IT-FORSCHER ALS POTENTIELLE STRAFTÄTER?

IT-Sicherheitsforschung zwischen Wissenschaftsfreiheit und Strafrecht

Jochen Krüger / Christoph Sorge / Stephanie Vogelgesang

Vizepräsident des Amtsgerichts Saarbrücken a.D. und wissenschaftlicher Mitarbeiter, juris-Stiftungsprofessur für Rechtsinformatik und CISPA, Universität des Saarlandes
66123 Saarbrücken, DE
jochen.krueger@uni-saarland.de

Universitätsprofessor, juris-Stiftungsprofessur für Rechtsinformatik und CISPA, Universität des Saarlandes
66123 Saarbrücken, DE
christoph.sorge@uni-saarland.de

Referentin für den Bereich elektronischer Rechtsverkehr, Saarländisches Justizministerium / wissenschaftliche Mitarbeiterin, juris-Stiftungsprofessur für Rechtsinformatik und CISPA an der Universität des Saarlandes
66123 Saarbrücken, DE
stephanie.vogelgesang@uni-saarland.de

Schlagworte: ***IT-Sicherheitsforschung, Wissenschaftsfreiheit, Strafrecht, Europäische Datenschutz-Grundverordnung (DSGVO), Ethikkommission***

Abstract: *Die Digitalisierung der Gesellschaft hat zu einem Bedeutungszuwachs der IT-Sicherheitsforschung geführt. IT-Sicherheitsforschung soll u.a. Antworten auf digitale Angriffe finden und hat so eine ausgeprägte Nähe zu strafrechtlichen Normen. Der vorliegende Beitrag befasst sich mit der Frage, inwieweit IT-Sicherheitsforscher selbst in die Gefahr strafrechtlicher Sanktionierung geraten können. Anhand der Straftatbestände zum Schutz von Daten (§§ 202a–202c StGB) wird das Verhältnis von Wissenschaftsfreiheit und Strafrecht näher analysiert. Angesprochen wird auch, ob durch Einschaltung fachspezifischer Ethikkommissionen der skizzierte Konflikt entzerrt werden kann.*

1. Einleitung

Die allgemein festzustellende Digitalisierung der Gesellschaft hat auch Auswirkungen auf Umfang und Stellenwert der IT-Sicherheitsforschung. Zum einen nimmt faktisch die Bedeutung der IT-Sicherheitsforschung zu. Digitalisierung benötigt Vertrauen. Ohne Gewährleistung eines angemessenen Datenschutzniveaus im weitesten Sinn kann die Digitalisierung nicht auf die notwendige breite gesellschaftlicher Akzeptanz hoffen. Zum anderen erzeugt Digitalisierung eine geradezu explosionsartige Vermehrung von Daten, die ihrerseits zu Forschungszwecken in allen Wissenschaftsbereichen genutzt werden können. Dazu gehört auch die IT-Sicherheitsforschung selbst.

Diese Entwicklung führt in weiten Bereichen zu neuen komplexen Fragestellungen im allgemeinen Zusammenspiel zwischen Informatik und Rechtswissenschaft. Dies soll im Folgenden mit Bezug auf das Strafrecht näher thematisiert werden.

Der vorliegende Beitrag konzentriert sich auf das Thema IT-Sicherheitsforschung zwischen Wissenschaftsfreiheit und Strafrecht. Dabei geht es um die Problematik, inwieweit Sicherheitsforschung bzw. die insoweit

handelnden Personen[1] selbst in die Gefahr einer strafrechtlichen Sanktionierung geraten können. Ausgeklammert wird dabei die spezifische Problematik, dass Forschungsdaten ihrerseits gegen unbefugten Zugriff zu schützen sind. Im Vordergrund steht hier die strafrechtliche Grauzone, in die IT-Sicherheitsforscher – etwa bei der Analyse von digitalen Angriffen – leicht geraten können. Als Beispiel kann die Einrichtung von Honeypots genannt werden.[2] Diese absichtlich verwundbaren Systeme sollen – echte – Angreifer anlocken und von diesen auch verwendet werden. Dadurch kann der Betreiber dieser Honeypots zu Analyse- und Forschungszwecken Informationen über die Angriffe erhalten. Formal kann der Forscher damit aber auch Bestandteil des illegalen Angriffs werden mit den daraus resultierenden strafrechtlichen Risiken bzw. Konsequenzen. Mit dem Begriff des illegalen Angriffs wird dabei die eindeutig gesetzeswidrige Aktion eines sog. Black-Hats beschrieben, dem es im Gegensatz zum sog. White-Hat nicht um die Förderung der IT-Sicherheit geht.[3]

Zugrunde gelegt wird in der Analyse der deutsche Rechtsrahmen, insbesondere das Grundgesetz (GG) und das Strafgesetzbuch (StGB). Die folgenden Ausführungen sollen jedoch verdeutlichen, dass die anzusprechenden strafrechtlichen Probleme nicht auf landesspezifische Regelungen reduziert werden können. Sie haben – zum Beispiel mit Blick auf die Europäische Datenschutz-Grundverordnung (DSGVO) – eine europäische Dimension.[4]

2. Zur Aktualität des Themas

2.1. Ausgangsüberlegungen

Erörterungen des hier interessierenden Grundsatzkonflikts zwischen IT-Sicherheitsforschung und Strafrecht sind, soweit ersichtlich, eher selten. Auch Lehrbücher zur IT-Sicherheit weisen insoweit typischerweise keine dogmatisch weiterführenden Angaben aus.[5] Dies könnte für eine nur geringe faktische Relevanz des Themas sprechen. Das Gegenteil ist jedoch der Fall. Angesichts der zuvor skizzierten wachsenden Bedeutung der IT-Sicherheit für die Gesamtgesellschaft ist jedenfalls in Zukunft vermehrt mit einschlägigen Konflikten zu rechnen. Dies gilt außerdem deshalb, weil die Digitalisierung der Gesellschaft mit einer digitalen Aufrüstung des Strafrechts einhergeht. Zu nennen ist beispielsweise die Einführung der Datenhehlerei (§ 202d StGB) im Jahre 2015 und die Diskussion um die Einführung eines neuen Tatbestands des digitalen Hausfriedensbruchs.[6] Damit wird das strafrechtlich relevante Normenprogramm ausgeweitet und so auch konfliktträchtiger für die IT-Sicherheitsforschung.

2.2. Anmerkungen zum allgemeinen Verhältnis von wissenschaftlicher Forschung und strafrechtlicher Limitierung

Wichtig erscheint zudem ein weiterer Aspekt. Wissenschaftliche Forschungsbereiche haben typischerweise eine unterschiedliche Nähe zu Fragen der strafrechtlichen Limitierung. Auf der einen Seite des Spektrums ist zum Beispiel die historische Forschung anzusiedeln. Dort ist ein Grundsatzkonflikt zwischen Forschungstätigkeit und strafrechtlichen Tatbeständen eher selten. Als Gegenpol ist die moderne biomedizinische Forschung zu nennen. Sie ist insbesondere dadurch charakterisiert, dass sie schnell in Grenzbereiche des sozial und recht-

1 Die Frage der Verantwortlichkeit für Handlungen von Mitarbeitern wird hier nicht weiter vertieft – vgl. dazu Schröder, Compliance an Universitäten – ein Albtraum oder überfälliges Strukturelement?, ZIS 2017, 281.

2 Vogelgesang/Möllers/Potel, Strafrechtliche Bewertung von «Honeypots» bei DoS-Angriffen, MMR 2017, 291 ff.

3 Vgl. zu diesen Angriffstypen Simon/Moucha, Verwundbarkeitsprüfungen mit Shodan, DuD 2016, 727 – vgl. zu unterschiedlichen Angreifer-Typen auch Eckert, IT-Sicherheit 9. Aufl. 2014, S. 34.

4 Dazu näher 4.3.

5 Eckert (Fn. 3), S. 40, erwähnt zwar Rechtsfragen der IT-Sicherheit, verweist diesbezüglich aber vorrangig auf Forschungsaktivitäten an juristischen Fakultäten (S. 43).

6 Dazu Tassi, Digitaler Hausfriedensbruch, DuD 2017, 175 ff.

lich Vertretbaren und damit in strafrechtlich relevante Bereiche gerät. Dies zeigt anschaulich die Diskussion um die Gen- und Stammzellenforschung.[7]

2.3. Zur strafrechtlichen Konfliktträchtigkeit der IT-Sicherheitsforschung

Die hier interessierende IT-Sicherheitsforschung, so die Ausgangsthese, hat eine ausgeprägte Nähe zu strafrechtlichen Normen, ist somit als strafrechtlich gefährdet einzustufen. Dies hat insbesondere die wissenschaftliche Diskussion um die Einführung des neuen § 202c StGB im Jahre 2007 in großer Deutlichkeit gezeigt. § 202c StGB sanktioniert strafrechtlich das Vorbereiten des Ausspähens (§ 202a StGB) bzw. des Abfangens (§ 202b StGB) von Daten. Wer zum Beispiel Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, einem anderen überlässt, kann mit Freiheitsstrafe bis zu zwei Jahren[8] bestraft werden.

Die hier angesprochene europäische Dimension des Konflikts kommt dadurch zum Ausdruck, dass gerade der zuvor genannte § 202c StGB als neuer Typus eines europäischen Softwaredelikts angesehen werden kann.[9] Deutschland hatte sich – wie zum Beispiel auch Österreich – im Rahmen der Budapester «Convention on Cybercrime» vom 23. November 2001 dazu verpflichtet, den Missbrauch von Vorrichtungen zur Begehung von Computerdelikten unter Strafe zu stellen.[10] Bei dieser Konvention handelt es sich um ein Übereinkommen im Rahmen des Europarats, an dem außer den meisten Mitgliedsstaaten des Europarats auch noch weitere Staaten wie die USA oder Japan beteiligt sind.[11] Mit der Regelung des § 202c StGB wurde Art. 6 Abs. 1 lit. a Cybercrime Convention für das deutsche Recht umgesetzt.

Die damalige Einführung des § 202c StGB stieß auf teilweise massive Kritik aus dem Bereich der Informatik und führte auch zu entsprechenden Verfassungsbeschwerden.[12] In diesem Zusammenhang wurde unter anderem auch die Gesellschaft für Informatik e.V. zu einer Stellungnahme aufgefordert. Sie hat sich in der Sache eindeutig ablehnend geäußert.[13] Die Stellungnahme wurde vom Präsidiumsarbeitskreis «Datenschutz und IT-Sicherheit» und damit von einem problemnahen Gremium erarbeitet. Inhaltlich wurde insbesondere die Problematik des «Dual Use» hervorgehoben. Betont wurde, dass alle Angriffsprogramme in Form von «Malware» sowohl für schlechte als auch für gute Zwecke (Informationssicherheit-Prüfprogramme) genutzt werden können. Weit überwiegend würden – ursprünglich als Malware entwickelte – Angriffsprogramme auch von wissenschaftlichen Anwendern zum Aufspüren von Sicherheitslücken in den Bereichen IT-Sicherheit und Datenschutz genutzt. Der Besitz und die Analyse von Malware sei daher zur Feststellung und Behebung von Schwachstellen in diesen Bereichen unverzichtbar. Als weitere Beispiele für diese Grundsatzproblematik wurden die Themen «Brechen von Verschlüsselung im Bereich der Kryptoanalyse» und «Entwicklung von Antiviren-Programmen» genannt. Beide Bereiche – so die Stellungnahme – setzen voraus, dass für die Entwicklung von Gegenmaßnahmen Informationen über die Funktionsweise illegaler Angriffe erlangt werden können. Strafnormen wie § 202c StGB würden daher wissenschaftliche Aktivitäten und Ausbildung in diesen Bereichen unmöglich machen.

Unabhängig von der Berechtigung jedes Einzelarguments erscheint gerade die zuvor skizzierte Stellungnahme geeignet, die hier interessierenden Grundsatzkonflikte zu veranschaulichen. Eine Besonderheit der IT-

---

7 Dazu Jung, Biomedizin und Strafrecht, ZStW 1988, 3 ff. bzw. Herzog, Gentechnologie-Forschungskontrolle durch Strafrecht?, ZStW 1993, 727; vgl. zu neuen Grundfragen im Bereich «Biosicherheit und Forschungsfreiheit» auch Würtenberger/Tanneberger, Biosicherheit und Forschungsfreiheit. Zu den Schranken des Art. 5 Abs. 3 S. 1 GG, Ordnung der Wissenschaft 2014, 1 ff.

8 Das Strafmaß wurde 2015 erhöht; vgl. Fischer, StGB Kommentar, 65. Aufl. 2018, § 202c, Rn. 1.

9 Popp, § 202c und der neue Typus des europäischen «Software-Delikts», GA 2008, 375 ff.

10 Vgl. dazu Popp, Computerstrafrecht in Europa, MR-Int 2007, 84 ff.

11 Dazu näher Popp (Fn. 10), 84/85.

12 Die Verfassungsbeschwerden wurden im Ergebnis nicht zur Entscheidung angenommen – vgl. BVerfG, Beschluss vom 18. Mai 2009, 2 BVR 2233/07, 2 BVR 1151/08, 2 BVR 1524/08; vgl. dazu näher Holzner, Klarstellung strafrechtlicher Tatbestände durch den Gesetzgeber erforderlich, ZRP 2009, 177 ff.

13 Dazu und zum Folgenden Pohl, Verfassungsmäßigkeit des § 202c StGB, Informatik Spektrum 2008, 485 ff.

Sicherheitsforschung liegt darin, dass sie Antworten auf illegale, insbesondere auch strafwürdige Angriffe finden soll und muss. Sie ist daher auf die Analyse derartiger realer Angriffe angewiesen. Dies begründet vorrangig die strukturelle Nähe der IT-Sicherheitsforschung auch zu Fragen des Strafrechts.

3. Zum allgemeinen rechtlichen Verhältnis von Wissenschaftsfreiheit und strafrechtlicher Sanktionierung

Für die weitere rechtliche Diskussion erscheint es methodisch naheliegend, zunächst an das allgemeine Verhältnis von Wissenschaftsfreiheit und Strafrecht anzuknüpfen. Die rechtlichen Eckpfeiler dieser Grundsatzproblematik werden durch die Themenwahl bereits konkretisiert: Auf der einen Seite steht die Wissenschaftsfreiheit in Form der Forschungsfreiheit.[14] Diese ist in Art. 5 Abs. 3 S. 1 GG verankert. Ausdrückliche Schranken nennt Art. 5 Abs. 3 S. 2 GG nur für die Freiheit der Lehre. Diese entbindet nicht von der Treue zur Verfassung.

Aus dem Grundgesetz selbst ergeben sich damit keine weiteren ausdrücklichen Schranken für die Forschungsfreiheit. Insbesondere ist anerkannt, dass die Schranken der allgemeinen Gesetze, die in Art. 5 Abs. 2 GG genannt sind und auch die Strafgesetze erfassen, auf Art. 5 Abs. 3 GG nicht anwendbar sind.[15] Das sich aus dieser Analyse aufdrängende Ergebnis – die Forschungsfreiheit kann durch Straftatbestände nicht begrenzt werden – ist jedoch in dieser Allgemeinheit offenkundig fehlerhaft. So kann die Forschungsfreiheit eine vorsätzliche Tötung nicht legitimieren. Dies ergibt sich bereits aus der Wertung des § 216 StGB (Strafbarkeit der Tötung auf Verlangen). Danach bleibt trotz der ausdrücklichen Einwilligung des Rechtsgutsträgers die Tat nicht sanktionslos.

Die Auflösung dieser Problematik liegt in der methodisch gesicherten Erkenntnis, dass dem Text nach unbeschränkte Grundrechte durch andere Grundrechtspositionen eingeschränkt werden können.[16] Bei Wertungskonflikten zwischen der Forschungsfreiheit und Tatbeständen des Strafrechts handelt es sich oftmals um einen Grundsatzkonflikt zwischen zwei verfassungsrechtlich abgesicherten Grundwerten. Dass gerade Strafrecht eine Stützfunktion für hohe Verfassungsgüter einnehmen kann, zeigt auch die Norm des Art. 26 Abs. 1 GG. Danach sind qua Grundgesetz Angriffskriege verboten. Entsprechende Handlungen sind gemäß Art. 26 Abs. 1 S. 2 GG unter Strafe zu stellen. Dieser Verfassungsauftrag wurde zunächst durch § 80 StGB erfüllt. § 80 StGB ist durch Gesetz vom 22. Dezember 2016 aufgehoben und durch § 13 Völkerstrafgesetzbuch ersetzt worden.[17]

4. Das Verhältnis von IT-Sicherheitsforschung und Strafrecht – dargestellt anhand der §§ 202a–202c StGB

Aus den bisherigen Überlegungen lassen sich erste methodische und inhaltliche Differenzierungsgesichtspunkte für die notwendige Sachdiskussion ableiten.

4.1. Der allgemeine Gedanke einer deliktsspezifischen Analyse

Die Wechselbeziehung zwischen grundgesetzlich geschützter Forschungsfreiheit (hier IT-Sicherheitsforschung) und strafrechtlicher Begrenzung entzieht sich offenkundig einer einheitlichen Bewertung. Strafnormen schützen oftmals grundgesetzlich abgesicherte Positionen von unterschiedlicher Wertigkeit. Daher kann die notwendige Abwägung zwischen Forschungsfreiheit und Straftatbegrenzung je nach Straftatbestand auch unterschiedlich ausfallen. Näher liegt daher eine deliktsspezifische Analyse mit Bezug auf die konkrete Themenstellung.

---

14 Wissenschaft als Oberbegriff besteht aus den Teilaspekten Forschung und Lehre – vgl. Jarass/Pieroth, Kommentar GG, 14. Aufl. 2016, Art. 5, Rn. 136 unter Hinweis auf BVerfGE 35, 79 (113).

15 Vgl. Jarass/Pieroth (Fn. 14), Art. 5, Rn. 148 unter Hinweis auf BVerfGE 47, 327 (368).

16 Vgl. BVerfGE 47, 327 (369).

17 Vgl. dazu näher Fischer (Fn. 8), § 80a, Rn. 1–2a.

4.2. Zum Verhältnis der IT-Sicherheitsforschung und §§ 202a–202c StGB

Dieser Gedanke soll im Folgenden anhand der §§ 202a–202c StGB mit Bezug auf die IT-Sicherheitsforschung verdeutlicht werden. Dafür spricht zum einen der bereits erwähnte Umstand, dass die hier angesprochenen Grundsatzprobleme gerade auch mit der Einführung des § 202c StGB erörtert wurden. Zum anderen hat die IT-Sicherheitsforschung allgemein eine inhaltliche Nähe zu Fragen der Datenerhebung und zu Fragen des Datenschutzes.[18] Die Datenbegriffsdefinition in § 202a Abs. 2 StGB erfasst nicht nur, aber auch personenbezogene Daten, die im Zentrum der Datenschutzdiskussion stehen. Zudem kann letztlich nur anhand von spezifischen Straftatbeständen die vom System her notwendige Frage beantwortet werden, auf welche Art verfassungsrechtlich abgesicherte Werte wie die Forschungsfreiheit methodisch und inhaltlich in das deutlich ausdifferenziertere System der Straftatbestände integriert werden können.

Zu berücksichtigen ist, dass auch der zuvor genannte § 202c StGB verfassungsrechtliche Bezüge aufweist. Über § 202c StGB werden unter anderem Vorbereitungshandlungen zu Taten gem. §§ 202a, 202b StGB unter Strafe gestellt. Damit geht es nicht nur um den Schutz persönlicher Daten und damit um das Grundrecht auf informationelle Selbstbestimmung.[19] Wesentlich ist auch der Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[20] Dieses vom BVerfG entwickelte Grundrecht erweitert den Schutz von Privatheit insbesondere mit Blick auf die Nutzung von IT-Systemen. Es wird zum Beispiel auch im Zusammenhang mit Fragen des sog. digitalen Hausfriedensbruchs für den Bereich des Computerstrafrechts verstärkt diskutiert.[21]

4.3. Zum Stellenwert der Forschungsfreiheit in der Europäischen Datenschutz-Grundverordnung (DSGVO)

Bei den potentiellen Wertungskonflikten zwischen Forschungsfreiheit und Strafrecht geht es auch um Abwägungsfragen und damit um den rechtlichen Stellenwert der Forschungsfreiheit. Dieser wird auch in der DSGVO[22] thematisiert.

Die DSGVO enthält europaweite Vorgaben zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DSGVO). Damit hat sie eine natürliche inhaltliche Nähe zu den zuvor genannten Straftatbeständen. Die Freiheit der wissenschaftlichen Forschung gehört zudem zu den Verfassungstraditionen der Mitgliedsstaaten[23] und wird auf europäischer Ebene zum Beispiel durch Art. 13 S. 1 Charta der Grundrechte der Europäischen Union (GRCh) anerkannt.

Bereits ein nur kursorischer Überblick zeigt: Im zuvor skizzierten Zusammenhang wird der Wissenschaftsfreiheit einschließlich der Forschungsfreiheit durch die DSGVO eine auffallend privilegierte Bedeutung zugesprochen. Dies kommt bereits in den Erwägungsgründen (EG) zum Ausdruck. So soll gemäß EG 159 die Verordnung auch für die Verarbeitung personenbezogener Daten zu Forschungszwecken gelten (S. 1). Berücksichtigt werden soll dabei das in Art. 179 Abs. 1 AEUV festgeschriebene Ziel, einen europäischen Raum der Forschung zu schaffen (S. 3). EG 157 betont im Zusammenhang mit medizinischer und sozialwissenschaftlicher Forschung, dass durch Verknüpfung von Informationen aus Registern bessere Forschungsergebnisse erzielt werden können. Ausweislich EG 156 soll es den Mitgliedsstaaten unter Wahrung geeigneter Garantien erlaubt sein, unter anderem zu wissenschaftlichen Forschungszwecken Einschränkungen bei den Rechten auf Berichtigung, Löschung, Vergessenwerden vorzunehmen.

---

18 Vgl. im Zusammenhang mit Fragen der De-Anonymisierung auch bereits Sorge, Empirische Forschung im technischen Datenschutz: Ein juristisches Problem?, IRIS 2013, 469–474.

19 Dazu BVerfGE 65, 1 (43).

20 Dazu BVerfGE 120, 274 (313).

21 Dazu näher Tassi (Fn. 6), DuD 2017, 178/179.

22 Vgl. zu Fragen von Wissenschaft und Forschung im Rahmen der DSGVO näher Johannes, in: Roßnagel (Hrsg.), Europäische Datenschutzgrundverordnung, 2017, S. 233 ff.

23 Vgl. Johannes, in: Roßnagel (Hrsg.) (Fn. 22), S. 234.

Diese Privilegierung der Forschungsfreiheit zeigt sich auch in den Regelungen der DSGVO selbst. Ausdruck davon ist insbesondere der für die Forschungsfreiheit zentrale Art. 89 DSGVO. Ausweislich Abs. 2 sind zahlreiche Abweichungen von den sonst geltenden Regelungen zum Zwecke der wissenschaftlichen Forschung erlaubt. Gleiches gilt für Art. 85 DSGVO.[24] Das für sensible Daten grundsätzlich bestehende Verarbeitungsverbot (Art. 9 Abs. 1) ist gem. Art. 9 Abs. 2 lit. j DSGVO für wissenschaftliche Forschungszwecke aufgehoben. Als eine Zentralnorm für die Privilegierung wissenschaftlicher Forschung kann auch Art. 5 Abs. 1 lit. b DSGVO angesehen werden. Dieser verweist zunächst auf das Gebot der Zweckbindung als zentrales Element der personenbezogenen Datenverarbeitung. Ausgenommen davon ist die wissenschaftliche Forschung. Eine Weiterarbeitung für wissenschaftliche Forschungszwecke gilt – qua rechtlicher Fiktion – nicht als unvereinbar mit den ursprünglichen Zwecken (Art. 5 Abs. 1 lit. b DSGVO).

4.4. Forschungsfreiheit und das Strafrecht

Im Folgenden soll skizziert werden, wie die verfassungsrechtlich geschützte Forschungsfreiheit inhaltlich und methodisch in das strafrechtliche System integriert werden kann.

4.4.1. Möglichkeiten auf Tatbestandsebene

Bei der bereits angesprochenen Problematik der Dual-Use-Programme im Bereich des § 202c StGB hat das BVerfG für einen Teilbereich eine tatbestandliche Lösung gefunden. Bei Programmen, die von der Wissenschaft entwickelt wurden, fehlt es bereits an der vom Tatbestand des § 202c StGB geforderten deliktischen Zweckbindung. Anders stellt sich aber die Sachlage dar, so das BVerfG, wenn das eingesetzte Programm zum Beispiel aus zweifelhafter Quelle im Internet beschafft wurde. Dann ist der Tatbestand zunächst erfüllt.[25]

4.4.2. § 202d StGB als methodischer Ausgangspunkt für eine strafrechtliche Privilegierung der Wissenschaftsfreiheit?

§ 202c StGB enthält keine ausdrückliche Regelung für Fragen der Forschungsfreiheit. Eine verallgemeinerungsfähige Privilegierung der Forschungsfreiheit im Bereich des Datenzugriffs könnte jedoch in § 202d Abs. 3 StGB gesehen werden. Gemäß dem 2015 neu eingeführten Tatbestand der Datenhehlerei (§ 202d Abs. 1 StGB) wird bestraft, wer Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt, sich oder einem anderen verschafft. Ausweislich § 202d Abs. 3 S. 1 StGB gilt Abs. 1 aber nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu zählen, wie bei § 184b Abs. 5 StGB auch[26], Rechte wie die Forschungsfreiheit.[27]

4.4.3. Weitere strafrechtliche Privilegierungen der Wissenschaftsfreiheit

Eine Privilegierung von Wissenschaft und Forschung zeigt sich insbesondere auch im Bereich der Äußerungsdelikte. So sanktioniert § 86 Abs. 1 StGB das Verbreiten von Propagandamitteln verfassungswidriger Organisationen. Abs. 1 gilt jedoch nicht, wenn die Handlung der Wissenschaft, der Forschung oder der Lehre dient (§ 86 Abs. 3 StGB). Diese sogenannte Sozialadäquanzklausel findet sich auch in § 86a Abs. 3 StGB (Verwenden von Kennzeichen verfassungswidriger Organisationen) bzw. § 130a Abs. 4 StGB (Anleitung zu Straftaten).

Auch in § 201a Abs. 4 StGB in der seit dem 27. Januar 2015 geltenden Fassung ist der zuvor angesprochene Gedanke der Sozialadäquanz enthalten. § 201a StGB sanktioniert die Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen. Gemäß § 201a Abs. 4 StGB werden bestimmte – an sich strafbare – Handlungen dann nicht sanktioniert, wenn sie in Wahrnehmung überwiegender berechtigter Interessen er-

[24] Die Schrankenregelungen in Art. 89 und Art. 85 DSGVO sind nicht aufeinander abgestimmt – vgl. Gola/Pötters, Datenschutz-Grundverordnung, 2017, Art. 89, Rn. 12.

[25] Vgl. BVerfG (Fn. 12), Rn. 61 bzw. 70; Gleiches gilt, wenn das Tool nicht vertrauenswürdigen Dritten überlassen wird (Rn. 75).

[26] § 184b Abs. 5 StGB betrifft die Verbreitung kinderpornographischer Schriften – vgl. Holzner (Fn. 12), ZRP 2009, 177.

[27] Vgl. Fischer (Fn. 8), § 202d, Rn. 11 i.V.m. § 184b, Rn. 43.

folgen, namentlich unter anderem der Wissenschaft, der Forschung oder der Lehre oder ähnlichen Zwecken dienen.

4.4.4. Zum Stellenwert der Forschungsfreiheit innerhalb des strafrechtlichen Systems

Die hier skizzierten Überlegungen haben gezeigt, dass innerhalb der Strafrechtsdogmatik ein klarer systematischer Stellenwert der Forschungsfreiheit nicht festgestellt werden kann. Methodisches Entwicklungspotential im Sinne einer innovativen Analogie[28] dürfte bei dem hier interessierenden Grundsatzkonflikt zwischen Forschungsfreiheit und Strafrecht vorrangig der zuletzt genannte § 201a Abs. 4 StGB besitzen. Zum einen wird darin die Forschungsfreiheit ausdrücklich angesprochen. Zum anderen wird mit dem Merkmal «Wahrnehmung überwiegender berechtigter Interessen» auch ein materielles Kriterium angegeben.

5. Zusammenfassung und Ausblick

Ziel des Beitrags war, die vermehrt zu erwartenden Grundsatzkonflikte zwischen IT-Sicherheitsforschung und Strafrecht aufzuzeigen und anhand von § 202c StGB mögliche Entscheidungskriterien über den Einzelfall hinaus zu verdeutlichen. Ein klarer strafrechtssystematischer Stellenwert der Forschungsfreiheit lässt sich nicht feststellen. Erforderlich ist daher typischerweise eine strafrechtsbezogene Folgenabschätzung analog der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO. Bezüglich der IT-Sicherheitsforschung lenkt dies den Blick auf zwei Themenbereiche mit wachsender Bedeutung:

1. So wird neuerdings das Thema «Compliance an Universitäten» im Sinne eines organisierten Managements der Regelbefolgung, als Organisation von Legalität, verstärkt diskutiert.[29] Dazu zählen Normenbereiche wie der Datenschutz und der Umweltschutz. Es betrifft jedoch auch das hier interessierende Strafrecht. So beschäftigt etwa das Universitätsklinikum Heidelberg in seiner Rechtsabteilung einen eigenen Chief Compliance Officer.
2. Daneben könnte es sachgerecht sein, vermehrt fachspezifische Ethikkommissionen einzuschalten.[30] Diese vorrangig aus der medizinischen Forschung entwickelte Form wissenschaftlicher Selbstkontrolle wird zwischenzeitlich auch im Bereich der Sozialwissenschaften angewendet.[31] Auch die Informatik kennt Ethikkommissionen. Dies gilt zum Beispiel für die Universität Hamburg[32] bzw. die Universität des Saarlandes[33]. Bezüglich der inhaltlichen Vorgaben für die Arbeit derartiger Kommissionen kann exemplarisch auf die ethischen Leitlinien der Gesellschaft für Informatik verwiesen werden.[34]

Die beiden organisatorischen Ansätze werden jedoch die skizzierten Grundsatzprobleme alleine nicht lösen können. Sie müssen sich beide der teilweise massiven wissenschaftlichen Binnenkritik stellen, dass sie ihrerseits der durch Art. 5 Abs. 3 GG geschützten Wissenschaftsfreiheit nicht genügend individuellen Raum lassen.[35] Bei Ethikkommissionen kann sich zudem die Grundsatzfrage stellen, ob oder inwieweit der ethische

[28] Vgl. zu innovativen Analogien insbesondere im Bereich des Computerstrafrechts, Tassi (Fn. 6), DuD 2017, 175 ff.
[29] Dazu insbesondere Schröder (Fn. 1), ZIS 2017, 285.
[30] So für die IT-Sicherheitsforschung auch Backes, Herausforderungen des Internet of Things, DuD 2016, 489.
[31] Dazu von Unger/Simon, Ethikkommissionen in den Sozialwissenschaften – Historische Entwicklungen und internationale Kontroversen, RatSWD Working Paper Series 2016. Nr. 253.
[32] Vgl. zum Beispiel Ethikkommission des Fachbereichs Informatik an der Universität Hamburg, abrufbar unter: https://www.inf.uni-hamburg.de/home/ethics.html (alle Websiten zuletzt abgerufen am 20. Dezember 2017).
[33] Ethikkommission der Fakultät für Mathematik und Informatik der Universität des Saarlandes, https://erb.cs.uni-saarland.de/.
[34] https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/.
[35] Vgl. zum Beispiel mit Bezug auf Ethikkommissionen von Unger/Simon (Fn. 31), S. 13 – Gefahr für Methodenpluralismus.

Ansatz[36] überhaupt mit der hier betonten strafrechtlichen Perspektive deckungsgleich ist.[37] Noch wichtiger erscheint im vorliegenden Zusammenhang, dass staatliche Gerichte nicht an die Auffassung von Ethikkommissionen gebunden sind. Zudem liegt die Besonderheit darin, dass auch für die Strafrechtswissenschaft selbst die skizzierten Probleme an der Schnittstelle von IT-Forschung und Strafrecht neuartig sind. Insbesondere hat sich noch keine obergerichtliche Rechtsprechung entwickelt, die in verlässlicher Weise Prognosen über die zu erwartende strafrechtliche Beurteilung zulassen würde. Verschärft wird diese Grundsatzproblematik durch die technische Entwicklung zum Internet der Dinge (IoT).[38] Das IoT kann zu Gefährdungslagen führen, die zurzeit noch nicht klar umrissen und wenig überschaubar sind.[39] Dies erschwert eine seriöse strafrechtliche Risikoanalyse.

Faktisch hilfreich für die strafrechtliche Entlastung kann ein positives Votum einer entsprechenden Kommission aber dennoch sein. Dies gilt etwa unter dem Gesichtspunkt, dass bei Vorsatztaten der Verbotsirrtum für den Handelnden gemäß § 17 S. 1 StGB unvermeidbar sein kann. Dann würde die Schuld entfallen. Bei Vermeidbarkeit kommt auch eine Strafmilderung gemäß § 17 S. 2 StGB in Betracht. Zwar hat der BGH in einem Urteil vom 16. Mai 2017[40] ausdrücklich betont, dass zum Beispiel die Einholung eines anwaltlichen Rats allein die Unvermeidbarkeit des Verbotsirrtums gemäß § 17 S. 1 StGB nicht zu begründen vermag. Bei einem positiven Votum eines fachkundigen Gremiums hätte der Betreffende aber seine bereichsspezifische Erkundigungspflicht erfüllt, die im Rahmen des § 17 StGB eine zentrale Rolle spielt.[41] Eine Ethikkommission wäre typischerweise auch ein Gremium, das Gewähr für eine objektive, sorgfältige, pflichtgemäße und verantwortungsbewusste Auskunftserteilung bietet.[42] Gerade bei neuartigen Problemen an der Schnittstelle von Technik und Recht stellt sich zudem die Frage, welche sonstigen Alternativen im Rahmen der rechtlich gebotenen Erkundigungspflicht überhaupt zur Verfügung stehen.

Bestehen bleibt auf jeden Fall auch in Zukunft der Grundsatzkonflikt: Wissenschaft braucht Freiheit, Freiheit erfordert Verantwortung.[43] Dies gilt auch mit Blick auf die geltenden Strafgesetze.

---

36 Dazu auch Wagner, Anmerkungen zu den vielfältigen Dimensionen einer Forschungsethik in den Sozial-, Verhaltens- und Wirtschaftswissenschaften, RatSWD Working Paper Series 2017, Nr. 265.

37 Vgl. zum Verhältnis von rechtlichen und ethischen Maßstäben näher Lindner, Deutscher Ethikrat als praeceptor iurisdictionis?, ZRP 2017, 148 ff. in Zusammenhang mit einer Kritik des Deutschen Ethikrats an einer Entscheidung des BVerwG vom 2. März 2017 zur Sterbehilfe.

38 Dazu Backes (Fn. 30), DuD 2016, 489.

39 Vgl. in diesem Zusammenhang auch Möllers/Vogelgesang, Smart-Home-Systeme in Zeiten digitaler Kriminalität, DuD 2016, 497 ff.

40 BGH NJW 2017, 2463.

41 Vgl. dazu näher Fischer (Fn. 8), § 17, Rn. 12.

42 Vgl. Fischer (Fn. 8), § 17, Rn. 13 unter Hinweis auf BGH St 40, 264 zu den Anforderungen an eine entsprechende Auskunft.

43 Deutsche Forschungsgemeinschaft (DFG) und Deutsche Akademie der Naturforscher Leopoldina – Nationale Akademie der Wissenschaften, Wissenschaftsfreiheit und Wissenschaftsverantwortung – Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung, 28. Mai 2014, Vorwort.