AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.7
www.austrian-law-journal.at

Cyber Crime – Der digitalisierte Täter

Christian Bergauer*, Universität Graz

***Kurztext**: Der vorliegende Kommentar bezieht sich auf den Beitrag „Cyber Crime – der digitalisierte Täter" von Susanne Reindl-Krauskopf (ALJ 2/2017, 110). Die Computerkriminalität ist aktuell wohl eines der am schnellsten wachsenden, aber auch unterschätztesten Kriminalitätsfelder und damit bereits zu einem massiven faktischen Problem in der Gesellschaft geworden. Allein im Jahr 2016 gab es in Österreich 13.103 Anzeigen wegen Cybercrime-Delikten.[1] Obwohl Cybercrime-Phänomene in allen Lebensbereichen zunehmen, sind sie noch nicht wirklich in der Rechtsprechung angekommen, was die äußerst wenigen Verurteilungszahlen bestätigen.[2] Dies beruht auf folgenden Gründen: Faktische Probleme der Täterausforschung in der informationstechnischen Umgebung, strafprozessuale Schwierigkeiten hinsichtlich IT-spezifischer Ermittlungsmaßnahmen insb bei Auslandsbezug und nicht zuletzt konzeptionell verbesserungsfähige Computerdelikte.[3]*

Die der Computerkriminalität zugrunde liegenden informationstechnischen Konzepte machen sie sehr facettenreich, weshalb die im Hauptvortrag von Reindl-Krauskopf diskutierten Phänomene lediglich eine kleine Auswahl an Erscheinungsformen der Computerkriminalität darstellen. In meinem Kommentar zu diesen Beispielsfällen, werde ich einige neue Herausforderungen für das Strafrecht dogmatisch sowie rechtspolitisch näher beleuchten.

***Schlagworte:** Cybercrime, Computerkriminalität, Computerstrafrecht, Hacking, Smart Cars, Ransomware, Medjacking*

Eingangs möchte ich mich bei den VeranstalterInnen für die Einladung bedanken, an dieser Tagung mit einem Kommentar zum Vortrag von Frau Univ.-Prof.in Dr.in *Susanne Reindl-Krauskopf* mitwirken zu dürfen. Der Mehrwert eines Kommentars liegt mE nicht in einem bloßen Resümee oder der besonderen Betonung jener Aspekte des Hauptvortrags, in denen ohnehin Einigkeit besteht (und solche gibt es viele), sondern insb in Ergänzungen und im Aufzeigen ggf etwas anders gelagerter Sichtweisen. So erlaube ich mir, einige ergänzende Bemerkungen zur dogmatischen Analyse von *Reindl-Krauskopf* ebenso wie einige rechtspolitische Gedanken zu einzelnen Themenberei-

* Az. Prof. Dr. *Christian Bergauer* ist assoziierter Professor am Institut für Rechtswissenschaftliche Grundlagen, Fachbereich Recht und IT, der Karl-Franzens-Universität Graz.

1 *BMI*, Sicherheit 2016 – Kriminalitätsentwicklung in Österreich 31, http://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj8pdrnr-DTAhUMbBoKHcATADQQFggsMAA&url=http%3A%2F%2Fwww.bmi.gv.at%2Fcms%2FBK%2Fpublikationen%2Fkrim_statistik%2F2016%2FWeb_Sicherheit_2016.pdf&usg=AFQjCNEDiNqkAwEFnZakxqWQtnIxYaQZXQ (abgefragt am 8. 5. 2017).

2 Siehe dazu die von der Statistik Austria publizierten Verurteilungszahlen insb zu den Computerdelikten §§ 118a, 119, 119a, 126a, 126b, 126c StGB auf www.statistik.at (abgefragt am 8. 5. 2017).

3 Siehe fünf generelle Thesen zu den aktuellen Herausforderungen im Bereich des Computerstrafrechts bei *Bergauer*, Das materielle Computerstrafrecht (2016) 597 ff.

Fundstelle: *Bergauer*, Cyber Crime – Der digitalisierte Täter, ALJ 2/2017, 119–124 (http://alj.uni-graz.at/index.php/alj/ article/view/84).

chen zu äußern. Ich kann allerdings in der mir zur Verfügung stehenden Zeit nicht auf alle mir wichtigen Aspekte dieses Vortrags eingehen.

Zutreffend thematisierte *Reindl-Krauskopf* sowohl in ihrem Sachverhaltsbeispiel zum „Smart Home-Hacking" als auch in ihren Ausführungen zum „Medjacking" § 118a StGB. Zu dieser Bestimmung ist allerdings anzumerken, dass sie seit ihrer Einführung im Jahr 2002[4] lange Zeit umstritten war, in den Jahren 2008[5] und 2016[6] aus diesem Grund novelliert wurde, und schließlich wohl nach wie vor umstritten ist. Wirft man einen Blick in die gerichtlichen Kriminalstatistiken der Jahre 2002 bis 2015 fällt auf, dass es in 14 Jahren lediglich 8 Verurteilungen österreichweit gab,[7] obwohl allein im Jahr 2014 677 Fälle eines Widerrechtlichen Zugriffs auf ein Computersystem angezeigt wurden.[8] Jeder, der sich den Wortlaut dieses Tatbestands ansieht, kann sich leicht selbst ein Bild von der Komplexität dieser Bestimmung machen. In beiden Sachverhaltsbeispielen (Smart Home-Hacking und Medjacking) ist auffällig, dass keine Feststellungen zum jeweiligen computertechnischen *modus operandi* bezüglich der „Überwindung einer spezifischen Sicherheitsvorkehrung" getroffen wurden, sondern dieser Sachverhaltskomplex mit dem Begriff „knacken" pauschalisiert wurde. Nach dem allgemeinen Sprachgebrauch bedeutet „knacken" aber nicht nur etwas physisch aufzubrechen oder durch Einwirken auf die Daten- bzw Sachsubstanz „auszuschalten", wie es im Vortrag verortet wurde, sondern insb auch einen Sperrmechanismus zu überlisten (man denke an die Wendung „einen Code knacken"). In solchen Formen computerspezifischer Handlungsweise liegt nun aber gerade das Wesen der Computerkriminalität im Allgemeinen und die besondere Herausforderung der Subsumtion solcher Sachverhalte unter den objektiven Tatbestand des § 118a StGB im Besonderen. Es ist daher notwendig, sich mit Fragen bezüglich des Überwindens (in Abgrenzung zur Verletzung und Umgehung[9]) ebenso auseinanderzusetzen wie mit der Frage, wie geeignet und tauglich eine Sicherheitsvorkehrung zu sein hat und wo eine solche angebracht bzw implementiert sein muss, um dem konkreten Tatobjekt „Computersystem" zurechenbar zu sein (zB im Falle eines LAN).[10] Wie sieht es aus, wenn zwei Wege ins Zielsystem führen, aber nur einer davon – was der Täter weiß – gesichert ist? Man denke etwa an ein externes Booten des fremden Computersystems oder den schlichten Ausbau der Festplatte, um diese Speichermedien auszulesen, ohne auf einen im System implementierten Sicherheitsmechanismus stoßen zu müssen. Wie wäre die Tatbestandsmäßigkeit iSd § 118a StGB zu beurteilen, wenn der Täter das zutreffende Passwort gekannt hätte? Wie ist der Täter in einem solchen Fall an das Passwort gelangt und welcher Aufwand ist hierfür notwendig gewesen, um das für eine „Überwindung" verlangte Mindestmaß an krimineller Energie[11] auszuloten und im Einzelfall festzustellen.[12] Wird darüber hinaus ein Schadprogramm zur Erlangung eines Passworts eingesetzt

4 StRÄG 2002 BGBl I 2002/134.
5 StRÄG 2008 BGBl I 2007/109.
6 StRÄG 2015 BGBl I 2015/112.
7 Siehe dazu die von der Statistik Austria publizierten Verurteilungszahlen auf www.statistik.at (abgefragt am 8. 5. 2017) (diversionelle Erledigungen wurden in diesen Statistiken nicht berücksichtigt).
8 Siehe die parlamentarische Anfragebeantwortung der Innenministerin betreffend die „Internetkriminalität – Strafdelikte durch IT-Medium im Jahr 2014" (AB 3400 BlgNR 25. GP 1).
9 Ein Überwinden erfordert mE die Konfrontation des Täters mit der spezifischen Sicherheitsvorkehrung, etwa durch Ausarbeitung eines Überwindungsplans und die anschließende direkte Bezwingung der Sicherheitsvorkehrung und verlangt daher mehr als ein bloßes Umgehen siehe *Bergauer*, Computerstrafrecht 100 f.
10 Siehe dazu insb *Bergauer*, Computerstrafrecht 88 ff.
11 Siehe dazu ErläutRV 285 BlgNR 23. GP 7; *Reindl-Krauskopf* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB[2] § 118a Rz 28 (Stand 1. 10. 2014, rdb.at); *Bergauer*, Computerstrafrecht 98 f.
12 Zu diesen Fragestellungen siehe *Bergauer*, Computerstrafrecht 88 ff.

(wie etwa ein brute force-Tool zur Errechnung eines Passworts durch Permutation vordefinierter Zeichensätze bzw keylogger- bzw sniffer-Programme zum Abfangen von Zugangsdaten am Zielsystem bzw Übertragungsweg[13]), wäre auch an das Vorbereitungsdelikt des § 126c StGB zu denken.

Schaut man sich die komplizierten Elemente der überschießenden Innentendenz des subjektiven Tatbestands des § 118a StGB an, so fällt auf, dass aktuell gegenüber der Vorfassung die „Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden" entfallen ist und daher auch für bestimmte Fälle die Strafbarkeit (noch weiter) zurückgenommen wurde. Man denke an unberechtigte Geldtransaktionen über online-banking-Systeme durch Eingabe „abgefischter" Passwörter oder an Bitcoin-Mining über (zweckentfremdete) Bot-Netze. In solchen Fällen kommt es dem Täter nämlich nicht darauf an, im Sinne der Absichtlichkeit des § 5 Abs 2 StGB, einem anderen durch die Verwendung des Computersystems einen „Nachteil" zuzufügen (siehe § 118a Abs 1 Z 2 StGB). Dem Täter kommt es idR wohl ausschließlich darauf an, sich oder einem anderen einen Vermögensvorteil zuzuwenden bzw sich oder einen anderen zu bereichern. Die Zufügung eines – wie auch immer gearteten – Nachteils für andere wird daher vom Täter nur in Kauf genommen (arg *„dolus eventualis"*), nicht aber anvisiert.[14] Daran ändert sich auch nichts, wenn er das Eintreten eines solchen Nachteils bei einer anderen Person für gewiss hält. Es sollte daher diskutiert werden, ob für die Verwirklichung des subjektiven Tatbestands bezüglich des erweiterten Vorsatzes tatsächlich an der stärksten Form der Vorsatzausprägung, nämlich der Absicht, festgehalten werden sollte bzw ob nicht der entsprechende Teil der Definition der überschießenden Innentendenzen der Stammfassung des § 118a StGB (idF BGBl I 2002/134), dh die „Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden", wieder Eingang in den subjektiven Tatbestand finden sollte. Wer bei solchen Bereicherungsfällen an den Betrügerischen Datenverarbeitungsmissbrauch (§ 148a StGB) denkt, wird wohl damit konfrontiert, dass § 148a StGB ebenfalls aus legistischer Sicht nicht unumstritten konzipiert ist und folglich auch ein „Sammelbecken für Rechtsfortbildungen" darstellt.[15] So muss man sich etwa – wie ein Großteil der Lehre sowie die Rsp[16] – sehr weit „hinauslehnen", um das bloße Auslösen eines Datenverarbeitungsvorgangs (zB die Eingabe eines widerrechtlich erlangten aber zutreffenden Passworts) bereits als eine „Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung" zu erachten.[17] Tatsächlich ist es wohl äußerst fraglich, ob dieses Delikt überhaupt jene strafbedürftigen Sachverhaltskonstellationen erfasst bzw „erfassen darf", für die es eigentlich geschaffen wurde.

Wie im Ausgangssachverhalt des Smart Home-Beispiels ersichtlich, kann das Opfer aber auch stundenlang keine Kontrolle über das System ausüben. Aus diesem Grund wäre daran zu denken, dass der Täter die Zugangsdaten geändert hat und das Opfer daher die Änderung selbst nicht – zB über die Bedienkonsole – rückgängig machen kann. Für solche Fälle wäre jedenfalls auch § 126a StGB (Datenbeschädigung) in den Varianten der Datenveränderung sowie Datenunterdrückung einschlägig. Da ein Smart Home-System aber neben Softwarekomponenten auch

13 Zur Beschreibung dieser Schadprogramme siehe an unterschiedlichen Stellen *Bergauer*, Computerstrafrecht.

14 Vgl *Bergauer*, Fall 12 – Phishing for nothing, in *Hinterhofer/Schütz* (Hrsg), Fallbuch Straf- und Strafprozessrecht[2] (2016) 189.

15 Siehe OGH 1. 6. 2006, 12 Os 45/06v (12 Os 46/06s); OGH 13. 10. 2005, 15 Os 99/05 f; siehe auch OLG Innsbruck 16. 12. 2014, 11 Bs 353/14w iZm Paysafecards; OGH 14.12.1995, 15 Os 131/95; *Bergauer*, Computerstrafrecht 353 ff mwN; *Bergauer*, Computerstrafrecht, in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht (2016) Rz 11.136 f; *Komenda/Madl* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), StGB – Salzburger Kommentar zum Strafgesetzbuch[36] (2016) § 148a Rz 39 ff; weiters *Birklbauer/Hilf/Tipold,* Strafrecht Besonderer Teil I[3] (2015) § 148a Rz 7 f mwN.

16 Siehe die Positionen zusammenfassend *Komenda/Madl* in *Triffterer/Rosbaud/Hinterhofer*, SbgK[36] § 148a Rz 68.

17 Siehe dazu *Bergauer*, Computerstrafrecht 361 ff.

aus Hardwareteilen besteht (Thermostate, Schließmechaniken usw), die laut Sachverhalt nicht mehr ordnungsgemäß funktionieren, ist darüber hinaus in echter Konkurrenz an die Sachbeschädigung durch Unbrauchbarmachen iSd § 125 StGB zu denken.

Geradezu im Vorbeigehen wurde im Vortrag die einzig gerichtliche Strafbestimmung des § 51 DSG 2000[18] im Zusammenhang mit der Nutzung ausspionierter personenbezogener Daten angesprochen. Zur Aussage, dass das Sammeln solcher personenbezogener Informationen noch nicht strafrechtlich relevant sei, ist allerdings anzumerken, dass im sog „iPhone-Fall“[19] hinsichtlich des bloßen Speicherns digitaler Bildaufnahmen von einer Frau, welche sich gerade auf der Toilette befand, die grundsätzliche Anwendbarkeit des § 51 DSG 2000 bejaht wurde. Man muss daher wohl davon ausgehen, dass das Ermitteln der personenbezogenen Informationen durch den Täter mittels Kamerafunktion seines Smartphones als Akt des widerrechtlichen Verschaffens und das daran in unmittelbarer zeitlicher Abfolge erfolgte Speichern dieser (nunmehr digitalisierten) Daten auf der Speicherkarte des iPhones als Tathandlung des „Selbst-Benützens“ beurteilt wurde. Schließt man sich dieser Auffassung an, wäre – anders als im Vortrag kommuniziert – auch das bloße Sammeln personenbezogener Daten von § 51 DSG 2000 erfasst.[20]

Höchst interessant erweisen sich die von *Reindl-Krauskopf* in ihrem Vortrag angestellten Überlegungen zur Anwendung des § 118a StGB auf Fälle des sog „Medjacking“, gerade auch, weil sie selbst hierbei eine gewisse „Irritation“ verortet, die mE jedenfalls aus rechtspolitischer Sicht näher zu untersuchen wäre. Schon allein aus Sachlichkeitsüberlegungen wäre zu hinterfragen, ob aktive Implantate bzw Prothesen (wie zB bionische Arme oder Beine, Herzschrittmacher, Insulinpumpen usw) tatsächlich mit einer Sicherheitsvorkehrung iSd § 118a StGB ausgestattet sein müssen, um dem Träger einen strafrechtlichen Schutz vor Angriffen auf diese Prothesen zu gewähren? Vorauszuschicken ist, dass man als Mensch schon grundsätzlich keine „Ritterrüstung“ tragen muss, um seinen Willen zum Ausdruck zu bringen, nicht in der körperlichen Integrität verletzt werden zu wollen. Der im Vortrag angesprochene Fall des Medjacking könnte zur Verdeutlichung dieser Überlegungen etwas variiert werden. Man denke dabei an eine Sachverhaltsvariante, die nicht zu einer Tötung des Opfers führt, sondern sich die Tathandlung lediglich an einer bionischen Armprothese oder anderer elektro-mechanischer oder mittels Mikrochip gesteuerter, medizinischer Hilfsmittel (wie zB ionischem Auge, Retina-Stimulator, Hörgerät, funktioneller Muskelreizung, Neuro-Stimulator, Blasenschrittmacher usw) auswirkt. Der Täter manipuliert dabei das aktive Implantat, das per Bluetooth justiert und (fern-)bedient werden kann, derart, dass sich etwa ein bionischer Arm lediglich ständig auf und ab bewegt. Versucht man nun die Strafbarkeit einer solchen „Manipulation des Körpers“ zu ermitteln, zeigt sich schnell, dass es *de lege lata* schwierig ist, ein für solche Manipulationen geeignetes Delikt zu finden. Die Intensität der Beeinträchtigung der körperlichen Integrität erreicht wohl nach hM nicht die geforderte Intensität einer Körperverletzung iSd § 83 Abs 1 StGB. Bloße Misshandlungen sind noch keine Verletzungen am Körper.[21] Doch auch ein vorsätzliches Misshandeln iSd § 83 Abs 2 StGB scheidet aus, da wohl die fahrlässig herbeigeführte Folge fehlt (eine Gesundheitsschädigung mit Krankheitswert könnte sich allenfalls

18 BGBl I 1999/165 idF BGBl I 2009/133.

19 LG Salzburg 29. 4. 2011, 49 Bl 17/11v; *Thiele*, LG Salzburg: Datenverwendung in Schädigungsabsicht durch Aufnahme mit iPhone beim Toilettenbesuch, jusIT 2011, 185.

20 Siehe zu § 51 DSG 2000 ausführlich *Bergauer*, Computerstrafrecht 117 ff.

21 Siehe ganz allgemein *Burgstaller/Fabrizy* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB[2] § 83 Rz 6 f (Stand 1. 8. 2016, rdb.at).

aufgrund eines aus der dauerhaften Manipulation entstehenden seelischen Leidens ergeben). Auch die Heranziehung des Delikts der Nötigung gem § 105 StGB wäre problematisch und zumindest im Lichte der Rsp wohl nicht anwendbar, da bei dieser Art der computertechnischen Manipulation nicht auf die Willensbildung des Opfers eingewirkt wird (arg *„vis absoluta"*). Für den OGH kommt prinzipiell nur *vis compulsiva* als Tatmittel der Nötigung in Frage.[22] Aber auch der hier relevante Gewaltbegriff bezüglich des Einsatzes „physischer Kraft" könnte zu Anwendungsschwierigkeiten der Nötigung im Zusammenhang mit computertechnischen Handlungsweisen des Medjacking führen. Des Weiteren wird auch die Sachbeschädigung durch Unbrauchbarmachen iSd § 125 StGB ausscheiden müssen, da nach hM nicht leicht zu entfernende Prothesen oder Implantate dem Körper zugerechnet werden und diese keine selbstständigen Sachen mehr darstellen.[23] Für solche mE strafwürdigen und strafbedürftigen Fälle bleibt *de lege lata* offenbar tatsächlich nur der „Widerrechtliche Zugriff auf ein Computersystem" (§ 118a StGB) übrig, allerdings lediglich unter der Voraussetzung, dass eine spezifische Sicherheitsvorkehrung im „Computersystem" vorhanden ist und diese vom „Hacker" auch überwunden wurde. Hier gibt es mE jedenfalls einen Nachbesserungsbedarf in der Strafrechtsdogmatik.

Die „digitale Erpressung" mittels des Einsatzes sog „Ransomware"[24] ist wohl das derzeit praxisrelevanteste Phänomen der im Vortrag angesprochenen Fallbeispiele. Da hier eine spezielle Schadsoftware, sog „Malware",[25] zum Einsatz kommt, wäre jedenfalls für diesbezügliche Vorbereitungshandlungen an das Vorbereitungsdelikt des § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) zu denken, das selbst wiederum jede Menge Besonderheiten aufweist.[26] Dieses Vorbereitungsdelikt tritt allerdings aufgrund materieller Subsidiarität zurück, sobald eines der dort in § 126c Abs 1 StGB genannten Hauptdelikte zumindest versucht wurde.

Abschließend möchte ich noch ein Statement zum letztbesprochenen Fall hinsichtlich vollautonomer Smart Cars abgeben. Die Entwicklungen im Bereich des maschinellen Lernens sind mittlerweile soweit fortgeschritten, dass intelligente Systeme tatsächlich eigenständig Entscheidungen treffen können. Es handelt sich dabei um selbstlernende Algorithmen, wie sie etwa im Bereich der Gesichtserkennung oder bei Fahrerassistenzsystemen in der Automobilindustrie bereits eingesetzt werden. Ein solches intelligentes System wird mittels eingespielter Beispieldatensätze quasi „erzogen". Das heißt, es werden nicht einfach Beispieldaten im System abgespeichert, welche in weiterer Folge bezüglich vordefinierter, dh dem System bereits bekannter, Sachverhalte abgerufen werden, sondern das System „erkennt" durch Analyse der Beispielsdaten Muster und Gesetzmäßigkeiten und wendet diese auf neue Szenarien völlig autonom auf Grundlage dieses „Erfahrungswissens" an. Aus heutiger Sicht ist es dabei undenkbar, alle möglichen Systementscheidungen hinsichtlich aller möglichen Sachverhalte vorauszudenken.

Besondere strafrechtliche Herausforderungen treten dabei insb bei einem verursachten Schaden im Zusammenhang mit selbstlernenden Algorithmen und einer etwaigen Fahrlässigkeitsstrafbarkeit in Erscheinung. Diese beginnen bereits bei der Frage, wer – also Programmierer, Hersteller uÄ –

22 Siehe dazu *Schwaighofer* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB[2] § 105 Rz 24 und 27 (Stand 1. 5. 2016, rdb.at).

23 Vgl *Burgstaller/Fabrizy* in *Höpfel/Ratz*, WK[2] § 83 Rz 4; in diesem Sinne auch *Bachner-Foregger* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB[2] § 190 Rz 4 (Stand 1. 11. 2009, rdb.at).

24 Siehe dazu *Bergauer* in *Kert/Kodek* Rz 11.31.

25 Zusammengesetztes Kurzwort für *„malicious software"*.

26 Siehe dazu ausführlich jüngst *Bergauer*, Computerstrafrecht 317 ff.

nach dem Schuldprinzip überhaupt als Tatsubjekt für das konkrete objektiv sorgfaltswidrige Verhalten der Maschine, das konzeptionell nicht immer mit einem Programmfehler verbunden sein muss, in Frage kommt und ob dieser Person der eingetretene Erfolg überhaupt objektiv zugerechnet werden kann. Hauptsächlich wird dabei wohl die Nachweisbarkeit im Bereich der normativen Zurechnung problematisch sein, wie vor allem die objektive Vorhersehbarkeit des Erfolgs oder die Frage nach der Risikoerhöhung bei rechtmäßigem Alternativverhalten, wenn nämlich einerseits gar kein Programmierfehler im Herstellungsprozess vorgelegen hat, sondern der Erfolg durch eine selbstständige Entscheidung im Rahmen der autonomen Fortentwicklung des Systems eingetreten ist, und andererseits, es faktisch gar nicht möglich ist, alle System-Entscheidungen im Hinblick auf sämtliche zukünftigen Sachverhaltskonstellationen vorherzusehen. Es wäre allerdings auch daran zu denken, dass etwa dem Hersteller und/oder Fahrzeughalter eine Überwachungspflicht für die besondere Gefahrenquelle „Smart Car" auferlegt sein kann, weshalb der Überwachungsgarant dafür Sorge tragen muss, dass andere Rechtsgüter durch die von ihm zu überwachende Gefahrenquelle nicht geschädigt werden dürfen (zB Verkehrssicherungspflichten). Wird gegen eine solche Überwachungsverpflichtung verstoßen, kann dies ebenfalls eine Fahrlässigkeitshaftung für den Einzelnen auslösen, sofern – wie für den Bereich der strafbaren Handlungen gegen Leib und Leben zutreffend – ein entsprechendes Fahrlässigkeitsdelikt existiert.

Unabhängig davon kann dem Halter eines voll-autonomen Autos ebenso wie dem Lenker eines Kfz, das nur gewisse Fahrmanöver unter der Aufsicht des Lenkers mittels Fahrerassistenzsystemen (wie zB Parkpilot) ausführt, eine sog „Einlassungsfahrlässigkeit" vorgeworfen werden, wenn ein autonomes Smart Car bzw ein Assistenzdienst in Betrieb genommen wird, obwohl dieses/ dieser bereits in der Vergangenheit ein dem Lenker bekanntes „auffälliges (Fehl-)Verhalten" gezeigt hatte.

Die Computerkriminalität ist aktuell wohl eines der unterschätztesten Kriminalitätsfelder, obwohl sie bereits zu einem massiven gesellschaftlichen Problem geworden ist. Die im Hauptvortrag angerissenen Phänomene bilden lediglich eine kleine Auswahl an Erscheinungsformen der Computerkriminalität. Im Jahr 2016 gab es allein in Österreich 13.103 Anzeigen wegen Cybercrime-Delikten.[27] Dennoch ist sie noch nicht wirklich in der Rechtsprechung angekommen, was die zu Beginn meines Kommentars präsentierten Verurteilungszahlen belegen dürften. Faktische Probleme der Täterausforschung, strafprozessuale Schwierigkeiten diverser informationstechnischer Ermittlungsmaßnahmen aber insb auch konzeptionell verbesserungsfähige Computerdelikte sind mE die Gründe dafür.[28] Proportional zur rasanten informationstechnischen Fortentwicklung und deren gesellschaftlichen Durchdringung werden jedenfalls die strafwürdigen Cybercrime-Phänomene in allen Lebensbereichen zunehmen, was zwingend auch dazu führen wird, dass der Computerkriminalität im Allgemeinen sowie der Computerstrafrechtsdogmatik im Besonderen in den nächsten Jahren eine viel höhere Aufmerksamkeit in Theorie und Praxis gewidmet werden muss, als ihr heute noch eingeräumt wird.

---

[27] *BMI*, Sicherheit 2016 – Kriminalitätsentwicklung in Österreich 31, http://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj8pdrnr-DTAhUMbBoKHcATADQQFggsMAA&url=http%3A%2F%2Fwww.bmi.gv.at%2Fcms%2FBK%2Fpublikationen%2Fkrim_statistik%2F2016%2FWeb_Sicherheit_2016.pdf&usg=AFQjCNEDiNqkAwEFnZakxqWQtnIxYaQZXQ (abgerufen am 8. 5. 2017).

[28] Siehe fünf generelle Thesen zu den aktuellen Herausforderungen im Bereich des Computerstrafrechts bei *Bergauer*, Computerstrafrecht 597 ff.