Journal of Siberian Federal University. Humanities & Social Sciences 3 (2019 12) 438-454
~ ~ ~

УДК 343.13(430)

Challenges for Criminal Law in a Digitized World – the Solutions of German Criminal Legislation

Edward Schramm*
Friedrich Schiller University of Jena
Germany

Received 04.02.2019, received in revised form 14.02.2019, accepted 06.03.2019

The digitization of our world is causing a profound change in living conditions. The article discusses how German criminal law and criminal procedure law deals with the resulting challenges. In substantive criminal law, the technology required for digitization and the datas are protected against harmful manipulation by various german criminal offenses specifically related to computer software and hardware. The data change does not require that the offender overcomes certain access safeguards. In the offense of sabotage of hardware and software, the hacker attacks on the computer-controlled supply of systemically important infrastructures (water, electricity, gas) are threatened with increased punishment. Privacy in digital communication is protected against spying on data. In Germany is also a discussion about the introduction of a new criminal offense "digital trespassing". Unlawful content on the internet is largely criminalized, such as insults, discrimination, child and youth pornography, cybergrooming, cyberbullying and cybermobbing.

Also the german criminal procedure law contains a wide range of instruments that enable the state to observe digital communication. Thus, the German StPO (Criminal Procedure Code) allows the search and seizure of computers and cloud computing. The planned EU-Regulation of Production and Preservation Orders for electronic evidence in criminal matters is designed to oblige telecommunications companies to secure and release electronic evidence for criminal proceedings throughout the EU. The monitoring of encrypted Skype and Whats App phone calls is possible in the installed software on the device, so the call can be unencrypted listened and recorded before encryption. In addition, law enforcement institutions are allowed to monitor a computer via the Internet using software installed externally on the PC (so-called „online searchings"). However, insights that come solely from the core area of personal life may not be gained by police and used in procedure (§ 100d StPO). In the end, the critique of digitization and the political demands for a post-digital age are briefly discussed.

Keywords: Spying on data, computer sabotage, cybergrooming, cyberbullying, digital detox, core area of personal life, online searches, post-digital age, sabotage of systemically important infrastructure.

Research area: law.

* Corresponding author E-mail address: edward.schramm@uni-jena.de

Citation: Schramm, E. (2019). Challenges for Criminal Law in a Digitized World – The Solutions of German Criminal Legislation). J. Sib. Fed. Univ. Humanit. soc. sci., 12(3), 438-454. DOI: 10.17516/1997-1370-0403.

Herausforderungen an das Strafrecht in einer digitalisierten Welt. Die Lösungsansätze der deutschen Strafgesetzgebung

Edward Schramm
Friedrich-Schiller-Universität Jena
Faculty of Law
Carl-Zeiss-Strasse 3, Jena 07743, Germany

Die Digitalisierung unserer Welt führt zu einer tief greifenden Veränderung der Lebensbedingungen. Im Beitrag wird - im Überblick - dargestellt, wie das deutsche Strafrecht und Strafverfahrensrecht bislang auf die sich daraus ergebenden Herausforderungen reagiert hat. Im materiellen Strafrecht werden die für die Digitalisierung erforderliche Technologie und die Daten gegen schädliche Manipulationen durch verschiedene deutsche Straftatbestände geschützt, die sich speziell auf die Software und Computerhardware erstrecken. Die Strafnorm der Datenveränderung (§ 303a StGB) setzt dabei nicht voraus, dass der Täter bestimmte Zugangsbarrieren überwindet. Beim Straftatbestand der Computersabotage (§ 303b StGB) ist der Angriff auf die computergesteuerte Versorgung von systemisch wichtigen Infrastrukturen (wie z. B. Wasser, Strom, Gas) mit einem erheblich erhöhten Strafrahmen verbunden. Die Daten in der digitalen Kommunikation werden strafrechtlich vor dem Ausspähen geschützt (§ 202 a StGB). Auch werden in Deutschland verstärkt Forderungen nach der Einführung eines neuen Straftatbestands, des „digitalen Hausfriedensbruchs", erhoben. Rechtswidrige Inhalte im Internet wie z. B. Beleidigungen, Diskriminierungen, Kinder- und Jugendpornografie, Cyber-Grooming und Cybermobbing sind übrigens ebenfalls sehr weitgehend unter Strafe gestellt.

Auch das deutsche Strafprozessrecht enthält ein breites Spektrum von Instrumenten, die es dem Staat ermöglichen, die digitale Technik und Kommunikation zu überwachen. So erlaubt die deutsche StPO (Strafprozessordnung) die Durchsuchung und Beschlagnahme von Computern und Inhalten im Cloud Computing (§§ 94, 102, 110 StPO). Die geplante EU-Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen hat zum Ziel, Telekommunikationsunternehmen zur Sicherung elektronischer Beweismittel zu verpflichten und diese Beweise bei grenzüberschreitender Strafverfolgung erleichtert zur Verfügung zu. Die Überwachung verschlüsselter Skype- und Whats App-Telefonanrufe ist ebenfalls seit 2017 erlaubt: Sie geschieht dergestalt, dass auf dem Gerät eine Software installiert wird, mittels derer der Anruf unverschlüsselt abgehört und vor der Verschlüsselung aufgenommen werden kann (sog. Quellen-Telekommunikationsüberwachung; § 100a Abs. 1 S. 2 StPO). Darüber hinaus können Strafverfolgungsorgane seit 2017 einen Computer über eine Internetverbindung überwachen und durchsuchen, in dem von außen auf dem PC eine Software heimlich installiert wird (sog. Online-Durchsuchung, § 100 b StPO). Informationen aus dem Kernbereich der persönlichen Lebensgestaltung dürfen aber weder bei der Online-Durchsuchung noch bei der Quellen-

Telekommunikationsüberwachung von der Polizei erhoben oder verwertet werden (§ 100d StPO). Am Ende des Beitrags werden die Kritik an der Digitalisierung und politische Forderungen nach einem postdigitalen Zeitalter angesprochen.

Stichworte: Ausspähen von Daten, Computersabotage, Cybergrooming, Cybermobbing, digitales Detox, Kernbereich persönlicher Lebensgestaltung, Online-Durchsuchung, post-digitales Zeitalter, Sabotage von systemrelevanter Infrastruktur.

I. Der strafrechtlicher Schutz von Daten und Technik

1. Die Veränderung von Daten

Zum Schutz der Daten enthält das deutsche Strafrecht den Straftatbestand der Datenveränderung (§ 303 a StGB).[1]

a) Tatobjekt

Tatobjekt sind Daten. Daten definiert das Strafgesetzbuch in § 202a Abs. 2 StGB als Informationen, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202 a Abs. 2 StGB). Es sind beispielsweise alle Informationen, die auf der Festplatte eines Computers oder auf der Speicherkarte eines Smartphones gespeichert sind und die erst über den Bildschirm des Geräts optisch wahrgenommen werden können. Ob die Daten einen Vermögenswert besitzen, ist unerheblich. Es fallen darunter auch Programmdaten, da auch sie aus einer Vielzahl von nicht sinnlich unmittelbar wahrnehmbaren Informationen enthalten.

b) Tathandlung

Die vom Tatbestand umschrieben Tathandlung lässt sich unter den Oberbegriff der „Veränderung“ von Daten fassen, Sie erstreckt sich neben der (inhaltlichen) Veränderung der Daten auch auf das Löschen, Unterdrücken (= Verhinderung des Zugangs zu den Daten) oder das Unbrauchbarmachen. Soweit aufgrund des Zugriffs die Daten nachteilig verändert wurden, könnte man § 303a StGB auch als „digitale Sachbeschädigung“ umschreiben. Es ist für die Strafbarkeit übrigens nicht erforderlich, dass der Täter eine Zugangssicherung auf die Daten überwindet.

So hatte der Bundesgerichtshof (BGH) *in seinem sog. „Bitcoin-Urteil“*[2] *über die Strafbarkeit eines angeklagten Computerprogrammierers zu befinden, der mit Hilfe eines illegalen Botnets sog. Bitcoins geschaffen hatte. Bitcoins sind eine virtuelle Währung, mit der man im Internet bezahlen kann (z. B. Dienstleistungen,*

[1] Die Strafnorm lautet: § 303a Abs. 1: Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Abs. 2 Der Versuch ist strafbar.

[2] BGH Neue Zeitschrift für Strafrecht, 2018, S. 401 mit Bspr. *Safferling*.

Serverleistungen, Kleidung, Bücher usw.). Damit dieses bargeldlose Zahlungssystem funktioniert, müssen sehr rechner- und stromintensive Rechenoperationen durchgeführt werden. Wer sein Computersystem für diese Rechenoperationen zur Verfügung stellt, wird dafür mit Bitcoins belohnt, seine Rechnerleistungen sind quasi die Goldmine, die Bitcoin-Mine, daher Bitcoin-Mining.

Der Angeklagte, ein 29jähriger Mann aus Bayern, entwickelte eine spezielle Schadsoftware. Es verbreitete sie, indem er im sog. Usenet, einem kostenpflichtigen Teil des Internets, das für illegale Zwecke genutzt wird, Dateien Video- und Musikdateien zum Download bereitstellte. Die Dateien waren mit Trojanern, also einer getarnten Schadsoftware, infiziert. Wäre die Schadsoftware nicht als Musik- oder Videodatei getarnt gewesen, hätte die auf den Computern installierte Schutzsoftware, die Firewall, das Schadprogramm erkannt und die Installation verhindert. Mit dieser Software schloss er 325.000 Rechner zu einem Netzwerk zusammen. Unter einem Botnetz lässt sich der illegale Zusammenschluss einer Vielzahl (von wenigen Hundert bis hin zu mehreren Millionen) Systemen bezeichnen, welche unerkannt infiziert und mittels eines sogenannten „Command-and-Control-Servers" ferngesteuert und damit für kriminelle Zwecke missbraucht werden können. Damit konnte er die Rechenleistung, die diese Computer erbrachten, zur Generierung von Bitcoins verwenden. Er schuf so rund 1870 Bitcoins, das entspricht einem Geldwert von ungefähr 500.000 EUR. Der 1. Strafsenat des Bundesgerichtshofs erblickte bereits in dem Hinzufügen von Einträgen in die sog. Registry-Datei der Computer Computers und der damit verbundenen Veränderung des in der Datei nt.user.dat hinterlegten Benutzerprofil eine Veränderung von Daten i. S: d. § 202a StGB. [1]

c) Schutzzweck und Geschichte

Die Strafnorm des § 202a StGB wurde bereits 1986 in das Strafgesetzbuch eingefügt.[2] Ihr Schutzzweck besteht darin, demjenigen, der über die Daten verfügungsberechtigt ist, die Unversehrtheit seiner Daten und eine nicht durch Dritte manipulierte Verwendung seiner Daten[3] zu sichern. Anders formuliert: Strafbar macht sich derjenige, der die Datenautonomie des „Dateneigentümers" oder des sonst Nutzungsberechtigten verletzt.[4] Wer also unberechtigt, d. h. ohne die Zustimmung

1 BGH NStZ 2018, S. 401 Rn. 34.

2 Durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (zur Entstehungsgeschichte vgl. *Hilgendorf,* in: Satzger/Schluckebier/Widmaier, Kommentar zum Strafgesetzbuch, 4. Aufl. 2018, § 303a Rn. 1.

3 *Schramm*, Strafrecht Besonderer Teil 1, Straftaten gegen das Eigentum und das Vermögen, Baden-Baden 2017, § 6 Rn. 46.

4 Zum Personenkreis der Nutzungsberechtigten vgl. *Wieck-Nodt*, in: Münchener Kommentar zum StGB, 3. Aufl. 2019, § 303a Rn. 9.

Verfügungsberechtigten, die Daten auf einem Server oder einem Computer ändert, löscht oder unterdrückt, macht sich strafbar.

Dazu gehören auch Attacken auf ein Computersystem, die dazu führen, dass es eine gewisse Zeit nicht genutzt werden kann. Beispiele hierfür bilden das Senden massenhafter E-Mails an einen Server oder sogenannte Denial-of-Service-Attacken, die ein Computersystem lahmlegen.[1]

Bedauerlicherweise verzichtet das deutsche Strafrecht darauf, für die Strafbarkeit den Eintritt eines Schadens zu verlangen, obwohl die Cybercrime-Konvention des Europarats diese Einschränkung erlaubt hätte. Die nichtschädigende Datenveränderung als solche genügt dagegen bereits in Deutschland für die Strafbarkeit.[2] Unerheblich ist auch, ob die Daten irgendeinen Beweiswert haben.[3]

d) Vorsatz, Versuch, Vorbereitung

Die Tat ist ein Vorsatzdelikt. Der Versuch ist strafbar (§ 303a Abs. 2 StGB). Dabei ist infolge einer Gesetzesänderung aufgrund der Cybercrime-Konvention des Europarats 2007 die Strafbarkeit weit in das Vorbereitungsstadium ausgedehnt worden (§ 303 a Abs. 3 StGB i. V. m. § 202 a StGB): Denn es ist bereits strafbar, wenn sich der Täter sich die Mittel besorgt, mit denen er später auf die Daten zugreifen möchte (z. B. durch den Kauf oder die Entwicklung einer Software, eines Sicherheitscodes oder Passwörtern). Diese Vorfeldkriminalisierung wird in der Rechtswissenschaft kritisiert, für überflüssig gehalten und auch nicht nach den europarechtlichen Vorgaben für erforderlich gehalten.[4]

2. Beschädigung von Computer-Hardware und Software

a) § 303 b, Computersabotage

Über den Straftatbestand der Computersabotage (§ 303b Abs. 1 StGB) [5] wird das Interesse aller Betreiber und Nutzer von Computern an einem störungsfreien Ablauf der Datenverarbeitungsvorgänge geschützt.[6] Die betriebliche und behördliche

1 *Schramm*, BT-1, § 6 Rn. 52.
2 *Schramm,* BT-1, § 6 Rn. 45.
3 *Hilgendorf,* in: Satzger/Schluckebier/Widmaier, § 303a Rn. 4.
4 *Hilgendorf,* in: Satzger/Schluckebier/Widmaier, § 303a Rn. 14.
5 § 303b Abs. 1 StGB lautet: Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er 1. eine Tat nach § 303a Abs. 1 begeht, 2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder 3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
6 *Hecker,* in: *Schönke/Schröder*, StGB, 30. Aufl. 2018, § 303b Rn. 1.

Datenverarbeitung und damit das kollektive Interesse an der Aufgabenerfüllung durch bestimmte Verwaltungs- und Wirtschaftseinheiten[1] wird eigens und mit höher Strafdrohung in § 303b Abs. 2 geschützt.[2]

Der Tatbestand erfasst zunächst (§ 303 b Abs. 1 Nr. 1 StGB) die Datenmanipulation, die zu Störungen in der Datenverarbeitung führt (z. B. die Verarbeitung fehlerhafter Software). Er bestraft auch (§ 303 b Abs. 1 Nr. 2 StGB) die Eingabe von Daten zum Zweck der Nachteilszufügung. Gemeint sind damit z. B. Denial of Service-Attacken, d. h. kontrollierte Angriffe auf Computer durch eine Vielzahl von Anfragen, die zur Überlastung des Computersystems führen.[3] Auch die Durchführung einer DDos-Attacke auf einen fremden Server über ein sog. Bot-Netz (d.h. ein Netzwerk von Rechnern, die durch illegales Aufspielen von Schadsoftware ferngesteuert werden können), kann den Tatbestand einer Computersabotage erfüllen.[4] Die Norm pönalisiert aber auch Angriffe auf die Hard- und Software in der Form, dass ein Computer oder ein Computerprogramm beschädigt, zerstört, unbrauchbar gemacht oder beseitigt wird (§ 303 b Abs. 1 Nr. 3).

Durch diese Sabotagehandlungen muss eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich gestört werden. Damit sind Computervorgänge im Rahmen einer wissenschaftlichen, künstlerischen oder schriftstellerischen Tätigkeit oder einer Erwerbstätigkeit erfasst (z. B. die auf einem Computer gespeicherte Seminar- oder Doktorarbeit), nicht aber Computerspiele. Die Störung ist erheblich, wenn die Datenverarbeitung nicht unerheblich beeinträchtigt wird. Daran würde es fehlen, wenn ein Virus die Ausführung einzelner Programme stört oder verhindert, die für den Betroffenen nicht wesentlich sind.[5]

b) Besonders schwere Fälle der Computersabotage

Eine Strafschärfung ist im Falle der Computersabotage namentlich für diejenigen Fälle vorgesehen (§ 303b Abs. 4 Nr. 3 StGB), in denen durch die Manipulation die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt werden.[6] Hier beträgt

---

1 *Hoyer,* Systematischer Kommentar, 9. Aufl, 2016, § 303b Rn. 3.

2 § 303 b Abs. 2 lautet: Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

3 *Fischer,* StGB, 66. Aufl. 2019, § 303b Rn. 11.

4 *Hilgendorf*, in: Satzger/Schluckebier/Widmaier, § 303b Rn. 10.

5 *Fischer*, StGB, § 303b Rn. 10.

6 *Schramm,* BT-1, § 6 Rn. 59.

die Freiheitsstrafe mindestens 6 Monate, die Höchststrafe 10 Jahre Freiheitsstrafe (§ 303 b Abs. 4 StGB). Vor dem Hintergrund der zunehmenden Digitalisierung der Lebenswelten (sog. Internet der Dinge) betreffen die Hackerattacken auch die computergesteuerte Versorgung mit systemrelevanten kritischen Infrastrukturen. Dazu zählen Ressourcen wie z. B. der Datenaustausch über das Internet (z. B. Hackerangriffe auf deutsche Internet-Router), auf das Wasser, den Strom, das Gas oder medizinischen Dienstleistungen.

Digitale Angriffe auf Computersysteme können auch vom Ausland aus erfolgen. So wurde in Deutschland schon mehrfach über Angriffe berichtet, die von den USA oder von Russland aus auf deutsche Computer vorgenommen werden und dabei erhebliche infrastrukturelle Schäden anrichten. Eine Strafbarkeit nach deutschem Recht ergibt sich bei solchen Hackerattacken aus dem Ausland deshalb, weil der schädliche Erfolg in Deutschland eintritt (§ 9 Abs. 1 StGB) und damit der Tatort (§ 3 StGB) nicht nur am ausländischen Handlungsort, sondern auch am deutschen Erfolgsort liegt.[1]

II. Der Schutz der Privatsphäre bei digitaler Kommunikation

1. Ausspähen von Daten

Unter Strafe gestellt ist auch das Ausspähen von Daten (§ 202 a StGB).[2] Die Norm ist auf die strafrechtliche Erfassung des „einfachen" Hackens (ohne Datenveränderung oder Datensabotage) gerichtet. Rechtsgut ist mithin das Geheimhaltungsinteresse des Verfügungsberechtigten sowie die Verfügungsbefugnis über Daten.[3] Tatobjekt sind dabei Daten, die nicht für Täter bestimmt sind. Die Tathandlung ist dabei das Gewinnen des Zugangs zu Daten durch Überwindung einer Zugangssicherung. So soll die russische Hackergruppe Snake im März 2018 einen Hackerangriff auf die Computer der Deutschen Bundesregierung vorgenommen und dadurch Regierungsgeheimnisse erlangt haben.[4]

Der BGH hatte es in den vergangenen Jahren dabei zweimal mit einem besonderen Phänomen des Ausspähens von Daten zu tun, nämlich dem bereits oben erwähnten

---

1 Zum Territorialitätsprinzip vgl. *Schramm*, Internationales Strafrecht: Strafanwendungsrecht – Völkerstrafrecht – Europäisches Strafrecht, 2. Aufl. 2018, 1. Kap. Rn. 34 ff.

2 Die Norm lautet: § 202a Abs. 1 Wer unbefugt 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, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Abs. 2: Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

3 *Heger,* in: Lackner/Kühl, 39. Aufl. 2018, § 202a Rn. 1.

4 https://www.zeit.de/politik/deutschland/2018-03/cyber-attacke-hackerangriff-parlamentarisches-kontrollgremium-armin-schuster-reaktionen

sog. Bitcoin-Mining.[1] Hierzu wird vielfach eine schädliche Software heimlich auf hunderttausende Computer aufgespielt, mittels dessen dann Bitcoins, also digitales Geld, geschaffen werden kann. Die Frage, die den BGH insbesondere beschäftigte, war, ob derjenige, der die Software in die fremden Computer eingeschmuggelt hatte, dabei eine Zugangssicherung überwunden hat.[2] Denn die Software wurde von den Nutzern selbst unbemerkt beim Herunterladen von Musikdateien oder Spielfilmen heruntergeladen. Genügt hierfür bereits eine Firewall, und wie kann man feststellen, ob die Computer überhaupt eine Firewall hatten? Der BGH bejaht dies, obwohl die Existenz dieser Firewall beim konkreten Benutzer nur vermutet, nicht aber konkret festgestellt werden konnte.[3] Durch die Überwindung der Firewall hat sich der Täter den Zugang auf die Daten des Computers verschafft und einen Teil dieser Daten dann auch auf seinen Computer kopiert.[4]

2. Forderung nach einem Straftatbestand „Digitaler Hausfriedensbruch"

Aus diesem Grund wird nun in Deutschland die kriminalpolitische Forderung erhoben, einen neuen Straftatbestand zu schaffen, nämlich den sogenannten digitalen Hausfriedensbruch.[5] Diese Norm würde dann das „digitale Hausrecht" erfassen, vergleichbar dem über § 123 StGB, Hausfriedensbruch, geschützten Recht am Haus oder der Wohnung. Damit würde es bereits unter Strafe gestellt, wenn jemand unbefugt fremde informationstechnische Systeme nutzt. Der Überwindung einer besonderen Zugangssicherung bedürfte es dann nicht. Kritiker weisen dagegen darauf hin, dass eine solche Norm nicht nötig sei. Vielmehr sollten Softwarehersteller bessere Programme erfinden, die den Zugriff von außen verhindern. Den Einsatz des Strafrechts bedürfe es nicht.[6]

---

1 BGH, Neue Juristische Wochenschrift (NJW), 2015, S. 3463;

2 Von BGH ursprünglich noch bezweifelt (BGH NJW 2015, 3463), vom selben 1. Strafsenat dann aber wegen der vom Tatgericht LG Memmingen getroffenen Feststellungen nicht mehr beanstandet; vgl. BGH, NStZ 2018, S. 401.

3 BGH NStZ 2018, 401.

4 BGH NStZ 2018, 401 Rn. 43.

5 Gesetzesinitiative des Landes Hessen, Bundesratsdrucksache 338/16. Der Gesetzentwurf lautet: § 202e, Unbefugte Benutzung informationstechnischer Systeme: Wer unbefugt 1. sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft, 2. ein informationstechnisches System in Gebrauch nimmt oder 3. einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt, wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft (..)

6 *Kahler/Hoffmann-Holland*, Digitale Rechtsgüter zwischen Grundrechtsschutz und kollektiver Sicherheit, KriPoZ (Kriminalpolitische Zeitschrift) 2018, 267; *Movany*, Pferde, Würmer, Roboter, Zombies und das Strafrecht? Vom Sinn und Unsinn neuer Gesetze gegen den sog. digitalen Hausfriedensbruch, KriPiZ 2016, 106.

III. Die Bekämpfung von rechtswidrigen Inhalten im Internet

1. Die Strafbarkeit der Verbreitung der Inhalte

Das Internet ist kein rechtsfreier Raum. Beleidigung (§ 185 StGB) und Volksverhetzung (§ 130 StGB) im Internet sind genauso strafbar wie die Verbreitung von Kinder- und Jugendpornographie (§ 184 ff. StGB) oder das sog. Cyber-Grooming, d. h. die sexuelle Belästigung von Kindern und Jugendlichen im Internet etwa innerhalb eines Chats (§ 176 Abs. 4 StGB).

In Deutschland ist außerdem das Verbreiten bestimmter Fotos im Internet unter Strafe gestellt. So hat Deutschland einen Straftatbestand des Cyber-Mobbing geschaffen (§ 201 a Abs. 2 StGB). Danach macht sich strafbar, wer Bildaufnahmen im Internet verbreitet, die geeignet sind, dem Ansehen der abgebildeten Person erheblichen Schaden zuzufügen. Dem Gesetzgeber geht es dabei um Abbildungen von Situationen, die nach gesellschaftlicher Bewertung als minderwertig, peinlich, eklig oder unfreiwillig offenbarend angesehen werden.[1] Das kann bei Bildern der Fall sein, mit denen die Betrunkenheit oder die Nacktheit einer Person gezeigt wird.

Es wird aber auch die sonstige Verbreitung von Bildern im Internet unter Strafe gestellt, die aus dem höchstpersönlichen Lebensbereich eines Menschen stammen (§ 201 a Abs. 1 Nr. 1 StGB). Ebenso dürfen Bilder nicht im Internet verbreitet werden, mit denen die Hilflosigkeit anderer zur Schau gestellt wird (z. B. Handyaufnahmen von Schwerverletzten eines Unfalls; § 201 a Abs. 1 Nr. 2 StGB). Sogar das käufliche Anbieten oder Verschaffen bloßer Nacktaufnahmen von Jugendlichen und Kindern wurde vom Deutschen Bundestag 2017 unter Strafe gestellt (§ 201 a Abs. 3 StGB), nachdem sich ein hochrangiger deutscher Bundestagsabgeordneter in großem Umfang Nacktfotos von jungen Männern über das Internet gekauft hat.[2] Dies ist eine Norm, die von vielen deutschen Rechtswissenschaftlern zu Recht als verfassungswidrig angesehen wird, da hiermit nur unmoralisches, nicht aber schädliches Verhalten bestraft wird.[3]

2. Einbindung von Netzwerkbetreibern

Durch das im Oktober 2017 in Kraft getretene deutsche Netzwerkdurchsetzungsgesetz (NetzDG) werden zudem Netzwerkbetreiber mit einer Teilnehmerzahl von mindestens 2 Millionen – also vor allem Facebook, You Tube und Twitter -, zu folgendem verpflichtet: Auf Beschwerden von betroffenen Benutzern müssen sie rechtswidrige

---

1 *Heger,* in: Lackner/Kühl, § 201a Rn. 9a.
2 *Heger,* in: Lackner/Kühl, § 201 a Rn. 9 b.
3 So z. B. *Heger* ebd. m. w. N.

Inhalte innerhalb von 24 Stunden löschen oder den Zugang dazu zu sperren (§ 3 Abs. 2 Nr. 2 NetzDG). Im Einzelfall kann die Frist auch 7 Tage oder länger dauern (§ 3 Abs. 2 Nr. 3 NetzDG). Verstöße gegen diese Berichtspflicht sowie eine mangelhafte Organisationen des Beschwerdeverfahrens werden mit einem Bußgeld behandelt. Wenn die Netzwerke nicht schnell genug reagieren, können sich die Anwender beim neugeschaffenen deutschen Bundesamt für Justiz beschweren. Es handelt sich somit um ein Gesetz, das zur Kategorie der „Compliance" gehört, die in diesem Fall speziell zur Sicherstellung der Regelkonformität bei Anbietern sozialer Netzwerke dienen soll. Das Netzwerkdurchsetzungsgesetz soll vor allem der Bekämpfung von Hasskriminalität (z. B. rechtsextremistische, rassistische, antisemitische oder homophobe Propaganda) und von Kinderpornographie im Internet dienen.

Das Netzwerkdurchsetzungsgesetz war in Deutschland zunächst sehr umstritten. Man befürchtete einen Angriff des Staates auf die Meinungsfreiheit. Hiermit würde Zensur im Internet eingeführt. Das Gesetz diene auch dem Mundtotmachen des politischen Gegners. Inzwischen ist die Kritik aber schwächer geworden, aber noch nicht völlig verstummt. Die politische Notwendigkeit, gegen Hass und Hetze im Internat auch von staatlicher Seite vorzugehen, wird inzwischen überwiegend bejaht und das Netzwerkdurchsetzungsgesetz auch von Menschrechtsgruppen als denkbarer Lösungsansatz positiv wahrgenommen. Auch hat das Gesetz bislang nicht dazu geführt, dass in Deutschland der politische Diskurs im Internet wesentlich gestört oder gar zerstört wurde. Vielmehr gehen die Netzwerkbetreiber, wie es scheint, verantwortungsvoll mit dem Gesetz um und löschen nur solche Inhalte auf ihren Servern, die ganz offensichtlich unter einen Straftatbestand wie etwa die Beleidigung oder die Volksverhetzung fallen. So wurden zwischen Juli und Dezember 2018 von Twitter 23.000 Einträge, bei Youtube 54.000 Inhalte und bei Facebook (nur) 369 Inhalte gesperrt oder gelöscht. Der größte Teil bezog sich auf Hassrede und politischen Rechtsextremismus.[1] Gleichwohl darf nicht die Gefahr übersehen werden, dass rechtsunkundige Mitarbeiter von Netzwerkbetreibern vorschnell Inhalte löschen, die in Wahrheit gar nicht strafbar, sondern z. B. von der verfassungsrechtlich garantierten Meinungsfreiheit (Art. 5 Grundgesetz) gedeckt sind.

[1] Diese Zahlen stammen aus sog. Transparenzberichten, welche die großen Internetplatformen veröffentlichen müssen.

IV. Der Zugriff des Staates im Strafprozess auf die digitale Kommunikation

Die deutsche Strafprozessordnung enthält inzwischen ein breites Instrumentarium, mittels dessen der Staat die digitale Kommunikation überwachen und Zugriff auf die dabei eingesetzte Technik nehmen kann.

1. Durchsuchung und Beschlagnahme von Computer und Cloud Computing

Bei einem entsprechenden Tatverdacht können Computer und Smartphones des Tatverdächtigen beschlagnahmt werden (§ 94 StPO). Die auf ihnen gespeicherten Inhalte wie z. B. E-Mails oder Whats App-Nachrichten werden hierzu zunächst ausgeforscht (§ 102 StPO). Das gleiche gilt übrigens für in Cloud-Computing gespeicherte Daten.[1] Hierzu dürfen auch die vom Computer räumlich getrennte Speichermedien (§ 110 StPO) durchsucht werden. Die nicht ermittlungsrelevanten Gegenstände und Daten werden dann bei der Durchsuchung aussortiert. Die ermittlungsrelevanten Beweise dagegen werden dann in Beschlag genommen. Sie werden später im Strafprozess in der Beweisform des Urkundenbeweises bzw. des Augenscheins eingeführt.

Beschlagnahmen und Durchsuchungen dürfen wegen der Intensität der damit verbundenen Grundrechtseingriffe in Deutschland übrigens nur durch ein Gericht angeordnet werden. Im Eil-Fall (sog. „Gefahr im Verzug“) sind auch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zuständig (§§ 98, 105 StPO). Die Rechtmäßigkeit der Eil-Anordnung durch die Staatsanwaltschaft und ihrer Ermittlungspersonen muss dann aber später von einem Gericht bestätigt werden.

2. Durchsuchung und Beschlagnahme im Ausland

Befindet sich das Speichermedium, z. B. der Server des Netzwerkbetreibers, nicht in Deutschland, sondern im Ausland, kann auf diese im Wege der internationalen Rechtshilfe zugegriffen werden. Bei Mitgliedsstaaten, die der Cybercrime-Konvention des Europarats[2] beigetreten sind, gelten dann die Spezialregelungen der CCC, vor allem Art. 32 CCC.[3] Für den Raum der Europäische Union bereitet die Kommission eine Verordnung vor,[4] mit der die grenzüberschreitende Beweiserhebung erheblich vereinfacht werden soll: Die Vorschläge sehen vor, dass Strafverfolgungsbehörden eines

---

1 *Schmitt,* in: *Meyer-Goßner/Schmitt*, StPO, 61. Aufl. 2018 § 102 Rn. 10a.

2 CET Nr. 185.

3 *Hadamitzky,* in: *Satzger/Schluckebier/Widmaier*, StPO, 3. Aufl. 2018, §110a StPO Rn. 23.

4 Europäische Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel (COM/2018/225); zu dem Entwurf vgl. *Schramm,* Internationales Strafrecht, 4. Kap. Rn. 148j.

EU-Mitgliedstaats solchen Unternehmen, die elektronische Kommunikationsleistungen in anderen Mitgliedstaaten anbieten, unabhängig vom Sitz des Unternehmens und vom Ort der Speicherung der Daten dazu verpflichten können, elektronische Beweismittel für laufende Strafverfahren zu sichern (Europäische Sicherungsanordnung) und an die Strafverfolgungsbehörden im Anordnungsstaat herauszugeben (Europäische Herausgabeanordnung). Befreit von den üblichen Restriktionen der internationalen Rechtshilfe soll nun der beantragende Staat unmittelbar den Zugriff auf Daten beim Netzwerkbetreiber erhalten, d. h. sie dort anfordern können. Es ist nicht vorgesehen, dass Institutionen des Staates, in dem vollstreckt wird, diese Anordnungen noch bestätigen oder kontrollieren können. Nach diesem sog. Marktortprinzip bestimmt sich die Zulässigkeit der Beschlagnahme dann nach dem Recht des Staates, der die Beschlagnahme anordnet. Ein kompliziertes Rechtshilfeverfahren, bei dem bislang zwei Staaten involviert waren – nämlich der Anordnungsstaat und der Vollstreckungsstaat – soll dann nicht mehr nötig sein. Dieser Wegfall einer gerichtlichen oder zumindest behördlichen Überprüfung der Maßnahme im Vollstreckungsstaat wird in Deutschland zu Recht sehr stark kritisiert.[1]

3. Überwachung von Skype- und Whats App- Telefonaten

Normale, unverschlüsselte Telefonate über das Festnetz und das Mobilfunknetz dürfen in Deutschland nach richterlicher Anordnung überwacht und aufgezeichnet werden (§ 100a Abs. 1 S. 1 StPO). Hierzu muss allerdings der Verdacht einer schweren Straftat vorliegen, wobei das Gesetz den Kreis dieser schweren Straftaten relativ weit zieht. So ist eine Telekommunikationsüberwachung beispielsweise zulässig bei einem Betrug oder Computerbetrug, sofern die Tat durch eine Bande begangen wird (§ 100a Abs. 2 Nr 1 lit. n StPO), aber auch bei einer einfachen Geldwäsche (§ 100 a Abs. 2 Nr. 1 lit. m StPO)

Abgehört und aufgezeichnet werden darf auch die diejenige Telefonie über das Internet, die in verschlüsselter Form erfolgt (z. B. Skype-Telefonate oder Whats App-Telefonate). Zwar sind die Strafverfolgungsbehörden offensichtlich noch nicht imstande, die Verschlüsselung technisch aufzuheben und das Telefonat während der Übertragung der Inhalte unmittelbar abzuhören. Allerdings dürfen die Strafverfolgungsbehörden in Deutschland neuerdings eine Software auf den Computer oder des Smartphones des Tatverdächtigen heimlich aufspielen. Durch das Aufspielen dieser Software,

[1] Vgl. *Schramm,* Internationales Strafrecht, 4. Kap. Rn. 148k.

die häufig als „Staatstrojaner“ bezeichnet wird, kann der Inhalt des verschlüsselten Internettelefonats vor dem Moment der Verschlüsselung unverschlüsselt abgehört und aufgezeichnet werden (§ 100 a Abs. 1 S. 2 StPO). Diese Form der Überwachung von verschlüsselter Internet-Kommunikation bezeichnet man in Deutschland als „Quellen-Telekommunikationsüberwachung“: Denn sie wird an der Quelle der Kommunikation vorgenommen, nämlich an dem Gerät, in das gesprochen wird (Mikrofon am Smartphone, Mikrophon am Computer).

4. Online-Durchsuchung

Ebenso erlaubt die deutsche Strafprozessordnung seit 2017 die sogenannte Online-Durchsuchung (§ 100 b StPO). Sie ermöglicht den Eingriff der Strafverfolgungsbehörden in ein vom Beschuldigten genutztes informationstechnisches System. Durch sie kann die Polizei von außen, mittels einer von der Polizei heimlich auf dem PC aufgespielter entsprechenden Ausspäh-Software, den Inhalt eines Computers über eine Internetverbindung durchsuchen. Außerdem kann durch die Online-Durchsuchung das gesamte Nutzungsverhalten des Betroffenen überwacht werden, da zugleich die beim Surfen aufgesuchten Webseiten systematisch und vollständig erfasst werden [1] Das heimliche Aktivieren der Kamera- oder Mikrofonfunktion des Computers oder Smartphones erlaubt das Gesetz jedoch nicht.

Diese Online-Durchsuchung ist aber nur beim Verdacht einer besonders schweren Straftat möglich (z. B. terroristische Straftaten oder Mord) und die Wahrheitsermittlung durch andere Beweismittel wesentlich schwerer sein.[2] Zudem darf die Onlinedurchsuchung nur auf Antrag der Staatsanwaltschaft durch eine Kammer des Landgerichts (und nicht bloß durch einen einzelnen Richter) angeordnet werden (§100e Abs. 2 StPO).

5. Schutz des Kernbereichs der persönlichen Lebensgestaltung

Es gehört zu den elementaren Grundprinzipien des deutschen Beweisrechts, dass Erkenntnisse, die den Intimbereich des Menschen betreffen, im Strafprozess nicht verwertet werden dürfen. Man nennt dies auch die sog. „Sphärentheorie“ des Bundesverfassungsgerichts:[3] Erkenntnisse aus der Sozialsphäre des Menschen dürfen

---

1 *Schmitt,* in: *Meyer-Goßner/Schmitt*, § 100b Rn. 1.

2 Zum neuen § 100b StPO vgl. *Schmitt*, in: *Meyer-Goßner/Schmitt*, § 100 b Rn. 1 ff.

3 Vgl. BVerfG, Amtliche Sammlung, Bd. 34, S. 238 (heimliche Tonbandaufeichnung); BVerfG, Amtliche Sammlung, Bd. 109, S. 279 (Großer Lauschangriff).

immer verwertet werden, solche aus der Privatsphäre des Menschen nur bei überwiegendem Verfolgungsinteresse des Staates, und solche aus dem Kernbereich der privaten Lebensgestaltung, dem Intimbereich der Persönlichkeit, dürfen niemals verwertet werden. Selbstgespräche dürfen z. B. demnach überhaupt nicht verwertet werden, selbst wenn sie ein Mordgeständnis enthalten,[1] während Tagebuchaufzeichnung nur dann ausnahmsweise verwertet werden dürfen, wenn der Täter darin die Straftat gesteht.[2]

Für die eben genannten, modernen Ermittlungsmaßnahmen (Online-Durchsuchung, Quellen-Telekommunikationsüberwachung) im Bereich digitalisierter Technik wurde diese verfassungsrechtliche Beschränkung der Beweiserhebung und Beweisverwertung sogar ausdrücklich in das Gesetz aufgenommen: Die Maßnahmen stehen unter dem Vorbehalt, dass Erkenntnisse, die allein aus dem Kernbereich der persönlichen Lebensgestaltung stammen, nicht gewonnen und nicht verwertet werden dürfen (§ 100 d Abs. 1 StPO). Was unter dem Kernbereich der Persönlichkeit zu verstehen ist, wird in der StPO nicht definiert. Es darf aber durch die Maßnahme nicht die vom deutschen Grundgesetz in dessen Art. 1 genannte Menschenwürde des einzelnen nicht verletzt oder gefährdet werden. Zum Kernbereich zählen etwa Ausdrucksformen der Sexualität oder Äußerungen innerster Gefühle. Nicht zum Kernbereich gehören Gesprächsinhalte, die einen unmittelbaren Zusammenhang zu geplanten oder vergangenen Straftaten stehen.

Das Gesetz verbietet dabei aber von vorneherein nur derjenigen Überwachung, die nach einer objektiven Ex-ante-Prognose *ausschließlich* den Kernbereich der Persönlichkeit umfasst. Werden durch die Maßnahme hingegen zwar auch, aber *nicht nur* Informationen aus dem Kernbereich der Persönlichkeit gewonnen, so ist die Anordnung zulässig.[3] Es dürfen dann aber später nur diejenigen Erkenntnisse aus der Überwachung in den Prozess eingeführt werden, die *nicht* den Kernbereich betreffen. Wenn es also unvermeidbar ist, dass auch höchstpersönliche Informationen bei der Überwachung erlangt werden, so macht dies die Maßnahme nicht rechtswidrig. Aber diese höchstpersönlichen Informationen dürfen dann im Strafprozess nicht verwertet werden und müssen gelöscht werden (§ 100 d Abs. 2 StPO). Für Informationen aus dem Kernbereich der persönlichen Lebensgestaltung besteht ein umfassendes, absolutes Verwertungsverbot. Wenn sich also aus der Überwachung z. B. ergibt, dass der Angeklagte ein psychisch Kranker,

---

1 Vgl. BGH in Strafsachen, Amtliche Sammlung (BGHSt), Band 57 S. 71: Geständnis eines Mordes in einem abgehörten Selbstgespräch im Auto.

2 Vgl. BGHSt 19, S. 325 Randnote 22: Straftäter fertigt in Tagebuch Aufzeichnungen über seine Verbrechen und Opfer an.

3 *Schmitt,* in: *Meyer-Goßner/Schmitt*, § 100d StPO Rn. 5.

ein Homosexueller, ein Atheist, ein Sozialist, ein Anarchist, ein Regimegegner oder ein Alkoholiker ist, so darf dies im Strafprozess nicht verwertet werden, es sei denn, es ist für die strafrechtliche Bewertung der Tat von Bedeutung.

V. Resümee und Ausblick

Die Frage, ob die Digitalisierung zu einer Transformation oder einer Modernisierung des Rechts geführt hat, möchte ich für das deutsche Strafrecht und Strafprozessrecht so beantworten: Es hat eine Modernisierung, aber keine Umwandlung stattgefunden. Es wurden neue Straftatbestände und neue Eingriffsmöglichkeiten für die Strafverfolgung geschaffen, die sich hinsichtlich der materiellen Voraussetzungen, der zuständigen Entscheidungsträger (meist die Gerichte) und dem Umfang der Eingriffe an den analog-technischen, vor der Digitalisierung bestehenden Ermittlungsmaßnahmen orientieren. Die dabei zu beachtenden verfassungsrechtlichen und europarechtlichen Vorgaben und Beschränkungen sind nichts neues, sondern stehen in der rechtsstaatlichen Tradition wie z. B. das Gesetzlichkeitsprinzip, das Verhältnismäßigkeitsprinzip und der Schutz der Persönlichkeitsrechte. Das Strafrecht unterstützt und schützt einerseits die Digitalisierung, es versucht aber auch, den Einzelnen vor den schädlichen Auswirkungen der Digitalisierung zu schützen. Neu ist es freilich, dass es noch nie für den Staat so einfach war, einen Menschen mittels der von ihm verwendeten Informationstechnik in einem solch großen Umfang zu überwachen und auszuforschen.

Übrigens gibt es in Westeuropa seit wenigen Jahren eine wachsende Kritik an der Digitalisierung. Es wird ein postdigitales Zeitalter gefordert. Es werden im Silicon Valley in Kalifornien und von manchen Universitäten schon digitale Detox-Kurse angeboten (also Entgiftungskurse).[1] Manche Hotels in Südtirol bieten ihren Gästen bewusst kein Internet an. Manche Uni-Dozenten verlangen von ihren Studenten den Verzicht auf den Einsatz des Internets. Der Grund für diese Ablehnung liegt zum einen in der Macht der Internetkonzerne (wie Google, Facebook, Twitter) und der Macht der staatlichen Institutionen. Denn sie können das Verhalten der Nutzer für ihre Zwecke kontrollieren, manipulieren und ausnutzen. Der weißrussische Publizist *Evgeny Morozov* meint: Anstatt staatliche, wirtschaftliche oder soziale Hierarchien zu schwächen oder zu ersetzen, habe das Digitale die Hierarchien verstärkt und unsichtbar gemacht.[2] Der andere Grund für die Forderung nach einem postdigitalen

[1] vgl. *Obertreis*, Digitale Entgiftung, FAZ v. 15. 9. 2018.

[2] zitiert bei *Lovink*, Epidemie der Ablenkung – Von der digitalen Utopie zur Entzauberung des techno-sozialen Raums, Lettre International 120, 1/2018, S. 17.

Zeitalter liegt im zunehmenden Verlust des persönlichen Kontakts, des unmittelbaren persönlichen Austausches: „Vor 15 Jahren war das Internet ein Ausweg aus der realen Welt. Heute ist die reale Welt ein Ausweg aus dem Internet“, wie es der amerikanische Computerexperte *Noah Smith* unlängst bezeichnet hat. “15 years ago, the internet was an escape from the real world. Now, the real world is an escape from the internet.”[1]

Angesichts der fortschreitenden Digitalisierung unserer Welt bleibt abzuwarten, ob die Digitalisierung wirklich zurückgedrängt wird oder ob wir nicht uns schon längst mit ihr abgefunden haben und sie selbst intensiv nutzen. Die Menschheit hat auch die Entdeckung des Feuers, die Erfindung des Rades und die Erfindung des Buchdrucks nicht rückgängig gemacht, und alles spricht dafür, dass sie die digitale Technik in Zukunft noch viel stärker nutzen wird, als es bereits heute der Fall ist. Wohin die Digitalisierung führen wird – ob zu mehr Freiheit oder zu mehr Knechtschaft, ob zu mehr Wohlstand oder zu mehr Armut durch eine Umverteilung der Güter von „unten“ nach „oben“, ob zu einer besseren oder zu einer womöglich (noch) krimineller werdenden Welt -, das kann keiner vorhersagen.

Проблемы уголовного права в информационном мире и пути их решения в соответствии с немецким уголовным правом

Э. Шрамм
Университет Йены им. Фридриха Шиллера
Германия, Йена

Дигитализация нашего мира вызывает глубокие изменения в условиях жизни. В статье рассматривается, как немецкое уголовное и уголовно-процессуальное законодательство решает проблемы, возникающие в этой связи. В материальном уголовном праве технология, необходимая для оцифровки данных, и сами данные защищены немецким законодательством от различных уголовных преступлений, особенно в области программного и аппаратного обеспечения. При изменении данных нарушителю необязательно обходить меры безопасности доступа. В случае саботажа аппаратного и программного обеспечения за хакерскую атаку на управляемые компьютером поставки значимых инфраструктур (вода, электричество, газ) вменяется повышенное наказание. Конфиденциальность при цифровой коммуникации позволяет защитить от слежки за данными. В Германии также ведется дискуссия о введении наказания за «цифровое вторжение». Незаконный контент в Интернете в значительной степе-

[1] zitiert bei *Lovink (*Fn. 12), S. 17.

ни криминализирован и содержит оскорбления, дискриминацию, детскую и молодежную порнографию, обольщение, запугивание и кибертравлю.

Также немецкое уголовно-процессуальное законодательство содержит широкий спектр инструментов, которые позволяют государству наблюдать за цифровой связью. Таким образом, немецкий уголовно-процессуальный кодекс (StPO) позволяет осуществлять поиск и захват компьютеров и облачных вычислений. Запланированный регламент ЕС «О порядке представления и обеспечения сохранности электронных доказательств» по уголовным делам предназначен для того, чтобы обязать телекоммуникационные компании обеспечивать безопасность и предоставлять доступ к электронным доказательствам, необходимым для уголовных разбирательств, на всей территории ЕС. Мониторинг зашифрованных телефонных звонков Skype и Whats App возможен при помощи установленного на устройстве программного обеспечения, поэтому звонок может быть расшифрован, прослушан и записан перед шифрованием. Кроме того, правоохранительным органам разрешается отслеживать компьютер через Интернет с использованием программного обеспечения, установленного на компьютере извне (так называемые онлайн-поиски). Несмотря на это, информация из сферы личной жизни не может быть получена полицией и использована в процессе (§ 100d StPO). В конце кратко обсуждается критика дигитализации и политические требования к постцифровой эпохе.

Ключевые слова: шпионаж за данными, компьютерный саботаж, киберзапугивание, основная сфера личной жизни, онлайт-обыск, постинформационный век, саботаж системной инфраструкуры.

Научная специальность: 12.00.00 – юридические науки.