
Datum: 27.07.2023
Gericht: Landgericht Aachen
Spruchkörper: 10. große Strafkammer
Entscheidungsart: Urteil
Aktenzeichen: 60 Qs 16/23
ECLI: ECLI:DE:LGAC:2023:0727.60QS16.23.00

Schlagworte: Ausspähen von Daten; Passwortsicherung; Dekompilierung
Normen: StGB § 202a
Leitsätze: Die Sicherung des Zugangs mittels Passwort reicht als Zugangssicherung aus (BGH, Beschl. vom 13.05.2020 - 5 STR 614/19)

Tenor: Auf die sofortige Beschwerde der Staatsanwaltschaft Köln vom 22.05.2023 wird der den Strafbefehlsantrag der Staatsanwaltschaft Köln vom 13.02.2023 ablehnende Beschluss des Amtsgerichts Jülich vom 10.05.2023 aufgehoben und die Sache zur erneuten Entscheidung über den Strafbefehlsantrag der Staatsanwaltschaft Köln an das Amtsgericht Jülich zurückverwiesen.

Gründe: 1

I. 2

Die Staatsanwaltschaft Köln führt gegen den Angeschuldigten ein Ermittlungsverfahren wegen Ausspähens von Daten gemäß § 202 a Abs. 1, Abs. 2 StGB. 3

Dem Verfahren liegt nach Aktenlage folgender Sachverhalt zugrunde: 4

Die geschädigte Firma V. ist Webhosting – Anbieter unter anderem für Online- Handel mit JTL- Software, einem Warenwirtschaftssystem. Diese Software stellt die V. über eine hauseigene Schnittstelle zahlreichen Firmenkunden entgeltlich zur Verfügung. Bestandteil 5

des Hostings ist die Zurverfügungstellung von Kundendatenbanken der Endkunden der jeweiligen Firmenkunden. Zu den Großkunden der V. gehören unter anderem der F., G., M. und N., sodass die V. auch im Besitz der Daten von ca. 600.000 – 700.000 Endkunden, verteilt auf die verschiedenen Online- Händler, die ihrerseits Kunden der V. sind, ist.

Zu einem nicht näher bekannten Zeitpunkt in nicht verjährter Zeit vor dem 00.00.0000 nahm der Angeschuldigte von seiner Wohnung in der Z.-straße in H. aus Zugriff auf den Datenbankserver der V.. Dies tat er, indem er zunächst mittels eines sog. Decompilers – eines für jedermann zugänglichen Programms - aus der von der geschädigten Firma genutzten Software einen Quellcode erzeugte. Dem durch die Dekompilierung erlangten Quellcode entnahm er anschließend das dort im Klartext hinterlegte Passwort, mit dem er dann die Zugangsdaten zu den jeweiligen Kundendatenbanken auslas und diese auf seinen eigenen Computer kopierte. 6

Mit Verfügung vom 13.02.2023 hat die Staatsanwaltschaft Köln den Erlass eines Strafbefehls wegen Ausspähens von Daten sowie die Festsetzung einer Geldstrafe in Höhe von 90 Tagessätzen zu je 60,00 Euro gegen den Angeschuldigten beantragt. 7

Mit Beschluss vom 10.05.2023 hat das Amtsgericht Jülich den Antrag der Staatsanwaltschaft auf Erlass des Strafbefehls aus rechtlichen Gründen abgelehnt. 8

Zur Begründung hat das Amtsgericht u.a. ausgeführt, der Tatbestand des § 202 a StGB sei nicht erfüllt. Dem Schutzbereich des Straftatbestandes unterlägen nur Daten, die gegen den unberechtigten Zugang besonders gesichert seien. Dies setze voraus, dass Maßnahmen getroffen wurden, die objektiv geeignet und nach dem Willen des Berechtigten auch dazu bestimmt seien, den Zugang zu den Daten zu verhindern. Ein Passwortschutz als solcher genüge bereits nach Auffassung des Amtsgerichts nicht, um eine besondere Sicherung im Sinne des § 202 a StGB zu begründen. Darüber hinaus habe der Angeschuldigte die Dekompilierung mittels eines gängigen Hilfsprogrammes durchgeführt, was für eine tatbestandsmäßige Überwindung einer besonderen Zugangssicherung im Sinne des § 202 a StGB nicht ausreiche. 9

Der vorgenannte Beschluss ist am 16.05.2023 der Staatsanwaltschaft Köln zugestellt worden. 10

Mit Verfügung vom 22.05.2023, bei dem Amtsgericht Jülich eingegangen am 25.05.2023, hat die Staatsanwaltschaft Köln sofortige Beschwerde gegen den Beschluss eingelegt. 11

Zur Begründung hat die Staatsanwaltschaft u.a. ausgeführt, für das geschützte Rechtsgut sei unerheblich, ob die Sicherung von Daten vor unberechtigtem Zugang schnell oder langsam, mit viel oder wenig Aufwand überwunden würde. Die Dekompilierung setze – auch wenn sie mit frei zugänglichen Programmen möglich sei – ein tiefes Verständnis über Programmiersprachen und Softwareentwicklung voraus, um mit dem Ergebnis der Dekompilierung umgehen zu können. Folglich seien die hier in Rede stehenden Daten und Passwörter nur für einen eingeschränkten Personenkreis, der über das erforderliche Fachwissen verfügt, zugänglich. 12

Die Staatsanwaltschaft Köln beantragt, 13

den Beschluss des Amtsgerichts Jülich vom 10.05.2023 aufzuheben und dem Antrag auf Erlass eines Strafbefehls der Staatsanwaltschaft Köln vom 13.02.2023 entsprechend dem Entwurf stattzugeben. 14

Mit Verfügung vom 31.05.2023 hat das Amtsgericht Jülich die Verfahrensakte dem Landgericht Aachen – Beschwerdekammer – vorgelegt. 15

II. 16

Die sofortige Beschwerde der Staatsanwaltschaft Köln vom 22.05.2023 ist gemäß §§ 408 Abs. 2 Satz 2, 210 Abs. 2 StPO statthaft und auch im Übrigen form- und insbesondere fristgerecht eingelegt worden. Die sofortige Beschwerde ist darüber hinaus begründet. Der angegriffene Beschluss war daher aufzuheben und die Sache zur erneuten Entscheidung über den Strafbefehlsantrag an das Amtsgericht zurückzuverweisen. 17

1. 18

Der Beschluss des Amtsgerichts Jülich ist aufzuheben, da das Amtsgericht zu Unrecht den Antrag auf Erlass eines Strafbefehls abgelehnt hat. Entgegen der Auffassung des Amtsgerichts besteht ein hinreichender Tatverdacht für eine Strafbarkeit des Angeschuldigten wegen Ausspähens von Daten gemäß § 202 a StGB. 19

Nach § 202 a Abs. 1 StGB macht sich strafbar, wer sich oder einem anderen Zugang zu Daten verschafft, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung. 20

Indem der Angeschuldigte dem Quellcode der Software, den er mittels Dekompilierung erlangte, dort hinterlegte Passwörter entnahm und die Daten auf seinen Rechner übertrug, hat er nicht nur das schon tatbestandsmäßige Verschaffen des bloßen Zugangs zu Daten verwirklicht, sondern zusätzlich sich die Daten selbst verschafft, was durch die Einträge in seiner Datenbank belegt wird. 21

a) Dass die Daten nicht für den Angeschuldigten bestimmt waren, folgt aus der Tatsache der Zugangsbeschränkung in Form eines Passwortes. Denn nach dem Willen der Verfügungsberechtigten - der V. - sollte der Angeschuldigte keinen Zugang zu diesen haben und die Daten sollten nicht in seinen Herrschaftsbereich gelangen (vgl. *Bär* in Wabnitz/Janovsky/Schmitt, Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl. 2020, 15. Kapitel Rn. 77; Lackner/Kühl/Heger StGB, 30. Aufl. 2023, § 202 a Rn. 3). Soweit es um den dekompierten Quellcode der Software als solcher geht, ist auch dieser nicht für den Angeschuldigten bestimmt gewesen. Denn insoweit gelten die für Daten entwickelten Grundsätze entsprechend auch für Computerprogramme. Soweit eine Dekompilierung des Objektcodes in den Quellcode urheberrechtlich nach den § 69 e i.V.m. § 69 c Nr. 1 UrhG unzulässig ist – etwa wenn sich der Täter nicht an die durch den Lizenzvertrag und den Programmschutz gezogenen Grenzen hält - fehlt es an einer Datenbestimmung für den Täter mit der Folge, dass eine Strafbarkeit nach § 202 a StGB – vorbehaltlich des Vorliegens der weiteren Tatbestandsvoraussetzungen – eröffnet ist (vgl. *Bär* a.a.O. Rn. 78; MüKoStGB/Graf StGB 4. Aufl. 2021 § 202a Rn. 34). 22

b) Die Daten waren auch gegen unberechtigten Zugang besonders gesichert. Dies ist der Fall, wenn Vorkehrungen getroffen sind, den Zugriff auf Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Das Erfordernis der besonderen Sicherung gegen unberechtigten Zugang zeigt die Schranke an, deren Überwindung kriminelles Unrecht begründet. Sie rechtfertigt sich, weil der Verfügungsberechtigte mit der Sicherung sein Interesse an der „Geheimhaltung“ - ähnlich wie in § 202 Abs. 2, § 243 Abs. 1 Satz 2 Nr. 2 - dokumentiert und - das ist in normativer Hinsicht ausschlaggebend - durch diese Wahrnehmung eines ohne Weiteres zumutbaren Selbstschutzes auch des zusätzlichen 23

Strafrechtsschutzes würdig und bedürftig wird (vgl. BGH, Beschl. v. 13.05.2020 – 5 StR 614/19 – NStZ-RR 2020, 279 (280); *Hilgendorf* in: LK- StGB, 13. Aufl. 2023, § 202 a Rn. 18).

Im vorliegenden Fall war der Zugang durch Passwörter gesichert, deren Abrufen zudem nur nach einer Dekompilierung möglich war. Die Sicherung des Zugangs mittels Passwort reicht als Zugangssicherung aus (BGH, Beschl. v. 13.05.2020 – 5 StR 614/19 –, a.a.O.). 24

Bei einem Passwort handelt es sich um eine typische Software- Sicherung, die das Interesse an einer Zugangssicherung eindeutig dokumentiert. Maßgeblich ist, ob die Sicherung geeignet erscheint, einen wirksamen, wenn auch nicht absoluten Schutz zu erreichen. Erforderlich ist - nach der Gesetzesbegründung - dass die Überwindung dieser Sicherung einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordert (vgl. BT- Drs. 16/3656). Dies wäre jedenfalls dann zu verneinen, wenn die Aufhebung des Schutzes ohne weiteres möglich ist und durch jeden interessierten Laien leicht überwunden werden könnte. Vom Schutzbereich ausgenommen sind insbesondere auch Fälle, in denen das Opfer selbst nachlässig mit den eigenen Daten umgeht und eine sehr leicht ausschaltbare Sicherung wählt. Keine technischen Vorkehrungen wären folglich standardisierte Logins und Passwörter (zB Ziffernfolge 0000 bei allen Geräten), da hier zur Dokumentation der Geheimhaltung zunächst eine Änderung notwendig wäre (vgl. *Eisele* in: Schönke/Schröder, StGB 30. Aufl. 2019 § 202a Rn. 14; *Kargl* in: Kindhäuser/Neumann/Paeffgen/Saliger, StGB, 6. Auflage 2023, § 202a Rn. 42). 25

Entgegen der Auffassung des Amtsgerichts stellt das Auslesen des Passwortes nach Dekompilierung des Objektcodes in den Quellcode eine Überwindung einer besonderen Zugangssicherung im Sinne des § 202 a StGB auch dann dar, wenn sie mit für jedermann zugänglichen Tools erfolgt ist. 26

Soweit in den Gesetzesmaterialien von einer „Überwindung mit einem nicht unerheblichen zeitlichen oder technischen Aufwand“ die Rede ist, ist dies dahingehend zu verstehen, dass die Überwindung der Zugangssicherung typischerweise – also unabhängig von spezifischen Möglichkeiten oder Kenntnissen des konkreten Täters – einen nicht unerheblichen Aufwand erfordern muss. Auch wenn eine Zugangssicherung auf Grund besonderer Kenntnisse, Fähigkeiten oder Möglichkeiten schnell und ohne besonderen Aufwand überwunden wird, ist der Tatbestand erfüllt (BGH, Beschl. v. 13.05.2020 – 5 StR 614/19, a.a.O.). 27

Mit der Änderung des § 202a StGB durch das 41. StrÄndG im Jahre 2007 hat der Gesetzgeber unter Umsetzung des Übereinkommens des Europarates über Computerkriminalität aus dem Jahre 2001 und des entsprechenden Rahmenbeschlusses, u.a. das „Hacking“ unter Strafe gestellt. Maßgeblich ist seitdem bereits das Verschaffen von Zugang, nicht erst das Abrufen der Daten. Der Tatbestand soll damit den persönlichen- und Geheimbereich des Verfügungsberechtigten der Daten sichern, als auch seine wirtschaftlichen Interessen auf seine Daten vor unbefugtem Zugriff schützen (vgl. Fischer, StGB, 70. Aufl. 2023, § 202a Rn. 2; *Vassilaki* in: CR 2008, 131). Der Umstand, dass bereits der Zugang - unabhängig von der Motivation mit der sich der Betreffende den Zugang verschafft - unter Strafe gestellt ist, zeigt, dass die Norm zudem auch dem Schutz der Integrität der Informationssysteme als solchen und nicht nur dem Datenschutz des Einzelnen dient. Dieser Schutzzweck wäre nicht gewährleistet, wenn die Strafbarkeit alleine an die Verwendung bestimmter Programme geknüpft wäre. Schließlich wäre eine Abgrenzung zwischen leicht und schwer zugänglichen Hilfsprogrammen zu unkonkret, um dem im Strafrecht gebotenen Bestimmtheitsgrundsatz gerecht zu werden. 28

Die Anforderungen an den notwendigen „nicht unerheblichen zeitlichen oder technischen Aufwand“ zur Überwindung der Sicherung (so BT-Drs. 16/3656 S. 10) dürfen daher zum Schutz technischer Laien und vor dem Hintergrund des Bestimmtheitsgrundsatzes nicht zu hoch angesetzt werden. Der Zugangsschutz muss nicht vollständig sein. Es ist ein „weites Verständnis“ des Überwindens einer Zugangssicherung zugrunde zu legen, bei dem eine Orientierung am technischen Laien angezeigt ist. Denn auch dem technischen Laien muss die grundrechtlich garantierte Möglichkeit eingeräumt werden, geschützte formale Geheimbereiche zu schaffen. Auch dass der Gesetzgeber mit § 202 a StGB nur einen eingeschränkten Täterkreis erfassen wollte, ergibt sich weder aus dem Wortlaut der Norm noch aus den Motiven. § 202 a StGB ist kein auf professionelle Angreifer beschränktes Sonderdelikt (vgl. *Kargl* in: Kindhäuser/Neumann/Paeffgen/Saliger StGB a.a.O. Rn. 42; *Schumann*, NStZ 2007, 677).

Es ist auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter abzustellen, nicht darauf, ob Eingeweihte oder Experten leicht auf die Daten zugreifen können. Für das geschützte Rechtsgut ist es unerheblich, ob die Sicherung von Daten vor unberechtigtem Zugang schnell oder langsam, mit viel oder wenig Aufwand überwunden wird. Der Gesetzgeber wollte aus dem Tatbestand neben Bagatelldaten lediglich solche Fälle ausschließen, in denen die Durchbrechung des Schutzes für jedermann ohne weiteres möglich ist, nicht aber solche, in denen die Zugangssicherung auf Grund spezieller Kenntnisse oder Möglichkeiten im Einzelfall leicht überwunden wird. Nur eine solche abstrakt-generelle Betrachtungsweise lässt sich mit dem Schutzzweck der Norm vereinbaren (vgl. BGH, Beschl. v. 13.05.2020, a.a.O).

Ausgehend hiervon hat der Angeschuldigte eine Zugangssicherung überwunden, durch die der Verfügungsberechtigte erkennbar den Zugang zu den Daten verhindern wollte und dadurch die strafwürdige kriminelle Energie manifestiert. Dass dies für ihn einfach – und gegebenenfalls mit wenigen „Maus- Clicks“ möglich war - hindert eine Strafbarkeit nicht (vgl. BGH, Beschl. v. 13.05.2020 a.a.O). Auch wenn er für die Dekompilierung frei zugängliche Programme verwendet hat, so setzt eine solche Vorgehensweise sowohl ein tieferes Verständnis über Programmiersprachen und Softwareentwicklung als auch ausgeprägte Kenntnisse im Bereich der Anwendungsentwicklung und die Fähigkeit zum sogenannten Reverse Engineering der Softwareschnittstelle voraus. Die in Rede stehenden Daten waren – eine abstrakt generelle Betrachtungsweise zugrunde gelegt - für den Angeschuldigten aufgrund seiner Kenntnisse leicht abgreifbar, indes „typischerweise“ nicht für Jedermann ohne weiteres möglich.

c) Dazu war er nicht befugt im Sinne des § 202 a StGB, da die ausgespähten Daten nicht zu seiner Kenntnisnahme bestimmt waren (vgl. Fischer, StGB, a.a.O. Rn. 12).

2. 33

Die Kammer hat die Sache zur erneuten Entscheidung über den Strafbefehlsantrag der Staatsanwaltschaft Köln vom 13.02.2023 an das Amtsgericht Jülich zurückverwiesen. Eine an sich gemäß § 309 Abs. 2 StPO gebotene Entscheidung in der Sache kann die Kammer nicht treffen, da für den Erlass des von der Staatsanwaltschaft beantragten Strafbefehls im Hinblick auf §§ 407 Abs. 1 Satz 1, 408 Abs. 1 StPO allein der Strafrichter zuständig ist (vgl. hierzu Löwe-Rosenberg/Gössele, StPO, 26. Aufl. 2009, § 408 Rn. 24 m.w.Nachw.). Auch eine Aufhebung des Beschlusses mit der Anweisung an den Strafrichter, den Strafbefehl antragsgemäß zu erlassen oder über den Antrag der Staatsanwaltschaft unter Beachtung der Rechtsauffassung des Beschwerdegerichts erneut zu entscheiden, ist nicht möglich, da damit in unzulässiger Weise in die Entschließungsfreiheit des Strafrichters eingegriffen würde 34

(zutreffend Löwe-Rosenberg/GösseI, StPO, a.a.O. Rn. 24, 25; KK-StPO/Maur, 8. Aufl. 2019, § 408 Rn. 13; ohne nähere Begründung a.A. LG Landshut, Beschl. v. 20.10.2009 – 4 Qs 237/09, NStZ-RR 2010, 78 f.). Aus diesem Grund kann die Kammer – wie geschehen – den angegriffenen Beschluss lediglich aufheben und die Sache zur neuen Entscheidung an das Amtsgericht zurückverweisen (vgl. LG Aachen, Beschl. v. 05.10.2020 – 60 Qs 43/20; LG Saarbrücken, Beschl. v. 17.10.2017 – 8 Qs 112/17, juris Rn. 6; Löwe-Rosenberg/GösseI, StPO, 26. Aufl. 2009, § 408 Rn. 25; KK-StPO/Maur, 8. Aufl. 2019, § 408 Rn. 13).

3. 35

Eine Entscheidung über die Kosten des Beschwerdeverfahrens und die notwendigen Auslagen der Beteiligten ist nicht veranlasst. Die Kosten- und Auslagentragung im Beschwerdeverfahren folgt vielmehr jener in der Hauptsache (vgl. OLG Stuttgart, Beschl. v. 07.06.2001 – 5 Ws 4/01, juris; OLG Rostock, Beschl. v. 27.11.2015 – 20 Ws 192/15, juris Rn. 41; OLG Hamm, Beschl. v. 29.09.2016 – 4 Ws 302/16, juris; ohne nähere Begründung a.A. LG Saarbrücken, Beschl. v. 17.10.2017 – 8 Qs 112/17, juris Rn. 7). 36

Die Kosten des Beschwerdeverfahrens werden der Staatskasse auferlegt. 37

K.	U.	D.	38
----	----	----	----