16, aaO; vgl. zum Schutzzweck auch Ceffinato, JuS 2019, 337, 338 mwN) – ist es unerheblich, ob die Sicherung von Daten vor unberechtigtem Zugang schnell oder langsam, mit viel oder wenig Aufwand überwunden wird. Der Gesetzgeber wollte nach Auffassung des Senats aus dem Tatbestand neben Bagatelltaten lediglich solche Fälle ausschließen, in denen die Durchbrechung des Schutzes für jedermann ohne weiteres möglich ist, nicht aber solche, in denen die Zugangssicherung aufgrund spezieller Kenntnisse oder Möglichkeiten im Einzelfall leicht überwunden wird. Nur eine solche abstrakt-generelle Betrachtungsweise lässt sich mit dem Schutzzweck der Norm vereinbaren.

25 (2) Nach diesen Maßstäben hat der Angeklagte H. die Zugangssicherung überwunden. Den Passwortschutz der persönlichen E-Mail-Accounts hat

er dadurch umgangen, dass er sich als Administrator in verbotener Weise und unter Manipulation des Ordners „Zugriffsberechtigung“ den Zugriff auf die E-Mail-Daten der Behördenmitarbeiter verschafft hat. Diese Zugangsart wollte der Verfügungsberechtigte erkennbar durch die klare Beschränkung der Administratorenrechte und die Vorgabe eines bestimmten Prozederes beim Zugriff auf einen E-Mail-Account verhindern. Dass dem Angeklagten die Überwindung des Passwortschutzes mit wenigen „Maus-Clicks“ möglich war, hindert seine Strafbarkeit nach § 202a Abs. 1 StGB nicht.

26 dd) Dies geschah auch unbefugt (vgl. zu dieser Voraussetzung BT-Drucks. 16/3656 S. 10), denn dem Angeklagten H. war ein derartiger Zugriff auf E-Mail-Inhalte ausdrücklich verboten.

27 c) Allerdings kann die Einziehungsentscheidung nur in Höhe von 53.300 Euro bestehen bleiben. Zu Recht weist der Angeklagte H. mit seiner Revision darauf hin, dass es vorliegend nicht möglich ist, hinsichtlich der nach § 154 Abs. 2 StPO eingestellten Taten den Wert der Taterträge einzuziehen (vgl. BGH, Beschluss vom 18. Dezember 2018 – 1 StR 407/18, NStZ-RR 2019, 153 mwN). Der Senat hat den dafür angesetzten Betrag entsprechend § 354 Abs. 1 StPO von der im Übrigen zutreffend berechneten Summe (52.300 Euro durch den Wohnungseinbruchdiebstahl und 1.000 Euro für die Taten 28 und 40 erlangt) in Abzug gebracht.

28 d) Der nur geringfügige Erfolg seines Rechtsmittels lässt es nicht unbillig erscheinen, den Angeklagten H. mit dessen gesamten Kosten zu belasten (vgl. § 473 Abs. 4 Satz 1 StPO).

B) Revision des Angeklagten B.

29 1. Die Auffassung des Landgerichts, der Angeklagte B. sei Mittäter dieser Taten gewesen, hält revisionsgerichtlicher Überprüfung nicht stand (vgl. zum Prüfungsmaßstab BGH, Beschlüsse vom 6. August 2019 – 3 StR 189/19, NStZ 2020, 22, und vom 19. November 2019 – 4 StR 449/19, jeweils mwN).

30 Auf die konkrete Tatbegehung, das Ausspähen von Daten, hatte der Angeklagte B. keinen Einfluss und konnte auch keinen nehmen. Ihm war auch nicht bekannt, wie H. eine mögliche Zugangssicherung überwinden würde; er nahm allein an, dass dieser dabei möglicherweise würde „tricksen“ müssen. Zwar hatte er ein erhebliches Interesse am Taterfolg und durch das Versprechen einer Bezahlung sowie die Nennung der konkret auszuspähenden Postfächer auch Einfluss auf das Tätigwerden von H. . Damit unterscheidet er sich aber nicht von anderen Fällen am Taterfolg interessierter Anstifter, denen es an der Einflussnahme auf die konkrete Tathandlung fehlt (vgl. zur Abgrenzung von Mittäterschaft und Anstiftung bei vergleichbaren Fällen der Einfuhr von Betäubungsmitteln etwa BGH, Beschluss vom 15. Mai 2019 – 4 StR 591/18 mwN).

31 2. Die Feststellungen sind von diesem Wertungsfehler nicht betroffen und können deshalb bestehen bleiben (vgl. § 353 Abs. 2 StPO). Insoweit bleibt die Revision des Angeklagten B. erfolglos.

32 3. Der Senat hat erwogen, ob er auf der Grundlage der rechtsfehlerfreien Feststellungen entsprechend § 354 Abs. 1 StPO selbst den Schuldspruch auf Anstiftung zum Ausspähen von Daten in zwei Fällen ändert. Dem stünde nicht entgegen, dass der Angeklagte H. möglicherweise allgemein zur Begehung entsprechender Taten bereit war und diese Bereitschaft auch aufgezeigt oder sogar selbst die Initiative zu den Taten ergriffen hat (vgl. BGH, Urteil vom 25. Oktober 2017 – 1 StR 146/17, NStZ-RR 2018, 80, 81 mwN); ausreichend dafür wäre, dass B. – wie festgestellt – in ihm jeweils durch Benennung der

auszuspähenden Postfächer den konkreten Entschluss zur Tatbegehung geweckt hat. An einer solchen Schuldspruchänderung sieht sich der Senat allerdings durch § 265 Abs. 1 StPO gehindert, denn es erscheint nicht gänzlich ausgeschlossen, dass sich der Angeklagte B. gegen diesen Vorwurf anders – und zwar erfolgreicher – als bislang geschehen verteidigt hätte.

Cirener Mosbacher
Köhler

Resch von Häfen

Vorinstanz:
Berlin, LG, 10.04.2019 - 222 Js 1953/12 (501 -) (39/13)