AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.6
www.austrian-law-journal.at

Cyber Crime – Der digitalisierte Täter

Susanne Reindl-Krauskopf*, Universität Wien

Kurztext: *„Smart Home: Hacker übernehmen Kontrolle über Thermostat“,[1] „Medjacking – Attacke auf Herzschrittmacher“,[2] „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid“,[3] „Ransomware: Erpressung per Lösegeld-Trojaner“,[4] „Tesla's Self-Driving System Cleared in Deadly Crash.“[5]*

Schlagzeilen wie diese beschreiben den digitalisierten Täter der heutigen Zeit. Die Liste der Beispiele an modernen Straftaten lässt sich zwanglos erweitern durch Phänomene wie Online-Pornographie, Online-Glückspiel und Geldwäsche, digitale Erpressung, Cybermobbing und überhaupt Hate speech im Internet oder durch Eingriffe in die Privatsphäre über das Internet.[6]

Wie stets, wenn der technische Fortschritt für den Einzelnen und die Gesellschaft Vorteile bringt, zeigt sich auch bei der fortschreitenden Digitalisierung die Kehrseite der Medaille, nämlich der Kriminelle, der die neu eröffneten Möglichkeiten zu verpönten Zwecken nutzt. Was der solcherart digitalisierte Täter für das gerichtliche Strafrecht bedeutet, möchte ich im Folgenden exemplarisch beleuchten.

Schlagworte: *Cyber Crime, Hacking, Smart Home, digitale Erpressung, Smart Car.*

I. Smart Home gehackt – Eigentümer frierend gefangen

Ausgangsbeispiel: X bewohnt ein sog Smart Home. Das Smart-Home-System steuert alles, was man so braucht. Die Strom- und Wasserzufuhr wird „smart“ an die analysierten Bedürfnisse des Nutzers angepasst, der Lebensmitteleinkauf durch den Kühlschrank automatisch geplant und durchgeführt usw. Ua werden auch das Heizungs- und das Sicherheitssystem intelligent gesteuert. Zu diesem Smart Home System verschafft sich der Täter Zugriff, indem er Sicherheitsvorkehrungen

* Univ.-Prof. Hon.-Prof. Dr. *Susanne Reindl-Krauskopf* ist Universitätsprofessorin am Institut für Strafrecht der Universität Wien.

1 https://www.heise.de/newsticker/meldung/Smart-Home-Hacker-uebernehmen-Kontrolle-ueber-Thermostat-3291209.html (abgefragt am 17. 3. 2017).

2 http://www.tagesanzeiger.ch/sonntagszeitung/Attacke-auf-den-Herzschrittmacher/story/28372909 (abgefragt am 22. 3. 2017).

3 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (abgefragt am 20. 3. 2017).

4 http://www.computerbetrug.de/ransomware-erpressung-per-losegeld-trojaner (abgefragt am 22. 3. 2017).

5 https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html?_r=0 (abgefragt am 17. 3. 2017).

6 http://www.ubergizmo.com/2017/02/smart-teddy-bear-leaks-recordings/ (abgefragt am 22. 3. 2017), wonach mittels internettauglicher Bestandteile von Teddybären geheim Aufnahmen von Eltern und Kindern angefertigt und verbreitet worden sein sollen.

Fundstelle: *Reindl-Krauskopf*, Cyber Crime – Der digitalisierte Täter, ALJ 2/2017, 110–118 (http://alj.uni-graz.at/index.php/alj/ article/view/85).

im System knackt. Einmal ins System vorgedrungen, manipuliert er es derart, dass die Heizung abgeschalten und der Sperrmechanismus verschlossen wird. X ist aufgrund der Manipulation durch den Täter nicht in der Lage, wieder Kontrolle über Heiz- und Sicherheitssystem zu erlangen. Er muss stundenlang im Dunkeln und in der Kälte ausharren.

Betrachtet man dieses Beispiel aus strafrechtlicher Sicht, so wird schnell deutlich, dass es um zwei Komplexe geht: zum einen um das Knacken des Systems und zum anderen um das Gefangenhalten und Frierenlassen.

A. Systemhack

Für das Eindringen in fremde Computersysteme sieht das Strafrecht als spezifisches Delikt seit 2002[7] den widerrechtlichen Zugriff auf ein Computersystem nach § 118a StGB vor.

§ 118a Abs 1 StGB idF StRÄG 2015:[8]

> *„Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,*
>
> *1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder*
> *2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,*
>
> *ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen."*

Nach der Kurzbeschreibung des Beispiels könnte der Täter durchaus entsprechend dem objektiven Tatbestand handeln: Da Computersystem jede einzelne oder verbundene Einrichtung ist, die der Datenverarbeitung dient, ist auch das vernetzte intelligente Zuhause, in dem die verschiedenen Funktionen durch miteinander verbundene Datenverarbeitungseinrichtungen gesteuert werden, ein Computersystem im Sinne der Legaldefinition des § 74 Abs 1 Z 8 StGB[9] und damit Tatobjekt des § 118a StGB. Der Täter hat im Beispiel keine rechtmäßige Verbindung zum Smart Home, er ist offenkundig weder Eigentümer noch Nutzungsberechtigter. Daher greift er auf ein Computersystem zu, über das er nicht allein verfügungsbefugt ist.[10] Dringt der Täter durch Überwinden von spezifischen Sicherheitsvorkehrungen in dieses System ein, so hat er den objektiven Tatbestand verwirklicht. Nachdem die Formulierung im Beispiel darauf abstellt, dass das System geknackt wurde, ist davon auszugehen, dass der Täter tatsächlich Sicherheitsvorkehrungen ausgeschaltet

7 BGBl I 2002/134.

8 BGBl I 2015/112.

9 Näher zur Frage, welche Einrichtungen als Computersystem in diesem Sinne in Frage kommen, siehe ua bei *Bergauer*, Das materielle Computerstrafrecht (2016) 75 ff*; Fabrizy*, StGB[12] § 74 Rz 25; *Tipold* in *Leukauf/Steininger*, StGB[4] § 74 Rz 33; *Nittel* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB[36] § 74 Rz 143 ff; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK[2] StGB (166. Lfg 2017) § 74 Abs 1 Z 8 insb Rz 58; *dies* in *Höpfel/Ratz*, WK[2] StGB (117. Lfg 2014) § 118a Rz 6–9.

10 Zur Verfügungsbefugnis siehe *Bergauer,* Computerstrafrecht 84 f*; Birklbauer/Hilf/Tipold,* Strafrecht BT I[3] § 118a Rz 3; *Fuchs/Reindl-Krauskopf*, Strafrecht BT I[5] 128; *Tipold* in *Leukauf/Steininger,* StGB[4] § 118a Rz 2; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK[2] StGB (117. Lfg 2014) § 118a Rz 10–18; *Thiele* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB[36] § 118a Rz 31 f.

hat,[11] um in das System vordringen zu können, was dem Erfordernis des Überwindens einer Sicherheitsvorkehrung jedenfalls entspricht.[12] Ungesicherte[13] Systeme werden demgegenüber von § 118a StGB nicht geschützt.[14]

Damit alleine ist es allerdings noch nicht getan. Um tatsächlich nach § 118a StGB strafbar zu sein, muss der Täter auch mit einem besonderen Vorsatz[15] handeln. Zum einen muss er es ernstlich für möglich halten und sich damit abfinden, dass er unter Überwindung von spezifischen Sicherheitsvorkehrungen in ein Computersystem eindringt, über das er nicht allein verfügungsberechtigt ist. Zum anderen braucht er aber auch eine zusätzliche Absicht. Diese kann sich seit dem StRÄG 2015 nunmehr alternativ auf drei unterschiedliche Aspekte beziehen:[16] Entweder kommt es dem Täter darauf an, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder es kommt ihm darauf an, einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, einen Nachteil zuzufügen. Schließlich kommt als dritte Alternative die Absicht in Frage, einem anderen durch die Verwendung des Computersystems selbst einen Nachteil zuzufügen. Der vom Tatbestand angesprochene Nachteil muss übrigens keineswegs finanzieller Natur sein, vielmehr kommen Nachteile jeder Art in Frage,[17] also etwa auch die Beeinträchtigung der Gesundheit, Freiheit und der Privatsphäre.

Im vorliegenden Fall geht es dem Täter offensichtlich darum, durch die Manipulation des Systems die Heizung abzudrehen sowie den Sperrmechanismus zu verschließen und den Bewohner frierend gefangen zu halten. In der Manipulation des Systems zu diesem Zweck liegt eine Verwen-

---

11 Wurden dafür spezielle Computerprogramme verwendet, die nach ihrer besonderen Beschaffenheit ersichtlich gerade zur Begehung des widerrechtlichen Zugriffs auf ein Computersystem iSd § 118a StGB hergestellt wurden, so kann bereits im Vorfeld zum eigentlichen Zugriff auf das System eine Strafbarkeit nach § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) bestehen. Diese kann ua den Hersteller, Veräußerer und Besitzer solcher Programme treffen. Näher zu § 126c StGB siehe nur ua *Bergauer,* Computerstrafrecht 317 ff; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (3 (A) Lfg 2008) § 126c.

12 Zur Streitfrage, ob das Umgehen von Sicherheitsvorkehrungen bereits ein Überwinden sein kann, siehe grundsätzlich befürwortend, sofern ein vorhandenes Sicherheitssystem aufgrund der Manipulation des Täters nicht aktiviert wird, *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 26 ff; aA *Bergauer,* Computerstrafrecht 100–104, dessen Vergleich mit dem Kurzschließen eines PKW aber insofern fehlgeht, als es beim Einbruchsdiebstahl weder um das Überwinden noch um das Umgehen einer Sicherung, sondern um das Aufbrechen einer Sperrvorrichtung geht und die Judikatur daher die Frage, ob das Kurzschließen ein Umgehen oder ein Überwinden ist, nicht zu beurteilen hatte; bleibt nur abschließend anzumerken, dass ein Aufbrechen einer Sperrvorrichtung ein Aliud sowohl zum Überwinden wie auch zum Umgehen einer Sicherung ist.

13 Zu den Anforderungen an die spezifische Sicherung siehe ua *Bergauer,* Computerstrafrecht 89*; Fabrizy,* StGB^{12} § 118a Rz 3; *Fuchs/Reindl-Krauskopf*, Strafrecht BT I^5 128; *Tipold* in *Leukauf/Steininger,* StGB^4 § 118a Rz 5; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 25; *Thiele* in *Triffterer/Rosbaud/Hinterhofer,* SbgK StGB^{36} § 118a Rz 37 ff.

14 So explizit ua auch *Seling,* Schutz der Privatsphäre durch das Strafrecht (2010) 77.

15 *Bertel/Schwaighofer/Venier*, Österreichisches Strafrecht BT I^{13} § 118a Rz 3; *Fuchs/Reindl-Krauskopf*, Strafrecht BT I^5 129.

16 Zuvor verlangte der Tatbestand die Absicht des Täters, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Diese hohe Anforderung an den subjektiven Tatbestand führte zur Straflosigkeit verschiedener Fallkonstellationen und damit zu unbefriedigenden Ergebnissen (siehe dazu nur *Bergauer,* Computerstrafrecht 104 ff*; Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 34–38; *Salimi,* Zahnloses Cyberstrafrecht? ÖJZ 2012, 998 (999 f); *Seling,* Schutz 78 ff.

17 Zum Begriff des Nachteils in diesem Zusammenhang siehe ua *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 37; *Thiele* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB^{36} § 118a Rz 68.

dung des Computersystems, denn als Verwendung ist jede Nutzung anzusehen. Dass es sich beim Frieren und bei der Unmöglichkeit, das Haus zu verlassen, um Nachteile für den Bewohner handelt, die durch die Verwendung des Systems bewirkt werden, liegt auf der Hand. Der Täter in diesem Beispiel erfüllt somit auch die Anforderungen des subjektiven Tatbestandes.[18] Schon durch das Eindringen in das Smart Home erfüllt der digitalisierte Täter somit den strafrechtlichen Tatbestand des § 118a StGB. Daneben könnte freilich abhängig von der technischen Vorgehensweise beim Eindringen uU auch eine Datenbeschädigung nach § 126a StGB gegeben sein.[19] Die Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) ist hingegen im Zusammenhang mit der Manipulation des Systems wohl eher zu verneinen, weil das System als solches nicht gestört ist.[20] Es kann bloß im Moment ausschließlich vom Täter genutzt werden. Diese Aspekte sollen hier aber nicht weiter vertieft werden.

B. Weitere Folgen

Im Ausgangsbeispiel wird der Bewohner frierend gefangen gehalten. Damit bewegt sich der digitalisierte Täter wieder im Bereich klassischer Delikte; es geht nämlich um Freiheitsentziehung nach § 99 StGB. Je nach Ausmaß und gesundheitlichen Folgen des Frierens könnte man auch noch an die Delikte zum Schutz von Leib und Leben denken. An der diesbezüglichen Verantwortlichkeit ändert auch die digitalisierte Begehungsweise nichts.

Der Täter des Ausgangsbeispiels könnte das geknackte Smart Home System natürlich auch für ganz andere Dinge nutzen. Intelligente Systeme können schließlich nur im beschriebenen Sinn funktionieren, wenn sie viele Daten über den Nutzer sammeln. Nur wenn die Systeme die Lebensgewohnheiten ihres Nutzers abbilden, wird zur richtigen Zeit die Stromzufuhr gestartet oder gedrosselt, die Tür ver- oder entsperrt etc. Der Täter kann das System folglich auch nutzen, um personenbezogene Informationen über sein Opfer zu sammeln. Abgesehen vom Eindringen in das System wäre das strafrechtlich noch nicht relevant. Nutzt der Täter diese Informationen allerdings für einen Einbruch, weil er nach dem Studium der Lebensgewohnheiten weiß, wann sein Opfer nicht zu Hause sein wird, so schließt an die Strafbarkeit wegen des Widerrechtlichen Zugriffs auf ein Computersystem eine mögliche Strafbarkeit wegen des Einbruchsdiebstahls nach §§ 127, 129 StGB ebenso wie wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG[21] an. Allerdings wäre § 51 DSG in einer solchen Konstellation aufgrund des expliziten Gesetzeswortlautes nur subsidiär anwendbar. Die ausspionierten personenbezogenen Daten lassen sich aber selbstverständlich auch anders, zB zu Erpressungen, kriminell nutzen.

Die Digitalisierung des Täters führt im Ausgangsbeispiel und diesen vergleichbaren Fällen zu keinen besonderen neuen Herausforderungen für das materielle Strafrecht. Das Phänomen des gehackten Smart Home zeigt aber deutlich, wie ganz traditionelle Ziele des Täters, nämlich etwa

18 Bis zum StRÄG 2015 wäre dieser Fall allerdings nicht von § 118a StGB erfasst worden, weil der subjektive Tatbestand wesentlich mehr Anforderungen enthielt.

19 Zur Datenbeschädigung iSd § 126a StGB allgemein: *Bergauer,* Computerstrafrecht 237 ff*; Bertel* in *Höpfel/Ratz*, WK² StGB (3 (A) Lfg 2008) § 126a; *Komenda/Madl* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB³⁶ § 126a; *Messner* in *Leukauf/Steininger*, StGB⁴ § 126a.

20 Allgemein zu diesem Delikt *Bergauer,* Computerstrafrecht 287 ff; *Daxecker* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB³⁶ § 126b; *Messner* in *Leukauf/Steininger,* StGB⁴ § 126b; *Öhlböck/Esztegar*, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126; *Reindl-Krauskopf in Höpfel/Ratz*, WK² StGB (3 (A) Lfg 2008) § 126b.

21 Zu § 51 DSG siehe näher nur *Bergauer*, Computerstrafrecht 117 ff; *Salimi* in *Höpfel/Ratz*, WK² StGB (84. Lfg 2012) § 51 DSG.

die Entziehung der Freiheit des Opfers, auch mit digitalisierten Handlungsweisen verwirklicht werden können.

II. Medjacking – Attacke auf Herzschrittmacher

Ausgangsbeispiel: Y ist auf einen Herzschrittmacher angewiesen, der mit dem System des Krankenhauses vernetzt ist, in dem Y ständig behandelt wird. Der Täter knackt das System, um Y zu töten.

Die Vorgehensweise des Täters ist im Grunde vergleichbar mit dem ersten Beispiel. Auch hier nutzt er die Vernetzung der Systeme aus, dringt in ein Computersystem ein und manipuliert dieses. Die mögliche Konsequenz wiegt aber wesentlich schwerer und reicht von der bloßen Gefährdung des Patienten bis hin zu seinem Tod.

Solche Attacken sind nicht bloß bei Herzschrittmachern vorstellbar. Bei Medizinprodukten besteht ein allgemeiner Trend hin zum Hightech-Produkt, etwa auch bei Insulinpumpen oder Hirnelektroden.[22] Auch solche medizinische Hilfsmittel arbeiten auf Basis der Vernetzung und reagieren abgestimmt auf und angepasst an den Bedarf des Patienten. Manipuliert sie der digitalisierte Täter, nachdem er sich Zugang zu den relevanten Systemen verschafft hat, kann der betreffende Patient vom Täter zB aufgrund einer im System herbeigeführten Verabreichung einer Überdosis an Insulin getötet werden.

Dass der Täter diesfalls für die verursachten Körperverletzungs- und Tötungsdelikte verantwortlich ist, steht außer Frage, weil es für die Strafbarkeit auf die technische Art und Weise der Herbeiführung einer Körperverletzung oder Tötung nicht ankommt. Die relevanten Delikte sind nämlich als Erfolgsverursachungsdelikte[23] und somit technikneutral konzipiert.

Es stellt sich aber wieder die zusätzliche Frage, ob bereits das Eindringen in das System strafrechtlich relevant sein kann, ob also strafrechtliche Verantwortung spruchreif wird, bevor überhaupt noch eine Gesundheitsgefahr entsteht. In Frage kommt wieder § 118a StGB. Der Täter verschafft sich Zugang zu einem Computersystem, über das er typischerweise nicht allein verfügungsbefugt ist. Er handelt im Ausgangsbeispiel auch in der Absicht, durch Verwendung des Computersystems dem betroffenen Patienten einen Nachteil zuzufügen; er will ihn ja töten.[24]

Ob § 118a StGB allerdings tatsächlich bereits im Vorfeld greift, wird oftmals davon abhängen, auf welche technische Art und Weise der Zugriff auf das Computersystem erlangt wird. Immer wieder wird nämlich berichtet, dass Zugriffe aufgrund von Sicherheitslücken möglich sind.[25] Nutzt der Täter allgemein bekannte Lücken aus und muss er daher für die Erlangung des widerrechtlichen Zugriffs auf das Computersystem gar keine besondere kriminelle Energie aufbringen, dann scheitert die Anwendung des § 118a StGB idR. Denn dann überwindet er bei seinem Zugriff nicht – wie

22 Ua http://www.tagesanzeiger.ch/sonntagszeitung/Attacke-auf-den-Herzschrittmacher/story/28372909 (abgefragt am 22. 3. 2017).

23 Zu diesem Begriff statt vieler *Fuchs,* Strafrecht AT I[9] Kap 10/41.

24 Denkbar sind freilich auch Fälle, in denen der Täter die Absicht hat, die jeweilige medizinische Einrichtung, die ein solches System betreibt, oder den Hersteller des betreffenden Medizinproduktes mit Geldforderungen zu konfrontieren und für den Fall der Zahlungsverweigerung mit der Schädigung des Patienten zu drohen.

25 Ua http://www.tagesanzeiger.ch/sonntagszeitung/Attacke-auf-den-Herzschrittmacher/story/28372909 (abgefragt am 22. 3. 2017).

vom Tatbestand gefordert – spezifische Sicherheitsvorkehrungen im System.[26] Er bleibt aus dem Blickwinkel des § 118a StGB straflos.

Das mag auf den ersten Blick irritieren, zumal es in dieser Konstellation um in weiterer Folge lebensbedrohliche Angriffe seitens des digitalisierten Täters geht. Doch ist das Gesetz hier durchaus konsequent. Deutlich wird dies etwa bei dem Vergleich mit dem Hausfriedensbruch.[27] Der bloß unbefugte Eintritt in eine fremde Wohnung durch eine offenstehende Türe ist als solcher kein Fall für das Strafrecht; auch nicht, wenn der Eindringling im Anschluss daran den Wohnungseigentümer ermordet. Der Mord bleibt als vorsätzliche Tötung eines Menschen selbstverständlich strafbar. Dasselbe gilt konsequenterweise auch für den digitalisierten Eindringling, der in weiterer Folge den Patienten durch Manipulation des Herzschrittmachers oder der Insulinpumpe vorsätzlich tötet: Das Eindringen in das System durch die offenstehende digitale „Tür" bleibt straflos, die nachfolgende vorsätzliche Tötung strafbar.

In Frage könnte für eine allfällige Beschädigung von Daten beim Eindringen ins System und für die weitere Manipulation im System uU aber auch in solchen Fällen wieder die Datenbeschädigung iSd § 126a StGB kommen.

Auch Fälle wie dieses zweite Beispiel werfen letztlich keine gänzlich neuen Fragen für das Strafrecht auf. Allerdings muss sich die Gesellschaft rasch der neuen kriminellen Werkzeuge und Handlungsformen bewusst werden, um sich vor Attacken schützen zu können. Dazu gehört ua auch die Bewusstseinsbildung dahingehend, bei welchen Computersystemen welche Sicherheitsrisiken und Anfälligkeiten bestehen und welche Sicherheitsstandards für bestimmte Anwendungen daher unbedingt einzuhalten sind. Das betrifft allerdings die Vorbeugung von Rechtsgutsbedrohungen und Verletzungen schon weit im Vorfeld allfälliger strafrechtlicher Fragen.

III. Digitale Erpressung

Fälle der digitalen Erpressung wurden der österreichischen Öffentlichkeit va durch den sog „Polizei-Trojaner"[28] bekannt. Dabei wurde der PC des Opfers zunächst mit einem Schadprogramm infiziert, das sich beim nächsten Starten des PC aktivierte. Am Bildschirm erschien dann die Mitteilung, dass der PC wegen angeblich auf dem PC gespeicherten strafrechtlich relevanten, zB kinderpornographischen, Materials von der Polizei gesperrt worden sei. Um die Echtheit der Mitteilung zu unterstreichen wurde das täuschend echte Logo der österreichischen Polizei verwendet. Das Opfer wurde nun darüber informiert, dass die Sperre erst nach Bezahlung eines Strafbetrages aufgehoben wird.[29]

Beurteilt man dieses Szenario aus strafrechtlicher Sicht, so ist zwischen dem Kapern des PC und der Geldforderung im Gegenzug zur Entsperrung des PC zu unterscheiden. Je nach technischer Vorgehensweise könnte auch hier für den ersten Tatkomplex, also für das Infiltrieren des PC mit der Schadsoftware, wieder an § 118a StGB zu denken sein. Voraussetzung ist freilich wieder, dass der Täter beim Einschleusen des Schadprogrammes eine spezifische Sicherheitsvorkehrung im

26 *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB (117. Lfg 2014) § 118a Rz 29; tendenziell enger *Bergauer,* Computerstrafrecht 88–104.
27 § 109 StGB.
28 Zum Ganzen insb Cybercrime-Report des ö BK 2012, 12; Cybercrime Bundeslagebild des dt BKA 2012, 7.
29 Siehe dazu auch *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015, 112 (112 f).

System überwindet. Tut er dies, so liegt eine Strafbarkeit nach § 118a StGB sehr nahe. Denn er handelt typischerweise auch in der Absicht, durch Verwendung des infiltrierten Computersystems dem berechtigten Nutzer einen Nachteil zuzufügen. Überwindet der Täter hingegen keine spezifische Sicherheitsvorkehrung, so scheidet eine Strafbarkeit nach § 118a StGB von Vornherein aus.

Beschädigt der Täter beim Installieren des Schadprogramms vermögenswerte Daten am PC des Opfers, so kann zumindest der Schutz der Datenbeschädigung nach § 126a StGB greifen. Ist aber auch das nicht der Fall, so bleibt das unbefugte Eindringen in das fremde Computersystem und das Infiltrieren mit dem Schadprogramm ohne strafrechtlichen Schutz. Erst die Tatsache, dass das Opfer sein System wegen der Sperre nicht nutzen kann, wird strafrechtlich relevant. Durch die softwaremäßige Sperre hindert der Täter das Opfer nämlich am Zugang zu den eigenen Daten. Da diese typischerweise zumindest Gebrauchswert haben werden, unterdrückt der Täter daher idR von § 126a StGB geschützte Daten in strafbarer Weise.[30]

Keine Beurteilungsschwierigkeiten bereitet hingegen nach der hM die Forderung des Täters, Geld im Gegenzug für die Aufhebung der Sperre zu bezahlen. Der Täter droht dem Opfer damit, den Gebrauch des PC weiterhin zu verhindern, also das Vermögen des Opfers weiter zu verletzen, und nötigt es so zur Zahlung einer gewissen Summe. Da die Aufhebung der Sperre im Gegenzug zur Zahlung keine anrechenbare Gegenleistung ist, weil nur etwas geschieht, worauf der am PC Berechtigte ohnedies einen begründeten Anspruch hat, geht die hM in vergleichbaren Fällen vom Vorliegen einer Erpressung nach § 144 StGB aus.[31] Folgte man hier der Mindermeinung, wäre die Schädigung des Betroffenen bereits mit der Sperre des PC eingetreten und die weitere Forderung bestenfalls noch als Nötigung strafrechtlich relevant.[32] Haben die Täter allerdings gar nicht vor, die Sperre für den Fall der Zahlung des „Lösegeldes" tatsächlich aufzuheben, wäre auch an eine Strafbarkeit wegen Betruges zu denken. Auch bei dieser Fallkonstellation bewegt sich der digitalisierte Täter somit letztlich im klassischen Strafrecht.

IV. Smart Cars und Unfälle

Abschließend noch zu einem Beispiel aus dem Fahrlässigkeitsbereich, nämlich Smart Cars und Verkehrsunfällen. Intelligente Autos sollen uns ua helfen, Sicherheitsrisiken rechtzeitig zu erkennen, uns vor Staus warnen usw. Nun ist es zwar denkbar, dass auch solche Autos bewusst dazu missbraucht werden, um zB eine Massenkarambolage herbeizuführen. Spannender erscheint mir aber die Frage, wie mit nicht vorsätzlichem Fehlverhalten umzugehen ist.

Intelligente Systeme in Autos wie zB Einparkhilfen können uns nur deshalb beim Fahren unterstützen, weil sie durch Sensoren Umweltdaten aufnehmen, Abstände messen, Geschwindigkeiten anpassen etc. Funktioniert ein solches System nicht oder fällt es aus und kommt es deshalb zu

30 Die Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) ist hingegen wohl wieder zu verneinen, weil das System als solches nicht gestört ist. Es kann bloß im Moment ausschließlich vom Täter genutzt werden.

31 Zur vergleichbaren Konstellation der „Kunsterpressung" siehe OGH 11 Os 3/07m SSt 2007/11 = EvBl 2007/86 = JBl 2008, 198 (krit *Schmoller*); *Eder-Rieder* in *Höpfel/Ratz*, WK^2 StGB (138. Lfg 2016) § 144 Rz 27; *Fabrizy*, StGB^{12} § 144 Rz 3; *Hintersteininger* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB^{36} § 144 Rz 33; *Lewisch,* Strafrecht BT I^2 (2006) 222.

32 IdS *Schmoller* in *Kienapfel/Schmoller* (Hrsg), Studienbuch Strafrecht BT II (2003) § 144 Rz 44; auch die Nötigung verneinend *Flora* in *Leukauf/Steininger*, StGB^4 § 144 Rz 9; *Venier*, „Kunsterpressung" – ein vermögensstrafrechtliches Paradoxon? JSt 2004, 73 ff (insb 74–76).

einem Unfall mit Personenschaden, stellt sich die Frage nach der Strafbarkeit.[33] Dabei denkt man unweigerlich an die Fahrlässigkeitsdelikte nach §§ 80, 81 und 88 StGB. Wie bei jedem Fahrlässigkeitsdelikt stellt sich auch in der Konstellation des Smart Car die Frage nach einer objektiven Sorgfaltswidrigkeit.[34] In der derzeitigen Situation wäre zunächst an die Pflichten des Lenkers zu denken. Dabei sieht auch die Sonderregel des § 102 Abs 3b KFG[35] für Fahrzeuge mit Assistenzsystemen bzw automatisierten oder vernetzten Fahrsystemen vor, dass der Lenker seine Fahraufgaben jederzeit wieder zu übernehmen hat, wenn dies notwendig wird. Ist also objektiv erkennbar, dass ein Systemfehler auftritt, muss der Lenker eingreifen. Tut er nichts, ist seine Untätigkeit objektiv sorgfaltswidrig. Seine Strafbarkeit kann in der Folge problemlos anhand der allgemeinen Prinzipien der Fahrlässigkeitshaftung geprüft werden.

Zusätzlich wäre zu untersuchen, worin die Ursache des Systemfehlers lag. Ist bspw dem zuständigen Systembetreuer ein Wartungsfehler unterlaufen, so wäre trotz des Zusammenhangs mit einem intelligenten System nach wie vor von einer objektiven Sorgfaltswidrigkeit eines Menschen, eben dieses Systembetreuers auszugehen. Auch für ihn käme – wie ggf auch zB für den Hersteller und Programmierer solcher Systeme – nach den klassischen strafrechtlichen Prinzipien eine Haftung wegen eines Fahrlässigkeitsdeliktes in Frage. Freilich: Je autonomer das jeweilige Fahrsystem und je komplexer das Zusammenspiel technischer Komponenten, desto schwieriger kann sich mitunter der Nachweis der Kausalität des einzelnen Fehlverhaltens für den eingetretenen Erfolg gestalten. Aus strafrechtlicher Sicht reicht allerdings auch bloße Mitverursachung aus. Auf dem Stand der derzeitigen Technik erscheint das Strafrecht auch für den digitalisierten „Fahrlässigkeits-Täter" gerüstet.

Problematisch könnte das langfristig geplante Ziel der technischen Entwicklung sein, nämlich den menschlichen Lenker, der noch eingreifen kann, irgendwann vollständig zu ersetzen.[36] Dahinter steht die Überlegung, dass Maschinen anders als Menschen keine Fehler machen und damit deren Einsatz Unfälle drastisch reduzieren und die Verkehrssicherheit enorm steigern könnte. Kommt es dennoch zu Schädigungen anderer Verkehrsteilnehmer, stellt sich freilich trotzdem die Frage nach der strafrechtlichen Verantwortlichkeit; auch unabhängig von außerstrafrechtlichen und verschuldensunabhängigen Haftungen. Der Lenker kommt in einem solchen Szenario als strafrechtlich Verantwortlicher nicht mehr in Frage, weil er faktisch nicht mehr ins Geschehen eingreifen kann. Ist erfolgsabwendendes Verhalten *de facto* nicht möglich, scheidet die Strafbarkeit – zumindest auf Basis der heutigen Dogmatik – aus.[37] Geschah der Unfall aufgrund eines Herstellungs-, Programmierungs- oder Wartungsfehlers, so könnte sich als Anknüpfung für eine strafrechtliche Haftung freilich wieder ein objektiv sorgfaltswidriges Verhalten eines Herstellers, Programmierers oder Systembetreuers ergeben.[38]

---

33 Siehe zur Frage der strafrechtlichen Verantwortlichkeit nach österreichischem Recht insb auch *Rohregger*, Autonome Fahrzeuge und strafrechtliche Verantwortlichkeit, JSt 2017, 196.

34 Zu grundsätzlichen Fragen der Fahrlässigkeitsdogmatik iZm hochautomatisiertem Fahren siehe ua *Gless*, „Mein Auto fuhr zu schnell, nicht ich!" – Strafrechtliche Verantwortung für hochautomatisiertes Fahren, in *Gless/Seelmann* (Hrsg), Intelligente Agenten und das Recht (2016) 225; allgemein zu intelligenten Systemen ua *Gless/Weigend,* Intelligente Agenten und das Strafrecht, ZStW 2014, 561.

35 Eingeführt durch BGBl I 2016/67.

36 Siehe zu den unterschiedlichen Automatisierungsgraden ua *Hötitzsch/May,* Rechtliche Problemfelder beim Einsatz automatisierter Systeme im Straßenverkehr, in *Hilgendorf* (Hrsg), Robotik im Kontext von Recht und Moral (2014) 189.

37 HM siehe nur *Hilf* in *Höpfel/Ratz*, WK^2 StGB (59. Lfg 2005) § 2 Rz 46 mwN.

38 Dazu und zur Frage der Verantwortungsverlagerung vom Lenker auf andere Personen siehe für Österreich *Rohregger*, JSt 2017, 196 (199 f).

Es wird aber auch Konstellationen geben, in denen das System aus technischer Sicht nicht fehlerhaft gearbeitet hat und dennoch Menschen zu Schaden kommen:

A ist mit seinem autonom fahrenden Smart Car unterwegs, bei dem er nur mehr Passagier ist und aus technischer Sicht gar keine Möglichkeit mehr zum Eingreifen in den aktuellen Fahrvorgang hat. Ein Kind läuft vor dem Auto (unerwartet) auf die Straße. Ein Aufprall, bei dem das Kind wahrscheinlich zu Tode käme, könnte nur durch ein Ausweichmanöver erreicht werden, bei dem der Wagen allerdings gegen eine Mauer prallen und dadurch seinen Passagier A töten würde.

Würde ein Mensch in einer solchen Konstellation nicht ausweichen, um sich selbst zu retten, so könnte er zwar nie gerechtfertigt sein, weil sich in der Güterabwägung zwei gleichwertige Rechtsgüter, nämlich das Leben des ausweichenden Menschen und das Leben des Kindes, gegenüberstehen. Aber wegen des Verlangens, das eigene Leben zu retten, könnte der Mensch uU aufgrund entschuldigenden Notstandes nach § 10 StGB straflos werden. § 10 StGB setzt dafür nämlich eine gegenwärtige oder unmittelbar drohende Gefahr für ein Rechtsgut verbunden mit einer aktuellen psychischen Drucksituation beim Täter voraus; eine Höherwertigkeit des zu rettenden Rechtsgutes wird dabei nicht gefordert.[39] In einer solchen Situation bleibt das menschliche Verhalten zwar rechtswidrig, aber aufgrund des akuten Ausnahmezustandes, in dem der Mensch sich befindet, entfällt der Schuldvorwurf.

Das Smart Car kann einer vergleichbaren Drucksituation nicht ausgesetzt sein. Denn es trifft die Entscheidung nicht selbst, sondern die Reaktion muss vorweg für eine solche Situation programmiert werden. Diese Entscheidungen müssen also in einem Zeitpunkt getroffen werden, der weit vor dem eigentlichen Geschehen liegt. Damit stellt sich aus Sicht der Strafrechtsdogmatik die Frage, ob Entschuldigungsgründe auch denjenigen zugutekommen können, die die Entscheidung darüber treffen, wie das Smart Car für solche späteren Interessenskollisionen zu programmieren ist, oder ob traditionelle schuldausschließende Instrumente im Zusammenhang mit intelligenten Systemen für solche Interessenkollisionen schlicht unanwendbar sind. Denn immerhin wird die Entscheidung lange vor der eigentlichen akuten Unfallsituation getroffen. Auf Basis des derzeitigen Stands der Technik ergeben sich solche Konstellationen zwar noch nicht. Doch sollte sich die Strafrechtsdogmatik rechtzeitig solchen Herausforderungen stellen, um auch für die Zukunft befriedigende Lösungen für den Umgang mit digitalisierten Tätern bereit zu halten.

V. Conclusio

Mag die zuletzt aufgeworfene Fragestellung uU auch neue Überlegungen zur Strafrechtsdogmatik notwendig machen, so kann man doch nach derzeitigem Stand der technischen und rechtlichen Entwicklung festhalten, dass das Strafrecht – nicht zuletzt aufgrund der Anpassungen durch das StRÄG 2015 – im Großen und Ganzen auch für den digitalisierten Täter in den geschilderten Kriminalitätsbereichen gerüstet ist.

39 Zum entschuldigenden Notstand nach § 10 StGB und dessen Prinzipien *Fuchs*, Strafrecht AT I[9] Kap 24/8 ff; *Fabrizy*, StGB[12] § 10; *Höpfel in Höpfel/Ratz*, WK[2] StGB (22. Lfg 2012) § 10; *Kienapfel/Höpfel/Kert,* Lernprogramm Strafrecht AT I[15] (2016) Z 20; *Koller/Schütz* in *Leukauf/Steininger,* StGB[4] § 10; *Moos* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB[36] § 10.