Strafrechtsvergleichende Beiträge im Spiegel der digitalen Herausforderungen

Aufsätze ungarischer und deutscher Studenten

Konstanz – Szeged – Tübingen – Göcek

Lectiones Iuridicae
31

https://mcgillpolicyassociation.com/latest-articles/2022/2/23/artificial-intelligence-in-criminal-justice-sustained-or-overruled

Der Band wurde am
Institut des Strafrechts- und Kriminalwissenschaften
der Staats- und Rechtswissenschaftlichen Fakultät
der Universität Szeged fertiggemacht.

Institutsleiterin:
Prof. Dr. h. c. *Krisztina Karsai*

Strafrechtsvergleichende Beiträge im Spiegel der digitalen Herausforderungen

Aufsätze ungarischer und deutscher Studenten
Konstanz – Szeged – Tübingen – Göcek

Herausgegeben von:
Erzsébet Molnár

Iurisperitus Verlag
Szeged, 2022

Lectiones Iuridicae

Herausgeber der Sriftenreihe:
Prof. Dr. Elemér Balogh

Sprachlektor:
Dániel Pöschl

Miniszterelnökség
Családokért Felelős Tárca Nélküli Miniszter

Nemzeti Tehetség Program

A kötet a Miniszterelnökség Családokért Felelős Tárca Nélküli Minisztere által kiírt Az Országos Tudományos Diákköri Konferencián, valamint tudományos műhelyein való részvétel és a lebonyolítási feladatok ellátása – A jogi kari hallgatók és a középiskolások megismertetése a diákkörökkel és motiválásuk a kutatásra című, NTP-HHTDK-21-0056 kódjelű pályázat támogatásával valósult meg.

Technischer Editor:
Ildikó Kovács

Verantwortlicher Herausgeberin *Márta Görög*
Dekan, Vorsitzender des Kuratoriums der Pólay Elemér Stiftung
Hergestellt in Innovariant Kft.
Verantwortlicher Leiter: *György Drágán*

ISSN 2062-5588
ISBN 978-615-6268-30-3

INHALT

VORWORT

Das vorliegende Buch enthält eine Auswahl aus Beiträgen, die im Rahmen zwei strafrechtsvergleichenden Seminars entstanden sind: sowohl die ausgezeichneten Aufsätze des Dreiländerseminars (Göcek, 2021, organisiert von Universität Istanbul, Universität Konstanz und Universität Szeged im Rahmen der DIGICRIMJUS Projektkonsortium für Erasmus+ strategische Partnerschaften; „Digitalization and Criminal Law – Specific Criminal Offences with respect to the new types of criminality arising from Digitalization") und als auch die besten Beiträge des Austauschseminars „Cybercrime" (Szeged/Tübingen, 2021, Netzwerk Ost-West) können in diesem Band gelesen werden.

Die Arbeiten wurden in zwei Seminaren erstellt, die den Jurastudenten die Möglichkeit boten, sich akademisch zu einem bestimmten strafrechtlichen Thema zu vertiefen. Die Seminare ermöglichten auch es den Studierenden, mit Kommilitonen und Professoren aus verschiedenen Ländern vergleichende Untersuchungen durchzuführen und auch ihre akademischen Debattierfähigkeiten zu entwickeln.

Beide Seminare befassten sich mit aktuellen gesellschaftlichen Herausforderungen, insbesondere mit den Veränderungen durch die digitale Revolution, auf die das Rechtssystem jeder Gesellschaft, einschließlich des Strafrechts, entsprechend reagieren muss. Die Digitalisierung verändert die Lebensweise der Menschen grundlegend, auch Art, Intensität und Morphologie der Kriminalität verändern sich, so dass Raum für neue Wege und neue Regelungsmodelle im Bereich der strafrechtlichen Verantwortung und der Strafjustiz besteht. Sogar erforderlich wird. Um diese zu finden, ist die wissenschaftliche Forschung und insbesondere der Rechtsvergleich eine unabdingbare Voraussetzung, da sie es uns auch ermöglicht, „bewährte Praktiken" (gesetzliche Regelungen), die sich in anderen Ländern bereits bewährt haben, zu analysieren und die Anpassungsmöglichkeiten zu testen und schließlich Lösungen für die eigene Rechtsordnung zu finden.

Die Methodik der Seminare verlangte, dass nicht nur auf der Ebene der Auslandsrechtskunde gearbeitet werden sollte, was eigentlich immer der einfachste Weg im Strafrechtsvergleich ist, sondern auch auf der Ebene des Strukturvergleichs. Dazu mussten die Studenten in bilateralen (deutsch-ungarischen, Netzwerk Ost-West) und trilateralen (deutsch-ungarisch-türkischen, Dreiländerseminar – Digicrimjus) Studententeams arbeiten und zum einen die Kernpunkte des zu lösenden Rechtsproblems herausfinden, zum anderen die Gemeinsamkeiten und Unterschiede herausarbeiten, die im Vergleich zu sinnvollen und aussagekräftigen Ergebnissen führen.

Ich möchte hiermit auch mein Dankeschön aussprechen. Es gilt in erster Linie den Teilnehmerinnen und Teilnehmern der Seminars, auch denjenigen, deren Arbeit in diesem Auswahl jetzt nicht erscheinen kann. Mein Dank gilt aber insbesondere auch den Assistentinnen und Assistenten, von denen hier Frau Dr. Erzsébet Molnár, Herr Dr. Andor Gál, Herr András Lichtenstein, Frau Ibolya Almási, Herr Attila György Németh (alle aus Szeged), sowie Herr Nicolai Preetz (Konstanz), besonders erwähnt seien. Für ihren verdienstvollen

Einsatz bei der Vorbereitungen danke ich sehr herzlich. Meine Professorenkollegen, Prof. Dr. Liane Wörner (Konstanz), Prof. Dr. Bernd Heinrich (Tübingen), Prof. Dr. Adem Sözüer (Istanbul) haben ein engagiertes und unterstützendes Umfeld für die erfolgreiche Durchführung dieser Projekte geschaffen, indem sie selbst die Betreuung übernommen haben und ihre eigenen Kollegen bei ihrer Arbeit der Organisation und Mentorierung ermutigt haben.

Die Seminare wurden durch multiple Förderungsrahmen ermöglicht. Dem Digicrimjus-projekt und dem Netzwek Ost-West danke ich für die Gewährung ein Teil der finanziellen Grundausstattung, sowie ohne Land Baden-Wüttenberg und die eigenen Förderungskanälen der teilnehmenden Universitäten die Seminare nicht hätten stattfinden können. Der Erwähnung bedarf schließlich auch der NTP-HHTDK-21-0056 für sein Entgegenkommen bei der Veröffentlichung des Bandes in Ungarn.

Szeged, den 5. Oktober 2022

Prof. Dr. h. c. Krisztina Karsai,

Institutsleiterin
(Institut für Strafrecht und für Kriminalwissenschaften
der Staats- und Rechtswissenschaftlichen Fakultät der Universität Szeged)

ANMERKUNGEN DES HERAUSGEBERS

Digitalisierung und Rechtsvergleichung könnten die Schlüsselwörter dieses Bandes sein. Die Digitalisierung stellt nicht nur im Bereich der technologischen Entwicklung immer neue Herausforderungen dar, sondern auch in der Rechtswissenschaft. Die neuen technologischen Lösungen ergeben neue rechtswissenschaftliche Probleme. Im Bereich der Strafrechtswissenschaft ist es nicht anders. Dieser Band beschäftigt sich mit neuen technologischen Phänomenen, die auch die strafrechtliche Verantwortung betreffen. Es stellt sich immer die Frage: Wie können traditionelle Strafrechtsinstitute auf nichttraditionelle (nicht selten futuristische) Herausforderungen angewendet werden? Muss, oder darf eigentlich die auf dem Schuldprinzip und Individualverantwortungsprinzip beruhende klassische strafrechtliche Verantwortung wegen den durch die Digitalisierung verursachten neuen Problemen erweitert werden? Die Beiträge des Bandes beschäftigen sich mit solchen und ähnlichen Fragen. Es trägt immer viel zur Beantwortung der neuen Fragen bei, die Lösungen anderer Länder zu prüfen. Der gemeinsame Punkt der Beiträge ist neben der Prüfung der möglichen strafrechtlichen Reaktionen auf digitale Herausforderungen, dass sie mithilfe rechtvergleichender Methodologie ausgearbeitet wurden. Die Rechtsvergleichung umfasst drei Länder: Deutschland, Ungarn und die Türkei.

Der Band umfasst insgesamt acht Beiträge. Fünf Arbeiten wurden von Studenten oder ehemaligen Studenten der Juristischen Fakultät der Universität Szeged verfasst, drei Beiträge wurden von Studenten der Universität Konstanz, Juristische Fakultät in Deutschland geschrieben. Die Autoren sind also deutsche und ungarische Studenten und ehemalige Studenten. *Petra Agócs, Sándor Dörgő* und *Boglárka Pincési* sind Studenten der Universität Szeged, Juristische Fakultät. Ihre Beiträge wurden von *Dr. Erzsébet Molnár* betreut.

Diána Ember ist ehemalige Studentin der Juristischen Fakultät der Universität Szeged. *Dóra Mária Tamás* ist ehemalige Studentin der von der Universität Szeged betreuten Deutschen Rechtsschule (postgradualer Weiterbildungsstudiengang Deutsches Recht mit Ausbildung zur Fachübersetzerin, Szeged-Potsdam). Ihre Beiträge wurden von András Lichtenstein und Dr. Erzsébet Molnár betreut. András Lichtenstein ist wissenschaftlicher Mitarbeiter des Instituts für Strafrecht und für Kriminalwissenschaften der Staats- und Rechtswissenschaftlichen Fakultät der Universität Szeged.

Janine Blocher und *Sascha Daul* sind studentische Hilfskräfte am Lehrstuhl für Strafrecht, Strafprozessrecht, Strafrechtsvergleichung, Medizinstrafrecht und Rechtstheorie von Prof. Dr. Liane Wörner, LL.M. (UW-Madison) an der Universität Konstanz. *Jannick Stier* ist Student der Universität Konstanz, sein Beitrag wurde auch von Prof. Dr. Liane Wörner betreut.

Hier möchte ich im Namen des Nachwuchses ein großes Dankeschön aussprechen an *Prof. Dr. Krisztina Karsai, Prof. Dr. Liane Wörner, Prof. Dr. Adem Sözüer* und *Prof. Dr. Zsolt Szomora* für das Zustandebringen und die ununterbrochene und motivierende Be-

treuung der rechtsvergleichenden Zusammenarbeit und der immer fruchtbaren Beziehung zwischen den deutschen, ungarischen und türkischen Studenten sowie des Nachwuchses.

Dankeschön an *Dániel Pöschl* für das Korrekturlesen der von den ungarischen Autoren geschriebenen deutschen Beiträge.

Szeged, den 17. Oktober 2022

Dr. Erzsébet Molnár,

wissenschaftliche Mitarbeiterin, Herausgeberin des Bandes
(Institut für Strafrecht und für Kriminalwissenschaften
der Staats- und Rechtswissenschaftlichen Fakultät der Universität Szeged)

Agócs, Petra Márta
Studentin, Universität Szeged

DIE GEFAHRENGEMEINSCHAFT ALS LÖSUNG FÜR DILEMMA-SITUATIONEN BEIM AUTONOMEN FAHREN

I. Einleitung und Problemstellung

Dank der technologischen Entwicklung helfen uns viele neue Geräte in unserem Alltag, und das gilt auch für das Autofahren. Ein selbstfahrendes Auto ist ein Auto, das nicht mithilfe menschlichen Einflusses, sondern nur mit digitalen Technologien gesteuert wird. Wir befinden uns in einer ähnlichen Situation, als die Autos die Pferdekutschen ersetzt haben.[1] Das Ziel mit den autonomen Fahrzeugen ist, den Verkehr sicherer zu machen, indem das Auto die Fehlermöglichkeiten des Fahrers quasi ausschließt. Selbstfahrende Fahrzeuge können in 6 Stufen von 0 bis 5 klassifiziert werden,[2] wo das Auto bei Stufe 0 überhaupt nicht automatisiert ist und bei Stufe 5 die Technik im Auto alle Verkehrssituationen bewältigt.[3] Das Fahrzeug hat dann kein Steuer, kein Gas- und Bremspedal und der Pkw ist komplett von den Algorithmen abhängig. Er erkennt die Details der Umgebung, navigiert selbst, vermeidet Staus und vermindert die Wahrscheinlichkeit von Unfällen, aber wie erwähnt, es gibt zahlreiche unbeantwortete Fragen im Zusammenhang mit den möglichen Unfallsituationen.

Obwohl selbstfahrende Fahrzeuge in Ungarn noch nicht weit verbreitet sind, ist ihre Präsenz in vielen Ländern (z.B.: in den USA) gewohnt.[4] 2016 ereignete sich der erste tragische Unglücksfall. In diesem Fall war das Tesla S-Modell in den „Autopilot" -Modus geschaltet, der normalerweise dazu geeignet ist, dem Fahrer auf der Autobahn zu helfen. In diesem Fall erkannten die Sensoren des Autos bei starkem Sonnenschein den großen weißen LKW und seinen Anhänger nicht, weshalb es zu dem tragischen Zwischenfall gekommen ist.[5] 2021 wurden zwei weitere Menschen aus ähnlichen Gründen getötet.[6] Wie man sieht, wirft das Erscheinen der selbstfahrenden Autos viele Fragen auf. Wer hat die Verantwortlichkeit, wenn ein Unfall passiert? Welche Alternative sollte das Fahrzeug „wählen", wenn es mehrere Möglichkeiten gibt, den Unfall zu verhindern, oder wenn es

---

[1] *Gless/Ruth*, Hochautomatisiertes und autonomes Autofahren – Risiko und rechtliche Verantwortung, Juristisches Rundschau 2016, S. 561.

[2] SAE Standards News: J3016 automated-driving graphic update, 2019. https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic

[3] *Herke,* A kriminalisztika alapkérdései és az önvezető járművek, Belügyi Szemle 1/2021, S. 90.

[4] *Herke* (Fn. 3) S. 87.

[5] https://www.tesla.com/blog/tragic-loss

[6] https://www.nytimes.com/2021/04/18/business/tesla-fatal-crash-texas.html

feststeht, dass jemand verletzt werden muss? Wie sollen Algorithmen gesteuerte Autos im Konfliktfall entscheiden, wer stirbt und wer überlebt? Gibt es Unterschiede zwischen Menschenleben? Dieser Beitrag reflektiert über die schon existierenden Lösungsmöglichkeiten, und versucht, diesen Konflikt mittels der Gefahrengemeinschaft zu lösen.

II. Autofahren und Unfälle in einem neuen Licht

Wenn man mit einem nicht autonomen Fahrzeug einen Unfall erleidet, aber damit sich selbst, andere Personen oder deren Vermögenswerte aus einer unmittelbaren und nicht anders abzuwendenden Gefahr rettet, ist man gerechtfertigt. Der Täter kann auf der Ebene der Rechtswidrigkeit gerechtfertigt werden, wenn die Straftat durch einen Verstoß gegen die Verkehrsregeln begangen wird, wenn die Person sich selbst bzw. andere Personen oder deren Vermögenswerte vor einer unmittelbaren und nicht anders abzuwendenden Gefahr bewahrt oder zum Schutz öffentlicher Interessen handelt. Das heißt, er konnte beispielsweise einen frontalen Autounfall nur vermeiden, indem sie einen Fahrradfahrer absichtlich überfahren hat.

Interessante Fragen werden aufgeworfen, wenn man über dieses Problem im Zusammenhang mit selbstfahrenden Autos nachdenkt. In diesem Kapitel stelle ich das Grundproblem und seinen ethischen-moralischen Hintergrund ausführlich dar und versuche, es nach den ungarischen Strafrechtsvorschriften zu lösen, und die oben erwähnten Fragen zu beantworten.

II. 1. Über das Dilemma im Allgemeinen

Dieses Grundproblem kann man auf ethische, moralische Fragen zurückführen. Die Begegnung von Recht und Moral ist kein neues Phänomen, sie sind eng miteinander verbunden. Schon *Jellinek* meinte im Jahr 1887, dass das Recht ein „ethisches Minimum" sei.[7] Damit meint er, dass Moral mehr verlangen kann, als das Recht, aber das Recht hat auch moralischen Inhalt.[8] Man versucht dieses Dilemma schon seit langer Zeit zu lösen: es existierte schon vor unserer Zeitrechnung, zum Beispiel sei der Karneades-Fall genannt. Er wirft ähnliche Fragen auf: Zwei Schiffbrüchige (X und Y) klammern sich an eine Planke, aber das Brett ist nicht stabil genug. Deshalb stößt X den Y von dem Brett, um sein eigenes Leben zu retten.[9] Er hat ein doppeltes Ergebnis. Einerseits bleibt X am Leben aber auf der anderen Seite kommt Y als Konsequenz zu Tode. Ein anderes ähnliches Beispiel ist der sogenannte Bergsteiger-Fall, wo zwei Bergsteiger abstürzen und an einem Seil hängen. Der obere kappt das Seil, damit sie nicht zu zweit in den Abgrund und den sicheren Tod stürzen.[10] Das Dilemma lässt sich aber am besten durch das Trolley-Problem

---

[7] *Takács,* Államelmélet a XIX–XX. században. Georg Jellinek elmélete, Pro Publico Bono Online 2/2011, S. 2.

[8] *Pődör,* Az önvezető járművek, a trolley probléma és az emberi élet védelme – Széljegyzetek egy jogi-erkölcsi dilemma margójára, Alkotmánybírósági Szemle 1/2020, S. 12.

[9] *Nagy,* Esetek és nézetek a büntetőjogi végszükség köréből, Acta Juridica et Politica, 2004, S. 662-663

[10] *Nagy* (Fn. 9) S. 668.

(Weichenstellerfall) veranschaulichen. Es war für lange Zeit ein moralisch-philosophisches Problem, aber mit dem Erscheinen selbstfahrender Autos wurde es schnell bedeutsam, und dieses Gedankenspiel wird oft als Beispiel für die ethischen Zweifel in Zusammenhang mit autonomen Fahrzeugen erwähnt.[11]

Aber was ist das eigentliche Dilemma? Es besteht die Frage, wie der Weichensteller entscheiden sollte, wenn er überhaupt darf, wenn ein Zug auf fünf Gleisarbeiter zufährt, und es die einzige Abwehrmöglichkeit ist – damit die fünf Arbeiter gerettet werden – den Zug auf ein Nebengleis umzuleiten. Auf diesem Gleis arbeitet man auch, nur eine Person, die getötet wird, damit die anderen am Leben bleiben.[12] Aber während im Karneades-Fall die Anzahl der Menschenleben gleich ist (X und Y) sind bei dem Weichenstellerfall 5 Menschen bzw. 1 Mensch betroffen. In einer Waagschale liegt das Interesse, irgendwie das Leben von 5 Menschen zu retten, und in der anderen der Tod eines anderen Menschen. Man kann die Frage stellen, in welche Richtung sich die Waage neigen sollte. Was wichtig ist, dass man Menschenleben nicht gegeneinander abwägen kann. Sie sind gleichwertig – das wird von vielen nationalen und internationalen Rechtsinstrumenten garantiert.[13] Die Menschenwürde und das Recht aufs Leben – die allen Menschen gebühren – sind unantastbar,[14] und deshalb gibt es keine Person, die des Lebens würdiger ist als eine andere.

II. 2. Das Dilemma im Zusammenhang mit selbstfahrenden Autos

Wie man sieht, es ist ein ernstes Problem der Rechtsphilosophie, ob Leben gerettet werden kann, indem man ein anderes Leben opfert. In Zusammenhang mit autonomen Fahrzeugen sieht man dieses Problem in einem anderen Licht. Wenn man in einem vollständig autonomen Auto fährt, verfügt das Fahrzeug über kein Steuer, Bremspedal oder Gaspedal, der Benutzer kann die Fahrrichtung nicht beeinflussen, die Passagiere verlassen sich somit komplett auf das autonome Auto.

Deshalb kann man nicht von der Verantwortung der Passagiere sprechen, wenn die Fahrgäste sich mit dem Auto in einer Unfallsituation befinden, obwohl sie bei dem Unfall anwesend waren, denn der Erfolg ist nicht wegen ihrer Handlung eingetreten, sondern weil das Fahrzeug sich aufgrund des im Vorhinein eingegebenen Algorithmus bewegt hat. Die Entscheidung über „Leben und Tod" wird bei der Herstellung des Autos *„hinter dem Schleier des Nichtwissens"* getroffen.[15] Deshalb muss man mit dem Erscheinen der selbstfahrenden Technologie auch die Ethik berücksichtigen, bei der die Einbeziehung

---

[11] *Eisenberger,* Das Trolley-Problem im Spannungsfeld autonomer Fahrzeuge: Lösungsstrategien grundrechtlich betrachtet, in: Eisenberger/Lachmayer/Eisenberger (Hrsg.), Autonomes Fahren und Recht 2017, S. 96.

[12] *Thomson,* The Trolley Problem, The Yale Law Journal, vol. 94, no. 6, 1985, S. 1395.

[13] Grundgesetz Ungarns. Artikel XV. *„Ungarn gewährt jedem Menschen die Grundrechte ohne jegliche Diskriminierung, nämlich ohne Ansehen von Rasse, Hautfarbe, Geschlecht, Behinderung, Sprache, Religion, politischer oder anderer Meinung, nationaler oder sozialer Herkunft, Vermögenslage, Geburt oder sonstigen Situationen.";* „Alle Menschen sind frei und gleich an Würde und Rechten geboren." Artikel 1., Die Allgemeine Erklärung der Menschenrechte, 1948.

[14] 23/1990. (X. 31.) AB határozat a halálbüntetés alkotmányellenességéről

[15] *Weigend,* Notstandsrecht für selbstfahrende Autos? Zeitschrift für Internationale Strafrechtsdogmatik 10/2017, S. 602.

der modernen Philosophie, Psychologie und Rechtssoziologie nötig ist.[16] Allerdings kann man sagen, dass Programmierer nicht entscheiden können, in welche Richtung das Auto in Situationen wie das Trolley-Problem gelenkt werden soll, dies sollte gesetzlich geregelt werden. Wenn ein Mensch das Auto fährt, sieht man die Personen vor sich, man kann die Umstände in der konkreten Situation abwägen, und aufgrund dieser Kenntnisse die Entscheidung treffen. Im Gegensatz entscheidet das programmierte System hinter dem selbstfahrenden Auto nach abstrakten Merkmalen.[17]

Man kann die Frage stellen, welche möglichen Merkmale die Entscheidung beeinflussen könnten. Es gibt personen-, ergebnis- und prozessorientierte Theorien.[18] Bei der ersten würde das Fahrzeug den Mensch überfahren, der über bestimmten Eigenschaften verfügt.[19] Aber wie erwähnt, man kann es nicht entscheiden, welches Leben mehr Wert hat, es würde gegen vielen nationalen und internationalen Normen gegen Diskriminierung verstoßen werden, wenn man diese Lösung wählen sollte.[20] Die nächste Theorie ist die Ergebnisorientierung. Das bedeutet, dass das Fahrzeug in dem Fall, dass es unausweichlich ist, das es entweder mit einer kleineren oder mit einer größeren Gruppe von Menschen kollidiert, dergestalt gelenkt werden sollte, dass es die wenigste Verletzungen verursacht.[21] Unter Prozessorientierung versteht man, wenn der Zufall in diesem Fall entscheidet, wer getötet oder verletzt werden soll.[22]

III. Mögliche Antworten auf das Dilemma aufgrund der Dogmatik des ungarischen Strafrechts

In diesem Kapitel stelle ich die Möglichkeiten zur Lösung des Rechtsproblems des ungarischen Strafrechts mithilfe fiktiver Rechtsfälle dar, die die folgenden sind:

A) *A* ist allein in dem autonomen Auto unterwegs, und *B* erscheint auf dem Weg. Mit der einzigen Abwehrmöglichkeit würde A getötet werden, weil das Fahrzeug gegen einen Betonpfeiler prallen würde weshalb *A* stirbt.

B) Demgegenüber steht im zweiten Fall eine Gruppe vor dem Auto, die einzige Möglichkeit, die Kollision zu vermeiden, ist *C*, der allein auf dem Bürgersteig steht, zu überfahren.

Um über eine Straftat zu sprechen, sie muss sie vier Kriterien entsprechen: es handelt sich um eine Handlung, die tatbestandsmäßig, rechtswidrig und schuldhaft ist. Es ist schon ein ernstes dogmatisches Problem, zu bestimmen, was die Handlungen in diesen

---

[16] *Ambrus,* Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai, in: Mezei (Hrsg), A bűnügyi tudományok és az informatika, Magyar Tudományos Akadémia Jogtudományi Intézet, Budapest-Pécs, 2019, S. 15.

[17] *Weigend* (Fn. 16) S. 600-603.

[18] *Eisenberger* (Fn. 11) S. 99-100.

[19] z.B. Frauen – Männer, kranken – gesunden, Kinder – Erwachsene

[20] *Ungern-Sternberg,* Tod durch Algorithmus? Die Regulierung von Dilemma-Situationen beim autonomen Fahren, BRJ 2/2019, S. 99-100.

[21] *Weigend* (Fn. 16) S. 605.

[22] *Eisenberger* (Fn. 11) S. 100.

Situationen sind, wofür verschiedene mögliche Lösungen gefunden wurden.[23] Nach der Strafrechtsdogmatik ist eine Handlung ein menschliches Verhalten, das willkürlich ist und eine Wirkung entfaltet.[24] Wenn wir die Handlung auf die Programmierung der Algorithmen zurückführen, ist das erste Kriterium verwirklicht, beim Schreiben des Programms, aufgrund dessen das Auto auf den Straßen verkehrt.[25] Dann kann die Verantwortlichkeit des Betreibers der künstlichen Intelligenz festgestellt werden, der sie als Mittel zur Verwirklichung der Straftat einsetzt.

Laut *Ambrus* könnte die Verantwortung dann aufgrund seines zurechenbaren Verhaltens *(actio libera in causa)* auf den Programmierer zurückgeführt werden.[26] Interessante Fragen können auftauchen, wenn der Fahrer noch die Möglichkeit hat, zu beeinflussen, wie das Auto gelenkt wird.[27] Dann taucht zwischen der oben genannten Handlung (des Programmierers) und dem Ergebnis (Tod oder Verletzung) ein weiteres menschliches Verhalten auf, das sogar die Verantwortung des Fahrers begründen kann, aber die vorliegende Studie geht nicht näher auf diese Frage der Verantwortung ein.

Das zweite Element, das verwirklicht werden muss, ist die Tatbestandsmäßigkeit. Die Handlung fügt sich auf den ersten Blick in mehreren Tatbestände ein. Nach dem ungarischen Strafgesetzbuch (im Folgenden: uStGB) ist § 160, der vorsätzliche Mord, tatbestandsmäßig.[28] Das Bewusstsein des Täters (Programmierer) umfasst die relevanten Elemente der Handlung (Schreiben des Programms des Autos, was sich in einer bestimmten Situation verwirklicht) und, dass Kausalität zwischen dem Verhalten und dem eventuell eintretenden Todeserfolg besteht.[29]

Man könnte noch an die Verkehrsstraftaten denken, innerhalb dieser an die Gefährdung des Straßenverkehrs mit Todesfolge und an die Verursachung eines Verkehrsunfalls ebenfalls mit Todesfolge.[30] Die Verwirklichung beider Straftaten kann ausgeschlossen werden, da die Folge (Tod) nur auf Fahrlässigkeit des Täters zurückzuführen ist,[31] bei Vorsatz handelt es sich um keine Verkehrsstraftat, sondern um vorsätzlichen Mord. In diesem Fall ist das Schreiben des Programms vorsätzlich, da der Programmierer den Algorithmus speziell für eine Krisensituation schreibt, sodass sein Bewusstsein die Tatsache umfasst, dass das Auto den Tod von jemandem verursacht, wenn es „in eine Entscheidungssituation" gerät. [32]

Danach muss man die Prüfung auf der Ebene der Rechtswidrigkeit fortsetzen, ob es einen Rechtsfertigungsgrund gibt, der es ausschließt, über eine Straftat zu sprechen. Im Allgemeinen Teil regelt das ungarische Strafgesetzbuch drei Rechtfertigungsgründe, die

---

[23] *Ambrus,* Digitalizáció és büntetőjog, Budapest, 2021, S. 172.

[24] *Nagy*, Anyagi Büntetőjog Általános Rész, Iurisperitus Bt, Szeged, 2014, S. 148.

[25] *Weigend* (Fn. 16) S. 603.

[26] *Ambrus* (Fn. 24) S. 173-174.

[27] z.B. auf der dritten Stufe, wo der Fahrer die Aufgabe auf Anforderung des Systems innerhalb kurzer Zeit übernehmen muss. https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/grundlagen/autonomes-fahren-5-stufen/

[28] *„Wer eine andere Person tötet, ist wegen eines Verbrechens mit Freiheitsstrafe von fünf Jahren bis zu fünfzehn Jahren zu bestrafen."* § 160 uStGB

[29] *Karsai/Szomora/Vida,* Anyagi Büntetőjog, Különös Rész I, Szeged, 2013, S. 22.

[30] § 234 Abs 2 Punkt c) und § 235 Abs 2 Punkt b) uStGB

[31] *Tóth/Nagy* (Hrsg): Magyar büntetőjog. Különös rész, Osiris, Budapest, 2014, S. 212.

[32] *Karsai/Szomora/Vida* (Fn. 30) S. 231.

die folgende sind: Notwehr, Notstand und Erlaubnis der Rechtsnorm. Es gibt noch Gründe, die auf dem Gewohnheitsrecht beruhen.[33] Die Rechtfertigungsgründe, die in diesen Fällen relevant werden sind die folgenden: Erlaubtes Risiko und Pflichtenkollision.

III. 1. Prüfung in dem System der Rechtsfertigungsgründe

Zunächst einmal kann man die Notwehr[34] untersuchen, aber sie wird in dieser Situation nicht anwendbar sein. Der Angriff ist nicht unberechtigt, was eine nötige Voraussetzung der Notwehr ist,[35] zwei berechtigte Interessen kollidieren, deshalb ist es ausgeschlossen, diesen Rechtfertigungsgrund zu nutzen.

Im Folgenden werde ich die Untersuchung mit dem Notstand fortsetzen. Die zwei Personen, *A* und *B, C* und die Gruppe von Menschen sind in einer Gefahrgemeinschaft: sie sind zusammen in Gefahr und nur durch ein Menschenopfer kann der Tod der anderen verhindert werden.[36] Das berechtigte Interesse ist gefährdet, indem es nur auf Kosten des anderen gerettet werden kann.[37] Die Gefahrgemeinschaft ist ein Ausdruck der Solidarität gleichgefährdeter Rechtgutsträger,[38] und es bedeutet nicht nur dass die Güter der Beteiligten von derselben Gefahr bedroht sind, sondern auch, dass sich beide an der Schaffung der Gefahr beteiligen.[39]

III. 1. 1. Regelung des Notstands in dem ungarischen Strafrecht

Nicht zu bestrafen ist die Tat der Person, die sich selbst bzw. andere Personen oder deren Vermögenswerte aus einer unmittelbaren und nicht anders abzuwendenden Gefahr befreit oder zum Schutz öffentlicher Interessen so vorgeht, vorausgesetzt, dass die Tat keinen größeren Nachteil verursacht, als sie abzuwenden versuchte. (§ 23 Abs. 1 uStGB)

Im Gegensatz zur Notwehr setzt der Notstand eine berechtigte Interessenkollision voraus,[40,41] somit ist die Gefährdung der Gesellschaft ausgeschlossen, wenn eine Person Interessen durch die Schädigung anderer rettet.[42] Die Notstandsituation entsteht, wenn die schon genannten Interessen gefährdet sind.[43] Objektives Kriterium der Gefahr ist die Unmittelbarkeit, was bedeutet, dass sie selbst Verletzungen verursachen kann darüber hinaus

---

[33] *Nagy,* Anyagi Büntetőjog Általános Rész, Szeged, 2014, S. 208.

[34] „Nicht zu bestrafen ist die Tat, die zur Abwehr eines gegen die Person selbst bzw. andere Personen oder deren Vermögenswerte oder öffentliche Interessen gerichteten bzw. diese unmittelbar bedrohenden unberechtigten Angriffs notwendig ist." § 22 Abs. 1 uStGB

[35] *Kis/Hollán,* Büntetőjog I. Az anyagi büntetőjog általános része, Dialóg Campus Budapest-Pécs, 2013, S. 111.

[36] *Nagy* (Fn. 9) S. 667.

[37] *Mészáros,* A végszükség szabályozásának alakulása, tekintettel az új Btk.-ra, Jogelméleti szemle 4/2012, S. 94.

[38] *Deutsch,* Die Selbstopferung im Straßenverkehr, Archiv für die civilistische Praxis, 1965, S. 210.

[39] *Deutsch* (Fn. 39) 1965, S. 200.

[40] *Nagy* (Fn. 34) S. 225.

[41] *Tokaji*, A bűncselekménytan alapjai a magyar büntetőjogban, Budapest, 1984, S. 266.

[42] *Balogh/Tóth* (Hrsg), Magyar Büntetőjog. Általános rész, Budapest, 2010, S. 133.

[43] *Nagy,* Tanulmányok a Btk. Általános Részének kodifikációjához, Budapest, 2005, S. 117.

zeitlich und räumlich begrenzt ist. [44,45] Eine weitere Bedingung der Gefahr besteht darin, dass sie nicht anders, als mit einer Handlung die unter einen Tatbestand des Besonderen Teils des Strafgesetzbuchs subsumiert werden kann, abwendbar ist.[46] Wenn die Gefahr strafrechtlich neutral abgewendet werden kann, muss man diesen Weg wählen.[47] Das wichtigste ist die Verhältnismäßigkeit, was auch objektiv ist und durch sachliche Elemente geprüft werden sollte. [48] Bei der Kollision verschiedener Rechtsgüter kann die Verhältnismäßigkeit eindeutig festgestellt werden. Wenn man materielle Güter vor der Gefahr rettet, und damit das Leben eines anderen opfert, wird die Handlung immer unverhältnismäßig sein.[49]

Auf den ersten Blick erfüllen die vorliegenden Rechtsfälle die Kriterien des Notstands: Die Gefahr ist unmittelbar und nicht anders abwendbar, aber das Umlenken des Fahrzeuges wäre nicht gerechtfertigt nach dem § 23 uStGB. Die Tat entspricht nicht dem Kriterium *„keinen größeren Nachteil verursacht, als sie abzuwenden versuchte"*.

III. 1. 2. Übergesetzlicher Notstand

Wie erwähnt spricht man über einen übergesetzlichen Rechtfertigungsgrund, wenn ein Rechtfertigungsgrund nicht im Strafgesetzbuch oder in einem anderem Gesetz festgelegt ist.[50] Es sollte erwähnt werden, dass die Handlung nur dann rechtswidrig ist, wenn sie sowohl formell und als auch materiell rechtswidrig ist. Das bedeutet, es muss ein Verstoß gegen die Normen vorliegen und sie muss mit Sanktionen bedroht[51] und für die Gesellschaft gefährlich sein.[52,53]

An der materiellen Rechtswidrigkeit kann es in manchen Fällen außerhalb des Rechtsbegriffs des Notstands mangeln, und deshalb wird keine Straftat begangen, wenn *„der übergesetzliche Notstand"* die Rechtswidrigkeit ausschließt.[54] Die fehlende Gefahr für die Gesellschaft sei laut *Belovics* kein Ausschlussgrund für die Rechtswidrigkeit, und eine Straftat kann nur auf einer Bestimmung des Strafgesetzbuches beruhen.[55] Nach *Viski* kann die nicht rechtswidrige Handlung ausnahmsweise dennoch gefährlich für die Gesellschaft bleiben, in diesem Fall wird die Handlung aus anderen kriminalpolitischen Erwägungen nicht rechtswidrig sein.[56]

---

[44] *Belovics* (et al.), Büntetőjog I. A 2012. évi C. törvény alapján, Budapest, 2012, S. 256.

[45] *Mészáros*, Az ártatlant sújtó szükségcselekmények a büntetőjogban, Budapest, 2017, S. 67.

[46] *Mészáros,* Adalékok a végszükség fogalmához, Iustim aequum salutare, 4/2014, S. 116.

[47] *Bodnár,* A végszükség a büntetőjogban, Acta juridica et politica, 1981, S. 33.

[48] *Belovics* (Fn. 45) S. 257.

[49] *Viski/Imre/Ternai,* Közúti közlekedési balesetek elbírálása, Budapest, 1963, S. 166-167.

[50] *Bodnár* (Fn. 48.) S. 13-14.

[51] *Bodnár* (Fn. 48.) S. 13.

[52] *„Eine für die Gesellschaft gefährliche Tat ist die Tätigkeit oder das Versäumnis, welche(s) andere Personen oder deren Rechte bzw. die dem Grundgesetz entsprechende soziale, ökonomische bzw. staatliche Ordnung Ungarns verletzt oder gefährdet."* § 4 Abs. 2 uStGB.

[53] *Nagy* (Fn. 34) S. 194-197.

[54] *Bodnár,* A végszükség a büntetőjogban, Acta juridica et politica, 1981, S. 13-14.

[55] *Belovics,* A jogellenesség és a társadalomra veszélyesség konfliktusa, Iustum Aequum Salutare 3/2007, S. 38-42.

[56] *Bodnár* (Fn. 48) S. 28.

Im Falle einer Pflichtenkollision muss man zwei oder mehrere rechtliche Pflichten erfüllen, die Erfüllung einer der Pflichten bedeutet aber gleichzeitig eine Verletzung der anderen Pflicht,[57] und deshalb wird eine tatbestandsmäßige Handlung verwirklicht.[58]

Die Kollision kann in diesem Fall aus mehreren Perspektiven betrachtet werden. In dem ersten Fall hat der Programmierer eine Unterlassungspflicht gegenüber A: Er muss das Auto so programmieren, damit *A* nicht getötet wird. Aber auch gegenüber *B* hat er eine Handlungspflicht: das Fahrzeug sollte *B* ausweichen. Im Allgemeinen kann man sagen, dass man in solchen Situationen die höherrangige Pflicht erfüllen muss, aber in diesen Fällen sind die Pflichten gleichrangig: wenn die Rechtsgüter identisch sind, kommt die Unterlassungspflicht vor der Handlungspflicht.[59] Deshalb müsste der Programmierer im ersten Rechtsfall meiner Meinung nach seine Unterlassungspflicht erfüllen: das Auto so zu programmieren, dass er die Person in dem Auto nicht tötet.

In dem zweiten Fall ist die Kollision ebenfalls heterogen. Nach *Weigend* sollte in einer solcher Situation die Zahl entscheiden: das Auto sollte so umgelenkt werden, dass es mit der geringeren Zahl von Personen kollidiert, und das gilt auch wenn die Passagiere des Fahrzeuges betroffen sind.[60] Aber von der menschlichen Natur kann nicht erwartet werden, dass sie ihr eigenes Leben opfert.[61] Deshalb könnte man die Frage stellen, ob es richtig ist, dass die Programmierer statt des menschlichen Überlebenswillens rationale Ansätze berücksichtigen.[62]

III. 1. 3. Erlaubtes Risiko

Zahlreiche Unfälle passieren in Ungarn von Monat zu Monat. 2020 ereigneten sich 13 778 Verkehrsunfälle mit Personenschaden,[63] von denen 12 932 Fälle auf einen Fahrfehler zurückzuführen sind, und nur in 55 Fällen hat ein technischer Defekt die Unfälle verursacht,[64] so ist die Unfallursache in annäherungsweise 0,4% der Fälle auf ein technisches Problem zurückzuführen. Es kann festgestellt werden, dass die Zahl der Verkehrsunfälle durch selbstfahrende Autos voraussichtlich deutlich sinken würde. Durch die Automatisierung können viele typische Fahrerfehler, wie zum Beispiel Schläfrigkeit, Unwohlsein und Entscheidungsfehler, ausgesiebt werden und damit würde sich die Zahl der Verkehrsunfälle reduzieren.[65] Neben technologischen Fortschritten wird aber auch eine Reduzierung von Verkehrsunfällen und Verkehrstoten durch selbstfahrende Fahrzeuge erwartet. Dies wiederum wirft das folgende Dilemma für die strafrechtliche Beurteilung auf. Kann der Begriff des erlaubten Risikos als Grund für den Ausschluss der Rechtswidrigkeit angewendet werden, wenn durch autonome Fahrzeuge die Zahl der Unfälle und Verkehrsdelikte er-

---

[57] *Tokaji* (Fn. 42) S. 267.

[58] *Nagy* (Fn. 34) S. 240.

[59] *Nagy* (Fn. 34) S. 240-241.

[60] *Weigend* (Fn. 16) S. 605.

[61] *Nagy* (Fn. 34) S. 228.

[62] *Weigend* (Fn. 16) S. 603.

[63] https://www.ksh.hu/stadat_files/sza/hu/sza0073.html

[64] https://www.ksh.hu/stadat_files/sza/hu/sza0034.html

[65] *Hodula,* Az önvezető járművek és a büntetőjogi felelősség, Jogelméleti Szemle 3/2018, S. 70.

heblich reduziert wird?[66] Das Menschenleben kann jedoch nach *Ambrus* nicht aufgrund der gewohnheitsrechtlichen Rechtfertigungsgründe genommen werden.[67] Es kann sich jedoch die Frage stellen, inwieweit der Ausschluss der Schuld solcher Gefahrgemeinschaft-Situationen die Gesellschaft erschrecken und das Rechtssicherheitsgefühl erschüttert würde.[68] Deshalb würde eine gesetzliche Regelung anstatt eines gewohnheitsrechtlichen Rechtfertigungsgrundes eine beruhigende Lösung bieten.[69]

III. 2. Entschuldigender Notstand in dem ungarischen Strafrecht

Wie bereits dargelegt, ist der Notstand gemäß § 23 Abs 1 uStGB ein Rechtfertigungsgrund, aber dieses Problem muss man auf der Ebene der Entschuldigungsgründe untersuchen. Die Anwendung des zweiten Absatzes könnte ebenfalls einschlägig sein: Nach dem zweiten Absatz wird man nicht bestraft, wenn man wegen Schreck oder aus entschuldbarer Erregung den Umfang des Nachteils nicht erkennt, und deshalb größeren Nachteil verursacht, als abwenden versucht wurde.[70] Aber in diesem Fall ist das nicht relevant, weil die künstliche Intelligenz hinter dem selbstfahrenden Auto sich weder erschrecken, noch in erregten Zustand geraten kann,[71] darüber hinaus ist dies eine „vorgeplante" Handlung seitens des Programmierers, daher kann auch nicht von solchen Kriterien gesprochen werden.[72]

Die ungarische Regelung sieht den Notstand einheitlich als Rechtfertigungsgrund an, aber dogmatisch ist dies nicht konsequent. Wie erwähnt, ist der rechtfertigende Notstand nicht anwendbar, wenn der verursachte Nachteil größer oder gleich ist, als der, den man abwenden wollte, und die Tat deshalb nicht verhältnismäßig ist. Aber wenn man einen gleich großen oder größeren Nachteil verursacht, kann dies ein Grund für den Schuldausschluss sein, genauer gesagt es schließt die Schuld auf der Ebene der Zumutbarkeit aus.[73] Das hängt damit zusammen, dass es von niemandem erwartet werden kann, sein eigenes Leben in einer Gefahr zu opfern.

Es ist auch wichtig zu erwähnen, dass das Verfassungsgericht Ungarns 1990 in Zusammenhang mit der Todesstrafe festgestellt hat, dass das Nehmen eines Lebens nur auf rechtlicher Ebene (Todesstrafe) nicht erfolgen kann, aber die gleichen Werte – also die Existenz eines anderen und die Menschenwürde – können miteinander konkurrieren.[74] *Mészáros* meint, es könne für die Gesellschaft vorteilhafter sein, eine Person auf Kosten des anderen zu retten, als beide zu verlieren. Die Menschenleben sind gleichwertig, die

---

[66] *Ambrus* (Fn. 24) S. 171-172.

[67] *Ambrus,* Az autonóm járművek és a büntetőjogi felelősségre vonás akadályai, in: Mezei (Hrsg.), A bűnügyi tudományok és az informatika. Budapest-Pécs, 2019, S. 18-19.

[68] *Roxin,* Der verantwortungsausschließende Notstand und ähnliche Fälle (§ 22), Roxin/Greco, Strafrecht Allgemeiner Teil Band. 1: Grundlagen. Der Aufbau der Verbrechenslehre, 1997, S. 893.

[69] *Ambrus* (Fn. 68) S. 20.

[70] § 23 Abs. 2 uStGB

[71] *Ambrus,* A mesterséges intelligencia és a büntetőjog, Állam- és jogtudomány, 2020, S. 20.

[72] *Pődör* (Fn. 8) S. 21.

[73] *Nagy* (Fn. 34) S. 225-226.

[74] 23/1990. (X. 31.) AB határozat

Verhältnismäßigkeit kann nur „numerisch" entschieden werden, wenn die Zahl nicht gleich ist.[75] Und wenn das Leben von nicht gleichvielen Menschen wie im zweiten Fall gefährdet ist, wird die Frage der Verhältnismäßigkeit – denn das Leben aller Menschen ist gleich – nur anhand von Zahlen entschieden. Wenn wir diesen Gedankengang weiterführen und auf den vorliegenden Fall anwenden, können wir sagen, dass im ersten Rechtsfall nicht erwartet werden kann, das Leben des Passagiers zu opfern. Das macht das ansonsten tatsächliches, rechtswidriges Verhalten nach den Umständen nicht strafbar. Folglich müsste das Fahrzeug im zweiten Fall so umgelenkt werden, dass es den Weg der Kollision mit der geringeren Zahl wählt.

IV. Die deutsche und türkische mögliche Regelung

Die vorliegende Studie wurde im Rahmen einer deutsch-türkisch-ungarischen Rechtsvergleichskonferenz durchgeführt, wo die Gruppen das ungarische, türkische und deutsche Recht in bestimmten Themen verglichen haben.

Die Gruppe hat die Handlung des Programmierers untersucht. In allen drei Ländern würde der Totschlag tatbestandmäßig sein, die Voraussetzungen der Verkehrsdelikte verwirklichen sich nicht.[76,77] Was die Rechtswidrigkeit betrifft, ist in der Türkei im Vergleich zur ungarischen Regelung nur die Notwehr und die Pflichtenkollision zu prüfen, weil der Notstand ein Schuldausschließungsgrund ist. Demgegenüber ist in Deutschland neben der Notwehr, der Pflichtenkollision und dem rechtfertigenden Notstand auch die nur in Deutschland geregelte Gefahrgemeinschaft relevant, das türkische und ungarische Strafrecht kennen dieses Rechtsinstitut nicht. Der Ausgangspunkt dieser Konstellation ist, dass sich alle Personen im Gefahrenbereich befinden. Es besteht die Frage, ob der Programmierer bezüglich des Zufahrens auf eine gefährdete Personengruppe ein gefahrminimierendes Ausweichmanöver vorsehen darf. Die Frage, die sich stellt, ist, welche Personen dem Gefahrenbereich zuzuordnen sind. Jeder Mensch, der am Straßenverkehr teilnimmt, oder nur die Person, deren Weg das Fahrzeug kreuzt?

Die Notwehr ist in diesen Fällen in der Türkei und in Deutschland ähnlich der ungarischen Regelung ebenfalls nicht anwendbar, weil es keinen unberechtigten Angriff gibt. Der türkische und deutsche entschuldigende[78] (und der deutsche rechtfertigende[79]) Notstand

[75] *Mészáros* (Fn. 47) S. 122.

[76] § 81 des türkischen, § 160 des ungarischen, und § 212 des deutschen Strafgesetzbuches

[77] *Lenk*, Der programmierte Tod? SVR 2019, S. 169.

[78] § 35 dStGB (1) „Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib oder Freiheit eine rechtswidrige Tat begeht, um die Gefahr von sich, einem Angehörigen oder einer anderen ihm nahestehenden Person abzuwenden, handelt ohne Schuld. Dies gilt nicht, soweit dem Täter nach den Umständen, namentlich weil er die Gefahr selbst verursacht hat oder weil er in einem besonderen Rechtsverhältnis stand, zugemutet werden konnte, die Gefahr hinzunehmen; jedoch kann die Strafe nach § 49 Abs. 1 gemildert werden, wenn der Täter nicht mit Rücksicht auf ein besonderes Rechtsverhältnis die Gefahr hinzunehmen hatte."

[79] § 34 dStGB „Wer in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben, Leib, Freiheit, Ehre, Eigentum oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, handelt nicht rechtswidrig, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt. Dies gilt jedoch nur, soweit die Tat ein angemessenes Mittel ist, die Gefahr abzuwenden."

ist wegen des Mangels der Verhältnismäßigkeit ebenfalls nicht anwendbar, weil man die Menschenleben wegen der Grundrechtsdogmatik nicht gegeneinander abwägen darf.[80,81] Die Pflichtenkollision ist in allen drei Ländern nicht gesetzlich normiert und ein gewohnheitsrechtlich anerkannter Rechtfertigungsgrund. Was das erlaubte Risiko anbelangt, ist es wie dargelegt ein gewohnheitsrechtlicher Rechtfertigungsgrund in Ungarn, aber in den anderen zwei Ländern gehört es zur objektiven Zurechnung und ist ebenfalls nicht gesetzlich normiert.

Es wurde festgestellt, dass dieses Thema in allen drei Ländern ein ernsthaftes ethisches Dilemma aufwirft, und es besteht kein Zweifel, dass diese Situation in der Zukunft gesetzlicher Regelungen bedarf.

V. Zusammenfassung und offene Fragen

Alles in allem kann man sagen, dass das Aufkommen selbstfahrender Autos in unserem Land wahrscheinlich nur die Musik der fernen Zukunft ist, was aber aus strafrechtlicher Sicht viele relevante Fragen aufwirft. Das Trolley-Problem veranschaulicht das theoretische Dilemma, das in Bezug auf vollständig selbstfahrende Fahrzeuge entsteht, die kein menschliches Eingriff erfordern, am besten. Hoffentlich wird es in der Zukunft aber nicht viele solcher Situationen geben, es ist aber sicher, dass das Schreiben von Programmen auf Rechtsgrundlagen beruhen muss.

In dem ersten Rechtsfall sind die Pflichtenkollision und der rechtfertigende Notstand aufgetaucht. Aufgrund des ersten Grundes ist die Unterlassungspflicht zu erfüllen, da sie der gleichrangigen Handlungspflicht vorgeht. Es stellt sich jedoch die Frage, inwieweit das Rechtsicherheitsgefühl erschüttert würde, wenn sich die strafrechtliche Beurteilung eines solchen Rechtsfall auf einem gewohnheitsrechtlichen Rechtsfertigungsgrund beruhen würde. Die Verantwortlichkeit kann auch durch das letzte Schuldelement, die Zumutbarkeit ausgeschlossen werden, da von niemandem erwartet werden kann, sein eigenes Leben zu opfern, deshalb sollte der Programmierer das Programm des Fahrzeugs so schreiben, dass es in einer solchen Situation nicht das Leben des Passagiers nimmt.

Die Beurteilung des zweiten Falls würde wahrscheinlich die Gesellschaft spalten. Aus „numerischer" Sicht ist es für die Gesellschaft auf jeden Fall ein Vorteil, wenn mehr Menschen gerettet werden. Aber ethische und philosophische Fragen dürfen nicht außer Acht gelassen werden. Nach aktuellen Standpunkten könnte die beste Lösung darin bestehen, wenn das Auto weniger Menschen überfährt.

---

[80] *Lenk* (Fn. 78) S. 168.

[81] *Engländer,* Das selbstfahrende Kraftfahrzeug und die Bewältigung dilemmatischer Situationen, Zeitschrift für internationale Strafrechtsdogmatik, 2016, S. 609.

Blocher, Janine*
Cand. jur., Universität Konstanz

DIE DATENHEHLEREI DURCH DEN SYSTEMADMINISTRATOR

I. Einleitung

„So gut wie alle Deutschen (93%) [sind sich] einig, dass der Schutz persönlicher Daten wichtig ist." Andererseits geben mehr als 50% an, Zweifel an der Sicherheit ihrer Daten oder sogar das Gefühl keinerlei Kontrolle über die eigenen Daten im Internet innezuhaben.[1] Dabei gewinnen Daten eine immer gewichtigere Bedeutung in unserem Lebens- und Arbeitsalltag. Zahlreiche der von uns täglich genutzten Gegenstände enthalten informationstechnische Komponenten, die die ihnen gelieferten Daten auswerten, verarbeiten und speichern. Die Komplexität dieser Systeme ist aber derart hoch, dass der durchschnittliche Nutzer nicht in der Lage ist, die gespeicherten Daten selbst vor Zugriffen Dritter zu schützen.[2] Die moderne Informationstechnik eröffnet damit neue Möglichkeiten und begründet zugleich neuartige Gefahren.[3] Um so gewichtiger wird die Gewährleistung der Cyber- und Datensicherheit. Das Strafrecht muss sich diesen Herausforderungen der digitalen Welt stellen, um einen ausreichenden Schutz der Datenvertraulichkeit gewährleisten. Das zeigt sich etwa bei der hier untersuchten Datenhehlerei durch den Administrator[4] informationstechnischer Systeme[5]. Dies betrifft folgende Fallkonstellation[6]:

---

* *Cand. iur. Janine Blocher* ist studentische Hilfskraft am Lehrstuhl für Strafrecht, Strafprozessrecht, Strafrechtsvergleichung, Medizinstrafrecht und Rechtstheorie von Prof. *Dr. Liane Wörner,* LL.M. (UW-Madison) an der Universität Konstanz. Der Beitrag wurde im Rahmen des Drei-Länder-Seminars II zu „Digitalisierung und Strafrecht" unter Betreuung von Prof. *Dr. Liane Wörner,* LL.M. (UW-Madison) angefertigt.

1 SINUS-Studie zum Europäischen Datenschutztag v. 28.01.2021, S. 1; https://www.sinus-institut.de/media-center/presse/mehrheit-der-deutschen-zweifelt-an-datensicherheit, (zul. abgerufen am 24.09.2022).

2 BVerfGE 120, 274 Rn. 180 = NJW 2008, 822 (824f).

3 BVerfGE 120, 274 Rn. 170 = NJW 2008, 822 (824); *Eifert,* NVwZ 2008, 521.

4 Der Administrator ist für die Planung der Systeme, deren Kapazität, die Systemkonfiguration und deren Absicherung gegen Angriffe von innen und außen verantwortlich. Kraft seiner organisatorischen Stellung hat er berechtigten Zugriff auf die administrierenden IT-Systeme; *Müller,* Cloud Computing – Strafrechtlicher Schutz privater und geschäftlicher Nutzerdaten vor Innentäterangriffen de lege lata und de lege ferenda, 2020, S. 90ff.; *Schmidl,* IT-Recht von A-Z Accessprovider bis Zwischenspeicherung, 2. Aufl., 2014, S. 11; *Wicker,* Cloud Computing und staatlicher Strafanspruch, 2016, S. 48.

5 Der Begriff umfasst alle Systeme, die der Erfassung, Speicherung, Verarbeitung und Übertragung sowie Anzeige von Daten dienen, z.B. Server, Clients, Internetzugänge und damit verbundene Speichermedien, BMI, Fragenkatalog des Bundesministeriums der Justitz, 22.08.2007, https://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zul. abgerufen am 24.09.2022); zur Funktionsweise des Internets: *Koch,* Strafrechtliche Probleme des Angriffs der Verteidigung in Computernetzen, 2006, S. 25f.

6 dazu BGH NStZ-RR 2020, 278: in dem zugrunde liegenden Fall hatte ein Administrator auf passwortgeschützte E-Mail-Konten eines Bundesministeriums zugegriffen und dort gespeicherte Daten Dritten zur Verfügung gestellt.

Der einzelne Nutzer des IT-Systems räumt dem Administrator faktisch umfassenden Zugriff auf seine Daten ein. Die Zugriffsberechtigung ist vertraglich auf die Erfüllung von Wartungs- und Verwaltungsaufgaben beschränkt. Durch Missbrauch dieser Zugriffsmöglichkeit gelangt der Administrator an die Daten und begeht die für die Hehlerei erforderliche Vortat.[7] Anschließend verbreitet er die so erlangten Daten weiter, so dass ein Dritter daran Verfügungsgewalt begründen kann und die rechtswidrige Situation aufrechterhalten und vertieft wird.[8] Dieser Dritte ist Täter der Hehlerei.

Strafrechtsrelevant ist damit der unbefugte Zugriff des Administrators (II.) sowie die Weitergabe der Daten an Dritte (III.). Zur Gewährleistung eines umfassenden strafrechtlichen Schutzes bedarf der Entwicklung neuer Lösungen, die hier diskutiert werden sollen (IV.).

II. Unbefugter Zugriff auf Nutzerdaten

Mit dem Zugriff auf fremde Daten[9] wird nicht unerheblich in die Datenvertraulichkeit und in das Persönlichkeitsrecht des Einzelnen eingegriffen.[10] Schutz erfährt der persönliche Lebensbereich in diesem Zusammenhang durch die §§ 202a ff. StGB.[11] Diese schützen nach h.M. das sog. formelle Datengeheimnis.[12] Dies meint die formelle Verfügungsbefugnis[13] des Berechtigten, über Weitergabe und Übermittlung der ihm zugeordneten Daten zu entscheiden. In anderen Worten: Es wird das Interesse an der Aufrechterhaltung des

---

[7] Angriffe durch sog. Innentäter zeichnet ein enormes Schädigungs- und Gefährdungspotential aus. Der Innentäter hat direkten Zugriff auf die Systemkomponenten und Kenntnis über die Infrastruktur der Systeme. Im Gegensatz zu externen Angreifern muss dieser nicht erst eine Schwachstelle ausfindig machen, um Sicherheitsmaßnahmen überwinden zu können; *Bedner,* Cloud Computing, 2012, S. 209; *Müller,* DuD 2017, 371. S. (371f.).

[8] Zum Perpetuierungsgedanke: BT-Drs. 7/550, S. 252; *Ruhmannseder,* in: Beck'scher Online-Kommentar zum Strafgesetzbuch, 50. Ed., Stand: 01.05.2021, § 259 Rn. 3; Maier, in: Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 4. Aufl., 2021, § 259 Rn. 2; *Bosch,* JURA 2019, 826f.

[9] Nach h.M. sind Daten alle codierten oder codierbaren Informationen, die Gegenstand oder Mittel eines Datenverarbeitungsvorgangs sind, unabhängig von ihrem qualitativen Inhalt oder Verarbeitungszweck. Eine Einschränkung erfolgt über § 202a Abs. 2 StGB, vgl. DIN-Norm 443000/DIN ISO/IEC 2382; *Hilgendorf,* in: Leipziger Kommentar zum Strafgesetzbuch, 13. Auflage, 2019, § 202a Rn. 7f; *Jessen,* Zugangsberechtigung und besondere Sicherung im Sinne von § 202a StGB, 1994, S. 48ff.; *Koch* (Fn. 5) S. 44; *Krutisch,* Strafbarkeit des unberechtigten Zugangs zu Computerdaten und -systemen, 2004, S. 76, 80f.

[10] vgl. zum staatlichen Eingriff: BVerfGE 120, 274 = NJW 2008, S. 822.

[11] Außerhalb des Kernstrafrechts können Innenangriffe von § 23 Abs.1 GeschGehG erfasst werden, sofern es sich um ein Geschäftsgeheimnis handelt, *Joecks/Miebach,* in: Münchener Kommentar zum Strafgesetzbuch, Bd. 7, 3. Aufl., 2019, § 23 GeschGeh Rn. 20; zu § 17 UWG a.F. *Müller* (Fn. 4) S. 263ff. Zudem greift § 42 Abs. 2 Nr. 1 BDSG bzgl. personenbezogenen Daten, wenn der Täter gegen Entgelt oder in Bereicherungs- bzw. Schädigungsabsicht handelt, *Müller* (Fn. 4) S. 316; *Wicker* (Fn. 4) S. 240.

[12] vgl. BGH NStZ 2018, 401 (403); *Eisele,* in: Schönke/Schröder/Eser, Kommentar zum Strafgesetzbuch, 30. Aufl., 2019, § 202b Rn. 1; *Graf* in: Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 4. Aufl., 2021, § 202a Rn. 2; *Kargl* in: Kindhäuser/Neumann/Paeffgen, Nomoskommentar zum Strafgesetzbuch, 5. Aufl., 2017, § 202d Rn. 5; a.A, die § 202a als Vermögensdelikt qualifizieren: *Haft,* NStZ 1987, 6 (9); wohl auch *Bühler,* MDR 1987, S. 448 (452).

[13] Diese ergibt sich aus dem Recht über den gedanklichen Inhalt der Information, *Graf* (Fn. 12) § 202a Rn. 2; *Kargl* (Fn. 12) § 202a Rn. 3; *Dauster/Braun,* NJW 2000, 313 (315).

Herrschaftsverhältnisses über eine Information geschützt.[14] Berechtigter ist dabei derjenige, der die Daten speichert, also den Datenbestand selbst erstellt (sog. „Skripturakt").[15] Der vom Inhalt der Daten Betroffene ist vom Berechtigten zu unterscheiden. Die §§ 202a ff. StGB schützen allein das formalisierte Interesse an der Geheimhaltung, unabhängig von dem materiellen Inhalt, Sensibilität oder Schutzbedürftigkeit der enthaltenen Information.[16]

II. 1. Ausspähen von Daten, § 202a StGB

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

II. 1. 1. „nicht für den Täter bestimmt"

Für wen die Daten bestimmt sind, entscheidet der Verfügungsberechtigte: in der Regel der Nutzer des IT-Systems.[17] Entscheidend ist dabei das tatsächliche Gewähren einer Zugriffsmöglichkeit. Sobald der Nutzer einem Dritten den Zugriff auf seine Daten zur Verfügung stellt, sind diese für den Dritten auch bestimmt.[18] Der Nutzer kann zwar Rahmenbedingungen bzgl. der Zugangsberechtigung festlegen, diese sind nach überwiegender Ansicht strafrechtlich aber nicht von Relevanz.[19] Daten sind auch für denjenigen bestimmt, der einen berechtigten Zugang vertragswidrig ausnutzt.[20] Der Nutzer, der dem Systemadministrator den faktischen Zugriff auf seine Daten gewährt, bestimmt die Daten auch für den Administrator. Dass gerade keine Berechtigung zur Kenntnisnahme der Inhalte erteilt und der Zugriff auf den Zweck der Wartung beschränkt werden soll, ändert daran nichts.

II. 1. 2. „gegen unberechtigten Zugang besonders gesichert"

In den Schutzbereich des § 202a StGB fallen nur besonders gesicherte Daten. Durch die Sicherung soll das Geheimhaltungsinteresse des Nutzers an den Daten zum Ausdruck kommen.[21] Dabei sind zum Schutz von Laien keine allzu hohen Anforderungen an die

---

[14] *Hilgendorf* (Fn. 9), § 202a Rn. 6; *Kargl* (Fn. 12), § 202d Rn. 5; *Möhrenschlager,* wistra 1986, 128 (140); *Reinbacher,* GA 2018, 311 (312).

[15] *Hilgendorf* (Fn. 9) § 202a Rn. 26; *Hoeren,* MMR 2019, 5 (6f.); *Müller* (Fn. 4) S. 133.

[16] *Eisele* (Fn. 12) § 202a Rn. 1a; *Hoeren,* MMR 2019, 5 (7); *Jessen* (Fn. 9) S. 43; *Möhrenschlager,* wistra 1986, 128 (140); *Reinbacher,* GA 2018, 311 (312f.).

[17] *Graf* (Fn. 12) § 202a Rn. 19; *Wicker* (Fn. 4) S. 107.

[18] *Eisele* (Fn. 12) § 202a Rn. 11; *Graf,* (Fn. 12) § 202a Rn. 24; *Müller,* (Fn. 4) S. 135.

[19] Es können allenfalls zivilrechtliche Schadensersatzansprüche entstehen so, *Hilgendorf* (Fn. 9), § 202a Rn. 22; *Jessen* (Fn. 9) S. 62; *Müller* (Fn. 4) S. 135f.

[20] OLG Celle, Beschl. v. 31.08.2016, 2 Ss 93/16 Rn. 34 = StV 2017, 120; *Eisele* (Fn. 12) § 202a Rn. 11; *Fischer,* Strafgesetzgebuch mit Nebengesetzen, 68. Aufl. 2021, § 202a Rn. 7; *Hilgendorf* (Fn. 9) § 202a Rn. 22; *Müller* (Fn. 4), S. 135; a.A.: *Wicker* (Fn. 4) S. 107ff.

[21] BT-Drs. 10/5058 S. 29; *Kargl* (Fn. 12) § 202a Rn. 9; *Wicker* (Fn. 4) S. 108f.

Sicherung zu stellen.[22] Dennoch muss die Überwindung einen „nicht unerheblichen zeitlichen oder technischen Aufwand“ erfordern. Ist sie ohne Weiteres aufzuheben, ist das Merkmal nicht erfüllt.[23] Nicht erforderlich aber ist, dass die Sicherung auch für Täter mit eingehenden Kenntnissen und Erfahrungen ein unüberwindbares Hindernis bietet. § 202a StGB soll gerade nicht auf professionelle Angreifer beschränkt sein.[24] Der Tatbestand soll solche Fälle ausscheiden lassen, in welchen das Opfer selbst nachlässig mit seinen Daten umgeht und nur leicht überwindbare Sicherungen wählt.[25] Maßnahmen, die aufgrund der besonderen Kenntnisse des Innentäters ihm gegenüber nicht wirken, verlieren nicht deshalb den Charakter als Zugriffssicherung i.S.d. § 202a StGB.[26]

Zwar lässt der faktische Zugriff des Administrators nicht die besondere Sicherung gegenüber Externen entfallen, der Administrator selbst muss meist aber weder Sicherheitslücken umgehen noch Hindernisse überwinden, um auf die Daten zugreifen zu können.[27] Verschlüsselungsmechanismen und Kennwortschutz der Nutzerkonten entfalten keine Wirkung gegenüber den Systemadministratoren, die sich schon „hinter der Zugangssicherung“ befinden.[28] Mit dem Ausnutzen von Administratorenprivilegien bringt der Innentäter nicht die kriminelle Energie auf, tatsächliche Hindernisse zu überwinden, um in einen fremden Herrschaftsbereich einzudringen. Vielmehr benötigt er kaum zeitlichen oder technischen Aufwand, er erhält Datenzugriff „ohne Weiteres“.

Möglichweise könnte diese Schutzlücke durch eine extensive Auslegung des § 202a Abs. 1 StGB geschlossen werden, so dass auch der Missbrauch von faktischen Zugriffsmöglichkeiten erfasst ist. Dafür spricht der Normzweck: der Nutzer geht nicht nachlässig mit seinen Daten um, sondern versucht gerade seine Daten mit hinreichenden Verschlüsselungen und anderen Schutzmaßnahmen gegen externe Angriffe zu sichern und macht ein hinreichendes Geheimhaltungsinteresse deutlich. Das Rechtsgut des formellen Datengeheimnisses und die Verfügungsbefugnis des Berechtigten wird durch den Angriff des Systemadministrators ebenso verletzt, wie durch einen Dritten. Der zentrale Unterschied zum Angriff von außen besteht allein in der kriminellen Energie, die der Täter zur Überwindung eines Hindernisses aufbringen muss. Unter Berücksichtigung der erhöhten Schutzbedürftigkeit des Nutzers[29] und des gesteigerten Gefährdungspotenzials von Innenangriffen ist fraglich, ob dies ausreicht, um die Nichtstrafbarkeit des Systemadministrators zu rechtfertigen. Einer ähnlichen Argumentation folgend ist nach *Wicker* auch in der zweckwidrigen Nutzung das Umgehen von Sicherheitsvorkehrungen zu erkennen.[30]

Der Wortlaut des § 202a Abs. 1 StGB aber fordert das Verschaffen des Zugangs „unter Überwindung der Zugangssicherung“. Die extensive Auslegung ist damit

---

[22] *Eisele* (Fn. 12) § 202a Rn. 14; *Ernst,* NJW 2003, 3233 (3236); *Schumann,* NStZ 2007, 675 (676); a.A.: *Rübenstahl/Debeus,* NZWiSt 2012, 129 (131).

[23] BT-Drs. 16/3656 S. 10; *Graf* (Fn. 12) § 202a Rn. 40ff.; *Eisele* (Fn. 12) § 202a Rn 14.

[24] *Müller* (Fn. 4), S. 151; *Schumann,* NStZ 2007, 675 (676).

[25] BT-Drs. 16/3656; Kargl (Fn. 12), § 202a Rn. 14a.

[26] vgl. *Müller* (Fn. 4) S. 151.

[27] zu den punktuell vom Straftatbestand erfassten Angriffsszenarien, *Müller* (Fn. 4) S. 157 ff.

[28] *Müller* (Fn. 4) S. 16; *Wicker* (Fn. 4) S. 112, 116; vgl. *Graf* (Fn. 12) § 202a Rn. 47.

[29] *Wicker* (Fn. 4) S. 114.

[30] in Analogie zur Nutzungsberechtigung eines Schlüssels beim Einbruchsdiebstahl, *Wicker* (Fn. 4) S. 112f.

nicht vereinbar und verstößt gegen das strafrechtliche Gebot der Gesetzlichkeit gem. Art. 103 Abs. 2 GG, § 1 StGB.[31] Die Norm soll ausdrücklich diejenigen Täter bestrafen, die mit hoher krimineller Energie physische Hindernisse überwinden. Ausgenommen sollen gerade diejenigen sein, die ohne Weiteres Zugriff erlangen können und sich allein über vertragliche Vereinbarungen hinwegsetzten.[32] Mithin erfasst § 202a StGB Innenangriffe nicht, sofern die Administratoren ungehinderten faktischen Zugriff haben.

II. 2. Abfangen von Daten, § 202b StGB

Wer sich Daten unter Anwendung technischer Mittel oder aus einer elektromagnetischen Abstrahlung verschafft, die nicht für ihn bestimmt sind, erfüllt § 202b StGB. Der Tatbestand schützt neben dem formellen Geheimhaltungsinteresse des Berechtigten, das Fernmeldegeheimnis nach Art. 10 I GG. Die Daten müssen während einer nichtöffentlichen Datenübermittlung verschafft werden. Es ist erforderlich, dass ein IT-System mit anderen Servern über ein Netzwerk kommuniziert.[33] Der Schutzbereich endet dann, wenn der Adressat Herrschaft über die Daten erlangt hat, mithin wenn Daten auf dem Server gespeichert werden.[34] § 202b StGB gewährleistet damit nur einen punktuellen Schutz im Bereich von nichtöffentlichen Übermittlungsvorgängen. Daher ist § 202b StGB nicht in der Lage, die durch § 202a StGB offenen Lücken bei Innenangriffen zu schließen.

II. 3. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB

§ 202c StGB kriminalisiert Vorbereitungshandlungen von Computerstraftaten.[35] Wird der Zugriff auf die Daten mithin nicht von §§ 202a, 202b StGB erfasst, scheidet automatisch auch § 202c StGB aus. Jeglicher Missbrauch von Zugriffsrechten durch den Administrator bleibt straflos.[36]

II. 4. Verletzung des Fernmeldegeheimnisses, § 206 II Nr. 1 StGB

§ 206 II Nr. 1 StGB kann nur verwirklicht werden, wenn der Administrator Täterqualität hat, d.h. Inhaber oder Beschäftigter eines Unternehmens ist, das Telekommunikationsdienste erbringt. Dies trifft nur auf Communication-as-a-Service-Systeme (CaaS-Systeme) zu, die

---

[31] *Hassemer/Kargl,* in: Kindhäuser/Neumann/Paeffgen, Nomoskommentar zum Strafgesetzbuch, 5. Aufl., 2017, § 1 Rn. 1; *Hecker,* in: Schönke/Schröder/Eser, Kommentar zum Strafgesetzbuch, 30. Aufl., 2019, § 1 Rn. 1ff.; *Schmitz,* in: Münchener Kommentar zum Strafgesetzbuch, Bd. 1, 4. Aufl., 2020, § 1 Rn. 1f.

[32] BT-Drs. 16/3656 S. 10; BGH NStZ-RR 2020, 278; *Eisele* (Fn. 12) § 202a Rn. 15; *v. Gravenreuth,* NStZ 1989, 201 (206).

[33] *Hilgendorf* (Fn. 9) § 202b Rn. 11; *Kargl* (Fn. 12) § 202b StGB Rn. 4; *Kusnik,* MMR 2011, 720.

[34] *Kargl* (Fn. 12) § 202b StGB Rn. 4; *Müller* (Fn. 4) S. 173; *Schumann* NStZ 2007, 675 (677).

[35] zur Strafbarkeit des Anbietens eines IT-Systems zur Begehung von Straftaten gem. §§ 202a, 202b StGB, *Wicker* (Fn. 4) S. 126f.

[36] *Müller* (Fn. 4) S. 187, 193.

die eigenständige Übermittlung von Kommunikationssignalen erbringen.[37] Die meisten Systemadministratoren scheiden somit bereits aus dem Täterkreis des § 206 StGB aus.[38] Ferner fallen die verschlüsselten Daten der Nutzer nicht unter den Begriff der „verschlossenen Sendung", so dass der Zugriff auf diese nicht von § 206 StGB erfasst werden kann.[39]

III. Weitergabe der Daten an einen Dritten

Obwohl Innenangriffe das formelle Datengeheimnis ebenso schwer verletzen und von externen Angriffen kaum zu unterscheiden sind, greift das Kernstrafrecht nicht. Dies wirkt sich bei Weiterleitung der vertragswidrig erlangten Daten an Dritte fort.

III. 1. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB

Der Administrator hat die Möglichkeit durch Übermittlung eines Links, Daten an Dritte weiterzuleiten. Wird der Link von einem Dritten aufgerufen erhält dieser unverschlüsselten Zugang zu allen verlinkten Daten des Geschädigten.[40] Dieser kann dann mühelos auf die Datensätze zugreifen, ohne eine Zugangssicherung zu überwinden. Somit scheidet die Verwirklichung der §§ 202a, 202b StGB sowie § 202c Abs. 1. StGB durch die Übermittlung als Vorbereitungshandlung aus.[41] Strafrechtlich erfasst wird nur die unbefugte Weitergabe des Nutzerkennworts: darin liegt eine Beihilfe des Administrators zur Verwirklichung des § 202a Abs. 1 StGB durch den Dritten.[42]

III. 2. Datenhehlerei, § 202d Abs. 1 StGB

Auf den ersten Blick erscheint der Tatbestand der Datenhehlerei gem. § 202d StGB[43], der gerade den rechtswidrigen Datenhandel kriminalisieren soll, einschlägig.[44] Der Tatbestand soll das formelle Datengeheimnis[45] des Berechtigten schützen, welches bereits durch eine

---

[37] *Müller* (Fn. 4) S. 199; idR dienen IT-Systeme der Bereitstellung von Ressourcen zur Speicherung und Verarbeitung von Daten, gerade nicht aber dem technischen Transport von Signalen. vgl. *Wicker* (Fn. 4) S. 158; zur besonderen Form des Cloud-Sharings, *Müller* (Fn. 4) S. 196f.; *Wicker* (Fn. 4) S. 159f.

[38] *Wicker* (Fn. 4) S. 164.

[39] zur Argumentation, *Müller* (Fn. 4) S. 206; vgl. OLG Karlsruhe, Beschl. v. 10.1.2005 – 1 Ws 152/04 Rn. 17 = MMR 2005, 178 (180); *Eisele* (Fn. 12) § 206 Rn. 17; *Fischer* (Fn. 20) § 206 Rn. 13.

[40] *Müller* (Fn. 4) S. 116, 187.

[41] *Graf* (Fn. 12) § 202c Rn. 10; *Müller* (Fn. 4) S. 187.

[42] *Müller* (Fn. 4) S. 164.

[43] zur Genese ausführlich: *Stuckenberg,* ZIS 2016, 526 (527ff.); *Gercke,* ZUM 2013, 605; dazu *Klengel/Gans,* ZRP 2013, 16.

[44] dazu näher BT-Drs. 18/5088 S. 2.

[45] für ein formell-materielles oder rein materielles Schutzkonzept, *Reinbacher,* GA 2018, 311; *Rode,* in: Festschrift für Rudolf Rengier, 2018, S. 301; *Singelnstein,* ZIS 2016, 432; *Stuckenberg,* ZIS 2016, 526.

rechtswidrige Vortat verletzt worden ist.[46] Werden Daten rechtswidrig erlangt, kann der Berechtigte nicht mehr selbst entscheiden, wer von den Daten Kenntnis nimmt oder sie weitergibt, so wird seine formelle Verfügungsbefugnis verletzt.[47] Verschafft sich im Anschluss ein Dritter die rechtswidrig erlangten Daten und verbreitet diese weiter, erhält eine weitere Person die Möglichkeit, über die Zugänglichmachung der Daten zu entscheiden und zugleich wird die Nachverfolgung der Verbreitung der Daten erschwert. Die Verletzung der Verfügungsbefugnis wird nicht nur aufrechterhalten, sondern auch vertieft.[48]

In den zu untersuchenden Konstellationen gibt ein Administrator Daten, die in dem von ihm verwalteten System gespeichert werden an einen Dritten weiter. Der Systemadministrator als Vortäter muss zunächst eine rechtswidrige Tat i.S.d. § 11 Abs. 1 Nr. 5 StGB begangen haben, um die Daten zu erlangen. In Betracht kommen alle Tathandlungen, die einen Tatbestand des StGB erfüllen.[49]

III. 2. 1. Vortat durch rechtswidrigen Zugriff auf die Daten

Die Vortat muss sich gegen die formelle Verfügungsbefugnis des Berechtigten richten.[50] Dies ist jedenfalls dann der Fall, wenn der Vortäter die Daten durch Schaffung einer eigenen Verfügungsbefugnis erlangt.[51] Daten, die dem Vortäter bereits zur Verfügung stehen und nur unter Urheberrechtsverletzung, Vertragsverletzung, Disziplinarvergehen oder Ordnungswidrigkeit vervielfältigt werden, sind nicht durch eine rechtswidrige Tat erlangt.[52] § 202d StGB schützt nicht gegen die Weiterverbreitung von Daten durch denjenigen, dem Daten anvertraut und Zugriffsmöglichkeiten eingeräumt worden sind, auch wenn der Zugriff rechtswidrig ist.[53] Der Privilegienmissbrauch fällt also nicht in den Anwendungsbereich des § 202d StGB.[54]

III. 2. 2. Vortat durch Übermittlung der Daten an den Dritten

§ 202d StGB greift auch dann nicht, wenn die Vortat erst durch das Zugänglichmachen der Daten an den Hehler begangen wird.[55] Die Daten müssen „durch eine Vortat" erlangt werden. Dafür spricht der Charakter der Datenhehlerei als Anschlussdelikt, welcher eine zeitliche Zäsur zwischen Erfolg der Vortat und Hehlertat erforderlich macht.[56] Die Vortat muss beendet sein.[57]

---

[46] BT-Drs. 18/5088 S. 26

[47] BT-Drs. 18/5088 S. 26; Diese wird bereits durch §§ 202a, 303a StGB geschützt und soll durch § 202d im Hinblick auf Perpetuierungshandlungen ergänzt werden, *Reinbacher,* GA 2018, 311; *Stuckenberg,* ZIS 2016, 526.

[48] dazu ausführlich BT-Drs. 18/5088 S. 26.

[49] Zur Problematik der Vortaten mit Auslandsbezug, siehe *Brodowski/Marnau,* NStZ 2017, 377 (384f.).

[50] *Stuckenberg,* ZIS 2016, S. 526; zur Verfügungsbefugnis von Unternehmen: *Wilke,* NZWiSt 2019, 168.

[51] *Brodowski/Marnau,* NStZ 2017, 377 (381).

[52] BT-Drs. 18/5088 S. 46.

[53] *Brodowski/Marnau,* NStZ 2017, 377 (383).

[54] *Müller* (Fn. 4) S. 214; vgl. *Reh/Cosfeld,* NStZ 2019, 706 (708).

[55] *Müller* (Fn. 4) S. 215; ders., DuD 2017, 371 (375).

[56] BGH NJW 2012, S. 3736; BGH NJW-RR 2011, 245 (246); *Brodowski/Marnau,* NStZ 2017, 377 (382); zum Meinungsstreit, *Maier* (Fn. 8) § 259 StGB Rn. 47.

[57] BT-Drs. 18/5088 S. 46.

Die Weitergabe der Nutzerdaten durch den Systemadministrator an einen Dritten kann mangels strafrechtlicher Erfassung des unbefugten Zugriffs nicht gem. § 202d StGB bestraft werden.

III. 2. 3. Verletzung und Verwertung von Privatgeheimnissen, §§ 203 Abs. 4, 204 Abs. 1 StGB

Gelangen fremde Geheimnisse, die einem Berufsgeheimnisträger anvertraut worden sind, in den Herrschaftsbereich eines nicht eingeweihten Dritten werden diese gem. §§ 203, 204 StGB offenbart.[58] Der Systemadministrator fällt je nach organisatorischer Einbindung in den Betrieb eines Berufsgeheimnisträgers unter den Begriff des Gehilfen bzw. der sonstigen mitwirkenden Person i.S.d. § 203 Abs. 3 StGB und ist vom Täterkreis erfasst.[59] Die Datenvertraulichkeit ist vor Innenangriffen somit geschützt. Aufgrund der Sensibilität der Informationen, die aus dem engsten Persönlichkeitsbereich der Geheimnisträger stammen, ist ein solcher Schutz erforderlich. Im Ergebnis bleibt dieser jedoch punktuell, denn der Schutzbereich erfasst nur Berufsgeheimnisträger und die ihnen anvertrauten Geheimnisse. Zudem handelt es sich um absolute Antragsdelikte. Dies scheint problematisch, da die Wahrscheinlichkeit eine solche Weitergabe als Betroffener zu erkennen recht gering ist.

III. 2. 4. Verletzung des Fernmeldegeheimnisses, § 206 StGB

Die unbefugte Weitergabe von Inhaltsdaten könnte § 206 StGB unterfallen, sofern die Daten dem Fernmeldegeheimnis unterliegen. Der Täter muss die Informationen einem Dritten „mitteilen", diesem also die Gelegenheit zur Kenntnisnahme verschaffen.[60] Die Form der Mitteilung ist dabei unerheblich, auch die unbefugte Einräumung von Zugriffsrechten für einen Dritten wird erfasst.[61] Als taugliche Täter kommen jedoch allein die Betreiber von CaaS-Systemen in Betracht.[62] Die Administratoren der häufig betriebenen IaaS-, PaaS- und SaaS-Dienstleistungen fallen gerade nicht in den tauglichen Täterkreis.[63]

III. 2. 5. Nebenstrafrecht

Außerhalb des Kernstrafrechts bietet § 23 I Nr. 2 GeschGehG einen möglichen Anknüpfungspunkt zur Strafbarkeit des Administrators. Der Auffangtatbestand erfasst Fälle des unbefugten Ausspähens von Geschäfts- und Betriebsgeheimnissen, die durch rechts-, sitten-

---

[58] *Cierniak/Niehaus* in: Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 4. Aufl., 2021, § 203 Rn. 51; *Fischer* (Fn. 20) § 203 Rn. 33; *Hoyer,* in: Systematischer Kommentar zum Strafgesetzbuch, Bd. 4, 9. Aufl., 2017 § 203 Rn. 1, 31; *Kargl* (Fn. 12) § 203 Rn. 19, die Tatbestandsvariante des Verwertens scheidet jedoch aus, dazu *Schünemann* in: Leipziger Kommentar zum Strafgesetzbuch, 13. Auflage, 2019, § 204 Rn. 5; *Müller* (Fn. 4) S. 248.

[59] BT-Drs. 18/11936, S. 22; so ausführlich *Müller* (Fn. 4) S. 232ff. m.w.N.

[60] *Eisele* (Fn. 12) § 206 Rn. 10; *Heger* in: Lackner/Kühl, Kommentar zum Strafgesetzbuch, 29. Aufl., 2018, § 206 Rn. 7; *Kargl* (Fn. 12) § 206 Rn. 21.

[61] *Eisele* (Fn. 12) § 206 Rn. 10; *Heger* (Fn. 61) § 206 Rn. 7; *Müller* (Fn. 4) S. 226.

[62] siehe dazu Abschnitt A. IV.

[63] *Müller* (Fn. 4) S. 228.

oder vertragswidrige Mittel unter Verstoß gegen § 4 Abs. 1 Nr. 1 GeschGehG erlangt wurden.[64] Der Schutz vor Innenangriffen wird recht umfassend geregelt, insbesondere unter Berücksichtigung des § 23 Abs. 7 GeschGehG, der Vorbereitungshandlungen i.S.d. §§ 30, 31 StGB kriminalisiert. Daneben wird die Übermittlung der Daten an einen Dritten von § 42 Abs. 1 BDSG erfasst.[65]

IV. Lösungsbedarf

Der Administrator verletzt mit Zugriff auf die Daten die Verfügungsbefugnis des Berechtigten, ohne dass ein Unterschied zu einem externen Angriff erkennbar ist. Zudem wird durch die Weitergabe der erlangten Daten die Rechtsgutsverletzung in gleichem Maße aufrechterhalten und vertieft. In beiden Fällen wird dem Berechtigten die Entscheidung bzgl. der Zugänglichmachung seiner Daten aus der Hand genommen, sowie die Nachverfolgbarkeit seiner Daten deutlich erschwert.

Der Schutz der Datenvertraulichkeit vor Innenangriffen wird durch das deutsche Strafrecht jedoch nur sehr punktuell gewährleistet. Die datenschutzstrafrechtlichen Tatbestände nach §§ 202a ff. StGB finden keine Anwendung, wenn der Administrator (bloß) seine Privilegien missbraucht, um auf Nutzerdaten zuzugreifen.

Zwar werden besonders sensible Bereiche durch nebenstrafrechtlichen Schutz abgedeckt. Insbesondere § 42 BDSG gewährleistet einen umfassenden Schutz personenbezogener Daten. § 42 BDSG dient dem Schutz des Rechts auf informationelle Selbstbestimmung, des inhaltlich von den Daten Betroffenen.[66] Geschützt wird nicht das formelle, sondern vielmehr das materielle Geheimhaltungsinteresse des Betroffenen.[67] Aufgrund der unterschiedlichen Schutzrichtungen von § 42 BDSG und §§ 202a ff. StGB bleibt die formelle Verfügungsbefugnis und damit auch der Verfügungsberechtigte, der gerade nicht notwendigerweise auch materiell betroffen ist, jedoch weiterhin ohne strafrechtlichen Schutz vor Innenangriffen.

In Anbetracht der erhöhten Gefährlichkeit des Innenangriffs und der damit einhergehenden erheblichen Verletzungen des formellen Datengeheimnisses und der informationellen Selbstbestimmung des Nutzers, ist dies bedenklich.[68] Mit der aktuellen Rechtslage kann kein hinreichender Schutz der Datenvertraulichkeit gewährleistet werden, hier ist es an dem Gesetzgeber neue Regelungen zu treffen, um dem Konzept des Datenschutzstrafrechts im StGB umfassend gerecht zu werden. Ein Lösungsvorschlag bietet *Müller* mit dem Vorstoß, einen neuen Tatbestand in Form einer Datenuntreue zu schaffen, (IV. 1.), an

---

[64] vgl. *Hiéramente,* in: Beck'scher Online-Kommentar zum GeschGehG, 8. Ed., Stand: 15.06.2021, § 23 Rn. 25f.; *Joecks/Miebach* (Fn. 11) § 23 GeschGehG Rn. 59; noch zu § 17 UWG a.F., *Müller* (Fn. 4) S. 267, 272f.

[65] Sofern der Innentäter als Adressat des Art. 83 DSGVO erkannt wird, kommt wohl auch ein Verstoß gegen das Rechtmäßigkeitsgebot nach Art. 5 I Var. 1 i.V.m. Art. 6 I DSGVO in Betracht, *Müller* (Fn. 4) S. 303, 311.

[66] *Brodowski/Nowak,* in: Beck'scher Onlinekommentar zum Datenschutzrecht, 41. Ed., Stand: 01.08.2022, § 42 BDSG Rn. 7, m.w.N.

[67] *Brodowski/Nowak* (Fn. 66), § 42 BDSG Rn. 24, m.w.N.

[68] Insb. auch weil der Schutz des Fernmeldegeheimnisses schon mangels Täterqualität gegenüber den meisten Systemadministratoren nicht greift, so auch *Müller,* DuD 2017, 371 (375).

diesen Ansatz anknüpfend wird versucht den Rechtsgedanken des § 246 Abs. 2 StGB auf die hiesige Fallkonstellation zu übertragen (IV. 2.).

IV. 1. Ausgangspunkt – Datenuntreue[69]

Müller schlägt für eine Neuregelung die Übertragung des Rechtsgedankens der Untreue gem. § 266 StGB vor. Der Tatbestand soll alle Daten vor einem Privilegienmissbrauch des Administrators schützen und zu einem umfassenden Schutz des „digitalen Besitzes […] an sämtlichen gespeicherten und verarbeiteten Datenkategorien" beitragen.[70] Als Vortat soll die Datenuntreue auch die Strafbarkeit des Datenhehlers umfassend gewährleisten. Mit nachvollziehbarer Begründung führt *Müller* aus, dass das Strafrecht als „ultima ratio" zum Schutz vor Innenangriffen erforderlich ist, da zivilrechtliche Verpflichtungen oder die Auslagerung ins Ordnungswidrigkeitenrecht keinen hinreichenden Schutz gewährleisten können und vielmehr die Strafzwecke der General- und Spezialprävention erforderlich sind.[71] Dem kann nur zugestimmt werden, zumal es schon nicht überzeugen mag, weshalb bei gleichartiger Rechtsgutsverletzung und ähnlichem Handlungsunrecht ein Innentäter nur außerhalb des Strafrechts sanktioniert werden, der externe Täter dagegen den Normen des StGB unterfallen soll.[72] Der Ansatz hat durchaus Potential und führt im Ergebnis zu dem erforderlichen strafrechtlichen Schutz der Datenvertraulichkeit. Dennoch vermag ein anderer Anknüpfungspunkt dem Schutzzweck und der Systematik einer solchen Norm gerechter werden.

IV. 1. 1. Schutzkonzept des § 266 StGB

§ 266 StGB schützt allein das Vermögen, nicht geschützt ist die Dispositionsfreiheit des Geschädigten und das Vertrauen des Treugebers in die Redlichkeit des Täters bzw. den Rechts- oder Geschäftsverkehr.[73] Die Schutzbedürftigkeit des Vermögens ergibt sich aus der besonderen Verletzlichkeit vor Angriffen „von innen" bei der Überlassung von Vermögenswerten an Dritte.[74] Der Täter ist in die organisatorische Sphäre eingebunden und hat eine besondere Machtstellung, die es ihm ermöglicht das Vermögen von „innen auszuhöhlen".[75]

---

[69] Im Folgenden soll lediglich über die Übertragung des Rechtsgedankens, also die Vergleichbarkeit des Unrechtsgehalts und der Gefährdungslage zweier Tatbestände nachgedacht werden, so dass der eine für den anderen als Orientierung dienen kann. Es soll keine Analogie geschaffen werden.

[70] *Müller* (Fn. 4) S. 401f.

[71] *Müller* (Fn. 4) S. 402ff.

[72] aus viktimologischer Sicht, vgl. *Müller* (Fn. 4) S. 404.

[73] *Dierlamm/Becker* in: Münchener Kommentar zum Strafgesetzbuch, Bd. 5, 4. Aufl., 2022, § 266 Rn. 1; *Hoyer,* in: Systematischer Kommentar zum Strafgesetzbuch, Bd. 5, 9. Aufl., 2019, § 266 Rn. 4ff.; *Perron,* in: Schönke/Schröder/Eser, Kommentar zum Strafgesetzbuch, 30. Aufl., 2019, § 266 Rn. 1; *Wittig,* in: Beck'scher Online-Kommentar zum Strafgesetzbuch, 54. Ed., Stand: 01.08.2022, § 266 Rn. 3f.

[74] *Perron* (Fn. 73) § 266 Rn.1; *Saliger* in: Satzger/Schluckebier/Widmaier, Kommentar zum Strafgesetzbuch, 5. Aufl., 2020, § 266 Rn. 3; *Schünemann* (Fn. 58) § 266 Rn. 1f.

[75] *Dierlamm/Becker* (Fn. 73) § 266 Rn. 2; *Kindhäuser* in: Kindhäuser/Neumann/Paeffgen, Nomoskommentar zum Strafgesetzbuch, 5. Aufl., 2017, § 266 Rn. 3.

IV. 1. 2. Merkmale der Vermögensbetreuungspflicht

Die Untreue setzt eine Vermögensbetreuungspflicht des Täters voraus. Diese hat ihre Grundlage in einem Treueverhältnis, das über die Qualität und Intensität eines gewöhnlichen Schuldverhältnisses hinausgeht.[76] Es muss sich um eine Hauptpflicht handeln, die dem Schuldverhältnis sein entscheidendes Gepräge gibt, die der Obhutspflichtige selbstständig wahrnimmt. Dem Verpflichteten verbleibt ein gewisser Spielraum zur eigenverantwortlichen Entscheidung. Andernfalls fehlt ihm die erforderliche Dispositionsmacht.[77]

Zentrale Aufgabe des Administrators ist die Verwaltung des IT-Systems. In diesem Rahmen wird dem Administrator der Zugriff zu den Daten gewährt, demgegenüber ist er zur Fürsorge verpflichtet.[78]. Die administrative Pflicht – und so auch der Datenzugriff – ist wesentlich und nicht nur beiläufig. Grundsätzlich ist der Administrator auch frei in der Wahrnehmung seiner Wartungstätigkeiten. Er unterliegt diesbezüglich keinen Bindungen.

Das Merkmal der Selbstständigkeit iSd § 266 StGB erfordert daneben Dispositionsmacht über das Tatobjekt. Der Systemadministrator hat ein Zugriffsrecht auf die Daten, diese darf er aber im Innenverhältnis nur zu genau festgelegten Zwecken nutzen, er darf gerade nicht frei über den Zugriff auf die Daten entscheiden und schon gar nicht über diese disponieren. Im Rahmen der Kasuistik zu § 266 StGB kann eine Parallele zur Pflichtenstellung des Bankberaters gegenüber dem Kunden gezogen werden.[79] Dieser hat zwar Zugriff auf das angesparte Vermögen des Kunden auf dessen Girokonto, soll diesen aber allein zur Verwaltung des Kontos gebrauchen. Eine Vermögensbetreuungspflicht verneint das OLG München ausdrücklich, da der Berater gerade nicht eigenständig im Rahmen eines eingeräumten Entscheidungsspielraums über Einzeldispositionen entscheiden kann.[80] Ähnlich liegt die Situation beim Systemadministrator: auch dieser hat nur Zugriff zur Verwaltung der Systeme, er soll gerade keine eigenständigen Entscheidungen über den Gebrauch, die Verarbeitung oder Weitergabe der Daten treffen.

IV. 1. 3. Ergebnis

Der Systemadministrator hat keine Dispositionsmacht, sondern nur eine Verwaltungspflicht zur Gewährleistung der sicheren Speicherung und Verarbeitung der Daten im Sinne eines Verwahrungsverhältnisses inne. Die Tatsache, dass der Innntäter, eine mit der Vermögensbetreuungspflicht vergleichbare Pflichtenstellung gerade nicht innehat und ihm damit ein für die Untreue zwingend erforderliches Merkmal fehlt, deutet darauf hin, dass dieser Rechtsgedanke zum Schutz, der Datenverfügungsberechtigung und der Interessenlage zwischen Nutzer und Administrator nicht vollumfänglich gerecht wird.

---

[76] *Dierlamm/Becker* (Fn. 73) § 266 Rn. 41, 46; *Hoyer* (Fn. 73) § 266 Rn. 11; *Perron* (Fn. 73) § 266 Rn. 23.

[77] *Dierlamm/Becker* (Fn. 73) § 266 Rn. 55; *Kindhäuser* (Fn. 75) § 266 Rn. 47ff.; *Saliger* (Fn. 74) § 266 Rn. 8ff.

[78] *Müller* (Fn. 4) S. 90ff.; *Wicker* (Fn. 4) S. 48.

[79] *Dierlamm/Becker* (Fn. 73) § 266 Rn. 85; *Kindhäuser* (Fn. 75) § 266 Rn. 57.

[80] OLG München, Urt. v. 30.11.2009 – 5St RR 357/09, wistra 2010, 155 (156).

IV. 2. Übertragung des Rechtsgedankens des § 246 Abs. 2 StGB

In Betracht kommt diesen Gedanken fortführend eine Anknüpfung an das Schutzkonzept der „veruntreuenden" Unterschlagung gem. § 246 Abs. 2 StGB.

IV. 2. 1. Schutzkonzept und Tatbestandsstruktur

§ 246 Abs. 2 StGB bestraft denjenigen, der sich oder einem Dritten eine ihm anvertraute Sache rechtswidrig zueignet. Die Norm schützt das Eigentum an körperlichen Gegenständen. Daten selbst sind somit kein taugliches Tatobjekt, allein der sie verkörpernde Datenträger.[81]

Tathandlung ist die rechtswidrige Zueignung. Nach h.M.[82] muss sich der innere Zueignungswille nach außen durch ein Verhalten manifestieren, das den Erwerb einer eigentümerähnlichen Stellung erkennen lässt. Häufige Formen der Manifestation sind Verfügungen über das Tatobjekt, etwa die Weiterveräußerung, [83] oder der Ge- bzw. Verbrauch der Sache.[84] Mithin Verhaltensweisen durch die der Täter die Grenzen seiner rechtlichen Befugnis überschreitet.[85]

§ 246 Abs. 2 StGB regelt die Qualifikation des Eigentumsdelikts, wenn es sich beim Tatobjekt um anvertraute Sachen handelt. Anvertraut ist eine Sache, die der Täter vom Eigentümer oder einem Dritten mit der Verpflichtung erlangt, sie zu einem bestimmten Zweck zu verwenden, aufzubewahren oder zurückzugeben.[86] Voraussetzung ist dazu die tatsächliche Verfügungsgewalt des Täters.[87] Eine restriktivere Ansicht fordert die Überlassung der Sache an den Täter ohne Nutzungsbefugnis, so dass das gesteigerte Unrecht in der Enttäuschung des Vertrauens auf die Nichtnutzung liegt.[88] Die Anforderungen liegen dabei weit unterhalb der des Treueverhältnisses nach § 266 StGB.[89]

IV. 2. 2. Einordnung der formellen Verfügungsberechtigung über Daten

Der Rechtsgedanke des § 246 StGB kann nur dann auf die in IT-Systemen gespeicherten Daten und Administratorenrechte übertragen werden, wenn das Schutzgut der formellen Verfügungsberechtigung des Nutzers Ähnlichkeiten mit dem Eigentum aufweist. Ein „Dateneigentum" im Sinne eines absoluten Rechts an digitalen Daten existiert in unserer

---

[81] BayObLG NJW 1992, 1777 (1778); *Hohmann,* in: Münchener Kommentar zum Strafgesetzbuch, Bd. 4, 4. Aufl., 2021, § 246 Rn. 11; *Kudlich* in: Satzger/Schluckebier/Widmaier, Kommentar zum Strafgesetzbuch, 5. Aufl., 2020, § 246 Rn. 5.

[82] BGHSt 14, 38 (41); BGHSt 24, 115 (119); *Bosch,* in: Schönke/Schröder/Eser, Kommentar zum Strafgesetzbuch, 30. Aufl., 2019, § 246 Rn. 10; *Hohmann* (Fn. 81) § 246 Rn. 19; *Kindhäuser* (Fn. 75) § 246 Rn. 14.

[83] auf die rechtliche Wirksamkeit kommt es nicht an, *Hohmann* (Fn. 81) § 246 Rn. 25.

[84] *Bosch* (Fn. 82), § 246 Rn.14; *Kudlich* (Fn 81) § 246 Rn. 14; *Kühl* in: Lackner/Kühl, Kommentar zum Strafgesetzbuch, 29. Aufl., 2018, § 246 Rn. 5.

[85] nur *Kindhäuser* (Fn. 75) § 246 Rn. 6.

[86] RGSt 4, 386; 6, 117; 29, 239; 40, 223; BGHSt 9, 90 (91) = NJW 1956, 837 (Ls.); BGHSt16, 280 (282) = NJW 1962, 116 (117); *Hohmann* (Fn. 81) § 246 Rn. 56; *Wittig* (Fn. 73) § 246 Rn. 11.

[87] *Bosch* (Fn. 82), § 246 Rn. 29; *Hoyer* (Fn. 73) § 246 Rn. 44; *Wittig* (Fn. 73) § 246 Rn. 11.

[88] *Hohmann* (Fn. 81) § 246 Rn. 58; *Hoyer* (Fn. 73) § 246 Rn. 44.

[89] *Hohmann* (Fn. 81) § 246 Rn. 54; *Kindhäuser* (Fn. 75) § 246 Rn. 40; *Wittig* (Fn. 73) § 246 Rn. 11.1.

Rechtsordnung bis dato nicht.[90] Die Zuordnung von Daten an einen formellen Verfügungsberechtigten ist zudem weitaus komplexer als bei Sachen, insbesondere bei automatisch erzeugten Daten von selbstlernenden Maschinen kann nicht klar bestimmt werden, wem die Daten zuzuordnen sind und wer darüber verfügen darf.[91] Anders als bewegliche Sachen können Daten zudem beliebig häufig vervielfältigt und dem parallelen Zugriff beliebig vieler Personen ausgesetzt werden. Sie unterliegen keiner Abnutzung oder Alterung.[92]

Das Datenschutzstrafrecht schützt das formelle Datengeheimnis des Berechtigten. Es erfolgt eine Zuordnung von Daten an denjenigen, der die Daten speichert, mithin den Datenbestand selbst schafft und erstellt. Es wird vorausgesetzt, dass dieser eine Verfügungsberechtigung über die Daten hat.[93] Diese beinhaltet vordergründig die Möglichkeit des Berechtigten autonom zu entscheiden, wem er die Daten zugänglich macht, unter welchen Bedingungen und in welchem Umfang dies erfolgen soll.[94] Damit beinhaltet das Schutzgut des Datenschutzstrafrechts eine mit den des Eigentümers vergleichbare Befugnis, mit dem Bezugsobjekt nach Belieben zu verfahren und andere von der Einwirkung auszuschließen.[95] Gerade das Interesse an der Aufrechterhaltung eines Herrschaftsverhältnisses des Berechtigten ist von § 246 StGB geschützt. Die formelle Verfügungsberechtigung ist sicher nicht mit einem etwaigen „Dateneigentum" gleichzusetzen. Aber das damit einhergehende Verfügungsrecht des Berechtigten über seine Daten ist mit der von § 246 StGB geschützten uneingeschränkten Verfügungsbefugnis des Eigentümers vergleichbar. Daher scheint eine Übertragung des Rechtsgedankens der Unterschlagung auf Datenschutzstraftaten jedenfalls nicht abwegig.

IV. 2. 3. Einordnung der Tatsituation bei Innenangriffen

Neben der Ähnlichkeit des Schutzguts bedarf es zudem einer Übertragbarkeit der Gefährdungslage in der Tatsituation. § 246 StGB bestraft den Manifestationsakt eines Zueignungswillens.[96] Aufgrund der Unterschiede zwischen Daten und Sachen muss der Zueignungsbegriff abstrahiert werden. Unter Zueignung wird im Folgenden daher die Anmaßung eines Verfügungsrechts verstanden.[97] Der Administrator hat die faktische Möglichkeit zum Zugriff und nutzt diese vertragswidrig aus. Mit Kopie und Speicherung begründet er eine Herrschaftsposition über die Daten, die es ihm erlaubt über deren Zugänglichkeit künftig

---

[90] *Wagner,* in: Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 7, 8. Aufl., 2020 § 823 Rn. 332; *Hoeren,* MMR 2019, 5 (6).

[91] *Brodowski/Marnau,* NStZ 2017, 377 (378f.).

[92] *Hoeren,* MMR 2019, 5 (6); vgl. *Reinbacher,* GA 2018, 311 (315).

[93] siehe dazu Abschnitt II.

[94] *Graf* (Fn. 12) § 202a Rn. 2; *Kargl,* (Fn. 12) § 202a Rn. 3; *Dauster/Braun,* NJW 2000, 313 (315); *Kühling/Sackmann,* ZD 2020, 24 (27).

[95] soweit zum Eigentum, vgl. § 903 S.1 BGB; *Papier/Shirvani,* in: Dürig/Herzog/Scholz, Grundgesetz- Kommentar, 97. EL, 01/2022, Art. 14 GG Rn. 6.

[96] BGHSt 14, 38 (41); BGHSt 24, 115 (119); *Bosch,* (Fn. 82) § 246 Rn. 10; *Hohmann* (Fn. 81) § 246 Rn. 19; *Kindhäuser* (Fn. 75) § 246 Rn. 14.

[97] Das ist aufgrund der Ähnlichkeiten der Verfügungsbefugnis über Eigentum und der Verfügungsberechtigung über Daten, sowie dem Verständnis der Unterschlagung als Anmaßung eigentümerähnliche Rechte auch vertretbar, vgl. *Sinn,* NStZ 2002, 64 (69).

zu entscheiden. Mit der Weitergabe an Dritte verfügt er tatsächlich darüber. Eine solche Verhaltensweise entspricht der Anmaßung der geschützten Verfügungsberechtigung des Nutzers. Dies ist ferner vergleichbar mit einer Zueignung nach § 246 StGB, welche gerade die Weiterveräußerung, Weitergabe, sowie Gebrauch des Tatobjekts erfasst.[98]

Der Nutzer räumt dem Administrator von vornerein eine berechtigte Zugriffsmöglichkeit ein, ihm obliegen aber keine Dispositionsbefugnisse. Die Situation gleicht einem Verwahrungsverhältnis ohne Nutzungsbefugnis.[99] In dem Missbrauch der Administratorprivilegien liegt ein gesteigerter Unwertgehalt, der sich aus der treuwidrigen Verletzung des Vertrauensverhältnisses zum anvertrauenden Nutzer ergibt. So besteht eine vergleichbare Situation zu § 246 Abs. 2 StGB.

IV. 2. 4. Berücksichtigung der Besonderheiten von Daten

Insoweit sind die Innenangriffe des Systemadministrators und die dadurch gefährdeten Rechtsgüter der Unterschlagung nach § 246 Abs. 2 StGB und deren Schutzrichtung ähnlich. Ein Problem könnte sich jedoch aus den besonderen Eigenschaften von Daten ergeben. Diese lassen sich verlustfrei kopieren und duplizieren, so dass sie dem Verfügungsberechtigten unverändert weiterhin zur Verfügung stehen. Durch Zugriff und Weiterverbreitung werden die Daten dem Berechtigten nie vollständig entzogen.[100] Aus diesem Grund kann die Zueignung im Zusammenhang mit Daten auch nicht als vorübergehende Aneignung und dauerhafte Enteignung verstanden werden, sondern als Anmaßung der Entscheidung über die Zugänglichkeit der Daten. Die Rechtsgutsverletzung kann ferner auch nicht darin gesehen werden, dass Substanzverluste oder wirtschaftliche Nachteile durch Gebrauch der Sache entstehen.[101] Gerade wegen der Unterschiede von Daten und Sachen, fallen Daten nicht in den Tatbestand des § 246 StGB. Letztlich steht dies der Heranziehung des Rechtsgedankens nicht im Wege. Aufgrund der festgestellten Ähnlichkeiten sollen allein die der Norm zugrundeliegenden Wertungen aufgegriffen werden, um daraus einen neuen Tatbestand entwickeln zu können, der die formelle Verfügungsberechtigung schützt und Daten als Tatobjekte erfasst.

V. Fazit und Ausblick

Der bis dato nur sehr punktuell gewährleistete strafrechtliche Schutz der Vertraulichkeit von Daten im Bereich Innenangriffen, bedarf angesichts der enormen und zunehmenden Wichtigkeit von Daten in unserer Lebenswelt neuer Priorisierung. Vieles spricht für die Übertragung des Rechtsgedankens des § 246 Abs. 2 StGB auf Innenangriffe durch den Systemadministrator und die Einführung einer eigenständigen Norm. Jene sollte bestrafen,

---

[98] *Bosch* (Fn. 82) § 246 Rn.14; *Kudlich* (Fn. 81) § 246 Rn. 14; *Kühl* (Fn. 84) § 246 Rn. 5; *Hohmann* (Fn. 81) § 246 Rn. 25.

[99] vgl. *Hohmann* (Fn. 81) § 246 Rn. 58; *Hoyer* (Fn. 73) § 246 Rn. 44.

[100] BT-Drs. 18/5088 S. 27; *Hoeren,* MMR 2019, 5 (6); *Kühling/Sackmann,* ZD 2020, 24 (25).

[101] *Bosch* (Fn. 82) § 246 Rn. 13f., der es für erforderlich hält, dass die Zueignung auf Beeinträchtigung der Eigentümerstellung in ihrer wirtschaftlichen Funktion gerichtet ist.

wer sich oder einem Dritten die Verfügungsbefugnis über das ihm anvertraute Tatobjekt anmaßt und dies nach außen erkennbar manifestiert. Das bloße „Zugriff-Verschaffen“ und „Zur-Kenntnisnehmen“ der Daten genügt dazu nicht, vielmehr ist die Speicherung auf einem tätereigenen Datenträger erforderlich. Die Gefährdungslage, die mit Innenangriffen einhergeht, sowie das geschützte Rechtsgut würden dadurch schlüssig abgebildet. Systematisch wäre die Norm bei den §§ 202a ff. StGB zu verorten. Als „Datenveruntreuung“ erfasst sie das Erlangen von Daten entgegen der Zugriffszwecke und die Weitergabe an Dritte durch den Systemadministrator; hierin läge zugleich die taugliche Vortat für die Hehlerei. Dann ist auch umfassend der strafrechtliche Schutz der Datenvertraulichkeit und des Rechts auf informationelle Selbstbestimmung innerhalb von IT-Systemen gewährleistet.

Daul, Sascha*
Cand. jur., Universität Konstanz

DER DIGITALE „DIEBSTAHL“ VON KRYPTOWÄHRUNG – EINE RECHTLICHE EINORDNUNG

I. Einleitung

„GRÖSSTER RAUB DER GESCHICHTE – Unbekannte erbeuten 600 Millionen Dollar Digitalwährung“[1] lautet die Schlagzeile des Online-Portals der Frankfurter Allgemeinen am 11.08.2021 und berichtete über den größten „Diebstahl“, der jemals erfolgt ist. Dieser unglaubliche Akt krimineller Entschlossenheit steht nicht allein. Laut einem Beitrag der Internet World vom 29.10.2020[2] sei es innerhalb des Jahres 2020 zu 330 Cyber-Raubzügen gekommen. Nach einer Analyse des Atlas VPN-Team ist mit einem Schaden von 13,6 Milliarden US-Dollar zu rechnen. Pro Hack seien dabei Kryptowährungen im Wert von bis zu 200 Millionen US-Dollar erbeutet worden. Die „Raubzüge“ haben mit einer Vielzahl anderer erfolgreicher „Kryptodiebstähle“[3] eine Sache gemeinsam: in jedem Fall wurden Kryptowährungen erbeutet und der finanzielle Schaden ist enorm.

Die strafrechtliche Einordnung des zunächst exemplarisch vorzustellenden Tatablaufs scheint dabei bislang offen. Kann das Strafrecht *de lege lata* adäquat auf das realisierte Unrecht reagieren oder bedarf es der Nachbesserung des Gesetzgebers? Im Hinblick auf den ultima-ratio-Grundsatz[4] ist zu fragen, ob das Strafrecht das geeignetste Mittel ist, um diesem sozialschädlichen Verhalten Einhalt zu gebieten. Um keine rein oberflächliche katalogartige Aufführung möglicher einschlägiger Strafnormen vorzulegen, werden im Folgenden Konstellationen ausgeblendet, in denen der Taterfolg mittels *Phishing* erreicht

---

* Sascha Daul ist studentische Hilfskraft am Lehrstuhl von Frau Prof. Dr. Liane Wörner, LL.M. (UW-Madison) und seit dem März 2021 im Projekt DIGICRIMJUS tätig. Er studiert im siebten Fachsemester Rechtswissenschaft an der Universität Konstanz.

1 Siehe https://www.faz.net/aktuell/finanzen/kryptowaehrung-groesster-diebstahl-in-der-geschichte-der-defi-17480530.html, zuletzt abgerufen am 12.2.2022.

2 Siehe https://www.internetworld.de/sonstiges/bitcoin/blockchain-hacker-13-6-milliarden-us-dollar-gestohlen-2600349.html, zuletzt abrufen am 12.2.2022.

3 So sind der rheinland-pfälzischen Polizei im Jahr 2021 Bitcoins im Wert von 36 Millionen „gestohlen“ worden, hierzu: https://www.t-online.de/digital/id_89954924/36-millionen-euro-unbekannte-stehlen-polizei-beschlagnahmte-bitcoins.html, zuletzt abgerufen am 12.2.2022; Im Jahr 2020 wurde der Hamburger coinIX GmbH & Co. KGaA Opfer eines Diebstahls von Bitcoins im Wert von rund 900.000€, hierzu: https://www.fundview.de/posts/2020/10/2020-10-07-coinix-diebstahl-von-bitcoins-kryptowaehrungen-verwahrung-nordix.html, zuletzt abgerufen am 12.2.2022.

4 *Rengier,* Strafrecht Allgemeiner Teil, 13. Aufl. München 2021, § 3 Rn. 5; sowie *Kindhäuser,* Strafrecht Allgemeiner Teil, 8. Aufl. Baden-Baden 2017, § 2 Rn. 8.

wurde, sowie Betrugsstraftaten mittels *Frontrunning,*[5] *Scalping,*[6] und *Wash-Trades*[7] oder *Wash-Sales.*[8] Hier stehen im Mittelpunkt zunächst solche „digitalen Diebstähle", bei denen der Taterfolg mittels eines Hackerangriffs erreicht wurde, und zwar beschränkt auf die Prüfung des objektiven Tatbestands der infrage stehenden Norm.

Nach einer knappen Einführung zu den begriffen (II.) wird eine strafrechtliche Verortung möglich (III.) verbunden mit der Frage, ob neue Lösungswege erforderlich sind (IV.), und einem bewertenden Ausblick (V.).

II. Begriffsbestimmungen und der technische Ablauf der Transaktion

Kryptowährungen gibt es in vielen Formen. Die hier zugrunde gelegte Kryptowährung ist der *bitcoin,*[9] welcher am 3.1.2009 auf der Grundlage des Whitepapers von „Satashi Nakamoto"[10] gegründet wurde.[11] Der *bitcoin* ist jedoch nicht, wie etwa der Euro, als physische Münze zu verstehen. Er besteht nur innerhalb der Blockchain des Bitcoinnetzwerks als Zuordnung.[12] Das Netzwerk ist ein *„peer-to-peer"*-Netzwerk.[13] Die *bitcoins werden peer-to-peer,* also direkt vom Sender an den Empfänger, ohne vermittelnden Dritten, versendet. Es gibt keinen Finanzintermediär,[14] der in irgendeiner Weise eine Kontrolle ausüben kann. Das ist dadurch möglich, dass keine Währungseinheit übertragen wird, sondern das Netzwerk lediglich die Transaktion dokumentiert.[15] Die dokumentierte Transaktion wird in der Blockchain notiert, welche immer weiter fortgeschrieben wird.[16]

Die Blockchain ist eine Kette aus „Transaktionsblöcken".[17] Diese Transaktionsblöcke dokumentieren die Transaktionen von *bitcoins* und ermöglichen deren neuen Zuordnung. Die Integrität der Blockchain wird mittels einer Hash-Verknüpfung bzw. Verkettung ge-

---

[5] HK-KapMarktStrafR/*Zieschang,* 5. Aufl. Baden-Baden 2019, § 263 Rn. 112 ff.

[6] BGH BKR 2004, 74 (75); HK-KapMarktStrafR/*Zieschang* (Fn. 5) § 263 Rn. 147.

[7] *Börner,* Kryptowährungen und strafbarer Marktmissbrauch, NZWiSt 2018, 48 (51).

[8] HK-KapMarktStrafR/*Zieschang* (Fn. 5) § 263 Rn. 174; *Weber,* Konkretisierung des Verbotes der Kurs- und Marktpreismanipulation, NZG 2004, 23 (25).

[9] Folgenden wird die Kryptowährung anhand dem bekanntesten Token – dem Bitcoin – erklärt.

[10] Hierzu: *Nakamoto,* Bitcoin: Ein elektronisches Peer-to-Peer-Bezahlsystem.

[11] *Zöllner,* Kryptowerte vs. Virtuelle Währungen – Die überschießende Umsetzung der Fünften EU-Geldwäscherichtlinie, BKR 2020, S. 117 (117).

[12] Vgl. *Nakamoto* (Fn. 10) S. 2.

[13] Sixt, Bitcoins und andere dezentrale Transaktionssysteme, 2017, S.31; *Baier,* Kriminalpolitische Herausforderung durch Bitcoin und andere Kryptowährungen – Teil 1, CCZ 2019, S. 123 (124).

[14] *Brühl,* Bitcoins, Blockchain und Distributed Ledgers – Funktionsweise, Marktentwicklungen und Zukunftsperspektiven, ZBW 2017/2, 135 (135); Baier (Fn. 13) S. 123 (124).

[15] Siehe Fn. 22.

[16] *Medler,* Sterben 2.0: Erben und Vererben von Kryptowährungen, ZEV 2020, 262 (264); *Armend-Traut/Hergenröder,* Kryptowährung im Erbrecht, ZEV 2019, S. 113 (115).

[17] *Brühl* (Fn. 14) S. 135 (137); *Sixt* (Fn. 13) S. 30; *Börner* (Fn. 7) S. 48 (48); vgl. auch *Skauradszun,* Handels- und steuerrechtliche Bilanzierung von Kryptowerten und Kryptowertpapieren iSv § 1 Abs. 11 S. 4 KWG, § 4 Abs. 3 eWpG-E, DStR 2021, S. 1063 (1064).

wahrt.[18] Um einen neuen Transaktionsblock anzuknüpfen, greift der neue Block auf den bisherigen letzten Block zurück und bindet dessen Hash in den Algorithmus zur Verkettung ein. Mittels dieser Verkettung wird die Richtigkeit der Datensätze gewahrt.

Vereinfacht bedarf es, um in einem Bitcoinnetzwerk teilzunehmen, eines *public key*[19] und eines *private key.*[20]

Beide *keys* sind notwendig, um eine Transaktion vorzunehmen. Der *public key,* auch Bitcoinadresse genannt, dient als öffentliche Adresse, welcher die *bitcoins* zugeordnet werden.[21] Gleichzeitig ist sie das Pseudonym für den Keyinhaber in der Blockchain.[22] Der *private key* dient in einer Transaktion als digitale, nicht-öffentliche Signatur,[23] die nur für den Keyinhaber einsehbar ist. Wird eine Transaktion vorgenommen, signiert der Sender den Transaktionsauftrag mit seinem *private key* und sendet ihn als Hash samt allen weiteren relevanten Informationen an das Bitcoinnetzwerk.[24] Dieses leitet den Auftrag direkt an den Empfänger weiter. Die Empfängeradresse signiert und bestätigt die zu transferierenden *bitocins* mit dem *private key.* Mit der Bestätigung ist die Transaktion vollzogen, die *bitcoins* wurden neu zugeordnet.

III. Strafrechtliche Einordnung des digitalen „Diebstahls"

Der zur rechtlichen Beurteilung bereitstehende Sachverhalt gestaltet sich wie folgt:

Mittels Hackerangriffs[25] dringt der Täter in den Computer des Opfers ein und kopiert den dort hinterlegten *public*- und *private key.* Anschließend begibt sich der Täter auf eine Website, wo er mithilfe der *keys* die mit dem *public key* verbundenen *bitcoins* versenden kann. Er erstellt und sendet einen Transaktionsauftrag an das Netzwerk mit dem Ziel, die *bitcoins* an ein anderes Schlüsselpaar zu senden, welches allein in der Verfügungsgewalt des Täters liegt. Diese Transaktion wird anschließend darauf geprüft, ob der Bitcoinadresse des Senders die zu transferierenden *bitcoins* wirklich zugeordnet sind und insoweit versenden darf. Anschließend bestätigt das Netzwerk die Transaktion als gültig und gliedert sie in seine Transaktionskette ein. Der in alleiniger Verfügungsmacht

---

[18] *Brühl* (Fn. 14) S. 135 (137); vgl. auch *Eschenbruch/Gerstberger,* Smart Contracts – Planungs-, Bau- Immobilienverträge als Programm?, NZBau 2018, 3 (3); Dietsch, Umsatzsteuer 4.0 – wie Blockchain grenzüberschreitende Reihengeschäfte transparenter machen könnte, MwStR 2018, S. 813 (817).

[19] *Sixt* (Fn. 13) S. 9.

[20] Vgl. mit *Safferling/Rückert* Telekommunikationsüberwachung bei Bitcoins – Heimliche Datenauswertung bei virtuellen Währungen gem. § 100a StPO?, MMR 2015, 788 (790).

[21] *Sorge/Krohn-Grimberghe,* Bitcoin: Eine erste Einordnung, DuD 2012, S. 479 (480).

[22] Vgl. *Grzywotz/Köhler/Rückert,* Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention, StV 11/2016, S. 753 (757).

[23] Vgl. *Nakamoto* (Fn. 10) S. 2.

[24] Siehe hierzu: Bericht der Arbeitsgruppe „Digitaler Neustart" des nordrhein-westfälischen Justizministeriums vom 15.4.2019, S. 135; abrufbar unter: https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/index.php, zuletzt abgerufen am: 12.2.2022.

[25] Die Angriffsarten sind so vielfältig, dass sie unter dem allgemeinen Begriff „Hackerangriff" subsumiert werden. In jedem Fall geht es um das Eindringen in ein System gegen den Willen des Systembetreibers.

des Täters stehende *public key* wird damit mit den „versendeten" *bitcoins* verbunden. Damit ist die Tat beendet.[26]

Mangels Sachqualität der *bitcoins* kann diese Tathandlung kein Diebstahl gem. § 242 Abs. 1 StGB darstellen. Auch ein klassischer Betrug i.S.d. § 263 Abs. 1 StGB kann nicht einschlägig sein, der Täter interagiert nicht mit einer Person, sondern mit einem Computer. Infrage kommen dagegen die Betrugsdelikte der §§ 263 ff. StGB, insbesondere der klassische Betrug gemäß § 263 Abs. 1 StGB und der Computerbetrug gemäß § 263a Abs. 1 StGB.

Ein klassischer Betrug gemäß § 263 Abs. 1 StGB scheitert mangels einer Täuschung einer Person. Der Täter interagiert nur mit dem Computer und den *keys*.

III. 1. Computerbetrug gemäß § 263a Abs. 1 StGB

Ein Computerbetrug gem. § 263a Abs. 1 StGB erscheint hingegen denkbar. Der § 263a Abs. 1 StGB enthält vier Tatmodalitäten, wobei die dritte Variante, § 263a Abs. 1 Var. 3 StGB hinsichtlich der Verwendung fremder Daten einschlägig sein könnte. Diese sieht vor, dass der Täter sich oder einen Dritten eines Vermögensvorteils bereichert, in dem er mittels der unbefugten Verwendung von Daten den Datenverarbeitungsprozess beeinflusst und so unmittelbar eine vermögensmindernde „Computerverfügung" auslöst.[27] Eine Tatbegehung nach der ersten Variante scheidet aufgrund fehlender unrichtiger Gestaltung des Programms[28] aus. Die zweite Variante kann ebenfalls nicht einschlägig sein, da der Täter mit den richtigen *keys* arbeitet. Ob die vierte Variant als Auffangtatbestand des § 263a Abs. 1 StGB einschlägig sein könnte, hängt von dem Ergebnis der folgenden Untersuchungen ab und wird nach der Feststellung des Untersuchungsergebnisses erläutert.

III. 1. 1. Daten i.S.d. § 263a Abs. 1 StGB

Der Datenbegriff des § 263a Abs. 1 StGB besteht unabhängig vom Datenbegriff des § 202a Abs. 1 StGB[29] und setzt kodierte Informationen voraus.[30] Die *keys* bestehen aus 27 bis 34 alphanumerischen Ziffern und sind unproblematisch Daten i.S.d. § 263a Abs. 1 StGB.[31]

---

[26] Der hier beschriebene Angriff ist nur eine Variante von vielen. Eine weitere bedeutende Angriffsart ist das Ausnutzen von Fehlern im Code von *smart contracts,* wodurch die Umbuchung von Vermögenswerten auf seine Adresse erfolgt. Der Täter benötigt dabei nicht die Keys der Opfer.

[27] *Rengier,* Strafrecht Besonderer Teil I, 23. Aufl. München 2021, § 14 Rn. 3; ähnlich auch LK-StGB/*Tiedermann/Valerius,* 13. Aufl. 2019, § 263a Rn. 70.

[28] Fischer-StGB/*Fischer,* 69. Aufl. 2022, § 263a Rn. 6; MüKoStGB/*Mühlbauer,* Bd. 9 Teil 1 (§§ 263 – 266b) 12. Aufl. 2012, § 263a Rn. 23.

[29] MüKoStGB/*Mühlbauer* (Fn. 28) § 263a, Rn. 14; BT-Drs. 10/5058 S. 30.

[30] *Wessels/Hillenkamp/Schuhr,* Strafrecht Besonderer Teil 2 – Straftaten gegen Vermögenswerte: Lehrbuch, Entscheidungen, Gesetzestexte, 43. Aufl. Heidelberg 2020, § 14 Rn. 605.

[31] *Sixt* (Fn. 13) S. 37 Abschnitt 4.5.

III. 1. 2. Unbefugt i.S.d. § 263a Abs. 1 Var. 3 StGB

Der Begriff „unbefugt" ist seit Inkrafttreten des § 263a StGB strittig, es besteht nach wie vor keine Einigkeit. Hierzu werden hauptsächlich drei Ansichten vertreten.

III. 1. 2. 1. Subjektivierende Auffassung

So sei nach der subjektivierenden Auffassung die Verwendung von Daten „unbefugt", die dem wirklichen oder mutmaßlichen Willen des über die Daten Verfügungsberechtigten widerspräche.[32] Die Rechtsprechung schloss sich dieser Auffassung vereinzelt an und ließ dann eine Datenverwendung als „unbefugt" gelten, in denen die Verwendung der Daten in der konkreten Fallkonstellation dem mutmaßlichen Willen des Inhabers widerspricht.[33] Wer Inhaber und damit verfügungsberechtigt ist, richtet sich nach zivilrechtlichen Grundsätzen. Eine Inhaberschaft verbunden mit einer Verfügungsberechtigung ist das Eigentum an den Schlüsseln.[34] Die *keys* sind keine Sache, zugleich müsste das Opfer Eigentümer der *keys* gewesen sein, was jedoch mangels Sachqualität der *keys* scheitert. Dies ist für ein Eigentumsrecht nach § 903 BGB notwendig.[35] Der derivative Eigentumserwerb nach § 929 S.1 BGB bedarf neben einer Sache einen bisherigen Eigentümers. Als (Erst-)Eigentümer käme der Betreiber in Betracht. Doch auch hier, sowie beim originären Eigentumserwerb nach § 958 BGB, ist ein Erwerb mangels Sachqualität nicht möglich. Eine analoge Anwendung scheitert am *numerus clausus* des Sachenrechts.[36]

Anzudenken ist den Gewahrsam des Opfers anstelle einer Eigentümerstellung genügen zu lassen. Aus dem Gewahrsam ergibt sich jedoch nicht die notwendige Verfügungsberechtigung, da es möglich ist Gewahrsamsinhaber zu sein, ohne über die Sache verfügen zu dürfen.[37] Ein dinglicher Rechtserwerb eines absoluten Rechts ist nach aktuellem Rechtsstand nicht möglich.

Es müsste daher wie bei der Nutzung eines Girokontos,[38] ein Vertrag zwischen Zahlungsdienstleistender[39] und Zahlungsdienstnutzer[40] geben,[41] welcher die Inhaberschaft der *keys* vertraglich festlegt oder sich aus dem Vertrag durch Auslegung nach §§ 133,

---

[32] RegE BT-Drucks. 10/318, 19; *Lenckner/Winkelbauer,* Computerkriminalität – Möglichkeiten und Grenzen des 2.WiKG (II), CR 1986, 654 (656); Möhrenschlager, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2 WiKG) – Entstehungsgeschichte und Überblick, wistra 1986, 128 (132).

[33] BGH NJW 1995, 669 (670); BayObLG NStZ 1991, S. 343 (344).

[34] Vgl. *Viewger/Werner,* Sachenrecht, 8.Aufl. München 2018, § 2 Rn. 2; oder auch Palandt/*Herrler,* 81. Aufl. München 2022, § 903 Rn. 1, 3.

[35] *Weiss,* Zivilrechtliche Grundlagenprobleme von Blockchain und Kryptowährungen, JuS 2019, 1050 (1054); vgl. BeckOGK/*Lakkis,* (Stand 01.09.2022), BGB § 903, Rn. 2, 3, zuletzt abgerufen am 22.09.2022.

[36] Vgl. Palandt/*Ellenberger,* 80. Aufl. 2021, Überbl. v. § 104 Rn. 16; *Engelhart/Klein,* Bitcoins – Geschäfte mit Geld, das keines ist – Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, S. 355 (357).

[37] Zu den Unterschieden zwischen Eigentum und Gewahrsam siehe BeckOK StGB/*Wittig,* 50. Aufl. 2021, § 242 Rn. 13, zuletzt abgerufen am 12.2.2022.

[38] Zu den besonderen Merkmalen des Girokontos gegenüber einem normalen Konto siehe MüKoBGB/*Grundmann,* Bd. 2 (§ 241 - § 292) 9. Aufl. 2022, § 245 Rn. 101 f.

[39] MüKoHGB/*Herresthal,* Bd. 6 (Bankvertragsrecht), 4. Aufl. München 2019, A. Das Giroverhältnis Rn. 166.

[40] MüKoHGB/*Herresthal* (Fn. 39) Rn. 166.

[41] Siehe der Zahlungsdienstleistungsrahmenvertrag, OLG ZIP 2013, 1855 (1855).

157 BGB[42] ermitteln lässt. Die Generierung eines *public keys* samt zugehöriger *private key* kann in einem Client oder auch über etwaige Websites erfolgen.[43] Dabei werden die *keys* mittels Algorithmus generiert. In keinem der Fälle wird zwischen einem Betreiber des Bitcoinnetzwerks, noch demjenigen, der die *keys* generiert hat, ein Vertragsverhältnis geschlossen. Ein Vertragsschluss scheidet bereits mangels eines Betreiber, der Zahlungsdienstleistender sein kann, aus. Das Bitcoinnetzwerk basiert auf dem Zusammenschluss aller Computer der teilnehmenden Personen. Jeder angeschlossene Computer stellt eine *node* dar,[44] welche ebenso wie alle anderen *nodes* die Blockchain speichert und fortführt.[45] Ein relatives Recht scheidet aus.

Wer Inhaber der *keys* ist, ist mangels vertraglicher oder gesetzlicher Regelung abhängig davon, wer über die *keys* in tatsächlicher Hinsicht verfügt. Wenn mehrere Personen die *keys* haben, kommt jede Person als Inhaber in Frage. Im Falle des Täters, der die *keys* erlangt hat und in tatsächlicher Hinsicht darüber verfügen kann, käme die subjektivierte Auslegung zu dem Ergebnis, dass mangels widerstehenden Willens des Inhabers, welcher sowohl das Opfer als auch der Täter selbst ist, die Verwendung der Daten nicht „unbefugt" ist. Mangels Verfügungsbeschränkung ist jeder ein Inhaber, welcher zur Verfügung und damit zur Verwendung der Daten befugt ist, das Merkmal „unbefugt" mithin nach der subjektivierten Auslegung abzulehnen. Hiernach wäre eine Strafbarkeit nach § 263a Abs. 1 Var. 3 StGB nicht einschlägig.

III. 1. 2. 2. Computerspezifische Auslegung

Eine andere Beurteilung ergibt sich nach der ersten Interpretation der computerspezifischen Auslegung, welche eine Verwendung von Daten als „unbefugt" erkennt, wenn sich der einer Datenverwendung entgegenstehende Wille des Betreibers in der Programmgestaltung niedergeschlagen habe.[46] Das Programm müsse selbst die Befugnis des Verwenders prüfen.[47] Das Bitcoinnetzwerk müsste prüfen, ob der Verfügende mit der Befugnis des tatsächlich Berechtigten handelt. Eine solche Prüfung erfolgt im Regelfall durch die Abfrage von Pins, Passwörtern oder anderen alphanumerischen Zeichenketten.[48]

Ein mögliches Äquivalent zu einem Passwort ist der *private key,* die digitale Signatur. Sie kann die Funktion als Prüfungsinstanz der Befugnis des Verfügenden erfüllen, sofern ihr diese Funktion innerhalb der Transaktion zuteilwird. Der *private key* dient der Verifizierung der Transaktionen.[49] Mit ihm wird die Transaktion signiert und bestätigt so die tatsächliche

---

[42] Vgl. BGH NJW 1973, 1754 (1754); siehe auch MüKoHGB/*Herresthal* (Fn. 39) Rn. 210.

[43] *keys* können in Clients wie „Bitcoin Core" als auch über Websites wie www.bitaddress.org, zuletzt abgerufen am 30.9.2022, generiert werden.

[44] Der Begriff *„node"* ist Englisch und bedeutet „Knoten"; zur Bezeichnung eines Computers als *node* siehe *Rosenberger,* Bitcoin und Blockchain – Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik, S. 19.

[45] *Rosenberger* (Fn. 44) S.19; Baier (Fn. 13) S. 129 (125).

[46] MüKoStGB/*Mühlbauer* (Fn. 28) § 263a Rn. 45; OLG NStZ 1989, 367 (367); Arloth, Computerstrafrecht und Leerspielen von Geldspielautomaten, Jura 1996, S. 354 (357).

[47] *Rengier* (Fn. 27) § 14 Rn. 17; LK-StGB/T*iedermann/Valerius* (Fn. 27) § 263a Rn. 45.

[48] *Rosenberger* (Fn. 44) S. 15.

[49] *Hennecke,* „Darf ich in Bitcoin zahlen" – Geldwäscherisiken für Industrie- und Handelsunternehmen bei Bitcoin-Transaktionen, CCZ 2018, 120 (122); Hildner, Bitcoins auf dem Vormarsch: Schaffung eines regula-

Verfügungsberechtigung des Verfügenden über den infragestehenden *bitcoin*.[50] Zu unterscheiden ist die Art der Prüfung von der Kontrolle der Verfügungsberechtigung bei einem Bankkonto. Im Gegensatz zu einem Bankkonto gibt es bei einer Bitcoinadresse weder einen rechtlich bestimmten Inhaber, noch ist einer innerhalb des Bitcoinnetzwerks aufgrund der Pseudonymität erkennbar. Die Kontrolle einer Verfügungsberechtigung beschränkt sich zwangsläufig allein darauf, dass kein anderer Netzwerkteilnehmer mit seiner Bitcoinadresse einen „fremden" *bitcoin* transferiert. Der oftmals angeführte Vergleich des *private key* mit einem Passwort[51] ist angesichts dessen zu unpräzise. Die Funktion eines Passworts ist die Kontrolle der Zugangs- und der damit einhergehenden Verfügungsberechtigung, welche regelmäßig an eine Identität eines Berechtigten geknüpft ist.[52] An eben dieser Verknüpfung mangelt es bei dem *private key.* Dieser undifferenzierte Vergleich von *private key* und Passwort führt zu unsachgemäßen Ergebnissen, wie der Bejahung einer Prüfung der Verfügungsberechtigung wie sie die erste Interpretation der computerspezifischen Auslegung verlangt.

Denn für das Bitcoinnetzwerk zählt allein, dass die Transaktion vom Inhaber des Schlüsselpaars vorgenommen wird, wer das ist, ist überflüssig. In Frage kommt die Zugriffsberechtigung auf die *wallet,* sofern eine vorhanden ist. Jedoch existiert diese getrennt von dem Bitcoinnetzwerk und dient dem Schutz der *keys* vor der Wegnahme anderer, sowie dazu, die *keys* für den Inhaber zu speichern und gegen Vergessen zu schützen.[53] Das Merkmal „unbefugt" und eine Strafbarkeit ist daher nach der ersten Interpretation der computerspezifischen Auslegung abzulehnen. Die zwei weiteren Interpretationen der computerspezifischen Auslegung bedürfen insoweit keiner eigenen Beurteilung, da sie höhere Anforderungen an die Art des Niederschlags des entgegenstehenden Willen des Programmierers stellen und erst recht eine Strafbarkeit versagen.

III. 1. 2. 3. Betrugsspezifische Interpretation

Nach der dritten Interpretation soll eine von § 263a Abs. 1 Var. 3 StGB erfasste Handlung nur eine solche sein, die, würde nicht lediglich maschinell gesteuerte Geschehensabläufe ausgelöst werden, als Betrug durch täuschungsbedingte Veranlassung der Vermögensverfügung eines anderen zu bewerten wäre.[54] Hierfür spricht vor allem der gesetzgeberische Wille, wonach die Auslegung des § 263a StGB zu dessen Eingrenzung an der Auslegung des § 263 StGB zu orientieren hat.[55] Dies folgt der Stellungnahme des Ausschusses für Wirtschaft vom 23.1.1985, welcher die engere Angleichung an den Ausgangstatbestand des § 263 StGB erreichen wollte.[56]

---

torischen Level Playing Fields?, BKR 2016, S. 485 (488).

[50] Vgl. *Hildner* (Fn. 49) S. 485 (488); oder auch Rückert, Vermögensabschöpfung und Sicherstellung bei Bitcoins, MMR 2016, S. 295 (296).

[51] *Kuhlmann,* Bitcoins, Funktionsweise und rechtliche Einordnung der digitalen Währung, CR 2014, 691 (693); *Hildner* (Fn. 49) S. 485 (488).

[52] I.R.d. § 202a StGB schützt das Passwort gegen unberechtigten Zugang, siehe Fischer-StGB/*Fischer* (Fn. 28) § 202a Rn. 7a f. Berechtigter ist eine identifizierbare Person, denn Anknüpfungspunkt ist die Identität.

[53] Zur Speicherung der keys gegen Vergessen siehe *Andres,* Besteuerung von DLT – Systemen am Beispiel des Bitcoin ohne spezialgesetzliche Grundlage zulässig? DStR 2021, S. 1630 (1631).

[54] BGH StV 2014, 684 (685); vgl. auch Fischer-StGB/Fischer (Fn. 28) § 263a Rn. 11; BGH NStZ 1992, 180 (181) *Rengier* (Fn. 27) § 14 Rn. 19; *Kraatz,* Der Computerbetrug § 263a StGB, Jura 2010, 36, (41).

[55] BT-Drs. 10/5058, S. 30.

[56] BT-Drs. 10/5058, S. 23.

Der Täuschungswert der Handlung solle dann gegeben sein, wenn die Verwendung der Daten gegenüber einem Menschen als fiktive Vergleichsperson einer zumindest schlüssigen Vorspiegelung der Befugnisse entspräche.[57] Mit welcher Prüfungskompetenz diese Vergleichsperson ausgestaltet sein soll, ist umstritten.[58] Der 2. Strafsenat des BGH lehnt im Zusammenhang mit Abhebungen an Geldautomaten ab, für die Täuschungsäquivalenz auf einen fiktiven Bankangestellten abzustellen.[59] Er schloss sich der Ansicht von *Altenhain* an,[60] nach der sich der Vergleich nur auf einen Schalterangestellten beziehen dürfe, der sich mit den Fragen befasse, die auch der Computer prüfe.[61] Dieser Auffassung der Vergleichsperson wird mit der Kritik entgegengetreten, dass ein Schalterangestellter, der nur die im Programm enthaltenen Prüfungsschritte beachten solle, in Wahrheit zur computerspezifischen Meinung führe.[62] Die Bestimmung der Täuschungsähnlichkeit müsse ohne Rückgriff auf den Empfängerhorizont einer wirklichen Person erfolgen.[63] Dies leuchtet ein, denn eine Beschränkung der Prüfungskompetenz der Vergleichsperson auf nur das, was der Computer prüft, würde den Unterschieden eines Menschen und einer Maschine nicht gerecht werden. Was ein Computer in den in seinem Programm enthaltenen Prüfungsschritten prüft, kann ein Mensch an dessen Stelle oftmals gar nicht nachvollziehen. Es ist darauf abzustellen, welchen Zweck die Kontrolle verfolgt und auf Basis dieses Wissens die Prüfungskompetenz der Vergleichsperson zu konstruieren, die sich vom Zweck her auf die gleiche Prüfung wie das Programm beschränkt, funktional aber anders ausgestaltet ist.[64]

Wenn eine Transaktion im Bitcoinnetzwerk ausgeführt werden soll, prüft die Blockchain, ob der *private key* zu dem *public key* passt. Zweck dieser Prüfung ist es, sicherzustellen, dass nur derjenige eine Transaktion durchführen kann, der die zueinander gehörenden *keys* verwendet. Im weiteren Sinne soll damit geprüft werden, dass der *bitcoin* tatsächlich dem *public key* zugeordnet ist, mit welchem eine Transaktion ausgeführt werden soll. Nur der Inhaber des passendes *keys* kann eine Signatur erzeugen.[65] Diese Prüfung dient dem Erhalt der Integrität der Blockchain. Von einer Prüfung der Verfügungsberechtigung im zivilrechtlichen Sinne, also der Verfügungsberechtigung des Verfügenden über die dem *public key* zugeordneten *bitcoins,* kann nicht die Rede sein. Die Anwendung einer Ver-

---

[57] *Rengier* (Fn. 27) § 14 Rn. 19; vgl. auch BGH NJW 2002, 905 (906); *Zielinski,* Anmerkung zum Urteil des BGH, Beschl. v. 10.11.1994 – 1 StR 157/94 (AG Nördlingen), NStZ 1995, S. 345 (347).

[58] Zum Meinungsstand siehe *Mühlbauer,* Die Betrugsähnlichkeit des § 263a Abs.1 Var. 3 StGB anhand der „Geschäftsgrundlagen" beim Geldautomatengebrauch, wistra 2003, 244 (245).

[59] BGH NJW 2002, 905 (906), ergänzend die Anmerkung von *Martin,* Anmerkung zu BGH, Beschluss vom 21. 11. 2001 – 2 StR 260/01, JuS 2002, S. 506 (507).

[60] Siehe BGH NJW 2002, 905 (906), mit Verweis auf *Altenhain,* Der strafbare Mißbrauch kartengestützter elektronischer Zahlungssysteme, JZ 1997, 752 (758).

[61] *Altenhain* (Fn. 60) S. 752 (758); Kritisch *Mühlbauer* (Fn. 58) S. 244 (249); MüKoStGB/*Mühlbauer* (Fn. 28) § 263a Rn. 46.

[62] *Mühlbauer* (Fn. 58) S. 244 (249); Lackner/Kühl/*Heger,* 29. Aufl. 2018, § 263a Rn. 13.

[63] *Rengier* (Fn. 27) § 14 Rn. 22.

[64] Vgl. *Mitsch,* Strafrecht Besonderer Teil 2 – Vermögensdelikte (Randbereich) / Teilband 2, Berlin/Heidelberg 2001, § 3 Rn. 21; *Kindhäuser/Böse,* Strafrecht Besonderer Teil II – Straftaten gegen Vermögensrechte, 11. Aufl. Baden-Baden 2021, § 28 Rn. 25.

[65] *Kütük/Sorge,* Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie" zur „Bitcoinmanie", MMR 2014, S. 643 (643).

gleichsperson scheitert daher bereits an einer der Kontrolle der Verfügungsberechtigung gleichkommenden Prüfungsinstanz im Bitcoinnetzwerk.

III. 1. 2. 4. Auffangtatbestand des § 263 Abs. 1 Var. 4 StGB

Die tradierten Auslegungen des Begriffs „unbefugt" eröffnen damit keine Lösung für die Kryptowährung *bitcoin* und begründen keine Strafbarkeit nach der dritten Variante.

Aushelfen könnte die vierte Variante des § 263a Abs. 1 StGB – mit „sonstige unbefugte Einwirkung" – Abhilfe verschaffen. Sie erfasst alle übrigen Maßnahmen, die nicht in den Varianten eins bis drei enthalten sind. Abgezielt wird auf Hardware-, Konsol- und Outputmanipulationen und deren nicht vorhersehbaren Vorgehensweisen.[66] Doch auch diese Handlungen müssen unbefugt erfolgen, was aus den gleichen Gründen abzulehnen wäre.

III. 1. 2. 5. Der Grund der Unanwendbarkeit des § 263a Abs. 1 Var. 3 StGB

Die Unanwendbarkeit des § 263a Abs. 1 Var. 3 StGB ist auf die systematische und rechtliche Ausgestaltung des bisherigen zentralen Transaktionssystems und dessen Unterschiede zu dem neuen, dezentralen Transaktionssystem unter Berücksichtigung der Entstehungsgeschichte des § 263a Abs. 1 Var. 3 StGB zurückzuführen. Mit dem zweiten Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 15. 5.1986 wurde der § 263a StGB in das Strafgesetzbuch eingeführt.[67] Zweck dieser Einführung war es, eine Strafbarkeitslücke des § 263 StGB, ausgelöst durch eine neue Manipulationsform, die sich gerade dadurch auszeichnet, dass ein Mensch nicht getäuscht und zu einer vermögensschädigenden Vermögensverfügung veranlasst wird, zu schließen.[68] Der § 263a StGB wurde bewusst als Sondertatbestand in das Strafgesetzbuch eingefügt. Von einer Änderung des § 263 Abs. 2 StGB wurde aufgrund der Besonderheiten des Computerbetrugs abgesehen. Stattdessen wurde der § 263a StGB in starkem Bezug zu § 263 StGB konzipiert.[69]

Alle gesetzgeberischen Erwägungen basieren auf dem Verständnis eines zentralen Finanzsystems. Diese zeichnen sich dadurch aus, dass es Intermediäre wie Kreditinstitute gibt, welche als Kontrollinstanz für jegliche finanzenbezogene Handlung dienen. Um in einem zentralen Finanzsystem teilzunehmen, bedarf es eines Bankkontos. Das Sender- oder Empfängerkonto muss nicht beim gleichen Kreditinstitut eingerichtet sein, um die Zahlungsdienstleistung in Anspruch nehmen zu können,[70] es muss aber in jedem Fall ein Konto vorliegen. Durch einen Vertrag gem. § 675f Abs. 2 BGB wird der Kontoinhaber, welcher zugleich Inhaber der Guthabenforderung ist, festgelegt.[71] Die Notwendigkeit eines festgelegten Kontoinhabers führt zu einem Klarnamenzwang, wodurch Transaktionen immer

---

[66] Vgl. MüKoStGB/*Mühlbauer* (Fn. 28) § 263a Rn. 88; BT-Drs. 10/318, S. 20; BT-Drs. 10/5058, S. 30.

[67] Siehe Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) vom 23. Mai 1986 (BGBl. I S. 721).

[68] Stellungnahme im öffentlichen Ausschuss, BT-Drs. 10/5058 S. 30.

[69] Vgl. BT-Drs. 10/5058 S. 23, der Ausschuss für Wirtschaft vom 23.Januar.1985 bittet den Rechtsausschuss die engere Angleichung des § 263a StGB an den Ausgangstatbestand des § 263 StGB zu ermöglichen; vgl. auch *Mühlbauer* (Fn. 58) S. 244 (246).

[70] Überweisungen werden seit 2008 im Interbankverhältnis abgewickelt, siehe MüKoHGB/*Häuser,* B. Überweisungsverkehr Rn. 408.

[71] BGH NJW 1988, 709 (709 f.); BGH NJW 1994, 931 (931); BGH NJW 1973, 1754 (1755).

zurechenbar sind. Dies sorgt neben Rechtssicherheit zugleich dazu, dass es für kriminelle Geschäfte keine offensichtliche Möglichkeit gibt, Zahlungsverläufe zu vertuschen.

Gegenläufig hierzu sind die dezentralen Finanzsysteme konzipiert. Dezentrale Finanzsysteme wollen sich von den Ketten eines Intermediären lösen und ohne Zwischenmann auskommen. Sie basieren auf einem *peer-to-peer*-Netzwerk und können so die Kryptowerte direkt transferieren und auf einen Intermediär verzichten. Dabei wird auf eine Referenzadresse gesetzt welche für den Einzelnen als Pseudonym dient. Zwar ist das Transaktionsregister ein öffentliches Register,[72] durch das Pseudonym sind die Transaktionen jedoch nicht unmittelbar einer Person zurechenbar, sofern keine Referenzadresse bekannt ist. Dies führt dazu, dass Transaktionen zwar nachvollziehbar sind, aber die Zurechenbarkeit dieser nur in seltenen Fällen möglich ist.[73] Das notwendige Vertrauen in die Legitimität des Transaktionserfolg wird bei dezentralen Finanzsystemen aus der Blockchaintechnologie gezogen. Die Integrität der Blockchain ergibt sich aus der Verifizierung jeder einzelnen Transaktion, eine Aufgabe, die sonst der Intermediär wahrnehmen würde. Zum Zeitpunkt der Erlassung des § 263a Abs. 1 Var. 3 StGB kannte die Welt nur das zentrale Finanzsystem. Die Konzipierung des § 263a Abs. 1 Var. 3 StGB ist zwangsläufig durch die Funktionsweise eines Bankautomaten und im weiteren Sinne den strukturellen Gegebenheiten eines zentralen Währungssystems geprägt.

Ausgehend von zentralen Finanzsystemen, führt die Auslegung des § 263a Abs. 1 StGB an dezentralen Finanzsystemen zwangsläufig zu Problemen.

Die Auslegung anhand einer Verfügungsbefugnis, welche wohl der Zuordnungsfähigkeit von Konten so wie Transaktionen innerhalb des zentralen Finanzsystems entspringt, scheitert bei dezentralen Finanzsystemen an einem absoluten oder relativen Recht[74] bezüglich der Bitcoinadresse und deren *bitcoins*. Dies hat zugleich zur Folge, dass eine Prüfungskompetenz des Prüfungsmoduls des dezentralen Systems nicht die Verfügungsberechtigten des Einzelnen enthält.

Es ist bereits verfehlt, die Orientierung anhand eines Bankautomatens bei der Auslegung des Begriffs „unbefugt“vorzunehmen, da dessen Funktionsweise sich grundlegend von der eines dezentralen Systems unterscheidet. Es wäre falsch, künstlich eine Person in den Prozessablauf einer Transaktion einzubeziehen, wenn das System, welches die Transaktion vornehmen soll, sich gerade dadurch auszeichnet, nur die Integrität der Blockchain bewahren zu wollen und bewusst auf Personendaten verzichtet.

Weder funktional noch rechtlich sind die die beiden Transaktionssysteme vergleichbar. Infolgedessen scheitert eine Anwendung des § 263a Abs. 1 Var. 3 StGB im Fall von Transaktionen in dezentralen Transaktionssystemen.

III. 1. 3. Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs

Trotz der Unanwendbarkeit der dritten Variante des § 263a Abs. 1 StGB mangels unbefugter Verwendung von Daten bleibt die generelle Anwendbarkeit des Straftatbestandes auf

[72] Vgl. *Kleinert/Mayer,* Elektronische Wertpapiere und Krypto-Token – Aktuelle Rechtslage und die Blockchain-Strategie der Bundesregierung vom 18.9.2019, EuZW 2019, S. 857 (858).

[73] Vgl. *Sorge/Krohn-Grimberghe* (Fn. 21) S. 479 (480); *Fill/Meier,* Blockchain kompakt – Grundlagen, Anwendungsoptionen und kritische Bewertung, Wiesbaden 2020, Blockchain kompakt, S. 33.

[74] Vgl. *Engelhart/Klein* (Fn. 36) S. 355 (357); *Goger,* Bitcoins im Strafverfahren – Virtuelle Währung und reale Strafverfolgung, MMR 2016, 431 (432); *Kütük/Sorge* (Fn. 65) S. 643 (645).

dezentrale Transaktionssysteme fraglich. Durch das Absenden des Transaktionsauftrags an das Bitcoinnetzwerk durch den Täter, löst dieser eine Datenverarbeitung dahingehend aus, dass das Netzwerk die zur Transaktion bereitstehenden *bitcoins* neu zuordnet. Diese Transaktion gestaltet sich aufgrund der dezentralen Konzipierung des Netzwerks als eine Vielzahl an simultan ablaufenden Datenverarbeitungen an jeder *node*. Diese ausgelösten Datenverarbeitungen stehen in Tateinheit zueinander.

III. 1. 4. Vermögensschaden

Die Neuzuordnung der *bitcoins* an die Bitcoinadresse des Täters müsste sich als Schaden im Vermögen des Opfers niederschlagen. Während sich bei durch *Phishing* erlangten Kontodaten der Schaden i.d.R. bei der Bank niederschlägt,[75] ist im Falle eines digitalen „Diebstahls" der Schadensniederschlag regelmäßig unmittelbar beim Bitcoinadressinhaber. Im Gegensatz zu zentralen Währungssystemen wie dem Euro entstehen hier Unsicherheiten, ob ein Vermögensschaden vorliegt und wenn ja, wie dieser zu bestimmen ist. Dem Euro wird durch die Europäische Zentralbank ein Wert zugeordnet.[76] Dem *bitcoin* wird dagegen von keinem Institut ein fester Wert zugemessen. Der Vermögensschaden bei Kryptowährungen hängt von der zivilrechtlichen Natur der Kryptowährungen, die Bestimmbarkeit eines Vermögensschadens und die Frage, ob Kryptowährungen überhaupt als Teil des geschützten Vermögens gelten, ab.

III. 1. 4. 1. Zivilrechtliche Einordnung der Kryptowährung

Die Bestimmung eines Vermögenschadens wird maßgeblich von der Rechtsnatur der infragestehenden Einheit bestimmt. Es ist festzuhalten, dass Kryptowährungen jedenfalls keine Sachqualität aufweisen. Damit ist die Rechtsnatur des *bitcoins* als Kryptowährung aber noch nicht geklärt. Als nächste Werteinheit des alltäglichen Lebens kommt die Einordnung als Geld i.S.d. BGB in Betracht. Das BGB definiert das Geld zwar nicht positiv. Es herrscht jedoch Einigkeit darüber, dass Kryptowährungen nicht in die klassische Kategorien von Geld fallen.[77]

Eine Einordnung als Buchgeld ist hingegen nicht undenkbar. Der Rechtscharakter des Buchgelds bestimmt sich durch das Einräumen eines Rückzahlungsanspruchs durch ein Kreditinstitut gegen eine Einzahlung.[78] Die Höhe der Forderungen wird in seinem Konto angezeigt. Bei *bitcoin* werden die mit der Bitcoinadresse verbundenen *bitcoins* als Summe auf der Nutzeroberfläche angezeigt. Eine gewisse Ähnlichkeit ist daher nicht von der Hand zu weisen. Die Einordnung als Buchgeld scheitert aber letztlich an einer Forderung gegen ein Kreditinstitut.[79] Ein Recht auf Auszahlung ist ebenso nicht gesetzlich normiert.

---

[75] Fischer-StGB/*Fischer* (Fn. 28) § 263a Rn. 22; *Lenckner/Winkelbauer* (Fn. 32) S. 654 (659 f.).

[76] Im Euro-Währungsraum ist die EZB für die Preisstabilität des Euros verantwortlich, siehe Art. 127 I S.1 AEUV.

[77] *Weiss* (Fn. 35) S. 1050 (1055); *Omlor,* Digitaler Zahlungsverkehr, JuS 2019, 289 (290).

[78] Schimansky/Bunte/Lwowski/Haug, Bankrechts-Handbuch, Bd.1, 5. Aufl. München 2017, BankR-HdB § 123 Rn. 52.

[79] Zum fehlenden Forderungsschuldner und dessen Folge, siehe *Rückert* (Fn. 50) S. 295 (296); *Kütük/Sorge* (Fn. 65) S. 643 (644).

Die *bitcoins* sind damit forderungsfrei und nur reiner tatsächlicher Natur.[80] Es gibt nur die Verfügungsbefähigung durch die Verfügungsmacht über die *keys*.

Die gleiche Argumentation ist auch gegen eine Einordnung als E-Geld im Sinne des § 1 Abs. 2 S. 3 ZAG anzubringen. Diese Einordnung scheitert vor allem an einem Emittenten.[81] Einen greifbaren Charakter verleiht die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und ordnet den *bitcoin* nach § 1 Abs. 11 S. 1 Nr. 7 KWG als Rechnungseinheit ein.[82] Zugleich sind sie durch die Änderungen vom 1.1.2020 auch Kryptowerte nach § 1 Abs. 11 S. 1 Nr. 10 KWG.[83]

Bitcoins werden auch als virtuelle Währung eingeordnet. Nach der europäischen Bankaufsichtsbehörde (EBA) werden virtuelle Währungen als digitale Abbildung von Wert, der nicht von einer Zentralbank oder Behörde geschaffen wird und auch keine Verbindung zu gesetzlichen Zahlungsmitteln haben muss, verstanden.[84] Diese Einordnung verleiht der Kryptowährung zwar keine weiteren juristischen Konturen, es lässt aber die Schlussfolgerung zu, dass auch einer virtuellen Währung ein Wert zukommt.

III. 1. 4. 2. Bestimmbarkeit des Vermögensschadens

Der Wert der Währung hängt vom Vertrauen der einzelnen Investierenden in die Währung ab. Dies hat bereits in der Vergangenheit zu hohen Wertschwankungen geführt.[85] In einer Warnmeldung der ESMA, EBA und EIOPA wird auf die hohe Volatilität von virtuellen Währungen wie *bitcoin, Ripple* und *Ether* hingewiesen.[86] So soll der Wert eines *bitcoins* im Jahr 2017 stark von 1.000€ auf 16.000€ angestiegen sein, jedoch kurz danach wieder um 70% auf 5.000€ gesunken sein.[87] Es ist unklar, inwieweit die Volatilität und die damit verbundenen positiven sowie negativen Kursentwicklungen Einfluss auf den Vermögensschaden nehmen.

---

[80] *Boehm/Pesch,* Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung, MMR 2014, 75 (77); *Kütük/Sorge* (Fn. 65) S. 643 (644).

[81] *Schlund/Pongratz,* Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, DStR 2018, 598 (599 f.); Baier (Fn. 13) S. 123 (125); *Auffenberg,* E-Geld auf Blockchain-Basis, BKR 2019 (341).

[82] *BaFin,* Merkblatt „Hinweise zu Finanzinstrumenten nach § 1 XI Sätze 1 bis 5 KWG“, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111220_finanzinstrumente.html, zuletzt abgerufen am 12.2.2022.

[83] Siehe Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie vom 12 Dezember 2019 (BGBl. I S.2602).

[84] Die Europäische Bankaufsichtsbehörde warnt vor den Gefahren von virtuellen Währungen, zu welchen sie auch den Bitcoin zählt, EBA/WRG/2013/01, abrufbar unter: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/598344/b99b0dd0-f253-47ee-82a5-c547e408948c/EBA%20Warning%20on%20Virtual%20Currencies.pdf?retry=1, zuletzt abgerufen am 12.2.2022.

[85] EBC, Virtual currency schemes – a further analysis, S. 23, abrufbar unter: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf, zuletzt abgerufen am 12.2.2022.

[86] Warnmeldung, ESMA, EBA und EIOPA warnen die Verbraucher vor Risiken virtueller Währungen (Virtual Currencies, VC), S. 1, abrufbar unter: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2150185/def1ade8-9ce9-4f6f-a296-01d778c86afb/Joint%20ESAs%20Warning%20on%20Virtual%20Currencies_DE.pdf?retry=1, zuletzt abgerufen am 12.2.2022.

[87] Siehe den Kursverlauf an der Bitstampbörse unter: https://bitcoincharts.com/charts/bitstampUSD#rg360zczsg2017-01-01zeg2018-01-31ztgSzm1g10zm2g25zv, zuletzt abgerufen am 12.2.2022.

Grundsätzlich folgt die Schadensberechnung dem Prinzip der Gesamtsaldierung.[88] Der Schaden ist die Differenz zwischen dem Vermögen vor und nach der Vermögensverfügung.[89] Durch die Transaktion wurden *bitcoins* von der Bitcoinadresse des Opfers an eine andere Adresse zugeordnet. Diese *bitcoins* besitzen einen Wert, welcher dem Opfer entzogen wurde. Es ist unklar, an welchen Zeitpunkt im Tatablauf zur Bestimmung des Schadens anzuknüpfen ist.

Nachträgliche Werterhöhung oder -minderung nach der Beendigung der Tat haben keinen Einfluss auf dessen Vollendung. Der Täter kann sich später nicht darauf berufen, die Währung sei bereits wertlos geworden, weswegen dem Opfer kein Vermögensschaden entstanden sei.[90] Im Umkehrschluss ist dem Täter eine Wertsteigerung bei der objektiven Ermittlung eines Vermögensschaden nicht anzulasten. Mit Hinblick auf die starken Schwankungen erscheint es am sinnigsten, an den Zeitpunkt des Absendens des Transaktionsauftrags anzuknüpfen, da der Kurswert zu diesem Zeitpunkt regelmäßig dem Täter bekannt ist und so auch von dessen Vorsatz umfasst ist.

III. 1. 4. 3. Sind bitcoins Teil des geschützten Vermögens?

Als geeignetes Tatobjekt zur Verwirklichung eines Vermögensschadens müssten *bitcoins* dem geschützten Vermögen des Opfers zuzuordnen sein. Mangels rechtlicher Ausgestaltung gibt es keine rechtlichen, sondern nur rein tatsächliche Bezugspunkte, die eine Zuordnung der *bitcoins* als Teil des Vermögens des Opfers möglich machen. Dem vorzugswürdigen[91] juristisch-ökonomische Vermögensbegriff[92] nach zählt zum geschützten Vermögen jedes Einzelnen alle wirtschaftlich wertvollen, also geldwerten Güter einer Person, welche im Einklang mit der Rechtsordnung stehen.[93] Dabei ist es verfehlt, bei der Bewertung eines Vermögensschadens alleinig die Vermögensposition zu berücksichtigen, die einen rechtlichen Rahmen besitzen. Der juristisch-ökonomischen Vermögensbegriff bestimmt negativ, was nicht von diesem erfasst wird. Zugleich kann im Umkehrschluss angenommen werden, dass alles, was nicht im Widerspruch mit der Rechtsordnung steht, schutzwürdig ist. *Bitcoins* sind dem geschützten Vermögen des Opfers zu zurechnen und ein geeignetes Tatobjekt für den Eintritt eines Vermögensschadens.

---

[88] MüKoStGB/*Hefendehl,* § 263 Rn. 530 ff.; Schönke/Schröder/*Perron,* 30. Aufl. München 2019, § 263 Rn. 99.

[89] LK-StGB/*Tiedemann,* § 263 Rn. 161 f.; *Müller-Christmann,* Problematik des Vermögensschadens beim Betrug im Falle eines vereinbarten Rücktrittsrechts – BGH, NJW 1987, 388, JuS 1988, 108 (113), *Satzger,* Probleme des Schadens beim Betrug, Jura 2009, 518 (521).

[90] Vgl. *Ungern-Sternberg,* Wirtschaftskriminalität beim Handel mit ausländischen Aktien, ZStW 86 (1976), S. 653 (689).

[91] Siehe zur Vorzugswürdigkeit des juristisch-ökonomischen Vermögensbegriffs LK-StGB/*Tiedemann* (Fn. 89) § 263 Rn. 132 sowie *ders.*, Vor § 263 Rn. 31.

[92] NK-StGB/*Kindhäuser,* 5. Aufl. Baden-Baden 2017, § 263 Rn. 30; MüKoStGB/*Hefendehl* (Fn. 88) § 263 Rn. 383; LK-StGB/*Tiedemann* (Fn. 89) § 263 Rn. 132; Lackner/Kühl/*Kühl,* § 263 Rn. 33. Esser/Rübenstahl/Saliger/Tsambikakis/*Saliger,* Wirtschaftsstrafrecht, München 2017, § 263 StGB, Rn. 129.

[93] Schönke/Schröder/*Perron,* § 263 Rn. 82; NK-StGB/*Kindhäuser* (Fn. 92) § 263 Rn. 30; MüKoStGB/*Hefendehl* (Fn. 88) § 263 Rn. 383; Lackner/Kühl/*Kühl* (Fn. 92) § 263 Rn. 33.

III. 1. 5. Ergebnis

Nach dieser ausführlichen Untersuchung des digitalen „Diebstahls“ unter dem Straftatbestand des Computerbetrugs, wird man nach den derzeit vertretenen Auffassungen zu dem Ergebnis kommen müssen, eine Strafbarkeit zu verneinen. Mangels einer rechtlichen Ausarbeitung des Rechtsverhältnisses zwischen dem Inhaber und den *keys* sowie den der Bitcoinadresse zugeordneten *bitcoins*, kann eine rechtlich begründbare Befugnis, sowie der Mangel dessen, nicht festgestellt werden und führt zur Unanwendbarkeit der Norm auf dezentrale Transaktionssysteme.

III. 2. Sonstige Delikte

Eine Strafbarkeit nach § 270 StGB könnte angedacht werden, ist jedoch mangels Garantiefunktion – der Pseudonymität des Netzwerks verschuldet – der Blockchain abzulehnen.

Eine Strafbarkeit wegen Datenveränderung gem. § 303a Abs. 1 StGB könnte aufgrund der Verwendung der *keys* zur Transaktion einschlägig sein. § 303a Abs. 1 StGB schützt die Verfügungsgewalt des Berechtigten über die in Datenspeichern enthaltenen Informationen.[94] Es ist genau zu differenzieren, was durch die Transaktion verändert wurde. Durch die Transaktion wurden nicht die *key*-Daten, sondern die Anzahl der der Bitcoinadresse zugeordneten *bitcoins* verändert. Das unerlaubte Kopieren der *key* stellt keine Veränderung i.S.d. § 303a Abs. 1StGB dar.[95] Das Merkmal „berechtigt“ führt auch hier zu Problemen. Es treten die gleichen Schwierigkeiten wie bei dem Merkmal „unbefugt“ des § 263a StGB auf, weswegen eine berechtigte Person nicht bestimmt werden kann. Zu erwähnen ist auch, dass die Veränderung der Anzahl der *bitcoins* eine Veränderung der Blockchain darstellt – welche niemandem gehört – und keine direkte Manipulation eines Kontostands.[96] Eine Strafbarkeit nach § 303a Abs. 1 StGB ist klar abzulehnen.

Allerdings hat der Täter durch den Hackerangriff auf den Computer des Opfers sich unbefugt Zugang zu den *keys* verschafft und so den Tatbestand des § 202a Abs. 1 StGB erfüllt.

IV. Reicht unser aktuelles Recht aus?

Ist der Täter nach dem vorgegeben Tatablauf somit lediglich des Ausspähens von Daten nach § 202a Abs. 1 StGB strafbar, bleibt die Frage, ob es daneben einer weiteren Sanktionierung des digitalen „Diebstahls“ bedürfte.

---

[94] BT-Drs. 10/5058, S. 34; vgl. BGH NStZ 2018, 401 (403).

[95] Vgl. LK-StGB/*Wollf,* § 303a Rn. 29; StGB/Heintschel-Heinegg/*Weidemann,* 3.Aufl. München 2018, § 303a Rn. 14.

[96] *Grzywotz/Köhler/Rückert* (Fn. 22) S. 753 (754).

IV. 1. Pönalisierungsbedarf

Die eingangs genannten Schadenssummen allein geben einen deutlichen Impuls, das Verhalten strafrechtlich zu sanktionieren. Bestärkt wird der Bedarf durch die Unmöglichkeit einen zivilrechtlichen Rückforderungsanspruch festzustellen und durchzusetzen. Aufgrund der Pseudonymität des Bitcoinnetzwerks bleibt es sehr schwierig, die Identität der Person „hinter dem Computer" festzustellen. Zwar werden Methoden erarbeitet, wie man die IP-Adresse des Empfängers der bitcoins ausfindig machen kann.[97] In den meisten Fällen scheitert die Methode aber an der Verwendung des Tor-Netzwerks oder eines anderen VPN-Anbieters, welches die Ermittlung der IP-Adresse eines Computers im Netz praktisch unmöglich macht.[98] Gerichtlich erwirkte und vollstreckbare Titel können mangels durchführende zentrale Institution nicht mit Zwang durchgesetzt werden. Einen funktionierenden zivilrechtlichen Rechtsschutz gibt es nicht. Das Strafmaß des § 202a Abs. 1 StGB reicht angesichts der niedrigen Sanktion von maximal drei Jahren nicht aus, um Täter von Anschlusstaten abzuschrecken. Zugleich dient der Strafrahmen des § 202a Abs. 1 StGB nicht der Sanktionierung von Vermögensschäden, sondern nur der Sanktionierung von Verstößen gegen das formelle Datengeheimnis.[99] Der Schutz des Vermögens, welches hinter den *keys* steht, wird damit derzeit im deutschen Strafrecht nicht durch ein gesondertes Vermögensdelikt garantiert. Der Gesetzgeber ist angehalten, mittels Strafnormen der Ausnutzung dezentraler Systeme und den hierdurch verursachten Vermögensschäden entgegenzusteuern.

IV. 2. Eine fünfte Variante des § 263a Abs. 1 StGB?

Als eine Möglichkeit der Sanktionierung kommt die Erweiterung des § 263a Abs. 1 StGB mit einer fünften Variante in Betracht. Diese fünfte Variante müsste so ausgestaltet sein, dass sie auch Konstellationen erfasst, in denen die Vermögenszuordnung allein tatsächlicher Natur erfolgt. Nur so kann die Verwendung der Daten adäquat sanktioniert werden. Man kann hierzu an die bis dato vorliegende Stellung des Opfers als alleiniger Gewahrsamsinhaber der *keys* anknüpfen und die Verwendung von Daten bestrafen, die zuvor im alleinigen Gewahrsam eines anderen waren, wobei die Verwendung auch gegen den Willen des zu vorigen alleinigen Gewahrsamsinhaber erfolgen muss. Um ähnliche Problematiken zu vermeiden, wie sie i.R.d. Sachbegriffs des BGB auftreten, ist erforderlich, den bisherigen Gewahrsamsbegriff zu überdenken und ihn losgelöst von einer Sache zu definieren.

Gegen eine fünfte Variante des § 263a Abs. 1 StGB sprechen tatbestandliche Subsumtionsprobleme. So scheint der Gesetzgeber bei der Bestimmung des Tatbestandmerkmals „Beeinflussung einer Datenverarbeitung" davon ausgegangen zu sein, dass es nur einen Datenbankwert gibt, welcher durch den Computerbetrug verändert werden soll. Das Auslösen einer Massendatenverarbeitung wie sie in einem dezentralen Netzwerk auftritt, ist nicht vorgesehen. Dies führt dazu, dass das Delikt als mehrfach begangen erscheint, wobei

---

[97] Siehe hierzu: *Biryukov/Khovratovich/Pustogarov,* Deanonymisation of clients in Bitcoin P2P network, abrufbar unter https://arxiv.org/abs/1405.7418, zuletzt abgerufen am 12.2.2022.

[98] *Brühl* (Fn. 14) S. 135 (140).

[99] MüKoStGB/*Graf,* § 202a Rn. 2.

sich dessen Anzahl nach der Anzahl von *nodes* im Netzwerk richtet. Es wäre sinnvoller, einen neuen Tatbestand zu konzipieren, der die Datenveränderung nicht allein durch das Ingangsetzen bejaht, sondern erst dann als erfolgt gilt, wenn das Netzwerk die Transaktion verifiziert. So könnte man zwischen dem Versuch und dem tatsächlichen Erfolg sachgerechter differenzieren.

Gegen eine fünfte Variante sprechen auch systematische Bedenken. Der § 263a Abs. 2 StGB eröffnet die § 263 Abs. 2-6 StGB auch für Computerbetrüge und gibt dadurch Raum für einen besonders schweren Fall des Computerbetrugs. Nach § 263 Abs. 3 Nr. 2 Var. 1 StGB soll ein besonders schwerer Betrug vorliegen, wenn ein Vermögensverlust großen Ausmaßes herbeigeführt wurde. Schaut man sich an dieser Stelle das Jahr 2020 erneut an, so kann man bei Vermögensverfügungen pro Hack in Höhe von circa 200 Millionen nicht umhinkommen, in jedem Fall einen besonders schweren Fall des Computerbetrugs zu sehen. Der Strafrahmen des Grunddelikts von bis zu fünf Jahren oder Geldstrafe verschöbe sich mithin nahezu dauerhaft zu einem Strafrahmen von sechs Monaten bis zu zehn Jahren. Denn die Bewertung als besonders schwerer Fall orientiert sich am Durchschnitt gewöhnlich vorkommender Fälle des Delikts und soll die besondere Strafwürdigkeit der schulderhöhenden Faktoren der Straftat unterstreichen.[100] Es wäre nicht zurechtfertigen, wieso ein Vermögensschaden in Höhe von 200 Millionen keinen besonders schweren Fall darstellen sollte. Zu berücksichtigen ist freilich, dass den Regelbeispielen des § 263 Abs. 3 StGB lediglich eine Indizwirkung zukommt,[101] welche auch abgelehnt werden kann.[102] Ob das in jedem Fall vorgenommen werden sollte, um der ansonsten drohende Zweckentfremdung der besonders schweren Fälle entgegenzusteuern, ist aber fraglich.

IV. 3. Ein neuer Tatbestand: der § 263b StGB

Sollte sich der Gesetzgeber für einen neuen Straftatbestand entscheiden, muss dieser die Besonderheiten der dezentralen Systeme auch adäquat reflektieren. Dazu gehört auch, dass der Gesetzgeber bei der Konzipierung der Strafnorm anerkennt, dass er damit konfrontiert ist, strafwürdiges Handeln in einem Raum zu sanktionieren, in dem er unmittelbar keine Kontrolle ausüben kann.

Die Konzipierung einer eigenen Strafnorm, etwa als § 263b StGB, hat ihrerseits unter Berücksichtigung der aktuellen Problemen der Strafverfolgung in dezentralen Systemen zu erfolgen. Tatbestandlich wäre es zu empfehlen, von dem Konzept einer befugten Person Abstand zu nehmen und an den § 202a Abs. 1 StGB als vorbereitenden Tatbestand anzuknüpfen. Als Schutzgut des § 263b StGB kommt neben dem Vermögen als zentrales Element eines dezentralen Netzwerks die Integrität der Blockchain in Betracht. Durch Konzipierung als Anknüpfungsdelikt an den § 202a Abs. 1 StGB würde sich der § 263b StGB sowohl als Vermögensdelikt als auch als ein Datendelikt gestalten.

---

[100] Vgl. der höhere Unrechts- und Schuldgehalt eines besonders schweren Falls des § 243 I S. 2 StGB, *Eisele,* Strafrecht – Besonderer Teil II – Eigentumsdelikte und Vermögensdelikte, 6. Aufl. Stuttgart 2020, § 3 Rn. 101.

[101] Fischer-StGB/*Fischer* (Fn. 28) § 263 Rn. 209; BGH NJW 2004, S. 2394 (2395); BeckOK StGB/*Beukelmann,* § 263 Rn. 98.

[102] Vgl. *Bock,* Strafrecht Besonderer Teil 2 – Vermögensdelikte, Berlin 2018, S. 104; *Hoffmann-Holland,* Strafrecht Besonderer Teil, Tübingen 2015, 3. Kapitel Rn. 818.

Die Rechtsfolge des § 263b StGB sollte angesichts des hohen Vermögensschadens beim Opfer und der zugleich erheblichen Bereicherung des Täters darauf ausgerichtet sein, eine Freiheitsstrafe, anstatt einer Geldstrafe anzuordnen. Eine Geldstrafe würde in Anbetracht dessen, dass die Einziehung der Beute praktisch durchgesetzt werden kann, selbst bei einem Tagessatz von 30.000€ in Extremfällen nicht mehr als ein Tropfen auf dem heißen Stein sein. Im Zusammenhang mit einer Freiheitsstrafe kann auch ein Verbot der Nutzung dezentraler Systeme oder deren Clients angeordnet werden, wobei hierzu ebenfalls ein neuer Tatbestand vom Gesetzgeber erarbeitet werden müsste. Die dauerhafte Überwachung der Bitcoinadressen des Täters ist aus präventiver Perspektive unabkömmlich.

V. Fazit und Ausblick

Das Strafrecht ist noch nicht bereit, mit den vielfältigen Entwicklungen im digitalen Raum mitzuhalten. *De lege lata* ist bis auf das Ausspähen von Daten nach § 202a Abs. 1 StGB kein Straftatbestand im Falle eines digitalen „Diebstahls" einschlägig. Terminologisch ist das Handeln über das Ausspähen hinaus nicht strafrechtlich zu beschreiben. Möchte man *de lege ferenda* eine Bezeichnung finden, so könnte man den möglichen neuen Tatbestand § 263b StGB als „Netzwerkmanipulation" bezeichnen.

Um Strafbarkeitslücken bei digitalen „Diebstählen" zu verhindern, ist dem Gesetzgeber der Handlungsbedarf mehr als deutlich anzuzeigen. Sollte man die Strafbarkeit nach § 263a Abs. 1 Var. 3 StGB doch bejahen, kommt man aus systematischen Gründen nicht umhin, in jedem Fall einen besonders schweren Fall zu bejahen. Mit der Einführung des *bitcoins* als gesetzliches Zahlungsmittel in El Salvador ist ein weiterer Schritt in Richtung der Etablierung von Kryptowährungen als Alternative zu den bisherigen Zahlungsmitteln gegangen worden. Damit auch ein grenzübergreifender Handel mit El Salvador ohne Schwierigkeiten weiter möglich ist, ist die juristische Aufarbeitung der fehlenden zivil- sowie strafrechtlichen Lücken unabkömmlich. Die digitale Entwicklung schreitet voran und wartet nicht auf Gesetzesinitiativen. Schon heute gibt es neue digitale Konzepte wie die *„smart contracts",* die schuldrechtliche Verträge als Programmcode abbilden wollen.[103] Auch neue Tokens wie *„investment tokens"*[104] werden immer relevanter. Die Technologie gilt als ein vielversprechendes Konzept – welches ebenfalls Raum für kriminelle Aktivitäten gibt. Um nicht mit dem Schutz digitaler Vermögenswerte hinterher zu hängen, müssen die Datensätze, welche heute schon einen Wert besitzen und gehandelt werden,[105] zuordnungsunfähig gemacht werden. Es liegt beim nationalen Gesetzgeber mit einer umfangreichen Digitalisierungsinitiative die deutschen Gesetze in das 21. Jahrhundert zu überführen. Ansonsten besteht die Gefahr, dass sich die dezentralen Systeme anstatt zu einer ergänzende Parallelwelt voller Freiheit, zu einem unkontrollierbaren Ort voller Gefahren entwickeln.

---

[103] *Eschenbruch/Gerstberger* (Fn. 18) S. 3 (3); siehe auch *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um nichts?, ZfPW 2018, S. 431 (433 f.).

[104] *Kleinert/Mayer* (Fn. 72) S. 857 (858).

[105] *Wandtke,* Ökonomischer Wert von persönlichen Daten – Diskussion des „Warencharakters" von Daten aus persönlichkeits- und urheberrechtlicher Sicht, MMR 2017, S. 6 (9).

Dörgő, Sándor
Student, Universität Szeged

DIE SELBSTÄNDIGE STRAFRECHTLICHE VERANTWORTLICHKEIT DER KÜNSTLICHEN INTELLIGENZEN IN DEN VIRTUELLEN RÄUMEN UND DIE BACKDOOR-ATTACKE

I. Einführung

Die gesamte Menschheit war immer bestrebt, die – zum Überleben und Weiterbestehen erforderliche Arbeit – mit dem möglichst geringsten Einsatz durchführen. Einige, die körperliche Arbeit ersetzende Instrumente wurden schon in der Urzeit benutzt – zum Beispiel die Erfindung des Rades (aber die erste Instrumente, die keine körperlichen Kraft erforderten, wurden erst im 18. Jahrhundert – also ab der industriellen Revolution ab – umfassend verwendet.

Diese Geräte haben der Menschheit nur die körperliche Arbeit und den dazu erforderlichen Einsatz abgenommen, deshalb kam der Gedanke, wie es wäre, wenn denkende Maschinen hergestellt werden würden. Descartes hat mit diesem Gedanken gespielt und ihn weitergeführt. Wie wäre es, wenn diese Apparate menschenähnlich entworfen werden würden, dass während einer Unterhaltung nicht entschieden werden könnte, ob wir mit einer echten Person sprechen, oder nicht.[1]

Dieser Gedanke blieb bis zum 20. Jahrhundert nur eine Science-Fiction-Idee, danach hat sich die Lage geändert. Die denkenden Maschinen – die Descartes visioniert hat – sind – wenn nicht gleich in der Wirklichkeit, aber in der nahen Zukunft – zu den erreichbaren Entitäten geworden. Die Kapazität des Computers ist von Monat zu Monat gestiegen und zurzeit ist dieses wissenschaftliche-fantastische Phänomen Teil unserer Tage geworden. „Denkende Geräte" sind in unseren Verkehrsmitteln, Handys und sogar in den Kühlschränken vorhanden. Wie können wir diese Entitäten definieren? Zurzeit gibt es noch keinen einheitlichen Standpunkt in diesem Thema, aber vielleicht kann uns das informationstechnische Wörterbuch Oxford helfen, wonach die künstliche Intelligenz der Teil der Informationstechnik ist, der sich mit Softwares beschäftigt, die die menschliche Intelligenz ersetzen können.[2]

Nachdem *Isaac Asimov,* amerikanischer Science-Fiction-Schriftsteller die berühmten „Robotergesetze" geschrieben hat, formulierte sich der Anspruch, diese Geräte nicht nur nach den Regeln der Technologie zu beurteilen, sondern auf eine höhere Stufe, auf die Stufe der gesellschaftlichen und rechtlichen Regelung zu erheben.[3] Es war wichtig, weil

---

[1] *Descartes,* Értekezés a módszerről, Szemere/Boros (Übersetzung), 1993.

[2] *Siba,* (Hrsg.), Oxford számítástechnikai értelmező szótár, Novotrade Kiadó, 1989 „Mesterséges intelligencia"

[3] *Asimov,* Én, a robot, Kossuth Könyvkiadó, 1966.

diese Entitäten nicht nur einfache Instrumente waren, sondern imstande waren, mit menschlichen Wesen in Interaktion zu treten, und dadurch Einfluss auf das wirkliche Leben der Menschen zu nehmen.[4]

In diesem Beitrag möchte ich die Antwort darauf finden, ob die rechtliche- und strafrechtliche Verantwortlichkeit bei den Softwares mit künstlicher Intelligenz festgestellt werden kann.

Die meisten Forschungen beschäftigen sich mit der Frage der Verantwortlichkeit von mit künstlicher Intelligenz ausgestatteten Robotern in der körperlichen Welt. Zurzeit funktioniert ein bedeutender Teil unserer Gesellschaft in den virtuellen Räumen. Zum Beispiel: Banksysteme, soziale Plattformen und große Teile der Verwaltung werden über das Internet abgewickelt. Es kann erklärt werden, dass ein bedeutender Teil der möglichen Delikte von den KIs nur in den virtuellen Räumen realisiert werden kann – natürlich außer den Verbrechen gegen das Leben und die Gesundheit.

Zusammenfassend möchte ich mit der Untersuchung der erreichbaren Technologie analysieren, ob die strafrechtliche Verantwortlichkeit der KI festgestellt werden kann, und wenn nicht, wer für die von ihnen entfalteten und unter die Geltung des Strafrechts fallenden Handlungen haftbar gemacht werden kann.

II. Die Verlagerung des Missbrauchs aus der Computerumgebung in die virtuellen Räume

Mit der Entwicklung der Informatik sind die im wirklichen Leben verübbaren Delikten zuerst in der informatischen Umgebung und dann – mit der Verbreitung des Internets – in den virtuellen und online Gesellschaften erschienen. Im 21. Jahrhundert wurden die in dieser Umgebung begangenen Delikte mit dem Erscheinen des KI, viel leichter erreichbar und schwerer zu verfolgen.

Drei große Gruppen können unterschieden werden. Die „klassischen Computerdelikte", die meistens Vermögensdelikte und Verbrechen gegen wirtschaftliche Interessen darstellen. Diese sind auch heute noch von großer Bedeutung, wenn man die Straftaten gegen Kryptogeld und Wertgegenstände und Datensätze innerhalb bestimmter virtueller Gemeinschaften und Spielesoftware bedenkt.[5]

Die zweite Gruppe sind die modernen Computerstraftaten. Es handelt sich um Verbrechen gegen konkreten Menschen oder Menschen, wie zum Beispiel, die Belästigung und die Hassrede. Es stehen oftmals wirtschaftliche Interessen als Motivation im Hintergrund, aber nicht notwendigerweise.

Die dritte Kategorie fasst die ersten beiden zusammen, und wird als virtuelle Kriminalität bezeichnet. Aus der Perspektive unserer Zeit ist es die wichtigste. Hier ist der wirtschaftliche Missbrauch nicht so charakteristisch, wie die Delikte gegen Personen und

[4] *Eszteri*, A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései. Infókommunikáció és Jog 62-63/2015, S. 47-57.

[5] Federal Bureau of Investigation, Intelligence Assasment: Bitoin Virtual Currency: Unique Features Present Distinct Challanges for Deterring Illicit Activity (24. April 2012) Online: http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf, 2020.07.01., S. 7.

das Vermögen.[6] Es ist wichtig bei der Feststellung der strafrechtlichen Verantwortlichkeit zu anzumerken, dass diese Delikte gegen Personen real sind, aber sich nicht gegen reale Menschen, sondern gegen ihren virtuellen Avatar richtet. Diese Verbrechen sind dennoch geeignet, das Persönlichkeitsrecht des den Avatar kontrollierenden Spielers zu verletzen.

III. Klassifikation der künstlichen Intelligenzen

Wir haben uns in der Einführung mit der Definition der künstlichen Intelligenz beschäftigt, somit muss jetzt ihre Klassifikation analysiert werden. Aus Hinsicht der philosophischen Entwicklung des Begriffs, können vier Geistesrichtungen unterschieden werden.

III. 1. Die vier Hauptkategorien

Die erste Kategorie ist ein menschlich denkendes System. Die Fachliteratur zählt jene Systeme hierher, die Erkenntnisse des menschlichen Geistes modellieren.

Die zweite ist ein menschlich handelndes System. Die wichtigsten Kriterien sind, dass das Gerät sich als ein Mensch verhält. Diese Gedankenfolge stammt von *Alan Matheson Turing,* und kann mit dem Turing-Test geprüft werden.[7]

Die dritte Gruppe ist das rational denkende System. In dieser Geistesrichtung kann schon erkannt werden, dass KI in bestimmter Weiseperfekter und ausgefeilter als die kognitiven Fähigkeiten des Menschen sind.

Die vierte und auch letzte Geistesrichtung ist das rational handelnde System. In dieser Geistesrichtung handelt es sich um modernste und fortschrittlichste künstlichen Intelligenzen, die dem Menschen schon täuschend ähnlich sind, sowohl beim Denken, als auch beim Handeln. Bei der Untersuchung der strafrechtlichen Verantwortlichkeit muss man von dieser Geistesrichtung ausgehen.

III. 2. Schwache KI vs. Starke KI

John R. Searle hat in den ’80 Jahren den grundlegenden Unterschied zwischen den schwachen und starken KI festgestellt. Searle’s Meinung nach besteht der wichtigste Unterschied darin, dass die schwachen KI sich verhalten, als handelten sie rational, während die starken KI ein reales, vorhandenes und selbständiges Bewusstsein haben.[8] Diese Softwares funktionieren folgenderweise: die empfangenen Signale (input) werden anhand den eingespeisten Algorithmen nach außen gerichtete Signale (output) umgewandelt. Solange dieser Prozess nicht schneller als die menschliche Perzeption ist, ist der rechtliche Aspekt dieser Softwares nicht komplizierter als der eines Taschenrechners. Dank der technologischen Errungen-

---

[6] *Brenner,* Is There Such a Thing as „Virtual Crime”? California Criminal Law Rewiev 4/2001, S. 26-28.

[7] *Turing,* Computing Machinery and Intelligence, Mind 10/1950, S. 433-460.

[8] *Csáji,* A mesterséges intelligencia filozófiai problémái, Eötvös Lóránd Tudományegyetem, Budapest, 2002, S. 4.

schaften, haben diese Prozesse heutzutage schon die Kapazität des menschlichen Geistes überstiegen, und wenn der Mensch die Antwort auf das Input nicht mehr vorhersagen kann, kommt ein Wechsel, und die Softwares verwandeln sich im schwache KI.[9]

Die starken KI existieren zurzeit nur in der Welt des Science-Fiction. Das Haupthindernis ist, dass man die Funktion des menschlichen Geistes bis heute nicht verstanden hat. Ein anderes Hindernis ist, dass die Menschheit noch keine so große informatische Kapazität hat, die der Kapazität des Gehirns ebenbürtig wäre. Es sei angemerkt werden, dass das Erscheinen einer starken KI mit Bewusstsein die Gemeinschaft und das Bild der Zivilisation insgesamt verändern wird.[10]

Zusammenfassend soll der Schwerpunkt bei der Feststellung der strafrechtlichen Verantwortlichkeit auf das Verhalten der schwachen KI gelegt werden.

IV. Die Grundlagen des Rechts der künstlichen Intelligenzen

Seit Mary Shellys berühmtem Roman beschäftigt sich die Menschheit viel mit der Angst vor der Schöpfung. Es handelt sich um einen Menschen, der eine ihr fast gleiche Kreatur geschaffen hat, die sich am Ende gegen ihn wendete und ihm alles raubte. Gleichzeitig gesellte sich diese Angst zur in der menschlichen Natur liegenden Neugierde, die uns wieder und wieder motiviert.[11] Die Angst vor den künstlichen Intelligenzen kommt in vielen Fach-, Literatur und Pop-Kult Werken vor. Zur Absicherung hat sich die Menschheit an das Recht gewendet, und ist gleich auf ein neues Problem gestoßen. Einen künstlichen Verstand ohne Bewusstsein und Vermögen mit Rechtspersönlichkeit auszustatten ist nach unserer heutigen Auffassung fast unmöglich. Der strafrechtliche Aspekt dieses Phänomens ist, dass die Feststellung der strafrechtlichen Verantwortlichkeit bei fehlender Rechtspersönlichkeit auf Hindernisse stößt.[12]

Die Roboter und die Softwareagenten müssen in dieser Studie getrennt werden. Als Agenten bezeichnen wir Softwares, die in der realen Welt keine Projektion haben, keine Wirkung auf die Welt ausüben und die reale Welt mit Sensoren nicht sinnlich wahrnehmen.[13]

Die rechtlichen Grundlagen der Regelung der künstlichen Intelligenzen sind zuallererst in den Novellen von Isaac Asimov erschienen. Er hat drei Gesetze – und später noch eins – für das Verhalten von Robotern geschaffen, deren Verletzung wegen der Programmierung nicht möglich ist. Zur Rechtpersönlichkeit enthalten diese drei Gesetze nichts.[14]

Die Rechtslehre unternimmt auch Schritte, um diese Probleme zu lösen. *Peter M. Asaro* hat analysiert, ob den gültigen Gesetzen für die durch KI generierten Probleme geeignet sind. Bei dem Privatrecht hat er festgestellt, dass die Regelung der Tragung der

---

[9] *Flanagan,* The Science of the Mind, 1992, S. 1-22. in: Solum, Legal Personhood for Artificial Intelligences, NorthCarolina Law Review 70/1992, S. 1244.

[10] *Dennett,* Consciousness Explained. The Penguin Press, 1991, S. 435.

[11] *Shelley,* Frankenstein, avagy a modern Prométheusz (Übersetzung: Göncz Árpád), Budapest, 1977.

[12] *Eszteri* (Fn. 4)

[13] *Russell/Norvig,* Mesterséges Intelligencia – Modern megközelítésben, Budapest, 2000.

[14] *Murphy/Woods/Beyond,* The Three Laws of Responsible Robotics, IEEE Intelligent Systems 4/2009, S. 14-20.

Schadnesgefahr und der Verantwortlichkeit auf Entitäten mit künstlicher Intelligenz gültig ist. Bei Softwareagenten obliegt die Haftung fast immer dem Nutzer.[15]

Giovanni Sartor hat die Vertretungsfähigkeit der Agenten analysiert. Er hat darauf aufmerksam gemacht, dass bei zurzeit modischen elektronischen Vertragsschlüssen fast immer eine schwache KI als Vermittler tätig ist. Er hat darauf hingewiesen, dass diese Agenten kein Bewusstsein haben und es somit ausgeschlossen ist, sie zur Verantwortung zu ziehen. Nach seiner Auffassung kann eine KI in einigen Sachbereichen selbständig und rational vorgehen, die Haftung aber auf dem Nutzer lastet, weil – wenn es sich um ein Delikt handelt – er den Softwareagenten als Werkzeug gewählt hat.[16]

V. Die Grundlagen der Strafbarkeit der künstlichen Intelligenzen

In der Studie von *Gabriel Hallevy* aus dem Jahre 2010 kommt erstmals die Frage der strafrechtlichen Verantwortlichkeit von künstlichen Intelligenzen vor. Es wurde die Antwort gesucht, was zu tun ist, wenn eine solche Entität mit seinem Verhalten einen in dem jeweils gültigen Strafgesetzbuch geregelten und bestraften Tatbestand realisiert.[17] Diese Fälle – in denen es zur Untersuchung der strafrechtlichen Verantwortlichkeit kommt – sind seltener, als die, in denen die Haftpflicht festgestellt werden muss.

Ein wichtiges Kriterium ist, dass der Täter – bei dieser Studie die KI – das konjunktive Bedingungssystem eines der Tatbestände des Besonderes Teils des geltenden Strafgesetzbuchs *(actus reus)* verwirklichen muss, ein anderseits ist auch das Bewusstsein des Täters *(mens rea)* unverzichtbares Element. Nach dem gegenwärtig geltenden ungarischen Strafgesetzbuch ist nur die vorsätzliche Straftat zu bestrafen, die Fahrlässigkeitsdelikte sollen nur in speziellen, bestimmten Fällen bestraft werden (§ 7 uStGB).

Wenn wir den gegenwärtig in der Rechtliteratur gebräuchlichen Handlungsbegriff untersuchen, finden wir mehrere Ansätze. Nach der Meinung der klassischen Schule ist der sogenannte *kausale Handlungsbegriff* maßgebend. Im Sinn dieser Definition ist die Tat ein Verhalten, das in der Umwelt bestimmte Folgen hat.[18] Bei der anderen Definition – dem sogenannten *finalen Handlungsbegriff* – hängt die Tat von dem Willen ab, die Kausalität wird um Motivation und Zweckmäßigkeit ergänzt. Die beide Theorie werden von *József Földvári* vermengt, wonach die bestimmten Elemente der Handlung das Verhalten, das Bewusstsein und das Verhalten sind. Der Kampf dieser Motive wird durch einen Entschluss abgeschlossen, dem der Realisierung des Delikts folgt.[19] Es ist ersichtlich, dass die Strafbarkeit der künstlichen Intelligenzen im ungarischen Strafrecht auf fast unüberwindbare Hindernisse stößt. Denn der Wille und das Bewusstsein lassen sich nur schwer interpretieren, wenn es sich um eine schwache KI handelt. Wie oben

---

[15] *Asaro,* Robots and Responsibility from a Legal Perspective, Proceedings of the IEEE 1/2007

[16] *Sartor,* Cognitive Automata and the Law, Artificial Intelligence and Law 35/2006

[17] *Hallevy,* The Criminal Liability of Artificial Intelligence Entities – From Science Fiction to Legal Social Control, Akron Intellectual Property Journal 2010.

[18] *Nagy,* A bűncselekmény-fogalmi változások és irányzatok a német büntetőjog fejlődésében, Acta Juridica et Politica S. 142.

[19] *Földvári,* Magyar büntetőjog. Általános rész, Budapest, 2006, S. 98-99.

dargestellt, gibt es in diesem Fall kein wirkliches Bewusstsein, das sie von den starken KI abgrenzt.

Die Meinung von *Ugo Pagallo* in der ausländischen Fachliteratur dazu ist ähnlich.[20] Seiner Meinung nach verfügt die künstliche Intelligenz heutzutage über eine gewisse Intelligenz – und in Zusammenhang damit über eine Art von rationaler Entschlussfähigkeit – haben aber nach unserem heutigen Wissen kein Bewusstsein, und deshalb ist die Feststellung der Bewusstheit ausgeschlossen. Deswegen ist die vorsätzliche und fahrlässige Begehung von Straftaten durch KI unmöglich. Die schwachen KI sind mit ihrer Existenz nicht bewusst, sie können den moralischen Inhalt ihrer Taten nicht beurteilen, und insgesamt fehlt ihnen das Selbstbewusstsein. Sie können die Auswirkungen ihrer Taten für die Gesellschaft nicht ermessen, sie überlegen ganz einfach nach den einprogrammierten Algorithmen, egal, ob sie legal oder illegal sind.

VI. Die geltende ungarische Regelung

Nach der geltenden ungarischen Regelung ist die Untersuchung der strafrechtlichen Verantwortlichkeit einer Software ausgeschlossen. Die Geltung des ungarischen Strafgesetzbuches geht ausschließlich von den natürlichen und juristischen Personen aus (§ 1 des Gesetzes Nr. CIV aus dem Jahre 2001), die künstlichen Intelligenzen gehören nicht zu diesen Kategorien (§ 3 uStGB).

In diesem Sinne kann die künstliche Intelligenz nach dem jetzt geltenden ungarischen Strafrecht nicht sanktioniert werden.

VI.1. Die KI, als Werkzeug

Es gibt doch eine Methode, dass wir irgendwie – nicht auf klassische Weise – werten, dass ein Delikt von einem Softwareagenten begangen wurde. Wie oben dargelegt trifft die Software Entscheidung eigentlich nach ihren früher geschriebenen Algorithmen. So kann ihre Funktion noch berechenbar und kontrolliert bleiben.

Falls die Software tatbestandmäßiges Verhalten realisiert, soll nicht die Software, sondern der Benutzer verantwortlich gemacht werden. Typische Beispiele dafür sind mit Hilfe von KI begangene Betruge und die auf der Sozialplattform Twitter von den Social Bots mit künstlicher Intelligenz verwirklichten Hassreden und Hetze gegen die Gemeinschaft.[21]

Ein Werkzeug ist ein Mittel, das unabhängig vom Körper des Täters existiert.[22] Zu dieser Definition könnten auch die KI gehören. Bei dieser Theorie müssen wir akzeptieren, dass diese Entitäten nicht auf andere Weise sanktioniert werden können, da sie keine Bewusst oder Willen haben, und ihr unter die Tatbestände des Besonderen Teils zu subsumierenden Verhaltens nicht ihre eigene Entscheidung darstellen, sondern den programmierten Befeh-

[20] *Pagallo,* Killers, fridges and slaves: a legal journey in robotics, AI and Society 4/2011, S. 347-354.

[21] *Wakefield,* Microsoft chatbot is taught to swear on Twitter, 24 March 2016, https://www.bbc.com/news/technology-35890188 (2020.07.02.)

[22] *Földvári* (Fn. 19) S. 112.

len einer dritten Person oder des Nutzers zu verdanken sind. Aus diesem Gedankengang folgt unmittelbar, dass der Täter der Handlung ist, wer das Werkzeug des Verbrechens programmiert hat. Es könnte keine andere Lösung denkbar sein, weil der Kausalablauf fehlen würde, wird der Befehl zur Begehung eines Verbrechens nicht in die KI programmiert, wird auch keine Straftat verwirklicht.

Ähnlich verhält es sich, wenn eine rechtmäßig funktionierende Software mit künstlicher Intelligenz von außen angegriffen wird, daraufhin eine Dysfunktion entwickelt, und dankt dieser Dysfunktion eine Rechtverletzung verwirklicht wird. Typische Beispiele sind die Attacken gegen Finanzsysteme, wodurch die Täter durch das Ausnutzen der eigenen Software der Bank große Vermögensvorteile realisieren können.[23] Der einfachste Fall ist, dass auch eine nicht autorisierte Datenmodifikation in einem IT-System tatbestandmäßig ist. In diesen Fällen sind die künstlichen Intelligenzen das Werkzeug der Begehung einer Straftat [§ 423 Abs. 1 Buchstabe c) uStGB].

VI. 2. Backdoor-attack

Die sogenannten Backdoor-Attacken stellen eine spezielle Kategorie dar. Aber was bedeutet eine Backdoor-Attack? Nach der Definition: *„ist es ein Angriffsmittel, das auf der Ebene des Operationssystems unbemerkt Zugang zum Computer sichern kann. Die Hintertür wird durch einen Sicherheitsfehler ermöglicht, der schon vorhanden ist, oder mit etwa Softwarehilfe ausgenutzt werden kann. Spezielle Zugangsberechtigungen können als Hintertür angesehen werden“*.[24]

Wenn auch künstliche Intelligenz betroffen ist, stellen diese Angriffsversuche den Rechstanwender bei der Bestimmung der strafrechtlichen Verantwortlichkeit vor eine schwierige Frage. Diese Frage muss aus mehreren Richtungen analysiert werden. Aus der Richtung des Programmierers, der diese Lücke im Softwarekode vorsätzlich oder fahrlässig geöffnet hat. Anderseits soll die strafrechtliche Verantwortlichkeit der KI und des Benutzers untersucht werden.

Im ersten Fall ist es relativ einfach. Wenn der Programmierer vorsätzlich oder fahrlässig einen Fehler im Programmkode macht – und dadurch ein Sicherheitsrisiko in der Software entsteht – stellt das in erster Linie nach dem Zivilrecht – genauer im Schuldrecht – mindestens eine magelhafte Leistung dar. Natürlich bezieht sich das auf einen Fehler, der auf Fahrlässigkeit zurückzuführen ist. Die Lage der vorsätzlich versteckten Hintertür ist im Grunde ähnlich, wird sie aber dazu benutzt eine Rechtverletzung zu begehen, können die beiden Fälle unterschiedlichen Beurteilungen unterfallen. Im ersten Fall – der aus Unachtsamkeit realisiert wird – könnte die Verantwortlichkeit des Programmierers nur bis zur Fahrlässigkeit reichen. Unter diesem Aspekt kann er nicht Beteiligter der verwirklichten Straftat werden. In dem zweiten, vorsätzlichen Fall kann auch Beteiligung – in Gehilfenqualität – und Mittäterschaft festgestellt werden.

---

[23] Cowley, Stacy, Perlroth, Nicole: Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc, The New ork Times, July 30, 2019 https://www.nytimes.com/2019/07/30/business/bank-hacks-capital-one.html (2020.07.02.)

[24] *Fehér,* Kezdő hackerek kézikönyve, avagy informatikai támadások és kivédésük, Budapest, 2016, S. 34.

Die zweite Kategorie kann mit der Person des Betreibers der KI verbunden werden. Die Aufgabe ist hier schwieriger, die Funktion des in das Programm codierten Algorithmus und die Motivation des Betreibers muss überprüft werden. Wenn der Betreiber, die nicht für Rechtsverletzungen programmierte Software in gutem Glauben benutzt, aber durch die Hintertür eine Straftat – zum Beispiel nicht autorisierte Datenmodifikation oder unerlaubter Zugang – verwirklicht wird, kann die strafrechtliche Verantwortlichkeit nicht festgestellt werden. In diesem Zusammenhang stellt sich die Verantwortlichkeit des Programmierers, der die Sicherheitslücke entweder vorsätzlich oder fahrlässig zugänglich gemacht hat. Ein typischer Fälle dessen ist das sogenannte „leaking", wo die künstliche Intelligenz mit Hilfe der Schlüsselwörter unautorisiert Daten sammelt[25].

In dem Fall, in dem die Motivation einer Rechtsverletzung von der Seite des Benutzers angenommen werden kann, kann auf der Seite des Programmierers eine Mittäterschaft oder Beihilfe festgestellt werden. Bei dem Benutzer kann die vorher spezifizierte selbständige Täterschaft – und die künstliche Intelligenz als Werkzeug – bestimmt werden.

VII. Wer ist verantwortlich?

VII. 1. Die Verantwortlichkeit des Herstellers der KI

Es muss festgestellt werden, dass die Herstellung und der Betrieb einer KI nach der ungarische Rechtliteratur eine Betriebsgefahr darstellt. *Tamás Lábady* hat den Standpunkt der vorbereitenden Sachverständigenkommission der Regelung des Bürgerlichen Gesetzbuchs in Sachen Schadensersatzhaftung begründet.[26] Aber die ungarische Rechtsliteratur hat keine weiteren, die künstliche Intelligenz betreffenden Behauptungen aufgestellt. Die nächste Kategorie, in die die KI kategorisiert werden können, ist die Betriebsgefahr. Das bedeutet praktisch, dass es sich um eine Tätigkeit mit großer Gefahr handelt, und während dieser Tätigkeit können entstehende kleine Fehler unangemessen großen Schaden verursachen. Dieser Kategorie nach ist der Betrieb einer künstlichen Intelligenz eine Betriebsgefahr.[27] Es ist eine gut begründete Ansicht, weil das Verhalten des Agenten infolge der Mechanismen der Entscheidungsfindung nicht voraussehbar sind und ihr Betrieb eine erhöhte Gefahr darstellen kann. Dafür ist nicht nur der Benutzer, sondern auch der Hersteller verantwortlich. Wenn er nämlich eine solche Software mit künstlicher Intelligenz verkauft oder zur Benutzung überlässt, mit der potenzielle Straftaten begangen werden können oder die eventuell auf vorsätzliche Rechtverletzungen programmiert wurde, kann seine strafrechtliche Verantwortlichkeit festgestellt werden.

---

[25] *Clark,* When Does a Leak to the Media Violate the Law?, Goverment Executive, February 27, 2017, https://www.govexec.com/management/2017/02/when-does-leak-media-violate-law/135737/ (2020.07.02.)

[26] *Petrik* (Hrsg): Polgári jog. Kommentár a gyakorlat számára, HVG Orac, Budapest, 2014. S. 937.

[27] *Mázi,* A veszélyes üzemi kárfelelősség magyarországi fejlődése a polgári korszakban, http://www.jogiforum.hu/publikaciok/49.0.0 (2020.07.02.)

VII. 2. Die Verantwortlichkeit des Benutzers der KI

Von der Definition der Betriebsgefahr ausgehend, stellt sich die Frage der Verantwortlichkeit des Benutzers. Die Feststellung der strafrechtlichen Verantwortlichkeit steht im Zusammenhang mit der vorab besprochenen Regelung. Der größte Unterschied zur Verantwortlichkeit des Herstellers ist, dass eine Straftat auch mit solchen KI begangen werden kann, die eigentlich nicht zur Begehung einer Rechtverletzung geeignet ist, durch Modifikationen des Benutzers geeignet gemacht werden. Das kann mehrere Urheberrechtliche Fragen aufwerfen. Wichtig ist, dass der Benutzer für die von einer KI verursachten Schaden nur dann haftet, wenn sich seine Fahrlässigkeit darauf erstreckt. Der Nachteil dieses Gedankenganges ist, dass die Benutzer das Verhalten der KI nur in geringem Maß vorhersehen können, wodurch die Feststellung der Verantwortlichkeit selten erfolgreich ist.[28]

VII. 2. 1. Die Lehre von der objektiven Zurechnung

Bei der Forschung der selbständigen strafrechtlichen Verantwortlichkeit der künstlichen Intelligenzen kann die Lehre von der objektiven Zurechnung benutzt werden. Im Sinne dieser Lehre muss der Kausalzusammenhang zwischen der Tathandlung und des realisierten Resultats analysiert werden. In Relation der künstlichen Intelligenzen gibt es mehrere Möglichkeiten der Annäherung. Die Ähnlichkeit in allen Fällen ist die strafrechtliche Qualität des Resultats. Zur Feststellung der strafrechtlichen Verantwortlichkeit muss das Resultat strafrechtliche Relevanz haben. Der nächste analysierte Punkt muss das Verhalten sein. Im Sinne der Lehre von der objektiven Zurechnung müssen alles Verhalten, die mit dem Resultat im kausalen Verhältnis sind, gewürdigt werden. Eine Ausnahme bildet, wenn die Kausalität sehr entfernt ist und die Wirkung an dem Resultat nicht feststellbar ist. Ein typisches Beispiel ist, als die künstliche Intelligenz ein Virus an ausgewählte E-Mail-Adressen sendet, und später eine andere Person – unabhängig von den künstlichen Intelligenzen und von ihrem Verhalten – von dem Computer Daten unautorisiert herunterlädt. Es kann ein Zusammenhang zwischen den beiden Verhalten gefunden werden, aber eine solche Kausalität geht zu weit, deswegen muss man die Lehre von der objektiven Zurechnung nach dem gesunderen Verstand so wie in dem realen als auch in dem Virtualraum benutzen. Die Hauptfrage ist, ob wir das Kausalitätsverhältnis bis zum Benutzer oder bis zum Entwickler zurückführen. Meiner Meinung nach ist jede Annäherung richtig. In den meisten Fällen ist die Verantwortlichkeit des Entwicklers nicht feststellbar, vor allem im Zusammenhang mit den KIs im Handelsumsatz, die der Benutzer zur Begehung von Straftaten modifiziert hat, aber seine Tathandlung nur in geringem Zusammenhang mit dem später realisierten Delikt steht. Doch ist ein bewusstes Verhalten des Entwicklers vorstellbar, wodurch die Software zur Straftatbegehung geeignet gemacht wurde und die strafrechtliche Verantwortlichkeit im Sinne der Lehre von der objektiven Zurechnung auch auf den Entwickler erweitert werden kann, wenn sich das Resultat verwirklicht. Die Verantwortlichkeit des Benutzers kann meistens festgestellt werden, in Anbetracht dessen, dass er der Betreiber der KI ist, aber es kann vorkommen, dass er aus dem Kausalitätsverhältnis ausscheidet. In diesem Fall richtet sich die Begehung des Verbrechens gegen den Benutzer, oder gegen seine Daten.

[28] *Sartor* (Fn. 16)

In diesem Fall kann der Benutzer nicht in das Kausalitätsverhältnis eingepasst werden, also ist seine strafrechtliche Verantwortlichkeit ausgeschlossen und der Entwickler rückt an seine Stelle, angenommen, dass nicht ein Dritter die KI betreibt.

IX. Mögliche Lösungen

IX. 1. Regelung der Verantwortlichkeit der KI ähnlich der Haftung einer juristischen Person

Wie oben ausgeführt, haben Softwareagenten im ungarischen Recht keine Rechtspersönlichkeit. Dagegen haben die fortschrittlichsten KI eine reiche Wissensbasis, sie verhalten sich quasi selbständig, überlegen relativ rational und können sich selbständig entwickeln. Sie können mit anderen KI oder Personen in Interaktion treten, sowohl im wörtlichen, als auch im rechtlichen Sinne. Nach *Allan* und *Widdison* transformiert sich der Wirkungsbereich der Softwareagenten von der ehemals passiven technischen Seite, in aktive, handelnde, interaktionsfähige Entitäten.[29] Der größte Unterschied zu den klassischen, juristischen Personen ist, dass sie gar keiner Repräsentation bedürfen. Die juristischen Personen haben selbständige, von den der natürlichen Personen abweichende Interessen, ein Softwareagent hat keine Interessen, nur der Benutzter. Bis zu diesem Punkt wäre es eine mögliche Lösung, wenn wir bei der Bestimmung der strafrechtlichen Verantwortlichkeit einer KI die Regeln für die Feststellung der Verantwortlichkeit von juristischen Personen benutzen würden. Aber eine wichtige Komponente fehlt: um einen Softwareagenten für eine juristische Person halten zu können, braucht es ein getrenntes Vermögen, aber laut dem Standpunk der heutigen Wissenschaft und des Rechts hat ein Softwareagent kein getrenntes Vermögen.[30]

IX. 2. KI als Vertreter

Heutzutage haben sich die Onlineerwerbungen und Geschäftsabschlüsse beschleunigt. Die Online-Marktplätze benutzen oft intelligente Softwareagenten zur Optimierung der Einkäufe und der Profitsteigerung. Deshalb wurde ermöglicht, dass über KI ohne menschliche Intervention Willenserklärung abgegeben werden können, die die vertretene Person verpflichtet. Laut dem UNCITRAL Modellgesetz für elektronsichen Handel sind diese Willenserklärungen als *„automatische Vertragserklärung"* anzusehen, die von der juristischen Person stammt, die den Agent betreibt, also nicht von dem Agenten selbst.[31] Unter diesem Aspekt ist es unmöglich die KI als Vertreter anzusehen. Eine andere Schwierigkeit ist, dass die Vertretung im Bürgerlichen Gesetzbuch geregelt ist. In dem steht, dass ein Vertreter nur eine natürliche Person sein kann, kein Softwareagent.[32] So ist auch diese Lösung für die Bestimmung der strafrechtlichen Verantwortlichkeit unanwendbar.

[29] *Andrade/Novais/Machado/Neves,* Contracting Agents: Legal Personality and Representation. Artificial Intelligence and Law 15/2007, S. 359.

[30] *Eszteri* (Fn. 4)

[31] UNCITRAL Model Law on Electronic Commerce § 13 Abs. 2 Punkt b)

[32] *Petrik* (Fn. 26) S. 25-29.

IX. 3. Eine reale Lösung – Generalprävention

Zusammenfassend ist die selbständige strafrechtliche Verantwortlichkeit der KI in Ungarn heute begrifflich ausgeschlossen. Unter dem Aspekt der selbständigen Rechtspersönlichkeit kann weder der Begriffskreis einer juristischen Person noch der einer Vertretung auf Softwareentitäten verwendet werden. Weder die Zivilregelung noch die Strafregelung lässt zu, dass das rechtverletzende Verhalten dieser Programme selbständig bewertet wird. Auf eine künstlichen Intelligenz kann wegen des fehlenden Bewusstseins und des fehlenden rationalen Entscheidungen kann das heute geltende ungarische Sanktionssystem nicht angewendet werden. Bei diesen Entitäten sind Geldstrafe, Strafarrest und Zwangsbehandlung ausgeschlossen. So stellt sich die Frage, ob es erforderlich ist, sie strafrechtliche zur Verantwortung zu ziehen, oder nicht. Der heutigen Wissenschaft nach sind die Softwares, so selbständig und rational sie auch handeln, nicht in der Lage, ohne menschliche Eingriffe zu handeln.

In Bezug auf die strafrechtliche Verantwortlichkeit für das Verhalten der schwachen künstlichen Intelligenzen kann nachstehende Feststellung gemacht werden.

Wenn eine schwache KI das Werkzeug eines Deliktes ist, ist die Bestimmung der strafrechtlichen Verantwortlichkeit möglich, wenn das Verhalten des Softwareagenten tatbestandsmäßig ist und ein kausaler Zusammenhang einer vorsätzlichen oder fahrlässigen Begehung durch den Betreiber, Hersteller, oder einer dritten Person beweisbar ist.[33]

Wenn die Wissenschaft in der Zukunft starke MI entwickeln kann, wird sich die Gesellschaft derart ändern, dass die Feststellungen in dieser Studie nicht mehr gültig sein werden.

Der geeignete Schritt des Gesetzgebungssystems wäre, eine auf Generalprävention gerichtete Regelung anzustreben. Denn in einem rechtlichen Umfeld, in dem durch die Aufnahme und Aktualisierung der Asimovschen Gesetze in das Rechtssystem bereits die Herstellung und Verwendung einer potenziell rechtsverletzenden KI illegal ist, würde sich die Frage, ob das rechtsverletzende Verhalten von KIs zur Feststellung der individuellen Haftung des Agenten führen könnte, schnell erübrigen.

X. Erfahrungen des Dreiländerseminars

Vom 8. Juli bis 10. Juli 2021 wurde das rechtsvergleichende Dreiländerseminar in der Organisierung der Universität von Istanbul veranstaltet. Im Zusammenhang mit den deutschen und türkischen Kollegen untersuchten wir, welche Verantwortung die Handlungen der künstlichen Intelligenzen nach sich ziehen. Wegen der Ausbreitung des Coronavirus wurde die Konferenz online veranstaltet, aber es behinderte die erfolgreiche Arbeit nicht. Nach zweitägiger Konsultation haben wir in einer kurzen Präsentation die Unterschiede zwischen der türkischen, der ungarischen und der deutschen strafrechtlichen Regelung zusammengefasst.

Am Anfang unserer Präsentation haben wir anhand des unterschiedlichen *terminus technicus* der betroffenen Länder untersucht, ob es eine Möglichkeit gibt, die künstlichen Intelligenzen zu sortieren. Wir sind zum Schluss gekommen, dass die Regelung der

[33] *Eszteri* (Fn. 4)

schwachen und starken künstlichen Intelligenzen – wie oben dargelegt – nur sehr schwer in die staatliche strafrechtliche Dogmatik aller drei Länder integriert werden kann. Im Wege eines fiktiven Falles haben wir die Haupterfragen der strafrechtlichen Aspekte der künstlichen Intelligenzen präsentiert.

Kampfroboter X hat am 22.05.2021 in der Türkei anstelle eines Feindes einen Zivilisten erschossen. Obwohl zuvor einprogrammiert wurde, dass dies unter keinen Umständen passieren darf, ist aus unerklärlichen Gründen genau dies eingetreten. Problematisch ist nun, dass dieses rechtswidrige Verhalten – der Tod eines anderen Menschen – keiner natürlichen Person zugerechnet werden kann. Das gesamte Geschehen ist außerhalb jeglichen Verantwortungsbereichs einer oder mehrerer natürlichen Personen.

Da dies aber in der Türkei zu großem Aufruhen im Volk führt, beschließt die türkische Regierung gemeinsam mit der deutschen und ungarischen, ein Richter-Gremium mit der Frage zu beauftragen, ob man im vorliegenden Fall möglicherweise den Kampfroboter selbst bestrafen kann.

Angesichts der Spezifität des Themas und die Regelungen haben wir den Mittelpunkt unserer Untersuchung in der Trias der Handlungsfähigkeit und Schuldfähigkeit der künstlichen Intelligenzen und der Strafzwecke bestimmt.

Zuerst haben wir die Handlungsfähigkeit der intelligenten Agenten beobachten. Der Unterschied zwischen den Dogmatiken der drei Länder besteht darin, dass während wir in Ungarn nur die kausale Handlungslehre benutzen, was ein menschliches Verhalten darstellt, das in der Außenwelt bestimmte Folgen hat, in der Türkei daneben auch die finale Handlungslehre benutzt wird, was Handlungen als vom steuernden Willen beherrschtes, zielgerichtetes menschliches Verhalten definiert. Die deutsche Dogmatik enthält außerdem noch die soziale Handlungslehre – jedes vom menschlichen Willen beherrschtes oder beherrschbares sozial erhebliches Verhalten – und das sogenannte algorithmische Unrecht was vergleichbar mit der Forderung nach einer echten Unternehmensstrafbarkeit ist.

Im Vergleich der Schuldfähigkeit vertreten Ungarn und die Türkei die gleiche Ansicht. Es wird der normativer Schuldbegriff benutzt. Das bedeutet, dass die strafrechtliche Schuldfähigkeit mehrere Elemente umfasst. Diese sind das geeignete Absetzalter, die Zurechnungsfähigkeit, Vorsatz, Fahrlässigkeit und die Zumutbarkeit (maßgebliches Kriterium: freier Wille und Bewusstsein). In Deutschland wird er um den funktionalen Schuldbegriff erweitert, was bedeutet, dass eine Bestrafung in diesem Konzept nicht mit einem ethischen Vorwurf verbunden ist, sondern vielmehr symbolisch der Restauration der verletzten Normgeltung des Täters gilt, um ein Aufrechterhalten der rechtlichen Ordnung zu erwirken.

Bei der Frage der Strafzwecke vertreten die drei Länder fast übereinstimmende Meinungen. Die Generalprävention (Erhaltung und Stärkung des Vertrauens der Allgemeinheit in die Bestands- und Durchsetzungskraft der Rechtsordnung) und die Spezialprävention (durch Strafen wird der Täter davon abgehalten, wieder eine Straftat zu begehen) sind in der Strafdogmatik jedes der Länder präsent, mit einigen Ergänzungen, zum Beispiel in Deutschland um die Vereinigungstheorie und in Ungarn um die Funktion der Resozialisierung und Isolation.

Ember, Diána Magdolna
Ehemalige Studentin, Universität Szeged

RANSOMWARE – DIGITALE ERPRESSUNG DER VERURSACHTE SCHADEN IST GRÖSSER, ALS DIE WELTWEITEN EINNAHMEN AUS DEM ILLEGALEN DROGENHANDEL

I. Einführung

I. 1. Allgemeine Einführung in die Cyberkriminalität

Computer sind in unserem Leben allgegenwärtig, gesellschaftliche und wirtschaftliche Prozesse hängen zunehmend von Informationssystemen ab. Neben den Vorteilen der IT und der technologischen Entwicklung bestehen auch Gefahren, da die Chancen moderner Technologien auch von Kriminellen ausgenutzt werden. Als Ergebnis ist eine neue Art von Kriminalität entstanden: Cyberkriminalität. Dabei handelt es sich um eine besonders gefährliche grenzüberschreitende Kriminalität mit hoher Latenz.[1]

Heutzutage haben sich mit der Erweiterung der Möglichkeiten der Computernutzung verschiedene Schadprogramme (Malware, Viren) verändert. Für neue Zwecke werden sie in eine neue Nutzungsform hineingeboren. Durch die Möglichkeiten des Internets können Viren ihre ungewollte Wirkung entfalten und sich explosionsartig im World Wide Web verbreiten.[2]

I. 2. Anschläge in Ungarn

Schwerwiegende Angriffe auf Informationssysteme tauchen immer häufiger in den Nachrichten auf, unter denen immer mehr Fälle mit Ungarnbezug zu hören sind. Der weltweite Erpressungsvirus-Angriff im Mai 2017 traf auch Ungarn. Der WannaCry-Ransomware-Virus hat die Systeme von etwa 45 ungarischen Regierungsbehörden infiziert, und der durchschnittliche Benutzer hat auch die Auswirkungen des Angriffs erlebt. Ende Juni 2017 wirbelte ein Erpresservirus namens Petya ähnlichen Staub auf, der auch die Computer ungarischer Nutzer erreichte. Im November 2017 war die Website der Scientology Kirche in Ungarn überlastet.[3]

---

[1] *Mezei,* A kiberbűncselekmények hazai szabályozásának aktuális kérdései, Magyar Jog 5/2019, S. 305-314.

[2] *Nagy/Mezei,* A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa, in: Szent Lászlótól a modernkori magyar rendészettudományig. Pécsi Határőr Tudományos Közlemények (19), Pécs, 2017. S. 163-168.

[3] https://index.hu/tech/2017/05/12/kibertamadas_erhetett_angliai_korhazakat/

Bei Angriffen auf Informationssysteme spielt die Prävention eine zentrale Rolle, was wir schon unzählige Male über Cybersicherheit gehört haben. Ungarn ist weltweit führend bei Malware-Infektionen. Es ist problematisch, dass die für Cyberkriminalität verwendeten Begriffe nicht genau die gleiche Bedeutung haben. Um wirksame Maßnahmen zu ergreifen, ist es jedoch sehr wichtig, dass die Begriffe mit einer einzigen Bedeutung verwendet werden.[4]

I. 3. Aufbau des Aufsatzes

In der ersten Hälfte des Aufsatzes versuche ich die Begriffe zur Beschreibung von Cyberkriminalität zu systematisieren und abzugrenzen. Das zentrale Thema meines Beitrags sind die Erpressungsviren. Zuerst möchte ich das Konzept, die Typen und die Eigenschaften des Erpressungsvirus vorstellen. Ich versuche die ungarischen Regeln bezüglich Erpressungsviren darzustellen und die Möglichkeiten der Abwehr dieser Angriffe zu beschreiben. Dann nehme ich eine vergleichende Analyse zwischen der digitalen Erpressung und dem Verbrechen der „klassischen" Erpressung vor.

Zum Schluss würde ich *de lege ferenda* Vorschläge verfassen, wie man effektiv mit Erpressungsviren umgehen könnte.

II. Verbrechen gegen das Informationssystem

II. 1. Beschreibung der Konzepte, die im Zusammenhang mit dem Thema auftauchen, Darstellung der Unterschiede und Ähnlichkeiten zwischen ihnen

Insbesondere halte ich es für wichtig zu klären, was unter dem Begriff Cyberkriminalität zu verstehen ist. Weder Praxis noch Gesetzgebung haben bisher eine einheitliche Terminologie für den Begriff der Cyberkriminalität entwickelt. In der Literatur kursieren zahlreiche Konzepte über Straftaten mit einem informationstechnologischen Element. Das Thema wird auch in einer großen Menge ausländischer und ungarischer Literatur behandelt[5], aber die Konzepte im Zusammenhang mit IT-Kriminalität sind noch ziemlich unklar.

Neben dem terminologischen Unklarheit besteht das Problem darin, dass sich die Elemente der Informationstechnologie im Handlungsspielraum schneller ändern, als die Strafverfolgungsbehörden darauf reagieren könnten. Hier werden die Bedeutung und das Verhältnis der folgenden Begriffe diskutiert: Computerkriminalität, Computerbezogene Verbrechen, IT-Kriminalität, Cyberkriminalität, elektronische Kriminalität, Hightech-Kriminalität.[6]

---

[4] *Sorbán,* Vírusok és zombik a büntetőjogban: Az információs rendszer és adatok megsértésének büntető anyagi és eljárásjogi kérdései, In medias res 7/2018, S. 369-386.

[5] z. B. *Kiss,* Kibervédelem a bűnügyi tudományokban. Budapest, 2020; J. *Holt,* Cybercrime Through an Interdisciplinary Lens, London, 2016.

[6] Európai Közösségek Bizottság: „A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának-A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé", Közlemény, Brüsszel, 2007, S. 2.

Laut *Imre Szabó* umfasst der Begriff Cyberkriminalität *„Delikte, die mit einem Computersystem oder Computerdaten in Verbindung gebracht werden können, indem sie entweder als Mittel zur Begehung einer Straftat oder als Gegenstand der Straftat erscheinen“.*[7]

Laut *Eszter Siegler* gehören die Computerdelikte zu dieser Kategorie, für die der Computer das Instrument oder der Gegenstand einer Straftat ist. Sie wendet den Begriff der Cyberkriminalität nur auf Straftaten an, die sich speziell gegen das Computersystem richten.[8]

Laut der Bekanntmachung des Europäischen Gerichtshofs aus dem Jahr 2007 ist der Begriff der Cyberkriminalität folgender: Handlungen, die unter Verwendung oder mit Netzwerken und Informationssystemen dagegen begangen worden sind.[9]

Im ungarischen Rechtssystem ersetzte das Gesetz Nr. C aus dem Jahre 2012 (im Weiteren: uStGB) den Begriff des Computers durch den Begriff des Informationssystems, wodurch der Begriff der Computerkriminalität etwas obsolet wurde und dem Begriff der Cyberkriminalität und der Informationssystemkriminalität Platz machte. Das ungarische Strafgesetzbuch definiert jedoch den Begriff des Informationssystems mit dem gleichen Inhalt wie der bisherige Begriff des Computersystems, so dass die Begriffe der IT-Kriminalität in Bezug auf Computerkriminalität wesentlichen synonym interpretiert werden können. Die Bedeutungen der Begriffe IT und Computertechnik sind nicht genau gleich, aber dieser Unterschied ist rechtlich vernachlässigbar.

Die Kategorie der Cyberkriminalität bezieht sich auf Handlungen, an denen ein Computernetzwerk beteiligt ist.

Im Folgenden beschäftige ich mich kurz mit dem Begriff der elektronischen Kriminalität und der Hightech-Kriminalität (digital crime, e-crime, high-tech crime). E-Crime ist die Nutzung vernetzter Computer oder des Internets, um eine Straftat zu begehen oder deren Begehung zu erleichtern (ähnlicher Begriff: Elektronische Kriminalität, High-Tech Kriminalität). Die Kategorie der High-Tech-Kriminalität umfasst jede Handlung, die in einer Offline- oder Online-Umgebung begangen wird, bei der das Mittel oder der Gegenstand der Straftat auf dem höchsten Niveau des aktuellen Standes der Wissenschaft und der Technik liegt. Der Inhalt dieser Erläuterung ist ziemlich relativ, da sich Wissenschaft und Technologie ständig weiterentwickeln und verändern.[10]

II. 2. Typische Bereiche der Cyberkriminalität

Computerkriminalität berührt meist den wirtschaftlichen Bereich, da sie typischerweise im Interesse der materiellen, wirtschaftlichen und finanziellen Vorteile begangen wird. Der andere typische Bereich ist außerdem die Informationssicherheit. Das Interesse an der Integrität der verschiedenen geschützten, vertraulichen Daten ist von größter Bedeutung

---

[7] *Szabó,* Informatikai bűncselekmények, in: Dósa Imre (Hrsg.), Az informatikai jog nagy kézikönyve, Budapest, 2008.

[8] *Siegler,* A számítógéppel kapcsolatos és a számítógépes bűncselekmények, Magyar jog, 12/1997, S. 736-742.

[9] Európai Közösségek Bizottság: „A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és a Régiók Bizottságának-A számítógépes bűnözés elleni küzdelemre vonatkozó általános politika felé”, Közlemény, Brüsszel, 2007, S. 2.

[10] *Sorbán* (Fn. 4) S. 369-386.

und deren Erwerb durch Unbefugte oder Gruppen verursacht nicht nur einen schweren Schaden, sondern stellt auch eine unvorstellbare Einnahmequelle für die Täter dar.

II. 2. 1. Täter von Cyberkriminalität

Bei den Tätern von Cyberkriminalität im kriminologischen Sinn handelt es sich im Allgemeinen um hochqualifizierte Fachleute. Je nach Alter sind sie in der Regel 18-45 Jahre alt und in der Regel männlich. Typisch ist auch, dass diese Taten allein begangen werden, möglicherweise von einer kleinen Gruppe von Kriminellen.[11]

Der Begriff „Hacker" wird üblicherweise für IT-Experten verwendet, die über ein außergewöhnlich hohes Maß an Fachwissen und Erfahrung verfügen. Nach einer der gängigsten Ansichten lassen sich Hacker nach folgendem Aspekt unterscheiden. Es gibt die sog „Black Hat"-Hacker, auch „Cracker" genannt, die unter anderem in das System eindringen, um Schaden anzurichten oder sich Zugang zu wertvollen Informationen zu verschaffen. Der „White Hat"-Typ ist auf Fälle beschränkt, in denen der Hacker ausdrücklich dazu autorisiert ist. Als Ethical Hacker gelten daher nicht diejenigen Personen, die von sich aus unbefugt nach Programmfehlern oder Sicherheitslücken suchen, sondern nur diejenigen, die dazu in irgendeiner Form berechtigt sind.[12]

Ein *psychologischer Manipulator* ist nichts anderes als ein Hacker, der die Schutzmaßnahmen umgeht, indem er Benutzer mit Privilegien täuscht. Das heißt, ein autorisierter Benutzer gibt vertrauliche Informationen, Daten oder Passwörter, die zum Anmelden erforderlich sind, an eine unbefugte Person weiter. Ein *Pirat,* der wegen Täuschung oder aus Überzeugung ein Verbrechen in einer Computerumgebung begeht, um finanziellen Gewinn zu erzielen.[13]

III. Ungarische Vorschriften zum Informationssystem

Dieser Teil der Arbeit stellt die ungarische Regulierung der Cyberkriminalität vor, ich möchte jedoch zunächst kurz auf die internationalen Dokumente verweisen, die für das uStGB maßgeblich waren. Die Budapester Konvention von 2001 wurde von den meisten Ländern unterzeichnet und ratifiziert. Die Budapester Konvention war das erste multilaterale Rechtsdokument in diesem Bereich, das eine einheitliche Definition der Computerbegriffe vorsah. Die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme in der Europäischen Union hat zwei Hauptziele: die Festlegung von Mindeststandards für Straftaten gegen Informationssysteme und strafrechtliche Sanktionen sowie die Erleichterung der Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten und den einschlägigen spezialisierten Agenturen der Union und ihrer Organe. Die Studie befasst sich mit „Straftaten gegen den Zugang, die Integrität und die Vertraulichkeit von Computersystemen und Daten" in Titel I des Budapester Übereinkommens[14].

---

[11] https://core.ac.uk/download/pdf/322883718.pdf

[12] *Furnell,* Hackers, viruses and malicious software. in: Jewkes/Yar, Handbook of Internet Crime. Willan Publishing, 2010, S. 43-45.

[13] https://core.ac.uk/download/pdf/322883718.pdf

[14] *Gyaraki,* A számítógépes bűnözés nyomozásának problémái. Dissertation, Pécs, 2018.

Im Folgenden möchte ich mich der Darstellung der im Strafgesetzbuch festgestellten Straftaten zuwenden.

III. 1. Verbrechen gegen das Informationssystem

III. 1. 1. Verletzung von Informationssystemen oder -daten:

In § 423 uStGB wird die Verletzung von Informationssystemen oder- daten geregelt.[15] Das geschützte Rechtsgut ist das Interesse am ordnungsgemäßen Funktionieren der Informationssysteme und der Zuverlässigkeit, Authentizität und Vertraulichkeit der darin gespeicherten, verarbeiteten und übermittelten Daten. Die Verletzung des mechanischen Schutzes des Computers wird durch den Tatbestand der Sachbeschädigung geregelt.[16]

Ein Informationssystem ist jedes Gerät, das automatisch eine Datenverarbeitung durchführt, d.h. Dateneingabe, -verwaltung, -speicherung und -übertragung. Informationssysteme umfassen auch Einheiten mit einem auf Computerdatenverarbeitung basierenden Speicher, die sich im Aussehen von herkömmlichen Computern unterscheiden.

Um der Tatbestand zu verwirklichen muss das Informationssystem über irgendeinen Schutz verfügen. Dies kann ein Passwort, eine Benutzer-ID oder eine Firewall sein. Ohne den Schutz kann man über keinen unbefugten Zugang bzgl. des Tatbestandes sprechen. Also der Zugang ist nicht unbefugt, wenn das Informationssystem nicht geschützt ist oder der Schutz nicht aktiviert wird, weil diese Bedingungen nebeneinander bestehen.[17]

Auch die Methode des Begehung wurde bestimmt, so dass der eigentliche Eintritt erfolgte, wenn der Eintritt unter Verletzung oder Umgehung der Sicherheitsmaßnahme erfolgte, beispielsweise durch Ausnutzen der Mängel des Sicherheitssystems, um unautorisiert, mit autorisierten Passwörtern oder Zugangscodes, aber die Art des Erwerbs ist

---

[15] § 423 (1) uStGB Wer unter Beschädigung oder Ausspielen der den Schutz der Informationssysteme gewährleistenden technischen Maßnahmen unerlaubt in ein Informationssystem eindringt oder unter *Überschreitung* bzw. Verletzung des Rahmens seiner Zugangsberechtigung im System verbleibt, ist wegen eines Vergehens mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
(2) Wer
a) den Betrieb des Informationssystems unerlaubt oder unter Verletzung des Rahmens seiner Berechtigung behindert oder
b) die im Informationssystem erfassten Daten unerlaubt oder unter Verletzung des Rahmens seiner Berechtigung verändert, löscht oder zugänglich macht,
ist wegen eines Verbrechens mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
(3) Die Strafe ist wegen eines Verbrechens eine Freiheitsstrafe von einem Jahr bis zu fünf Jahren, wenn die in Absatz 2 definierten Straftaten eine bedeutende Anzahl von Informationssystemen berühren.
(4) Die Strafe ist eine Freiheitsstrafe von zwei Jahren bis zu acht Jahren, wenn die Straftat
gegen öffentliche Versorgungsbetriebe begangen wird.
(5) Die Daten im Sinne dieses Paragraphen stellen das Erscheinen der in Informationssystemen gespeicherten, verwalteten, verarbeiteten oder weitergeleiteten Tatsachen, Informationen oder Begriffe in jeder Form dar, die zur Aufarbeitung durch das Informationssystem geeignet ist, einschließlich des Programms, das die Ausführung einer Funktion durch das Informationssystem gewährleistet."

[16] *Mezei,* A kiberbűnözés szabályozási kihívásai a büntetőjogban. Ügyészek Lapja 4-5/2019.

[17] *Nagy,* XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények, in: Tóth/Nagy (Hrsg), Magyar Büntetőjog: Különös rész, Budapest, 2014.

gleichgültig.[18] Ein Versuch kann erkannt werden, wenn der Täter versucht, den Schutz des Computers zu umgehen, sich aber noch nicht einloggen konnte.

Gemäß § 423 Abs. 2 Buchst. a) uStGB wird wegen eines Verbrechens mit Freiheitsstrafe bis zu drei Jahren bestraft, wer unbefugt oder unter Verletzung der Grenzen seiner Befugnisse den Betrieb des Informationssystems behindert. In diesem Fall definiert das Gesetz jedoch nicht die relevanten Täterverhalten, weshalb jede Tat tatbestandlich sein kann, die eine Behinderung des Betriebs des Informationssystems zur Folge hat. Behinderung bedeutet nicht nur, dass das System nicht oder nicht ordnungsgemäß funktioniert, sondern auch, dass das System nicht geeignet ist, die bestimmungsgemäße Aufgabe zu erfüllen. Und das Bewusstsein des Täters muss die Tatsache verstehen, dass seine Handlung den Betrieb des Informationssystems rechtswidrig behindert.[19]

Gemäß § 423 Abs. 2 Buchst. b) uStGB wird mit Freiheitsstrafe bis zu drei Jahren bestraft, wer auch nur ein einziges Datum im Informationssystem unbefugt oder entgegen seiner Befugnis verändert, löscht oder unzugänglich macht. Es ist nicht erforderlich, dass die Handlung das Ergebnis der Datenverarbeitung beeinflusst oder andere nachteilige Folgen eintreten.[20]

Die in § 423 Absatz 2 uStGB definierte Straftat betrifft eine erhebliche Anzahl von Informationssystemen, das Gesetz definiert jedoch nicht, was als erhebliche Anzahl gilt.

Der minder schwere Fall des § 423 Abs. 1 uStGB erklärt den unbefugten Zugriff auf das Informationssystem für strafbar. Unbefugte Zugriffe können auf den vom Täter verwendeten Rechner oder das darüber erreichbare geschützte Rechnernetz abzielen. Die Straftat ist nicht zielgerichtet, daher ist es keine Voraussetzung dafür, dass die Begehung mit der Absicht begangen wird, einen Gewinn zu erzielen oder Schaden zu verursachen. Es ist auch nicht erforderlich, dass der Täter später irgendwelche Operationen an den im Informationssystem gespeicherten Daten durchführt oder sogar den Betrieb des Systems behindert. Das unbefugte Betreten ist daher an sich strafbar. Wenn darauf weitere unerlaubte Handlungen folgen, ist eine der Wendungen in den folgenden Absätzen bereits realisiert.

Im anderen klassifizierten Fall beträgt die Strafe Freiheitsstrafe von zwei bis acht Jahren, wenn die Straftat gegen ein Unternehmen von öffentlichem Interesse begangen wird.

Digitale Erpressung ist ein sehr gutes Beispiel für diese Art von Kriminalität. Die größte Bedrohung in den letzten Jahren war die Ransomware ein bösartiges Programm, das Dateien entschlüsselt, die auf einem infizierten Computer oder mobilen Gerät gespeichert sind, sogar die gesamte Datendatei, wodurch sie für das Opfer völlig unzugänglich wird und dann ein hohes Lösegeld für die Wiederherstellung, den Entschlüsselungscode berechnet wird. Die Software kann auch eine Zahlungsfrist setzen, nach der die Daten dauerhaft gesperrt werden. Es ist fast unmöglich, die Identität der Täter herauszufinden, da das „Lösegeld" meist in der schwer auffindbaren virtuellen Währung, in einer sogenannten Kryptowährung wie Bitcoin oder Altcoin verlangt wird. Die Zahlung des Geldes garantiert auch nicht, dass der Erpresser die gesperrten Daten entschlüsseln wird.[21]

---

[18] *Mezei* (Fn. 15) S. 4-5.

[19] *Molnár,* A pénzmosás, in: Belovics/Molnár/Sinku (Hrsg.), Büntetőjog II. Különös Rész, Budapest, 2018, S. 948.

[20] *Mezei* (Fn. 15) S. 4-5.

[21] *Mezei,* A kiberbűncselekmények hazai szabályozásának aktuális kérdései, in: Magyar Jogászegyleti Értekezések, Magyar Jogász Egylet, Budapest, 2018. S. 157-173.

III. 1. 2. Betrug unter Nutzung eines Informationssystems

Der Betrug unter Nutzung eines Informationssystems, fällt unter das Strafgesetzbuch. Dieser Tatbestand wird in § 375 geregelt, der zu den Vermögensdelikten (und nicht den Computerdelikten) gehört. [22]

Im Gegensatz zur Benennung des Tatbestandes kann der Betrug unter Nutzung eines Informationssystem nicht als richtigen Betrug angesehen werden. Unter anderem fehlt es bei dem hier erörterten Tatbestand am Irrtumselement. Daher ist Betrug unter Nutzung eines Informationssystems kein spezifisches Delikt im Vergleich zum „klassischen" Betrug, sondern lediglich eine weitere Straftat, die im gegebenen Fall neben dem Betrug, unabhängig davon, festgestellt werden soll. Die Straftat ist zielgerichtet, kann also nur mit direkter Absicht begangen werden. Im Hinblick auf den Tatausgang und den Schadenseintritt genügt aber auch der Eventualvorsatz. Das Erzielen eines illegalen Gewinns ist jedoch nicht erforderlich, es liegt bereits außerhalb des Rahmens der Tatsachen. Die Tat beginnt in der Regel mit der Einleitung einer rechtswidrigen IT-Manipulation und endet mit dem Eintritt des Schadens.[23]

---

[22] § 375 uStGB Betrug unter Nutzung eines Informationssystems
(1) Wer zur Erzielung eines unberechtigten Vermögensvorteils Daten in ein Informationssystem eingibt bzw. die darin gespeicherten Daten verändert, löscht oder unzugänglich macht bzw. mit der Durchführung sonstiger Operationen die Funktion des Informationssystems beeinflusst und damit einen Schaden verursacht, ist wegen eines Verbrechens mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
(2) Die Strafe ist eine Freiheitsstrafe von einem Jahr bis zu fünf Jahren, wenn
a) der unter Nutzung eines Informationssystems begangene Betrug einen bedeutenden Schaden verursacht oder
b) der einen größeren Schaden verursachende und unter Nutzung eines Informationssystems begangene Betrug in einer Bande oder gewerbsmäßig begangen wird.
(3) Die Strafe ist eine Freiheitsstrafe von zwei Jahren bis zu acht Jahren, wenn
a) der unter Nutzung eines Informationssystems begangene Betrug einen besonders hohen Schaden verursacht oder
b) der einen bedeutenden Schaden verursachende und unter Nutzung eines Informationssystems begangene Betrug in einer Bande oder gewerbsmäßig begangen wird.
(4) Die Strafe ist eine Freiheitsstrafe von fünf Jahren bis zu zehn Jahren, wenn
a) der unter Nutzung eines Informationssystems begangene Betrug einen besonders bedeutenden Schaden verursacht oder
b) der einen besonders hohen Schaden verursachende und unter Nutzung eines Informationssystems begangene Betrug in einer Bande oder gewerbsmäßig begangen wird.
(5) Nach den Absätzen 1 bis 4 ist zu bestrafen, wer unter Verwendung falscher, gefälschter oder unerlaubt erworbener elektronischer bargeldloser Zahlungsmittel oder mit der Annahme einer Zahlung mit solchen Zahlungsmitteln einen Schaden verursacht.
(6) Im Sinne von Absatz 5 erhalten im Ausland ausgegebene elektronische bargeldlose Zahlungsmittel denselben Schutz wie im Inland ausgegebene bargeldlose Zahlungsmittel.

[23] *Szomora,* Btk. XXXV. Fejezet A vagyon elleni bűncselekmények, in: Karsai (Hrsg.), Kommentár a Büntető Törvénykönyvhöz, Complex Kiadó, Budapest, 2013, S. 788.

III. 1. 3. Ausspielen der technischen Maßnahmen zum Schutz von Informationssystemen

Insgesamt wird die Ausführung von Cyber-Angriffen durch den einfachen Zugang zu den für die Begehung von Straftaten erforderlichen Kenntnissen und Programmen sowie der bereits vorhandenen Botnet-Infrastruktur erheblich erleichtert. Deshalb ist es wichtig, dass auch vorbereitende Taten bereits als Straftaten definiert werden. § 424 uStGB regelt den Tatbestand der Umgehung einer technischen Maßnahme zum Schutz eines Informationssystems. Gegenstand der Straftat sind das Passwort, das Computerprogramm sowie die wirtschaftlichen, technischen und organisatorischen Kenntnisse im Zusammenhang mit deren Erstellung.[24]

IV. Allgemeine Eingenschaften der digitalen Erpressung

Neben den unbestreitbar positiven Auswirkungen der IT-Entwicklung hat sie leider auch eine Schattenseite, die sich am deutlichsten in der Verbreitung von Cyberangriffen zeigt. Eines der häufigsten Beispiele für einen Cyberangriff ist Ransomware. Mit der zunehmenden Nutzung des Internets nimmt heute auch die Verbreitung von Computerviren zu.

IV. 1. Was ist Ransomware / Erpressungssoftware?

Ein Erpresserprogramm ist ein bösartiges Programm (Malware, bösartige Software), das Benutzer daran hindert, auf ihre persönlichen Daten oder Dateien zuzugreifen, was dazu führt, dass der Erpresser ein Lösegeld fordert, um wieder Zugriff zu gewähren.

Nicht nur Einzelpersonen, sondern auch verschiedene Unternehmen, Krankenhäuser und Behörden können Opfer dieser Art von Angriffen werden, da die Letzteren viel stärker erpresst werden können, indem ihre Daten unzugänglich gemacht werden. In den meisten Fällen verlangen Erpresser, dass das Lösegeld wegen ihrer Unauffindbarkeit in Kryptowährung gezahlt wird.

[24] § 424 uStGB Ausspielen der technischen Maßnahmen zum Schutz von Informationssystemen
(1) Wer zum Begehen der in § 375, § 422 Absatz 1 Buchstabe d oder § 423 definierten Straftat
a) die dazu notwendigen oder dies erleichternden Passwörter oder Computerprogramme erstellt, übergibt, zugänglich macht, erwirbt oder in Umlauf bringt bzw.
b) sein ökonomisches, technisches bzw. organisatorisches Wissen zur Erstellung der zum Begehen der besagten Straftat notwendigen oder dies erleichternden Passwörter oder Computerprogramme einer anderen Person zur Verfügung stellt,
ist wegen eines Vergehens mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
(2) Nicht bestraft werden darf der Täter der in Absatz 1 Buchstabe a definierten Straftat, wenn er – bevor der in Strafsachen vorgehenden Behörde die Erstellung der zum Begehen der Straftat notwendigen oder diese erleichternden Passwörter oder Computerprogramme bekannt wird – der Behörde seine Tätigkeit aufdeckt, ihr die erstellten Sachen übergibt und die Ermittlung der Identität der an der Erstellung beteiligten anderen Personen ermöglicht.
(3) Passwörter im Sinne dieses Paragraphen sind alle aus Zahlen, Buchstaben, Zeichen, biometrischen Daten oder deren Kombination bestehenden Codewörter, die den Zugang zu Informationssystemen oder deren Teilen ermöglichen.

IV. 2. Wie gelangt das Schadprogramm in das System?

Ransomware dringt normalerweise wie ein Computervirus in das System ein. Dies geschieht häufig durch das Öffnen von E-Mail-Anhängen. Zu diesem Zweck werden E-Mails mit angeblichen Rechnungen oder Auftragsbestätigungen beispielsweise unter Verwendung von echten Firmennamen und Firmenadressen versendet. Allerdings befindet sich im Anhang kein Account, sondern ein sogenannter Downloader, der die Schadsoftware nachlädt.

IV. 3. Wie kann man sich gegen die Ransomware verteidigen?

Die wirksamste Abwehr solcher Viren ist die Prävention. Daher soll man sich der neuesten Bedrohungen bewusst sein, den Besuch verdächtiger Websites unterlassen, die Software auf dem neuesten Stand halten und ein Antivirenprogramm herunterladen, das erkennt, ob bei den Softwares ein Infektionsrisiko besteht.

Erpresser geben sich oft als Beamte (z. B. Finanzbehörde, Finanzamt oder andere Behörde) aus, aber solche Angriffe sind relativ leicht zu erkennen. Der Grund dafür ist, dass in der Formulierung ihrer Briefe manchmal grammatikalische Fehler und seltsame Ausdrücke im Vergleich zu echten offiziellen Briefen zu finden sind.

Sollte unser Computer bereits infiziert sein, ist es wichtig, auf keinen Fall Lösegeld zu zahlen, sondern die Hilfe eines IT-Sicherheitsexperten in Anspruch zu nehmen und in der Zukunft ein legitimes, zuverlässiges Antivirenprogramm zu verwenden.

Ohne eigenen IT-Sicherheitsspezialisten müssen sich Betreiber größerer IT-Infrastrukturen rechtzeitig externe Unterstützung holen, um Angriffe durch Kriminelle zu verhindern. Eine gute Prävention und Reaktion ist nur mit Hilfe von Fachpersonal möglich.

IV. 5. Vergleich mit der Erpressung

Wie ich bereits erwähnt habe, ist die digitale Erpressung eines der Verbrechen gegen das Informationssystem im ungarischen Strafgesetzbuch. Ich finde es aber auch wichtig, es mit dem Verbrechen der Erpressung zu vergleichen. Im Folgenden möchte ich auch auf die Unterschiede und Gemeinsamkeiten der beiden Delikte eingehen.

Der Name Ransomware als digitale Erpressung im ungarischen Strafgesetzbuch kann mit Erpressung in Verbindung gebracht werden.[25] Es zeigt sich auch, dass jeder, der digitale Erpressung begeht, tatsächlich eine Erpressung begeht, mit dem Unterschied, dass sie im

[25] § 367 uStGB Erpressung
(1) Wer zur Erzielung eines unberechtigten Vermögensvorteils eine andere Person mit Gewalt oder durch Drohung zu einer Handlung, Unterlassung oder Duldung nötigt und damit einen Vermögensnachteil verursacht, ist wegen eines Verbrechens mit Freiheitsstrafe von einem Jahr bis zu fünf Jahren zu bestrafen.
(2) Die Strafe ist eine Freiheitsstrafe von zwei Jahren bis zu acht Jahren, wenn die Erpressung
a) in einer Bande,
b) mit einer gegen Leib oder Leben gerichteten bzw. anderen *ähnlich* schweren Bedrohung,
c) als Amtsträger unter Nutzung dieser Eigenschaft,
d) unter Vortäuschung eines behördlichen Auftrags oder einer solchen Eigenschaft
begangen wird.

Cyberspace stattfindet. Allerdings erwähnt das ungarische Strafgesetzbuch sie dennoch nicht als Erpressung erwähnt, sondern als IT-Verbrechen einstuft, während Erpressung zu den gewalttätigen Vermögensstraftaten zählt.

V. Rechtsvergleich

Im nächsten Kapitel vergleiche ich die ungarischen und deutschen Vorschriften zum Thema Ransomware. Ich möchte die Gemeinsamkeiten und Unterschiede zwischen den beiden Rechtsordnungen darstellen.

V. 1. Unterschiede der Ahndung durch das deutsche und ungarische Recht bei Ransomware

V. 1. 1. Unterschiede

Die Bedeutung der Begriffe, die sich im Zusammenhang mit dem Gegenstand in der deutschen Gesetzgebung ergeben, ist im Großen und Ganzen die gleiche wie im ungarischen Recht. Der einzige Unterschied besteht in den Namen. Ein Beispiel dafür ist, dass das, was im deutschen Recht Internetkriminalität heißt, im ungarischen Recht als Informationssystemkriminalität bezeichnet wird.

Eine weitere wichtige Unterscheidung ist das differenziertere Tatbestandsverständnis. Nach deutschem Recht wird zwischen der Art und Weise des Begehens mit Ransomware unterschieden. Bei der Ansteckung mit dem Erpresservirus wird grundsätzlich zwischen zwei Typen unterschieden: der Infizierung durch eine versendete Datei oder dem „Drive-by-Download" beim Besuch einer inkriminierten Website.

In der ersten Version der Ransomware-Infektion werden manipulierte E-Mails an eine Vielzahl potenzieller Opfer verschickt, bekannt als der .zip-Trojaner. Es schlägt dem Opfer ein Bußgeld vor, das innerhalb kurzer Zeit bezahlt werden muss, da sonst alle Dateien auf dem Rechner gelöscht werden. Die zweite Version der Ransomware-Infektion ist der Drive-by-Download. Bei dieser Methode wird das Erpresserprogramm unwissentlich und unbeabsichtigt heruntergeladen, wenn Benutzer des Systems eine Website besuchen. Es installiert sich dann unbemerkt eine Ransomware. Es soll den automatischen Start des Programms manipulieren und sich darin integrieren. Wenn die Installation erfolgreich ist, dann startet die Malware jedes Mal, wenn das System gestartet wird, was es viel schwieriger oder unmöglich macht, sie zu entfernen.[26]

Im Ungarischen Recht hingegen, werden bei der Art der Begehung mit Ransomware keine Unterschiede gemacht. Vielmehr fasst das ungarische Recht alle Tatbestände und den der „Informationssystemkriminalität" zusammen. So findet der § 423 uStGB, Verletzung von Informationssystemen oder- daten universelle Anwendung. Die digitale Erpressung

[26] *Büchel/Hirsch,* Internetkriminalität. Phänomene-Ermittlungshilfen-Prävention Grundlage der Kriminalistik, Verlagsgruppe Hüthig Jehle Rehm, 2014, S. 88-90.

wird durch eine Straftat begangen (§ 423 uStGB: Verletzung von Informationssystemen oder- daten). Im ungarischen Recht kann es zwei Arten von Straftaten geben.

V. 1. 2. Erpressung

Im deutschen Recht ist der Straftatbestand der digitalen Erpressung in § 253 StGB geregelt. Als Erpressung gilt, wenn der Täter das Opfer bedroht oder mit Gewalt zu einer Handlung, Duldung oder Unterlassung zwingt. Dadurch erleidet das Opfer einen finanziellen Nachteil, mit dem der Täter sich selbst oder einem Dritten einen finanziellen Vorteil verschafft.[27]

Im ungarischen Recht erscheint die Nötigung auch im Verbrechen der Erpressung als Verhalten bei der Tathandlung des Verbrechens. Im Gegensatz zum deutschen Strafrecht ist der Tatbestand der „normalen" Erpressung nicht auf Informationssystemkriminalität anwendbar. Dabei unterscheidet das ungarische Recht zwischen der Erpressung im klassischen Sinn und der Tathandlung mittels eines Informationssystems, gegen ein Informationssystem.

Das Ungarische Recht hat genau für solche Fälle einen eigenen Tatbestand geschaffen, den des Betrugs durch Nutzung von Informationssystemen gem. § 375 uStGB. Auch diese Gesetzesnorm ist nicht auf einen einzigen Tatbestand begrenzt, er lässt sich auf eine Vielzahl von Vergehen neben der digitalen Erpressung, wie zum Beispiel die Datenhehlerei anwenden.

Im ungarischen Recht ist beim Tatbestand der digitalen Erpressung auch der der tatsächlichen Erpressung erfüllt, mit dem Unterschied, dass sie im Cyberspace stattfindet. Allerdings hat das ungarische Strafgesetz die digitale Erpressung als IT-Verbrechen eingestuft, während Erpressung zu den gewalttätigen Vermögensstraftaten gehört.

V. 1. 3. Haftungsprivilegierung

Im ungarischen Recht richtet sich dies nach den Tatsachen der Umsetzung technischer Maßnahmen zum Schutz von Informationssystemen (das ist § 424 II uStGB)

§ 424 uStGB regelt den Tatbestand der Umgehung einer technischen Maßnahme zum Schutz eines Informationssystems. Gegenstand der Straftat sind das Passwort, das Computerprogramm sowie die wirtschaftlichen, technischen und organisatorischen Kenntnisse im Zusammenhang mit deren Erstellung.

Der zweite Absatz besagt:

> *„Nicht bestraft werden darf der Täter der in Absatz 1 Buchstabe a) definierten Straftat, wenn er – bevor der in Strafsachen vorgehenden Behörde die Erstellung der zum Begehen der Straftat notwendigen oder diese erleichternden Passwörter oder Computerprogramme bekannt wird – der Behörde seine Tätigkeit aufdeckt, ihr die erstellten Sachen übergibt und die Ermittlung der Identität der an der Erstellung beteiligten anderen Personen ermöglicht."*

Wenn ich beispielsweise mit meinem Freund ein Programm erstelle, um mich in ein Banksystem einzuloggen, ich aber vor dem Login diese Aktion melde, kann ich nicht bestraft werden.

---

[27] *Joecks/Miebach,* Münchener Kommentar zum Strafgesetzbuch/ Sander 3. Auflage, München, 2017, § 253 StGB Erpressung

Im Gegensatz dazu sieht das deutsche Recht nur die Milderung von Straftaten vor:

„§ 46b StGB Hilfe zur Aufklärung oder Verhinderung von schweren Straftaten

(1) Wenn der Täter einer Straftat, die mit einer im Mindestmaß erhöhten Freiheitsstrafe oder mit lebenslanger Freiheitsstrafe bedroht ist,

1. *durch freiwilliges Offenbaren seines Wissens wesentlich dazu beigetragen hat, dass eine Tat nach § 100a Abs. 2 der Strafprozessordnung, die mit seiner Tat im Zusammenhang steht, aufgedeckt werden konnte,* oder

2. *freiwillig sein Wissen so rechtzeitig einer Dienststelle offenbart, dass eine Tat nach § 100a Abs. 2 der Strafprozessordnung, die mit seiner Tat im Zusammenhang steht und von deren Planung er weiß,* noch verhindert werden kann, kann das Gericht die Strafe nach § 49 Abs. 1 mildern, wobei an die Stelle ausschließlich angedrohter lebenslanger Freiheitsstrafe eine Freiheitsstrafe nicht unter zehn Jahren tritt. Für die Einordnung als Straftat, die mit einer im Mindestmaß erhöhten Freiheitsstrafe bedroht ist, werden nur Schärfungen für besonders schwere Fälle und keine Milderungen berücksichtigt. War der Täter an der Tat beteiligt, muss sich sein Beitrag zur Aufklärung nach Satz 1 Nr. 1 über den eigenen Tatbeitrag hinaus erstrecken. Anstelle einer Milderung kann das Gericht von Strafe absehen, wenn die Straftat ausschließlich mit zeitiger Freiheitsstrafe bedroht ist und der Täter keine Freiheitsstrafe von mehr als drei Jahren verwirkt hat."

V. 2. Gemeinsamkeiten der Ahndung durch das deutsche und ungarische Recht bei Ransomware

V. 2. 1. Haftungsverschärfung

Im nächsten Abschnitt werde ich die Gemeinsamkeiten zwischen der deutschen und der ungarischen Haftungsverschärfung hervorheben.

Nach beiden Gesetzen tritt die Haftungsverschärfung ein, wenn die Straftat eine erhebliche Anzahl von Informationssystemen betrifft, wenn sie gegen einen öffentlichen Dienst verübt wird, wenn sie einen besonders schweren Schaden verursacht oder wenn sie in einer Gruppe begangen wird.

Darauf aufbauend lauten die deutschen Regeln wie folgt:

„§ 303b StGB: Computersabotage

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt."

Das ungarische Recht umfasst auch Haftungsverschärfungen. Das sind die folgenden:

„§ 423: Die Strafe ist wegen eines Verbrechens eine Freiheitsstrafe von einem Jahr bis zu fünf Jahren, wenn die in Absatz 2 definierten Straftaten eine bedeutende Anzahl von Informationssystemen berühren.
Die Strafe ist eine Freiheitsstrafe von zwei Jahren bis zu acht Jahren, wenn die Straftat gegen öffentliche Versorgungsbetriebe begangen wird."

„§ 375: Die Strafe ist eine Freiheitsstrafe von zwei Jahren bis zu acht Jahren, wenn
a) der unter Nutzung eines Informationssystems begangene Betrug einen besonders hohen Schaden verursacht oder
b) der einen bedeutenden Schaden verursachende und unter Nutzung eines Informationssystems begangene Betrug in einer Bande oder gewerbsmäßig begangen wird.
Die Strafe ist eine Freiheitsstrafe von fünf Jahren bis zu zehn Jahren, wenn
a) der unter Nutzung eines Informationssystems begangene Betrug einen besonders bedeutenden Schaden verursacht oder
b) der einen besonders hohen Schaden verursachende und unter Nutzung eines Informationssystems begangene Betrug in einer Bande oder gewerbsmäßig begangen wird."

V. 2. 2. Datenveränderung

Auch in den deutschen und ungarischen Rechtsvorschriften zur Datenveränderung lassen sich Gemeinsamkeiten entdecken. In beiden Regeln gibt es drei gemeinsame Begriffe. Diese Daten werden gelöscht, verändert und unzugänglich gemacht.

Dazu reicht es aus, dass der Täter unerlaubt auf die Daten des Opfers zugreift oder diese einem Dritten zugänglich macht.[28]

Auch § 375 des ungarischen Strafgesetzbuches erwähnt diese Tathandlungen, wonach jeder, der Daten in das Informationssystem eingibt oder die darin gespeicherten Daten ändert, löscht oder unzugänglich macht, um einen unbefugten finanziellen Vorteil zu erlangen, oder den Betrieb beeinflusst das Informationssystem durch andere Handlungen beschädigt und dadurch Schaden verursacht, strafbar ist.

V. 2. 3. Andere Gemeinsamkeiten

Nun noch einige weitere Gemeinsamkeiten: Sowohl das deutsche als auch das ungarische Recht sehen das Vermögen als schützenswertes Individualrechtsgut an: das deutsche Recht im Rahmen des Computerbetrugs gem. § 263a StGB und das ungarische Recht gem. § 375 bei Betrug durch Nutzung eines Informationssystems.

Eine weitere Ähnlichkeit besteht darin, dass der Schaden (und die Verursachung des Schadens) bei beiden Verbrechen auftritt. Das ist die Erfolg dieser Verbrechen. Darüber hinaus haben beide Straftaten mehrere Arten der Begehung. Bei beiden Straftaten taucht auch das Motiv auf, sich einen rechtswidrigen Vermögensvorteil zu verschaffen. Abschließend möchte ich darauf hinweisen, dass beide Verbrechen vorsätzlich sind.

---

[28] *Joecks/Miebach,* Münchener Kommentar zum Strafgesetzbuch/ Sander 3. Auflage, München, 2017, § 303a. StGB

Unterschiede		
Deutsches Recht	**Ungarisches Recht**	**Gemeinsamkeiten**
Täter muss lediglich auf die Daten eines fremden Systems einwirken oder vorgeben dies zu tun	Das System **muss** mit einem Passwort gesichert sein →Täter muss die Schutzbarriere des Systems überwinden oder „brechen“	
	„Informationssystemkriminalität“ ➔ Computer wurde durch Informationssystem ersetzt ➔ Jedoch gleich definiert	Vermögen als Individualrechtsgut, durch § 263a StGB & § 375 uStGB
Die Arten der Begehung unterliegen unterschiedlichen Strafbarkeiten und werden demnach unterschieden .zip-Trojaner und Drive-by-Download	Art der Begehung ist egal, § 423 fasst alle Delikte zusammen, die „Informationssysteme“ betreffen	Computerbetrug, § 263a StGB = Betrug durch Nutzung eines Informationssystems, § 375 uStGB
	§ 423 II, III, IV uStGB Haftungsverschärfung beim Befall von mehreren Systemen sowie von solchen, die der öffentlichen Versorgung dienen oder wenn der Täter in einer Bande gehandelt hat	§ 202c Abs. I, Nr. 2 StGB - Vorbereiten des Ausspähens und Abfangen von Daten, = § 424 I a,b
§ 263a StGB Freiheitsstrafe bis zu 5 Jahre oder Geldstrafe	§ 375 Freiheitsstrafe bis zu 3 Jahre, keine Geldstrafe	
	§ 424 II uStGB – Haftungsprivilegierung für Kronzeugen	
Erpressung i.S.d. § 253 StGB kann vorliegen, wenn der Täter mit einem empfindlichen Übel, wie dem Löschen der Daten droht und das Opfer aufgrund dieser Drohung zur Zahlung genötigt wird. Infolgedessen muss beim Opfer Vermögensnachteil entstehen.	Ransomware ist keine Erpressung im klassischen Sinn, Nebentatbestand da Verbrechen gegen Informationssystem, also § 375 uStGB	
	Wortlaut im ungarischen Recht: „ digitale Erpressen“ = Ransomware	

VI. Schlussfolgerung

Die Zahl der Cyberangriffe steigt von Jahr zu Jahr mit immer gezielteren und komplexeren Angriffen, insbesondere auf kritische Infrastrukturen. Eines der größten Probleme bei Angriffen auf Informationssysteme ist die Ermittlung der Täter, da Ermittlungsbehörden oft nicht in der Lage sind, den genauen physischen Standort der Täter oder die kriminelle Infrastruktur, die für die Ermittlungen von größter Bedeutung sind und die elektronischen Beweismittel zu ermitteln. Bei Angriffen auf Informationssysteme verwenden Täter in der Regel gefälschte IP-Adressen, wodurch eine Identifizierung der Angreifer oder gar der für den Angriff verwendeten Computer unmöglich oder erschwert wird.

Ein weiteres Problem ist, dass sich Täter, Opfer, Daten und Teile der kriminellen Infrastruktur oft in verschiedenen Ländern befinden, was die Frage der Zuständigkeit aufwirft, sogar welches Land in dem Fall handlungsberechtigt ist und nach welcher Rechtsordnung. Dies könnte auch dazu führen, dass die am Fall beteiligten Länder parallel ein Strafverfahren einleiten. Ein weiteres Problem ist die fehlende Regulierung einiger Themen wie Online-Schwarzmärkte und virtuelle Währungen.

Es ist wichtig zu erkennen, dass Cyberkriminalität eine komplexe Reihe von Problemen beinhaltet, gegen die die Anwendung einer mehrstufigen Strategie gerechtfertigt ist. Dabei kommt der Prävention eine herausragende Bedeutung zu, insbesondere der nutzerzentrierten Aufklärung und Wissensvermittlung, denn der Mensch ist immer noch das schwächste Glied in Sachen Cyber-Sicherheit. Es gilt, harmonisierte, einheitliche internationale Regelungen sowohl im Straf- als auch im Verfahrensrecht zu schaffen. Die Förderung der verstärkten Zusammenarbeit ist auch ein wesentliches Element zwischen dem Privatsektor und den Strafverfolgungsbehörden sowie zwischen den einzelnen Strafverfolgungsbehörden. Auch der Gesetzgeber muss schnell auf neue Herausforderungen reagieren und die Straf-

verfolgungsbehörden darauf vorbereiten, da durch die technologische Entwicklung neue Täterschaftsformen geschaffen werden, deren rechtliche Einordnung fraglich sein kann.

Gemäß Richtlinie 2013/40/EUist es daher wichtig, de lege ferenda-Vorschläge wie das Strafgesetzbuch zu machen. Zur Ausweitung der qualifizierten Fälle des § 423 im Rahmen der organisierten Kriminalität oder durch Arbeitnehmer sowie zur Sanktionierung von Persönlichkeitsdiebstahl.

Pincési, Boglárka
Studentin, Universität Szeged

STRAFRECHTLICHE HAFTUNG FÜR HATE-SPEECH DURCH SOCIAL BOTS

I. Einführung

Heutzutage ist es keine Übertreibung zu behaupten, dass die technische Entwicklung Auswirkung auf unser Leben hat. Die dynamische Entwicklung der Technologie stellt eine Herausforderung für das Rechtssystem dar, deshalb ist es wichtig, dass wir diese Probleme und Rechtsfragen beantworten können. Hate-Speech ist kein neues Phänomen, aber es tritt in der Zeit des Internets und der Sozialen Medien in besonders hohem Maße auf. Im Allgemeinen tritt Hate-Speech bei Privatpersonen oder Organisationen dadurch in Erscheinung, dass sie in sozialen Medien posten und kommentieren. Es kann sich bei dem Verwender des Social Bots sowohl um eine natürliche Person, als auch um eine juristische Person handeln. Wobei sich diese Arbeit auf die Untersuchung der Strafbarkeit von natürlichen Personen beschränkt. Obwohl solche Fälle in Ungarn nicht vorgekommen sind, dass Hate-Speech durch Social Bots verwirklicht wird, aber zum Beispiel verbot Facebook aus diesem Grund einen koreanischen Chatbot.[1]

Die Arbeit besteht aus zwei großen Teilen. Der erste Teil befasst sich mit der Vorstellung der Funktionsweise und der technischen Grundlagen der sozialen Bots. In diesem Teil möchte ich den Betrieb und die Erscheinung der sozialen Bots in sozialen Medien darstellen.

Der zweite Teil enthält eine Rechtsvergleich: Wie stehen das deutsche und ungarische Rechtsystem zu diesem Thema? Wie regelt ihr Strafgesetzbuch Hate-Speech? Welche Lösungen verfolgen sie? Welche Ähnlichkeiten und Unterschieden ergeben sich?

Im Zuge der rasanten digitalen Technisierung treten neue Akteure auf die Plan, die nicht menschlich sind, aber aufgrund komplexer Programmierung Aktionen ausführen, die nach herkömmlichem Verständnis nur Menschen bewältigen können.[2] Dabei geht es um drei wohlbekannte Fragestellungen: Ist eine Bestrafung „intelligenter Agenten" denkbar? Kann das Geschehen nach objektiv-normativen Kriterien einer Person als „ihre Tat" zugerechnet werden? Kann diese Person persönlich dafür verantwortlich gemacht werden, das heißt hat sie dieses Geschehen vorsätzlich geprägt?[3]

---

[1] Facebook hat einen koreanischen Chatbot abgeschaltet, der homophobe Nachrichten an Nutzer verschickte. https://hvg.hu/tudomany/20210114_gyuloletbeszed_homofob_chatbot_lee_luda_facebook_messenger. (zugegriffen am 16. Juli 2021).

[2] *Gless/Seelmann,* Intelligente Agenten und das Recht, Baden-Baden, 2016, S. 46.

[3] *Gless/Seelmann* (Fn. 2) S. 46-47.

II. Die Funktionsweise und die Technologie hinter den sozialen Bots

II. 1. Die Funktionsweise

Soziale Bots sind automatisierte soziale Medien-Programme, die in sozialen Medien verwendet werden und menschliche Verhaltensmuster simulieren, daneben als falsches Konto auftauchen.[4] Diese Bots verhalten sich ganz oder teilweise autonom, und dabei handelt es sich um eine Software oder einen Dienst. Oft verwechselt man die sozialen Bots mit den Chatbots. Deshalb ist es erforderlich zwischen diesen beiden Begriffen zu unterscheiden.[5] Social Bots sind häufig mit künstlicher Intelligenz ausgestattet, durch die sie auf unterschiedliche Anfragen reagieren und sich selbständig durch die Möglichkeiten des „Machine Learning" weiterentwickeln können.[6] Dagegen verfügen Chatbots nicht über diese Fähigkeiten. Im Web kann die menschliche Anwesenheit durch Soziale Bots ersetzt werden und somit werden die Benutzer getäuscht. Viele Chatbots können nicht kommunizieren, sondern sind nur zu einfachen Interaktionen fähig. Sie machen z.B. „gefällt mir" Angaben, folgen den Seiten, kommentieren und markieren die Beiträge.[7] Gleichzeitig werden wohlwollende bzw. böswillige und manipulative Chatbots eingesetzt. Wohlwollende Chatbots gewähren Dienstleistungen, wie z.B. Hilfe, wenn man im Netz Produkte sucht. Sie empfehlen Berufsmöglichkeiten. Es existieren sogenannte böswillige und manipulative Chatbots. Diese können zu vielen verschiedenen Zwecken benutzt werden. Sie können den populistischen Politiker begünstigen und die Wahl beeinflussen. Sie erstellen und schicken den Benutzern Spam, außerdem manipulieren sie den Finanzmarkt.[8]

II. 2. Die Technologie hinter den Sozialen Bots

Bei den Sozialen Bots handelt es sich um Algorithmen, die als (semi)automatisierte Agenten vordefinierte Aufgaben wahrnehmen können. Die Aufgaben der sozialen Bots können in drei Teilen geteilt werden:

1. die Benutzerkonten in sozialen Netzwerken,
2. Programmierschnittstellen
3. sowie die in einer beliebigen Programmiersprache verfasste Software mit der Verhaltenslogik des Soziale Bots. Sie führen lediglich das aus, wozu sie von dem Entwickler programmiert wurden.[9]

Diese Bots sind also Roboter, die mit künstlicher Intelligenz arbeiten und mithilfe neuronaler Netze lernen und erstellt werden. Neuronale Netze sind Softwares, die ihre

---

[4] What is a social media bot? https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot. (zugegriffen am 16. Juli 2021).

[5] Ibid.

[6] Chatbots: Wer muss zahlen, wenn der Bot Fehler macht? Ines Rietzler https://www.exali.de/Info-Base/chatbot-haftung. (zugegriffen am 18. Juli 2021).

[7] Fn. 4.

[8] Ibid.

[9] *Kind/Jetzke/Weide//Ehrenberg-Silies/Bovenschulte*, Social Bots, 2017. S. 13.

Arbeitsweise verändern können. Die Bots werden gestartet, indem sie zunächst in einer großen Datenbank trainiert und dann auf die Reise geschickt werden. Die Lerndatenbank sieht in der Regel wie ein vom Bot gespeichertes Gesprächsmuster aus. Die Sätze und die Wörter sind in dem System nicht konkret vorgeschrieben. Wenn die Bots sich viele Gespräche ansehen, wissen sie, was sie sagen können, je nachdem, was die Leute sagen.

Auf dieser Grundlage können wir zwei Modelle von Sozialen Bots unterscheiden: 1. Regelbasierte Ansätze, 2. KI-basierte Ansätze.

1. Diese regelbasierten Frameworks sind im Wesentlichen in der Lage, auf Fragen zu reagieren, worauf es die feststehenden Antworten gibt. Sie stellen ein Gerüst zur Verfügung mit der die Logik für die Textverarbeitung bestimmt wird, die den Benutzer als ein vordefinierter Entscheidungspfad leiten kann. Ihre Logik, um eingehende Anfragen zu interpretieren und entsprechende Antworten zurückgeben zu können, besteht für gewöhnlich aus unzähligen implementierten Regeln. Entsprechen die Nachrichten, sprich Anfragen einem bestimmten Muster werden skriptbasierte Antworten zurückgeliefert.[10]
2. Der maßgebliche Unterschied zwischen KI-basierten und regelbasierten Ansätzen besteht darin, dass die KI-basierten Ansätze bestimmte Technologien wie z.B. „Machine Learning“ und „Deep Learning“ nutzen. Sowohl die vergangenen als auch die zukünftigen Konversationen können sie verstehen und dementsprechend darauf reagieren. Basierend auf Erfolgs- oder Fehlerquoten aus vergangenen Interaktionen können sie ihre Antworten auf Fragen anpassen oder ihre Reaktion ändern.[11]

Die Social Bots treten vor allem in zwei Erscheinungsformen in den sozialen Netzwerken auf, in der Form sog. Inhaltsgeneratoren und Reposts.

II. 2. 1. Inhaltsgeneratoren

Eine Variante, einen Social Bot in sozialen Netzwerken zu verwenden, ist die der sog. „Inhaltsgeneratoren“. Bei dieser Methode wird der Social Bot innerhalb eines begrenzten Userpools verwendet. Es handelt sich meistens um Gruppen innerhalb sozialer Netzwerke, welche sich beispielsweise über ein politisches Thema unterhalten. Je nach Themenschwerpunkt schnappen die Bots hier mal unterschiedliche mal ähnliche Begriffe und Wortkombinationen auf. Die von dem Bot später verwendeten Begriffe müssen daher zunächst auch von der entsprechenden Zielgruppe verwendet worden sein.[12]

II. 2. 2. Repostings

Unter „Reposten“ versteht man das erneute Verbreiten von Beiträgen anderer User innerhalb des sozialen Netzwerkes[13], womit dieser Beitrag auf der eigenen Seite beziehungsweise auf

---

[10] *Praher,* Regel oder KI-basiert: Die Technologien hinter Chatbots. https://inspire.mindbreeze.com/de/blog/regel-oder-ki-basiert-die-technologien-hinter-chatbots.html (zugegriffen am 17. Juli 2021).

[11] Ibid.

[12] *Volkmann,* Hate-Speech durch Social Bots, Multimedia und Recht 2/2018, S. 58-59.

[13] *Reinbacher,* in: Beck/Kusche/Valerius (Hrsg), Digitalisierung, Automatisierung, KI und Recht-Festgabe zum 10-jährigen Bestehen der Forsungsstelle RobotRecht, Nomos, 2020, S. 464.

dem eigenen Profil unter den eigenen Followern erneut veröffentlicht wird. Der Verwender kann hierbei eine Anzahl von Wörtern festlegen, welche häufig von der anzusprechenden Zielgruppe verwendet werden beziehungsweise die thematisch den Verwendungszweck der Social Bots erfüllen.[14] Sobald der Beitrag eines der festgelegten Wörter enthält, wird dieser durch den Social Bot repostet.[15] Damit die jeweilige Zielgruppe bestmöglich angesprochen wird, wird eine gewisse Anzahl an Begriffen selektiert, welche von der Zielgruppe besonders gerne verwendet werden. Sobald einer dieser Begriffe in einem Beitrag erscheint, wird dieser Beitrag durch den Social Bot repostet.

III. Strafrechtliche Reaktion gegen Hass

III. 1. Das ungarische Strafrecht

Das ungarische Strafrecht regelt Hate-Speech unter dem Titel *Verhetzung* im § 332, Abschnitt XXXII *„Straftaten gegen die öffentliche Ruhe"* uStGB. In Bezug auf den untersuchten Tatbestand ist der Standpunkt der herrschenden ungarischen Lehrbücher und Kommentarliteratur einheitlich darin, dass das Rechtsgut frei von Vorurteilen gegenüber Personengruppen ist und allen die gleiche Würde und den gleichen Respekt entgegenbringt, und deren öffentlichen Ruhe ohne Störung zu sein hat.[16] Es wird kein Tatobjekt definiert, sondern hat abstrakte Dinge, z.B. die ungarische Nation, ethnische, rassische, religiöse Gruppen zum Tatbestand.[17] Die tatbestandsmäßige Handlung ist die Verhetzung zur Gewalt und zum Hass. Im Tatbestand wird kein Erfolg geregelt und es ist ein abstraktes Gefährdungsdelikt, aber die Judikatur verwandelt es in ein konkretes Gefährdungsdelikt.[18] Das Vergehen kann mündlich, schriftlich oder durch aufdringliches Verhalten begangen werden.[19] Die Verhetzung muss öffentlich zugänglich gemacht werden, und unter der Angabe „öffentlich" ist auch das Begehen von Straftaten über Presseerzeugnisse bzw. Mediendienste, durch Vervielfältigung oder Veröffentlichung in einem elektronischen Kommunikationsnetz zu verstehen (§ 459 Abs. 1 Nr. 22). Das Verbrechen kann nur vorsätzlich begangen werden, und der Vorsatz kann entweder direkt oder bedingt sein.[20] Die Straftat kann von Jedermann begangen werden, sogar von einem Mitglied der angegriffenen Gruppe gegen die die Straftat begangen wird.[21]

Im Folgenden prüfe ich die Begriffselemente der Straftat in dieser Reihenfolge um die strafrechtliche Verantwortlichkeit des Entwicklers und des Verwenders zu bestimmen. Ich

[14] *Volkmann* (Fn. 12) S. 58-59.

[15] *Volkmann* (Fn. 12) S. 58-59.

[16] *Mezőlaki,* A köznyugalom elleni bűncselekmények XXXII. Fejezet, in: Karsai (Hrsg.), Nagykommentár a Büntető törvénykönyvről szóló 2012. évi C. törvényhez, Budapest, 2019, S. 755.

[17] *Mezőlaki* (Fn. 16) S. 755.

[18] *Szomora,* Alkotmány és büntetőjog. A büntetőjog-alkalmazás alkotmányosságának egyes kérdései, Szeged, 2015, S. 40.

[19] *Mezőlaki* (Fn. 16) S. 756.

[20] *Belovics,* A köznyugalom elleni bűncselekmények. Btk. XXXII. Fejezet, in: Belovics (Hrsg.), Büntetőjog II. Különös rész, Budapest, 2019, S. 588.

[21] *Mezőlaki* (Fn. 16) S. 756.

bin vom wissenschaftlichen Begriff des Verbrechens ausgegangen, der nichts anderes ist als *„Verbrechen ist eine Handlung, die tatbestandmäßig, rechtswidrig, und strafbar ist“*.[22]

III. 1. 1. Die Handlung

Ausgangpunkt ist, dass durch künstliche Intelligenz verursachte Verstöße eine staatliche Reaktion erfordern.[23] In diesem Zusammenhang beschreibt *István Ambrus* vier Modelle.

1. Selbständige Verantwortung KI.
   Dieses Modell ist abzulehnen, weil der wissenschaftliche Begriff des Verbrechens wie folgt lautet: *„Verbrechen ist eine Handlung, die tatbestandmäßig, rechtswidrig, und strafbar ist“*.[24] Die Handlung setzt ein menschliches Verhalten voraus, die willensgesteuert und wirkungsfähig ist.[25] Diese Theorie kann bereits im Hinblick auf den Begriff der Handlung ausgeschlossen werden. Ein weiteres Argument ist, dass das geltende Strafgesetzbuch den Täter definiert: *„Täter ist, wer den gesetzlichen Tatbestand der Straftat realisiert“* (§ 13 Abs. 1 StGB), wer den gesetzlichen Tatbestand also durch seine eigene Handlung verwirklicht.[26] Der Roboter kann nicht strafrechtlich haftbar gemacht werden. Soziale Bots sind Roboter, die durch künstliche Intelligenz angetrieben werden, deshalb braucht es menschliches Verhalten, damit sie funktionieren. Die Frage ist, wie weit das menschliche Verhalten sich erstreckt und wann der Roboter selbst handelt. Meiner Meinung nach geht das menschliche Verhalten so weit, dass diese Lerndatenbanken geschaffen werden, aus denen der Roboter selbst lernt.
   Die nächsten drei Modelle beziehen Stellung dazu, wie der Verwender und der Entwickler haftbar gemacht werden können.
2. Haftung für mittelbare Täterschaft
   Meiner Meinung nach ist dieses Modell das derzeit vorherrschende dogmatische Verständnis, dem nicht gefolgt werden kann. Ein mittelbarer Täter ist die Person, „*die den gesetzlichen Tatbestand der vorsätzlichen Straftat realisiert, indem sie eine für diese Tat wegen Kindesalters, eines krankhaften Geisteszustandes, Zwang bzw. Bedrohung nicht strafbare bzw. im Irrtum befindliche Person benutzt.“* Die Person, die sich der mittelbaren Täterschaft bedient, muss nicht die erforderlichen Merkmale aufweisen, um als Täter in Betracht zu kommen. Erforderlich ist jedoch die tatsächliche Feststellung einer Straftat.[27] Diese kann von der KI nicht verwirklicht werden, deshalb wird der Entwickler zu einem Nebentäter.
3. Führungsverantwortung
   Im nationalen Strafrecht findet man in Abschnitt XIV *(Kriegsverbrechen)* und in Abschnitt XIII *(Verbrechen gegen die Menschlichkeit),* zum Beispiel im § 452

[22] *Nagy,* Anyagi büntetőjog. Általános rész I. Szeged, 2014, S. 147-148.

[23] *Ambrus,* A mesterséges intelligencia és a büntetőjog, Állam- és Jogtudomány 4/2020, S. 11.

[24] *Nagy* (Fn. 22) S. 147-148.

[25] *Nagy* (Fn. 22) S. 148.

[26] *Nagy,* Anyagi büntetőjog. Alapvetések és a bűncselekmény tana, Szeged, 2020, S. 334.

[27] *Nagy* (Fn. 26)

Gefährdung der Bereitschaftsstufe, und im § 159 Haftung des Vorgesetzten oder der leitenden Amtsperson.[28]

4. Haftung für Sorgfaltspflichtverletzungen
   Nachdem bei Social Bots (aktuell) noch von keinem strafrechtlich relevanten Handeln ausgegangen werden kann, beschränkt sich der weitere Blick auf den Menschen hinter dem Social Bot. Das geltende Strafgesetzbuch regelt mehrere solcher Fälle. Zum Beispiel das Strafgesetzbuch unter den Titel Versäumen der Aufsichts- oder Kontrollpflicht in Verbindung mit einem Haushaltsbetrug in § 397[29] Diese Lösung ist jedoch sui generis, so dass der Gesetzgeber den Entwickler des Social Bot durch einen neuen Tatbestand haftbar machen könnte.

III. 2. Eine allgemeine dogmatische Darstellung der Feststellung der strafrechtlichen Verantwortlichkeit in zwei fiktiven Fällen.

Im Folgenden möchte ich die Möglichkeiten zur Feststellung der strafrechtlichen Verantwortlichkeit des Entwicklers und des Verwenders anhand verschiedener Varianten in zwei fiktiven Fällen aufzeigen.

Der Fall eins:

„A" (Verwender) beauftragt *„B" (Entwickler),* mit der Erstellung eines Social Bots, den er zur Generierung von Inhalten in den sozialen Medien verwenden möchte. *„B"* muss Worte programmieren, die geeignet sind, Leidenschaft zu wecken, und Frieden und Harmonie zu stören.[30]

Der Fall zwei:

„A" (Verwender) beauftragt *„B" (Entwickler),* mit der Erstellung eines Social Bots, damit *„A"* von anderen veröffentliche Beiträge reposten kann.

III. 2. 1. Strafbarkeit der Verwender, und der Entwickler

III. 1. 2. 1. Strafbarkeit der Entwickler

In der überwiegenden Anzahl der Fälle ist der Entwickler auch die Person, welche den Social Bot verwendet. In Situationen, in welchen der Verwender jedoch nicht auch der Entwickler ist, stellen sich weitere Fragen der Strafbarkeit. Zum Beispiel, wenn man Social Bots auf Bestellung erstellt.

Fall eins:

Diese Arbeit beschränkt sich auf die Untersuchung der Strafbarkeit einer natürlichen Person. Der Grund dafür ist, dass das ungarische Strafrecht die sui generis strafrechtliche Verantwortlichkeit von juristischen Personen nicht kennt.[31]

§ 332. Wer öffentlich zum Hass

---

[28] *Molnár,* A gazdálkodó szervezet vezetőjének speciális büntetőjogi felelőssége, Szeged, 2020, S. 52.

[29] *Ambrus* (Fn. 23) S. 14.

[30] *Mezőlaki* (Fn. 16) S. 756.

[31] Weitere Informationen über die strafrechtliche Verantwortlichkeit juristischer Personen finden Sie unter: *Fantoly,* A jogi személyek büntetőjogi felelőssége, Budapest, 2008.

a) gegen die ungarische Nation,
b) gegen eine nationale, ethnische, rassische bzw. religiöse Gruppe oder
c) gegen einzelne Gruppen der Bevölkerung – insbesondere hinsichtlich ihrer Behinderung, Geschlechtsidentität bzw. sexuellen Ausrichtung –
aufwiegelt, ist wegen eines Verbrechens mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Wie man sieht, enthält der Straftatbestand kein Ergebnis (z. B. ist die eigentliche Erweckung von Hass nicht Teil des Straftatbestands), so dass der Straftatbestand durch das Verhalten selbst, das nichts anderes als die Aufwiegelung zu Gewalt oder Hass ist, erfüllt wird. Nach der Judikatur muss die Aufwiegelung zum Hass jedoch geeignet sein, die soziale Ordnung und den sozialen Frieden zu stören.[32] So ist die Handlung des Täters faktisch, wenn die bedrohten Rechte konkret sind und die Handlung unmittelbar mit einer Gewalttat bedroht ist, somit untersuche ich im Folgenden die Frage der Kausalität zwischen Handlung und Erfolg.[33]

Nach der *conditio sine qua non Formel* ist die Handlung eine Ursache für einen Erfolg, wenn die Handlung nicht unterlassen werden kann, ohne dass der Erfolg unterbliebe.[34] Ohne diese Handlung wäre der Erfolg also nicht eingetreten. Darüber hinaus kann ein Kausalzusammenhang hergestellt werden, wenn ein legitimer Zusammenhang zwischen dem Ergebnis und der Handlung besteht.[35]

Der Social Bot führt die Handlung aus, aber ohne den Entwickler würde der Erfolg nicht eintreten.

Die nächsten zu prüfenden Punkte sind die subjektiven Merkmale. Das Verbrechen kann man mit bedingtem oder direktem Vorsatz gegangen werden. *Direkter Vorsatz ist zu bejahen, wenn der Täter weiß oder als sicher voraussieht, dass sein Handeln zur Verwirklichung des gesetzlichen Tatbestandes führt.*[36] Bedingter Vorsatz liegt vor, wenn der Täter dies ernstlich für möglich hält und sich damit abfindet.[37] Meiner Meinung kann bedingter Vorsatz festgestellt werden, wenn der Entwickler weiß, wofür der Verwender den Social Bot verwendet.

Auf dieser Grundlage glaube ich, dass das Verhalten des Entwicklers in dem Fall, dass er Social Bots nicht für die eigene Verwendung herstellt, als Beihilfe betrachtet werden kann. Gemäß § 14 Abs. 2 StGB *„ist Gehilfe, wer zum Begehen einer Straftat vorsätzlich Hilfe leistet“.* Die Tathandlung ist die Hilfestellung, die physisch oder psychisch sein kann.[38] Die physischen Beiträge tragen zu den äußeren Bedingungen der Grundtat des Täters bei, indem sie zum Beispiel die Mittel zur Begehung der Straftat bereitstellen.[39]

In diesem Fall ist das Mittel der Social Bot, der zur Ausführung der Straftat verwendet wird.

---

[32] *Mezőlaki* (Fn. 16) S. 785.

[33] *Mezőlaki* (Fn. 16) S. 786.

[34] *Nagy* (Fn. 26) S. 174.

[35] *Nagy* (Fn. 26) S. 173.

[36] *Wessels/Beulke/Satzger,* Strafrecht Allgemeiner Teil. 43. Auflage, C.F. Müller, 2013, S. 88.

[37] *Wessels/Beulke/Satzger* (Fn. 36) S. 88.

[38] *Nagy* (Fn. 26) S. 351.

[39] *Nagy* (Fn. 26) S. 352.

Fall zwei:

Wenn der Entwickler einen Social Bot erstellt, der den Beitrag repostet, der das programmierte Wort enthält, leistet er beim Verbrechen Beihilfe.

Wenn es sich bei dem Verwender und dem Entwickler um dieselbe Person handelt, so wird das Verhalten als Nebentäter begangen. In solchen Fällen, wenn der Entwickler den Social Bot in der Absicht erstellt, eine solche Straftat zu begehen, kann er sich bereits bei der Erstellung des Programms strafbar machen. Vor diesem Hintergrund ist mein Vorschlag de lege ferenda ein eigener Straftatbestand, der das Absenden unter Strafe stellt. Ich glaube, dass dies eine typische Vorverlagerung darstellen würde. „Der Vorverlagerung mithilfe der Grenze der Strafbarkeit in der zeitlichen Ebene erweitert werden kann."[40] „In diesem Fall war das konkrete Rechtsgut schon mit strafrechtlichen Mitteln geschützt, trotzdem entscheidet sich der Gesetzgeber für weiteren strafrechtlichen Eingriff, weil das Strafrecht wegen verschiedener und nachfolgend untersuchter Gründe zeitlich früher verwirklichte Handlungen kriminalisieren will."[41]

III. 1. 2. 2 Strafbarkeit der Verwender

Fall eins:

Die objektive Zurechnung trägt dazu bei, die Verantwortung des Verwenders festzustellen. Es können Ereignisse auftreten, bei denen keine Kausalität zwischen einer Handlung und einer anderen Handlung oder einem Erfolg besteht, die/der sich aus dieser Handlung ergibt.[42] Die objektive Zurechnung rechtet den Erfolg unter bestimmten Bedingungen dem Täter zu, wenn der Erfolg durch das Verhalten eines Dritten beeinflusst wurde.[43] Diese Theorie schließt nicht automatisch die Haftung der Person aus, die die ursprüngliche Handlung vorgenommen hat.[44] Sie schließt die strafrechtliche Verantwortung des Entwicklers nicht aus. Wenn der Verwender den Entwickler bittet, den Social Bot zu erstellen, ist er damit meiner Meinung nach der Anstifter[45] des Verbrechens, da die Erstellung eines Social Bots bereits eine Straftat darstellt. Da die Herstellung (noch) nicht strafbar ist, ist der Verwender meiner Meinung nach der Nebentäter der Volksverhetzung.

In diesem Zusammenhang schlage ich de lege ferenda vor, dass die Verwendung eine Straftat darstellen könnte, wenn der Verwender den Social Bot dazu bestimmt hat, sich an hasserfülltem Verhalten zu beteiligen. In diesem Fall kann eine weitere Frage lauten, ob die Verwendung solcher Social Bots an sich eine strafrechtliche Verantwortung begründet, oder der Social bot den Tatbestand die Verhetzung zum Hass erfüllen muss. In diesem Fall würde die Verhetzung zum Hass als objektive Bedingungen der Strafbarkeit in den Tatbestand aufgenommen werden.

---

[40] *Gál,* Die neuen Grenzen der strafrechtlichen Verantwortlichkeit. Über die Verstärkung des Phänomens der Vorverlagerung im ungarischen Strafrecht, in: Darázs et. al (Hrgs.), Neue Grenzen, Humboldt-Kolleg, Budapest 2021, S. 265.

[41] *Gál* (Fn. 40) S. 265.

[42] *Molnár* (Fn. 28) S. 139.

[43] *Molnár* (Fn. 28) S. 140.

[44] *Molnár* (Fn. 28) S. 140.

[45] § 14 Abs 1 uStGB *„Anstifter ist, wer jemand anderen vorsätzlich zum Begehen einer Straftat bringt."*

Objektive Bedingungen der Strafbarkeit ist die materiell–rechtliche Voraussetzung für die strafrechtliche Verantwortlichkeit, die sich aus dem gesetzlichen Tatbestand ergibt.[46] Eine Bedingung, die sich auf die objektiven Merkmale des Tatbestands bezieht, und eine Prüfung der subjektiven Merkmale überhaupt nicht erfordert.[47] Das Zustandekommen oder der Rückstand einer Bedingung ist ein objektiver Teil der materiellen Seite des Sachverhalts.[48]

Fall zwei:

Meiner Meinung nach kann der Verwender, der einen Beitrag mit volksverhetzender Äußerung teilt, als Täter zur Verantwortung gezogen werden.

IV. Rechtsvergleichung – Wie steht das deutsche Rechtsystem zu diesen Fragen?

IV. 1. Übersicht über die deutschen Strafmöglichkeiten

Das deutsche Strafgesetzbuch regelt Hate-Speech unter dem Namen Volksverhetzung im § 130. Die Taten richten sich gegen Teilen der Bevölkerung, gegen nationale, rassische, religiöse, ethnische Gruppen.[49] Tathandlungen des Abs. I Nr. 2. sind das Beschimpfen, böswillige Verächtlichmachen oder Verleumden.[50] Ähnlich dürfte es sich bei dem Billigen, Leugnen, und Verharmlosen einer NS- Völkermordshandlung gemäß § 130 Abs. 3, sowie dem in § 130 Abs. 4 geforderten Billigen, Verherrlichen und Rechtfertigen verhalten, da es sich auch hierbei um Äußerungsdelikte handelt, bei welchen der Täter eine eigene Stellungnahme zum Ausdruck bringen muss.[51] Die Tat ist ein abstraktes Gefährdungsdelikt. Der Vorsatz ist erforderlich, und bedingter Vorsatz ist ausrechend, aber § 130 I Nr.1 enthält eine zielgerichtete Handlung, so dass insoweit direkter Vorsatz erforderlich ist.[52]

---

[46] *Nagy* (Fn. 26) S. 281.

[47] *Molnár* (Fn. 28) S. 118.

[48] *Molnár* (Fn. 28) S. 118.

[49] *Fischer,* Strafgesetzbuch mit Nebengesetzen. 66. Auflage, München, 2019, S. 1007.

[50] *Fischer* (Fn. 49) S. 1010.

[51] *Fischer* (Fn. 49) S. 1015-1016.

[52] *Fischer* (Fn. 49) S. 1011.

IV.2. Vergleichung der Lösungen des geprüften Rechtsystems.

Nach den oben darstellten Gesichtspunkte gibt es viele Ähnlichkeiten und Unterschiede zwischen den zwei geprüften Rechtsystemen.

	Ungarisches Rechtsystem	Deutsches Rechtsystem
Beihilfe durch Unterlassen		
Strafbarkeiten des Social Bots	(-) „Handeln" setzt ein menschliches Verhalten voraus	(-) Kein „rechtlich relevantes Handeln" gegeben
Strafbarkeit des Entwicklers, wenn er auch der Verwender ist.	(+) Durch das Generieren eigener Posts ist eine Strafbarkeit zu bejahen (Inhaltgeneratoren) (+) Eine Strafbarkeit durch „Teilen" ist möglich. Bedingter Vorsatz ausreichend	(+) Durch Generieren eigener Post ist eine Strafbarkeit zu bejahen (Inhaltgeneratoren) (+) Eine Strafbarkeit durch „Teilen" ist möglich. Bedingter Vorsatz ist grundsätzlich ausreichend
Strafbarkeit des Verwenders, wenn der Entwickler eine andere Person ist.	(+) Entwickler als physische Beihilfe. Inhaltsgeneratoren (+) Verwender als Täter Repostings (+) Verwender als Täter	(+) Entwickler als physische Beihilfe. Inhaltsgeneratoren (+) Verwender als Täter Repostings (+) Verwender als Täter

Weder das deutsche noch das ungarische Recht sieht eine strafrechtliche Haftung des Sozialbots vor. Nach deutschem Recht wird bei einem rechtlich relevanten „Handeln" von einem Menschen als Handelndem ausgegangen.[53] Das Handeln eines Social Bots kann nicht mit dem Handeln einer menschlichen Person gleichgesetzt werden, da die Vornahme der Handlung durch ein aktuelles oder zumindest potenzielles Normverstehen geprägt sein muss, um das Verhalten als rechtlich relevantes Handeln einstufen zu können.[54] Da der Social Bot nicht haftbar gemacht werden kann, werden der Entwickler und der Verwender strafrechtlich zur Verantwortung gezogen. Wenn der Entwickler und der Verwender nicht dieselbe Person sind, können sie sowohl nach ungarischem als auch nach deutschem Recht wegen physischer Beihilfe zu einer Straftat zur Verantwortung gezogen werden. *„Als Gehilfe wird bestraft, wer vorsätzlich einem anderen zu dessen vorsätzlich begangener rechtswidriger Tat Hilfe geleistet hat"* (§ 27 StGB). Falls der Verwender diesen Social Bot zum Teilen von Beiträgen verwendet, wird das Teilen als eine Identifikation mit dem ursprünglichen Beitrag angesehen. Es stellt sich die Frage, ob die Weiterleitung der Erklärung einer anderen Person als eigene Erklärung angesehen werden kann. Wenn also der Verwender einen Beitrag teilt, in dem Beschimpfungen, böswilliges Verächtlichmachen oder Verleumdungen enthalten sind, ist er als Nebentäter strafrechtlich verantwortlich. Gemäß § 25 *„wird als Täter bestraft, wenn die Straftat selbst oder durch einen anderen begeht"* (§ 25 StGB). Ebenso gilt ein Verwender als Nebentäter, wenn er Beiträge mittels Social Bot erstellt.

[53] *Wessels/Beulke/Satzger* (Fn. 36) S. 40.

[54] *Gless/Seelmann* (Fn. 2) S. 49.

V. Fazit

Da von den Social Bots selbst, im aktuellen Entwicklungsstadium, noch kein rechtlich relevantes Handeln ausgeht, richtet sich die Strafbarkeit oftmals gegen ihren Verwender. Wobei in diesem Zusammenhang stets auf die Unterscheidung von Äußerungs- und Verbreitungsdelikten geachtet werden sollte. Sofern der Verwender nicht gleichzeitig auch der Entwickler ist, macht sich regelmäßig auch der Entwickler der Social Bots strafbar. Somit sind für Juristen, welche sich mit diesen Themen auseinandersetzen, weiterhin grundsätzliche technische Kenntnisse von besonderer Bedeutung.

Stier, Jannick*
Cand. jur., Universität Konstanz

Die Betrugsrelevanz der Täuschungshandlung durch Social Bots und gekaufte „Follower“?

I. Einleitung

Der US-Wahlkampf im Jahre 2016 hat gezeigt, dass Fragen nach Wahrheit, Wirklichkeit und das Vertrauen darauf mit voranschreitender Digitalisierung zunehmend komplexer werden. In diesem Wahlkampf wurden erstmalig öffentlichkeitswirksam „Social Bots“ verwendet, um mit „Tweets“ die Wähler suggestiv zu beeinflussen, um so den Anschein zu erwecken, dass die Positionen Donald Trumps mehr Zuspruch seitens der Bevölkerung erhielten.[1] Heute befürchten Politik und Medienöffentlichkeit eine zunehmende Beeinflussung der öffentlichen Meinungsbildung durch „Fake News“ und Social Bots.[2] Fernab der Beeinflussung politischen Wählerwillens wirken „Social Bots“ auch in anderen durch die Digitalisierung stark beeinflussten Bereichen: Nutzer sozialer Medien und Kunden von Onlineanbietern für Waren und Dienstleistungen sind in alltäglichen Situationen durch die Verwendung von Social Bots in ihrer Wahrnehmung der Wirklichkeit manipuliert, etwa wenn Influencer aufgrund von Werbekooperationen mit Unternehmen Produktempfehlungen abgeben oder mittels zahlreichen Produktbewertungen auf den Seiten der Online-Anbieter. Die Frage ist naheliegend, ob es sich daher bei der Beeinflussung durch „Social Bots“ und „gekaufte Follower“ um betrugsrelevante Täuschungshandlungen handelt. Die Antwort hängt nicht zuletzt davon ab, inwieweit die Wirklichkeitsbildung des Einzelnen für vermögensrelevante Entscheidungen durch das Betrugsstrafrecht geschützt werden muss.

Das erfordert seinerseits eine zweigelagerte Untersuchung zunächst der Täuschungshandlungen von Influencern (II.), welche für ihren Nutzeraccount zusätzliche Follower kaufen. Hier ist über den Vertragsschluss mit einem Werbepartner hinaus zu fragen, ob ein Influencer durch das „Zukaufen“ von „Followern“ seine realen menschlichen „Follower“ betrugsrelevant täuscht. Dagegen werden im Fall des sog. „Astroturfing“ (III.) mittels „Social Bots“ automatisiert Produktbewertungen online gestellt. Hier kann nur auf Bewertungsmöglichkeiten auf Anbieterseite selbst eingegangen werden; Bewertungs-

---

* Der Verfasser war Student im Schwerpunkt Strafrechtspflege: Wirtschaftsstrafrecht, Kriminologie, Europäisierung und Praxis und Teilnehmer im Seminar „Strafrecht vor den Herausforderungen der Digitalisierungen: Fragen des besonderen Teils mit Bezügen zum Wirtschaftsstrafrecht“ bei Prof. Dr. Liane Wörner LL.M. im Wintersemester 2021/ 2022 an der Universität Konstanz.

1 *Libertus,* Rechtliche Aspekte des Einsatzes von Social Bots de lege lata und de lege ferenda, ZUM 2018, S. 20.

2 *Rückert,* Fake News und Social Bots – Demokratieschutz durch Strafrecht?, in: Albrecht/Geneuss/Giraud/Pohlreich (Hrsg.), Politik und Strafrecht, 2018, S. 167; *Drexl,* Bedrohung der Meinungsvielfalt durch Algorithmen, ZUM 2017, 529 (530)

plattformen im engeren Sinne, die von privaten, unabhängigen Dritten betrieben werden, bleiben ausgespart.[3] Hier gemachte Aussagen zu Produktbewertungen lassen sich freilich auch auf Dienstleistungen übertragen. Die Untersuchung der konkludenten Täuschung in beiden Fallkonstellationen eröffnet den Blick auf die Opfermitwirkung und die sich daraus ergebende Fragen einer qualifizierten Täuschungshandlung und inwieweit es einer objektiven Einschränkung durch viktimodogmatische Ansätze und einer unionsrechtskonformen Auslegung bedarf (IV.).

II. Täuschungshandlungen des Influencers durch „gekaufte Follower“[4]

Beim Einkauf von Followern ist zunächst fraglich, ob dadurch die Werbeauftraggeber (II. 1.) beziehungsweise die eigenen reellen Follower getäuscht werden können (II. 2.).

II. 1. Täuschung des Auftraggebers durch den Influencer über die eigene Reichweite

Die erste mögliche betrugsrelevante Täuschung lässt sich im Bereich des Influencermarketing erkennen. Bei Influencern[5] handelt es sich um Personen, die auf Social Media Plattformen wie zum Beispiel „Instagram“, „Snapchat“ oder „TikTok“ mit Bildern, Videos oder auch kurzen Textbeiträgen in deren Bildtext einen Einblick in ihr Leben geben.[6] Follower und Influencer interagieren virtuell über die Beiträge, die Kommentarspalte und den „Likebutton“. Die Influencer produzieren fortdauernd neue Inhalte.[7] Diese authentische und zielgruppennahe Art der Kommunikation mit ihren Anhängern hat das Influencermarketing in den letzten Jahren zu einem relevanten Tool von Marketingabteilungen werden lassen.[8] Unternehmen bieten den Influencern im Rahmen von Werbekooperationen eine finanzielle Gegenleistung an, wenn diese zum Beispiel Fotos oder Videos vom zu bewerbenden Produkt machen und den Account oder die Website des werbenden Unternehmens im Bild oder

---

[3] Zur Abgrenzung: Vgl. *Wilkat,* Bewertungsportale im Internet, 2013, S. 31 f.

[4] Der Begriff des Follower wird hier als plattformunabhängiges Synonym verwendet für alle Nutzer, welche einen Account abonniert haben.

[5] In dieser Arbeit wird das Augenmerk lediglich auf die klassischen Influencer gelegt die ihre Bekanntheit einzig durch ihre Inhalte in den sozialen Medien erlangt haben. Zum Begriff und der Klassifizierung von Influencern u.a. *Nguyen,* Influencer Relations: Der neue King of Content, in: Schach/Lommatzsch (Hrsg.), Influencer Relations, 2018, S. 147 (150 ff.); *Kilian,* Testimonials wirkungsvoll in der Kommunikation einsetzen, in: Bruhn/Esch/Langner (Hrsg.), Handbuch Instrumente der Kommunikation, 2. Aufl. 2016, S. 355, (364 ff.).

[6] *Willems,* Influencer als Unternehmer, MMR 2018, 707; *Beck,* Digitale Rekonstruktionen von „Wirklichkeit“. Social Bots und gekaufte Follower als betrugsrelevante Täuschungen, in: Beck/Kusche/Valerius (Hrsg.), Digitalisierung, Automatisierung, KI und Recht, 2020, S. 401 (414).

[7] *Leeb/Maisch,* Social-Media-Stars und -Sternchen im rechtsfreien Raum?, ZUM 2019, S. 29

[8] *Laoutoumai/Heins,* Veranstaltung von Gewinnspielen im Influencer Marketing, IPRB 2018, 84; *Lichtnecker,* Neues aus dem Social Media-Marketing, MMR 2018, 512 (515); *Gerecke,* Kennzeichnung von werblichen Beiträgen im Online-Marketing, GRUR 2018, 153; *Remmertz,* Aktuelle Entwicklungen im Social Media-Recht, MMR 2018, 507 (511). *Kilian* (Fn. 6) S. 362.

im Bildtext verlinken.[9] Hierdurch ist für viele Nutzer von sozialen Medien eine Möglichkeit entstanden, Geld dazuzuverdienen und sich zum Teil sogar ein durchaus beachtliches Vermögen aufzubauen.[10] Um jedoch überhaupt erst die Chance zu bekommen, mit einem Unternehmen eine solche Werbekooperation eingehen zu können, muss der Influencer jedoch freilich zunächst den Kriterien des Unternehmens entsprechen.[11] Häufig ist für das Unternehmen die Reichweite, Relevanz und die Beliebtheit des Influencers von Bedeutung, welche sich in erster Linie quantitativ anhand seiner Follower bemisst.[12] Um die eigene Anzahl an Follower zu erhöhen und dem Account und somit auch der eigenen Person mehr Reichweite, Relevanz und Beliebtheit zu verleihen, kaufen sich manche Influencer oder Nutzer, welche dieses „Berufsziel" verfolgen, Follower bei Onlineanbietern. Hierdurch erhöhen sie die Wahrscheinlichkeit, den Kriterien des Unternehmens zu entsprechen, um so eine Kooperation zu erlangen oder sofern schon eine solche Kooperation besteht, die zukünftige Vergütung aufgrund der scheinbar höheren Reichweite zu erhöhen. Bei diesen gekauften Follower handelt es sich in der Regel um sogenannte Social Bots. Eine allgemein anerkannte Definition von Social Bots existiert nicht.[13] Ein Social Bot ist ein Algorithmus, welcher semi-automatisiert vordefinierte Aufgaben erledigen kann.[14] Technisch betrachtet sind Social Bots im Hinblick auf ihre Zielrichtung neutral, denn sie führen lediglich das aus, wozu sie vom Entwickler programmiert wurden.[15] Die Bezeichnung „social" kommt daher, dass diese Programme häufig in sozialen Netzwerken verwendet werden, indem der Social Bot auf diesen Plattformen einen eigenen Nutzeraccount hat.[16] Die Social Bots sind für den Nutzer der Natur der Sache nach optisch nicht als solche erkennbar.[17] Auch von ihrem Verhalten in den sozialen Netzwerken entsprechen sie weitestgehend einem normalen Nutzer, denn sie adaptieren das Nutzerverhalten, indem sie beispielsweise eigene Beiträge

---

[9] *Ruess/Bredies,* Millionäre dank Millionen Follower: Rechtliche Bewertung der Entscheidungspraxis zum Influencer-Marketing, WRP 2020, 18; *Kilian,* Influencer sind die neuen Promis, Absatzwirtschaft 7/8 2016, 76 (77); *Willems* (Fn. 7) S. 707; *Beck* (Fn. 7.) S. 415.

[10] *Hoene,* Influencer-Marketing, IPRB 2018, 58; *Willems* (Fn. 7) S. 707; *Lichtnecker* (Fn. 9) S. 512. (516)

[11] Eine Übersicht über die praktisch häufig genutzten Kriterien bietet *Kilian,* Markenkooperationen mit Influencern, Marke 41 1/2018, S. 40 (43). Über die Erfolgsmessung in sozialen Medien: *Dobbelstein/Walz,* TikTok und Instagram, 2021, S. 27 ff.

[12] *Kilian* (Fn. 12) S. 40 (41); *Kilian* (Fn. 6) S. 365; Vgl. auch *Lichtnecker,* Ausgewählte Werbeformen im Internet unter Berücksichtigung der neueren Rechtsprechung, GRUR 2014, 523 (525); *Leeb/Maisch* (Fn. 8), 29 (38).

[13] *Jülicher/Röttgen,* Bots im Kontext von Wirtschaftsrecht und Cybercrime, InTer, 2018, S. 15.

[14] *Thieltges/Hegelich,* Falschinformationen und Manipulation durch social bots in sozialen Netzwerken, in: Blätte/Behnke/Schnapp/Wagemann (Hrsg.), Computational Social Science, 2018, S. 357, (359); *Kind* et al., TA-Vorstudie Social Bots, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), 2017, S. 11; *Thieltges/Hegelich,* Manipulation in sozialen Netzwerken, ZfP (Zeitschrift für Politik) 2017, 493 (494); *Jülicher/Röttgen,* InTer 2018, 15.

[15] *Kind* (Fn. 15) S. 11.

[16] *Esser,* Strafrechtliche Aspekte der Social Media, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2. Aufl. 2021, S. 329 Rn. 54; *Reinbacher,* Social Bots aus strafrechtlicher Sicht, in: Beck/Kusche/Valerius (Hrsg.), Digitalisierung, Automatisierung, KI und Recht, 2020, S. 457; *Kind* (Fn. 15) S. 11; *Libertus* (Fn. 2) S. 20.

[17] Zu einer etwaigen Kennzeichnungspflicht: *Löber/Roßnagel,* Kennzeichnung von Social Bots, MMR 2019, S. 493 ff.

erstellen oder mit anderen Nutzern interagieren.[18] Diese Verschleierung ist notwendig, denn wenn man die Social Bots enttarnen würde, würden diese ihre Glaubwürdigkeit verlieren.[19] Ihre Zielrichtung besteht, wie bereits erwähnt, darin zu desinformieren und auf die öffentliche Meinungsbildung einzuwirken.[20] Man spricht insoweit häufig auch von „Meinungsroboter".[21] Die Verwendung dieser Social Bots in Form von gekauften Follower ist bei Influencern beliebt. Eine Studie besagt, dass jeder zehnte Influencer solche Follower kauft.[22] Aufgrund dieser hohen praktischen Relevanz stellt sich also die Frage, ob es sich beim Vertragsschluss des Influencers mit dem werbenden Unternehmen um eine betrugsrelevante Täuschung handelt.

Für die Frage, ob es sich bei der Verwendung von gekauften Followern um eine betrugsrelevante Täuschung handelt, müsste zunächst geklärt werden, ob es sich bei der Anzahl der tatsächlichen Follower um eine Tatsache handelt (II. 1. 1.). Darüber hinaus müsste ein Verschweigen des Followerankaufs als Täuschungshandlung (II. 1. 2.) zu qualifizieren sein. Fraglich ist insbesondere, inwieweit dem Opfer eine gewisse Mitverantwortung zur Last gelegt werden kann und welche Folge eine Opfermitverantwortung nach sich zieht (II. 1. 3.).

II. 1. 1. Tatsachen

Die Anzahl der Follower ist ein Zustand der Gegenwart und dem Beweis zugänglich, mithin handelt es sich um eine Tatsache. Die „Echtheit", also die Frage, ob sich hinter dem Account des Followers eine real existierende Person verbirgt, ist ebenso eine Tatsache, da sie mithilfe einer Analyse dem Beweis zugänglich ist.[23]

II. 1. 2. Täuschung

Bei der Tathandlung „täuschen" handelt es sich um ein zur Irreführung bestimmtes und damit der Einwirkung auf die Vorstellung eines anderen dienendes Gesamtverhalten.[24] Erfasst ist jedes Verhalten mit Erklärungswert, das darauf gerichtet ist, durch Einwirkung

---

[18] *Thieltges/Hegelich* (Fn. 15) S. 359; *Drexl* (Fn. 3) S. 529 (530).

[19] *Thieltges/Hegelich* (Fn. 15) S. 493 (495); *Esser* (Fn. 17) S. 329 Rn. 54; *Drexl* (Fn. 3) S. 529 (530).

[20] *Kind* (Fn. 15) S. 4; *Drexl* (Fn. 3) S. 529 (530); *Reinbacher* (Fn. 17) S. 457; Ferner auch der Antrag der BT-Fraktion von Bündnis90/Die Grünen BT-Drs. 18/118-56, S. 2.

[21] *Kind* (Fn. 15) S. 4; *Drexl* (Fn. 3) S. 529 (530); *Reinbacher* (Fn. 17) S. 457. Ferner auch der Antrag der BT-Fraktion von Bündnis90/Die Grünen BT-Drs. 18/118-56, S. 2.

[22] *Beck* (Fn. 7) S. 415. verweisend auf: *Meyer,* https://www.tagesspiegel.de/wirtschaft/bezahlter-ruhm-auf-instagram-jeder-zehnte-deutsche-influencer-kauft-sich-follower/24844910.html, (Abgerufen am 20.09.2022); Eine weitere Studie aus der Schweiz zeigt, dass von 115 Schweizer Influencer mit insgesamt sieben Millionen Follower, ein Drittel Fake-Follower sind. Bei der großen Mehrheit der Influencer handelt es sich hierbei um weniger als 20% der Follower. In: *Grossenbacher* et al., https://srfdata.github.io/2017-10-instagram-influencers/#5_classifying_7_million_followers, (Abgerufen am 11.08.21).

[23] *Grossenbacher* et al., (s.o. Fn. 22) ab dem Punkt 3. Hier findet sich auch ein detaillierter Ablauf einer Analyse.

[24] *Kühl* in: Lackner/Kühl, Strafgesetzbuch, 29. Aufl. 2018, § 263 Rn. 6. *Fischer* in: Fischer, Strafgesetzbuch, 69. Aufl. 2022, § 263 Rn. 14; *Dannecker* in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl. 2017, § 263 Rn. 28; *Duttge* in: Handkommentar Gesamtes Strafrecht, 4. Aufl. 2017, § 263 Rn. 8.

auf die intellektuelle Vorstellung eines anderen eine Fehlvorstellung hervorzurufen.[25] Der Influencer müsste somit bei Vertragsschlusses mit dem kooperierenden Unternehmen dieses mit seinem Verhalten bezüglich der Tatsachen, der Anzahl und der Echtheit seiner Follower irreführen. In Betracht kommen hierfür zwei mögliche Konstellationen.

Als erstes wäre die Täuschung durch ausdrückliches Erklären zu nennen. Hierbei handelt es sich aus praktischer Sicht um eine weniger problematische Konstellation.[26] Der Influencer bejaht der vor Vertragsschluss entweder wahrheitswidrig die Tatsache, dass es sich bei seinen Followern um echte, real existierende Personen handelt oder der unterzeichnete Vertrag beinhaltet eine Klausel, welche eine solche Passage enthält. Als zweite Konstellation kommt eine Täuschung durch konkludentes Erklären in Betracht. Hierbei stellt sich mangels ausdrücklicher Erklärung des Influencers die Frage, ob dieser beim Vertragsschluss konkludent miterklärt, dass es sich bei seinen Followern nicht um unechte und gekaufte Follower handelt und diese Erklärung Teil der gemeinsamen Geschäftsgrundlage wird. Die Frage, ob ein Vertragspartner einen Umstand, welcher zur Geschäftsgrundlage wurde, stillschweigend miterklärt war Kernthematik der Wettfälle des Bundesgerichtshofes.[27] Die obige Ausgangslage bei dem Vertragsschluss zwischen dem Influencer und dem Werbepartner weist Parallelen mit den Wettfällen des Bundesgerichtshofes[28] auf. Der BGH stellte fest, dass dem Wettenden mit dem Vertragsangebot die stillschweigende Erklärung entnommen werden könne, das dieser selbst die Geschäftsgrundlage der Wette nicht durch eine rechtswidrige Manipulation verändert habe.[29] Des Weiteren ergebe sich der Bedeutungsgehalt des Gesamtverhaltens aus dem Empfängerhorizont des Erklärungsempfängers sowie aus dessen ersichtlichen Erwartungen.[30] Der Erklärungsgehalt dieses Verhaltens sei durch Auslegung zu bestimmen, wobei die Pflichten- und Risikoverteilung zwischen den Parteien eine wichtige Rolle spiele.[31] Der BGH betonte zwar, dass die allgemeine Erwartung, der andere werde sich redlich verhalten, für die Annahme entsprechender konkludenter Erklärungen nicht ausreiche, der Vertragspartner müsse aber ein Minimum an Redlichkeit im Rechtsverkehr voraussetzen dürfen.[32] Die Erwartung, dass keine vorsätzliche sittenwidrige Manipulation des Vertragsgegenstands durch einen Vertragspartner in Rede steht, sei unverzichtbare Grundlage des Geschäftsverkehrs und deshalb zugleich miterklärter Inhalt entsprechender rechtsgeschäftlicher Erklärungen.[33] Im Regelfall könne

---

[25] *Fischer* (Fn. 24) § 263 Rn. 14; Graf/Jäger/Wittig/*Dannecker,* § 263 Rn. 28; Lackner/Kühl/*Kühl,* § 263 Rn. 6; HK-GS/*Duttge,* § 263 Rn. 8.

[26] Vgl. *Beck* (Fn. 7) S. 415.

[27] BGH Urt. v. 20.6.1961 – 5 StR 184/61 (BGHSt 16, 120 ff.) (Spätwettenfall); BGH Urt. v. 19.12.1979 – 3 StR 313/79 (BGHSt 29, 165 ff.) (Pferdewettenfall); BGH Urt. v. 15.12.2006 – 5 StR 181/06 (BGHSt 51, 165 ff.) (Hoyzer-Urteil); Die Konstellation der konkludenten Täuschung bei einer Wettabgabe wurde in der Rspr. 1928 das erste Mal in RGSt 62, 415 ff. diskutiert.

[28] BGH Urt. v. 15.12.2006 – 5 StR 181/06 (BGHSt 51, 165 ff.) Die im folgenden Absatz nachvollzogene Argumentation ist überwiegend dieser Entscheidung entnommen.

[29] BGHSt 51, 169 Rn. 17.

[30] BGHSt 51, 170 Rn. 20.

[31] BGHSt 51, 170 Rn. 21.

[32] BGHSt 51, 170 Rn. 22.

[33] BGHSt 51, 170 Rn. 22.

aus den allgemein verbreiteten Erwartungen auf den tatsächlichen Inhalt konkludenter Kommunikation geschlossen werden.[34]

Die obigen Ansätze der sog. „Wettfälle“[35] können auf die Konstellation beim Vertragsschluss der Werbekooperation übertragen werden. Die Anzahl und die Echtheit der Follower müssten somit Teil der Geschäftsgrundlage geworden sein. Diese umfasst die von den Parteien erkennbar gemachten wesentlichen Voraussetzungen für den Vertragsschluss.[36] Die vertragliche Pflicht des Influencers ist es, das Produkt des werbenden Unternehmens mithilfe von eigenen Beiträgen zu bewerben. Werbung soll Aufmerksamkeit erzeugen und dadurch einen Kaufanreiz bei der Zielgruppe setzen.[37] Hierfür müssen die Beiträge, in denen der Influencer für das Produkt wirbt, auch in einen Bereich der Zielgruppe kommen, wo diese den werbenden Beitrag des Influencers zur Kenntnis nehmen können. Durch die reine Anzahl an Followern des Influencers erreicht der Beitrag des Influencers jedoch nicht zwangsweise auch die Zielgruppe, denn die Follower des Influencers müssen nicht gleichbedeutend mit der etwaigen Zielgruppe sein. Relevant hierfür ist, wie im folgenden dargestellt wird, auch die Echtheit der Follower.

Soziale Netzwerke werden in der Regel über Algorithmen gesteuert, die „beliebte“ Inhalte präferieren. Wer viele Follower hat, wird von den sozialen Netzwerken privilegiert behandelt und erreicht somit auch mehr echte Nutzer.[38] Da Nutzer oft mit einer enorm hohen Zahl von anderen Nutzern verbunden sind und die Plattform deshalb gar nicht mehr in der Lage wäre, alle von den gefolgten Nutzern geteilten Inhalte auf dem „Feed“, also der Übersicht der Beiträge des einzelnen Nutzers darzustellen, ist die Plattform gezwungen, diese Inhalte mithilfe des Algorithmus zu filtern und nur noch die mutmaßlich für den Nutzer wichtigsten Beiträge in dessen Feed anzuzeigen und entsprechend zu ordnen.[39] Auf Plattformen wie Instagram erhöht sich durch einen Algorithmus die Wahrscheinlichkeit, dass der Beitrag in die Seite „Entdecken“ erscheint. Hier werden dem Nutzer neue, für ihn möglicherweise relevante und interessante Beiträge angezeigt.[40] Um auf die „Entdecken-Seite“ der Zielgruppe zu kommen, müssen andere Nutzer aus der Zielgruppe viele Interaktionen in Form von Likes, Kommentaren oder Verlinkungen mit dem Beitrag des Influencers getätigt haben.[41] Der von Instagram genutzte Algorithmus versucht so Ähnlichkeiten der Interessen der Nutzer zu identifizieren, um dem Nutzer so ähnlich interessante Beiträge anzuzeigen.[42] Die gekauften Fake-Follower lassen den Influencer

---

[34] BGHSt 51, 170 Rn. 22.

[35] Hier explizit: „Hoyzer-Urteil“ dies gilt jedoch auch für den „Pferdewettenfall“.

[36] *Kindhäuser* in: Nomos Kommentar zum Strafgesetzbuch, Band 3 §§ 232-358, 5. Aufl. 2017, § 263 Rn. 132; *Perron* in: Schönke/Schröder, Kommentar zum Strafgesetzbuch Strafgesetzbuch, 30. Aufl. 2019, § 263 Rn. 16e; *Tiedemann* in: Leipziger Kommentar zum Strafgesetzbuch, Band 9/1: §§ 263 bis 266b, 12. Aufl. 2012, § 263 Rn. 31.

[37] Vgl. *Kilian* (Fn. 6) S. 365.

[38] *Thieltges/Hegelich* (Fn. 15) S. 361.

[39] *Drexl* (Fn. 3) 529 (531) erklärt dies anhand der Platform „Facebook“.

[40] *Dobbelstein/Walz* (Fn. 12) S. 19 f; *Beck* (Fn. 7), S. 416.

[41] Vgl. *Beck* (Fn. 7) S. 416.

[42] Vgl. *Weißhaupt,* Algorithmen als Entscheidungsinstanz in Sozialen Medien, in: Stumpp/ Michelis/Schildhauer (Hrsg.), Social Media Handbuch, 4. Aufl. 2021, S. 317, (323); *Dobbelstein/Walz* (Fn. 12) S. 20.

in sozialen Medien so einflussreicher und vertrauenswürdiger erscheinen.[43] Dieses Phänomen hat sich in letzter Zeit vor allem in Wahlkämpfen mehrfach beobachten lassen.[44] Gekaufte Fake-Follower erhöhen jedoch lediglich die Anzahl der Follower, indes gibt es aber nicht mehr Interaktionen mit dem beworbenen Beitrag.[45] Der vermutete Erfolg beziehungsweise das Erreichen der Follower des Influencers und ferner der anderen Nutzer in der Zielgruppe stellt somit eine berechtigte Erwartung des Werbenden dar. Ansonsten würde die Werbemaßnahme schlechterdings ins Leere laufen. Der Influencer wäre für das Unternehmen überspitzt ausgedrückt genau so wirksam wie eine „Litfaßsäule inmitten der Wüste".[46] Die Anzahl und Echtheit der Follower ist somit Teil der Geschäftsgrundlage des Werbevertrags. Zu beachten ist ferner auch die Risikoverteilung zwischen den Vertragsparteien. Hinsichtlich dieser bildet insbesondere die Herrschaft über die maßgeblichen Informationen einen wesentlichen Gesichtspunkt.[47] Nicht jedes Ausnutzen eines Informationsvorsprungs ist strafwürdig, denn man kann von Wirtschaftssubjekten in der Marktwirtschaft nicht verlangen, jede Schwäche ihrer Angebote offen zu legen.[48] Im vom Gedanken der Privatautonomie geleiteten Zivilrecht besteht eine solche Aufklärungspflicht deshalb grundsätzlich nicht.[49] Gleichwohl besteht aber immer dann eine Aufklärungspflicht, wenn es entscheidend ist, ob der Vertragspartner aufgrund der konkreten Lage nach Treu und Glauben und nach der Verkehrsauffassung eine Aufklärung über solche Umstände erwarten durfte, die für ihn von entscheidender Bedeutung sind und die gebotene Aufklärung bewusst unterbleibt.[50] Handelt es sich also um eine Tatsache, welche so relevant ist, dass sie den Vertragszweck vereiteln oder wesentlich erschweren könnte, entsteht eine Aufklärungspflicht.[51] Der Influencer hat mit der Kenntnis, dass es sich bei seinen Follower auch um gekaufte Follower handelt, einen Informationsvorsprung vor seinem Vertragspartner. Wie bereits erwähnt, handelt es sich bei der Anzahl und Echtheit der Follower um die essentielle Geschäftsgrundlage des Werbevertrags. Das Nutzen von gekauften Followern stellt somit eine vorsätzliche Manipulation der Geschäftsgrundlage dar, wodurch das Erreichen des Vertragszwecks der Werbekooperation zumindest wesentlich erschwert wird. Das werbende Unternehmen darf sich darauf verlassen, dass der Influencer eine solche Erklärung abgibt. Durch das Unterzeichnen des Vertrages erklärt der Influencer, dass er ein Minimum an Redlichkeit im Geschäftsverkehr besitzt und den

---

[43] Vgl. *Jülicher/Röttgen* (Fn. 14) S. 15 (16); *Thieltges/Hegelich* (Fn. 15) S. 361.

[44] *Libertus* (Fn. 2) S. 20; *Thieltges/Hegelich* (Fn. 15) S. 361 m.w.N.

[45] Selbst wenn der Influencer sich mit Hilfe von Anbietern Interaktionen in Form von Likes oder Kommentaren kauft, entsprechen die Bots nicht der Zielgruppe, weshalb diese Interaktionen für das Erreichen dieser nahezu keine Relevanz haben. Vgl. *Beck* (Fn. 7) S. 416.

[46] *Beck* (Fn. 7) S. 416.

[47] *Kasiske,* Die konkludente Täuschung bei § 263 StGB zwischen Informationsrisiko und Informationsherrschaft, GA 2009, 360 (365 f.); Schönke/Schröder/*Perron* (Fn. 37) § 263 Rn. 14-15.

[48] *Erb,* Gängige Formen suggestiver Irrtumserregung als betrugsrelevante Täuschungen, ZIS 2011, 368 (375); *Pastor Muñoz,* Überlegungen zur tatbestandsmäßigen Täuschung beim Betrug, GA 2005, 129; *Ellmer,* Betrug und Opfermitverantwortung, 1986, S. 116; *Pawlik,* Das unerlaubte Verhalten beim Betrug, 1999, S. 71; LK/*Tiedemann,* vor § 263 Rn. 35; *Kasiske,* (Fn. 48) S. 360 (366.).

[49] *Kasiske* (Fn. 48) S. 360 (366).

[50] *Mansel* in: Jauernig Kommentar zum Bürgerlichen Gesetzbuch, 18. Aufl. 2021, § 123 BGB Rn. 5.

[51] *Kasiske* (Fn. 48) S. 360 (366).

Vertragsgegenstand nicht vorsätzlich manipuliert. Wendet man also die Argumentation des BGH im „Hoyzer-Urteil“ auf diese Konstellation an, so liegt bei der stillschweigenden Verwendung von gekauften Followern eine betrugsrelevante konkludente Täuschung über Tatsachen vor.

Die Lösungskonstruktion der konkludenten Täuschung des BGH im „Pferdewettenfall“ und im „Hoyzer-Urteil“ ist jedoch erheblicher Kritik aus der Literatur ausgesetzt.[52] Teilweise wird etwa kritisiert, dass in alltägliche Handlungen zu viel Erklärungsgehalt hineininterpretiert werde und der Tatbestand so normativ überdehnt werden würde.[53] Es handle sich um eine willkürliche Konstruktion, die die Garantenstellung gemäß § 13 StGB und die dadurch ergebende Aufklärungspflicht beim Betrug durch Unterlassen untergrabe.[54] Verstärkend wird zudem angeführt, dass es sich bei der Wette um ein formalisiertes und unpersönliches Alltagsgeschäft handle, angesichts dessen die Mitarbeiter in den Wettbüros aus dem Verhalten der Wettenden regelmäßig überhaupt keine Schlüsse zögen.[55] Mit einer Kontrollüberlegung soll gezeigt werden, dass sich der Senat „allzu weit“ von den „tatsächlichen Gegebenheiten“ entfernt habe.[56] Hätte der Wettende bei Abschluss des Vertrags ausdrücklich erklärt, dass er den Wettgegenstand nicht manipuliert habe, würde dies den Vertragspartner irritieren oder sogar Verdacht schöpfen lassen.[57]

Diese Kritik verdient jedoch aus den nachfolgenden Gründen keinen Beifall. Gegen das Argument, dass in eine alltägliche Handlung zu viel Erklärungsgehalt interpretiert werde, spricht zunächst, dass bei der Auslegung des Erklärungswertes der Handlung ein reines Abstellen auf den objektiven Empfängerhorizont nicht möglich ist.[58] Eine Handlung wird in den betroffenen Geschäftskreisen immer durch vorherrschende Verhaltensmaßstäbe und spezifische rechtliche Rahmenbedingungen normativiert.[59] Die „Kontrollfrage“ zeigt indes nicht auf, dass der Senat durch die normativen Kriterien sich weit von den Begebenheiten entfernt hat, sondern zeigt stattdessen ein Charakteristikum der konkludenten Täuschung.[60] Die Ungewöhnlichkeit einer ausdrücklichen Erklärung ist für die konkludente Täuschung konstitutiv, denn ausgesprochene Selbstverständlichkeiten sind zweckmäßig der konkludenten Erklärung zugewiesen, weil man diese zwar verbindlich voraussetzt und so erwartet,

---

[52] Ein Überblick über den Streitstand findet sich in *Kasiske* (Fn. 48) S. 360 ff.

[53] *Jahn/Meier,* Der Fall Hoyzer – Grenzen der Normativierung des Betrugstatbestandes, JuS 2007, 215 (217); *Schlösser,* Der „Bundesliga-Wettskandal” – Aspekte einer strafrechtlichen Bewertung, NStZ 2005, 423; *Sigmund,* Strafrecht gegen Korruption im Sport?, 2021, S.137; *Krack,* Betrug durch Wettmanipulation, ZIS 2007, 103 (104).

[54] *Jahn/Meier* (Fn. 54) S. 215 (217); *Schlösser* (Fn. 54.) S. 423; *Sigmund* (Fn. 54.) S. 137.

[55] *Schlösser* (Fn. 54.) S. 423 (426); *Jahn/Meier* (Fn. 54) S. 215 (218); Vgl. *Saliger/Rönnau/Kirch-Heim,* Täuschung und Vermögensschaden beim Sportwettenbetrug durch Spielteilnehmer – Fall „Hoyzer”, NStZ 2007, 361 (363); *Krack* (Fn. 54) S. 103 (106); *Sigmund* (Fn. 54.) S.137.

[56] *Jahn/Meier* (Fn. 54) S. 215.

[57] *Jahn/Meier* (Fn. 54) S. 215 (216).

[58] *Kasiske* (Fn. 48) S. 360 (364); *Saliger/Rönnau/Kirch-Heim* (Fn. 56) S. 361 (362); *Krack* (Fn. 54) S. 103 (107); *Saliger* in: Esser/Rübenstahl/Saliger/Tsambikakis, Wirtschaftsstrafrecht, 2017, § 263 Rn. 35; *Sigmund* (Fn. 54.) S. 138.

[59] *Kasiske* (Fn. 48) S. 360 (364); *Saliger/Rönnau/Kirch-Heim* (Fn. 56) S. 361 (362); *Krack* (Fn. 54) S. 103 (107); WiStra/*Saliger,* § 263 Rn. 35; *Sigmund* (Fn. 54.) S. 138.

[60] *Sigmund* (Fn. 54.) S. 137.

nicht jedoch aber zwingend auch explizit ausspricht.[61] Im Ergebnis erweist sich der Streit, ob der Täuschungsbegriff nach normativen oder faktischen Gesichtspunkten zu bestimmen ist, schlechterdings als Scheinstreit.[62] Auch die Behauptung, dass es sich hierbei um eine willkürliche Konstruktion handle, welche das Korrektiv der Aufklärungspflicht aus Garantenstellung untergrabe, vermag nicht zu überzeugen. Denn nach den obigen Grundsätzen wird gleichwertig sowohl auf faktische als auch auf normative Elemente abgestellt. Somit lässt sich die konkludente Täuschung nicht auf Basis von rein normativen Ansichten mit dem Betrug durch Unterlassen gleichschalten.[63] Demnach wird die Garantenstellung nach diesen Grundsätzen schlechterdings nicht untergraben. Im Gegensatz zu Sportwetten handelt es sich bei dem Werbevertrag nicht um ein anonymes Massengeschäft, denn das werbende Unternehmen sucht für die Werbekooperation ja gerade einen bestimmten Influencer, welcher sich als Repräsentant und für die zielgruppengerichtete Werbung eignet, als Vertragspartner aus. Die Auswahl des Influencers und die dabei entstehenden Kosten stellen für das Unternehmen eine marketings- und vermögensrelevante Entscheidung dar. Dass die Nichtmanipulation der Geschäftsgrundlage miterklärt wird, ist somit keine Überinterpretierung der Handlung, sondern im Geschäftsverkehr üblich und wird von den Vertragspartnern so vorausgesetzt.

Zusammenfassend lässt sich feststellen, dass ein Influencer, welcher einen Werbevertrag mit einem Unternehmen schließt, konkludent miterklärt, dass es sich bei seinen Followern nicht um unechte gekaufte Follower handelt.

II. 1. 3. Opfermitverantwortlichkeit

Wie obig bereits erwähnt, hat wohl bereits jeder zehnte deutsche Influencer Follower gekauft. Da es möglich ist, die Echtheit der Follower zu überprüfen, stellt sich die Frage, ob dem werbenden Unternehmen eine gewisse Leichtfertigkeit unterstellt werden kann, wenn dieses bei einer vermögensrelevanten Entscheidung die vorgelegten Reichweiteangaben des Influencers nicht prüft. Wie weit dem Opfer eine gewisse Mitverantwortung zur Last gelegt werden kann, welche Folge die Opfermitverantwortung nach sich zieht und bei welchem Tatbestandsmerkmal dies zu berücksichtigen ist, ist in der Literatur umstritten.[64] Im Kern wird sich darum gestritten, inwieweit das Opfer eigene Schutzmaßnahmen ergreifen muss oder es bereits durch öffentliches- und bürgerliches- Recht geschützt ist. Das Strafrecht ist als „schärfste der Gesellschaft zur Gebote stehende Waffe"[65] nur da einzusetzen, wo der Rechtsgüterschutz nicht anderweitig gewährleistet wird.[66] Die Rechtsprechung und

---

[61] *Gaede,* Betrug durch den Abschluss manipulierter Fußballwetten: Das Hoyzer-Urteil als Sündenfall der Ausdehnung des Betrugstatbestandes?, HRRS 2007, 18; Vgl. *Sigmund* (Fn. 54.) S. 137.

[62] *Krack* (Fn. 54) S.103 (107); Vgl. auch *Hefendehl* in: Münchner Kommentar zum Strafgesetzbuch Band 5: §§ 263-358, 4. Auflage 2022 Rn. 93.

[63] WiStra/*Saliger,* § 263 Rn. 32; Anders jedoch: *Gauger,* Die Dogmatik der konkludenten Täuschung, 2001, S. 167 ff.

[64] Eine Übersicht über die Entwicklung findet sich in LK/*Tiedemann,* vor § 263 Rn. 34 ff.; Im folgenden Abschnitt wird aufgrund der Fragestellung jedoch nur eine Opfermitverantwortlichkeit im Bereich der Täuschungshandlung diskutiert.

[65] BVerfGE 32, 109.

[66] *Hecker,* Strafbare Produktwerbung im Lichte des Gemeinschaftsrechts, 2001, S. 277; Schönke/Schröder/*Eisele,* vor §§ 13 ff., Rn. 70b.

ein Großteil der Literatur vertreten die Auffassung, dass das Mitverschulden des Opfers grundsätzlich die Tatbestandsmäßigkeit des § 263 nicht ausschließt.[67] Begründet wird dies damit, dass der Gesetzgeber sich bewusst für einen weiten Opferschutz entschieden habe und das Vertrauen des Opfers in eine nicht manipulierte Kommunikation schutzwürdig sei.[68] Ferner fehle es an einem geeigneten Maß für die angestrebte Tatbestandsrestriktion.[69] Auf der anderen Seite stehen die sog. viktimodogmatischen Ansätze, welche ein weites Verständnis des strafrechtlichen Subsidiaritätsprinzip an den Tag legen und auf die Selbstverantwortung des Opfers abstellen.[70] Zu den vereinzelten Stimmen, welche eine solche Restriktion annehmen, gehört *Ellmer.*[71] Dieser nimmt einen Vertrauensmissbrauch nur dann an, wenn durch den Täter das berechtigte Vertrauen des Opfers enttäuscht worden sei.[72] Das Vertrauen sei berechtigt, wenn das Opfer seiner Obliegenheit zur Kontrolle nachgekommen sei, außer es bestehe ein besonderes Näheverhältnis oder die Kontrollmaßnahme sei unzumutbar gewesen.[73] Würde man also *Ellmers* Ansicht folgen, so hätte dies zur Konsequenz, dass das Ausbleiben einer Überprüfung der Follower dazu führt, dass das Vertrauen des werbenden Unternehmens nicht mehr schutzwürdig wäre. Gegen diese Ansicht lässt sich jedoch anführen, dass der Wortlaut des Betruges nicht ausschließlich den durch die Täuschung begangenen Missbrauch des berechtigten Vertrauens, sondern auch Fälle des unberechtigten Vertrauens erfasst.[74] Auch wenn wie von *Ellmer* festgestellt, der Gesetzgeber primär Fälle des berechtigten Interesses vor Augen gehabt habe, wurde die Schutzwürdigkeit des Vertrauens nicht zur notwendigen Voraussetzung des Betruges erhoben, weshalb die Abschichtung des einfachen Vertrauens dem Wortlaut widerspricht.[75] *Wittig* bemängelte diese Ansicht auch in systematischer Hinsicht, denn die Ansicht *Ellmers* würde Täuschung und Irrtum vermengen, indem sie schon bei der Täuschung prüft, ob das Opfer der Lüge des Täters geglaubt habe.[76] Ferner erscheint die Sanktion in Form des generellen Verlustes der Schutzwürdigkeit aufgrund der Missachtung einer Obliegenheit zur Aufmerksamkeit nicht zwingend, denn die ausschließende grobe Fahrlässigkeit hängt nicht nur davon ab, wie leicht der Irrtum zu vermeiden war, sondern auch davon, welche Risikobereitschaft des Opfers als schutzwürdig erscheint.[77] Aus kriminalpolitischer Sicht kritisierte *Krack,* dass sich alle Betrüger und sonstige, welche sich von der Strafandrohung

---

[67] BGH NJW 2003, 1198; BGHSt 59, 195 (202); Schönke/Schröder/*Perron,* § 263 Rn. 40; LK/*Tiedemann,* vor § 263 Rn. 37; *Hecker* (Fn. 67) S. 275 ff.; HK-GS/*Duttge,* § 263 Rn. 5; Matt/Rezinkowski/*Saliger,* § 263 Rn. 7.

[68] *Basualto,* Täuschung und Opferschutzniveau beim Betrug – zwischen Kriminalpolitik und Dogmatik in: Sieber/Dannecker/Kindhäuser/Vogel/Walter (Hrsg.), Strafrecht und Wirtschaftsstrafrecht. Festschrift für Klaus Tiedemann zum 70. Geburtstag, 2008, S. 605, (606); *Hennings,* Teleologische Reduktion des Betrugstatbestands aufgrund von Mitverantwortung des Opfers, 2002, S. 141 ff. m.w.N.; LK/*Tiedemann,* vor § 263 Rn. 36; *Gaede* in: AnwaltKommentar StGB 3. Auflage, 2019, § 263 Rn. 21; Vgl. *Hecker* (Fn. 67) S. 275 ff. m.w.N.

[69] AK-StGB/*Gaede,* § 263 Rn. 21; Vgl. *Hennings* (Fn. 69) S. 164 ff. m.w.N.

[70] Vgl. Schönke/Schröder/*Eisele,* vor §§ 13 ff., Rn. 70b; *Hillenkamp,* ZStW 129 (2017), 596 (607 ff.).

[71] *Hennings* (Fn. 69) S. 162.

[72] *Ellmer* (Fn. 49) S. 281.

[73] *Ellmer* (Fn. 49) S. 281.

[74] *Hennings* (Fn. 69) S. 165; *Krack,* List als Tatbestandsmerkmal, 1994, S. 69.

[75] *Hennings* (Fn. 69) S. 165; *Krack* (Fn. 75) S. 69.

[76] *Wittig,* Das tatbestandsmässige Verhalten des Betrugs, 2005, S. 240.

[77] *Hennings* (Fn. 69) S. 165.

abschrecken ließen, sich auf besonders leichtgläubige Opfer „stürzen" würden, wo doch gerade diese besonders schutzwürdig sein.[78]

Im Ergebnis verdient die Ansicht der herrschenden Literaturmeinung und der Rechtsprechung Beifall. Die Restriktion der Täuschungshandlung ist im Hinblick auf die Systematik und dem Willen des Gesetzgebers nicht überzeugend. Diese Einschränkung befindet weniger im Rahmen der Gesetzesauslegung, sondern stellt viel mehr eine Neukonzeption im Lichte der eigenen kriminalpolitischen Ansicht dar, welche nicht mit dem bestehenden Tatbestand des Betruges in Einklang zu bringen ist.[79]

Eine fehlende Überprüfung des Influencers durch das Unternehmen mag zwar aus betriebswirtschaftlicher Sicht als ein leichtfertiges Handeln zu betrachten sein, jedoch kann es einem Unternehmen nicht dahingehend zur Last gelegt werden, dass es den strafrechtlichen Schutz durch den Betrugstatbestand verliert.

II. 1. 4. Ergebnis

Zusammenfassend lässt sich feststellen, dass der Influencer bei Vertragsschluss den Vertragspartner betrugsrelevant täuschen kann. Bei der Echtheit und der Anzahl seiner Follower handelt es sich um dem Beweis zugängliche Tatsachen. Die Täuschung kann sowohl ausdrücklich als auch konkludent erfolgen, wobei die erste Alternative wohl praktisch seltener vorkommen wird. Im Rahmen der konkludenten Täuschung lässt sich die Argumentation der Rechtsprechung in den „Wettfällen" auf die Situation bei Vertragsschluss zwischen dem Influencer und dem werbenden Unternehmen übertragen. Die Echtheit und Anzahl der Follower werden zur Geschäftsgrundlage, da die gewünschte Zielgruppe auch erreicht werden muss, denn anderweitig wäre die Werbekooperation mit dem Influencer schlechterdings sinnfrei. Überprüft das werbende Unternehmen die Follower des Influencers nicht auf die Echtheit, so vermag dies aus unternehmerischer Perspektive zwar leichtfertig erscheinen, führt jedoch nicht zum Verlust der Schutzwürdigkeit. Schlussendlich wird die Wirklichkeitsbildung des Geschäftspartners vor der Manipulation mittels Social Bots durch den Betrugstatbestand geschützt.

II. 2. Täuschung der „realen" eigenen Follower

Nachdem die Frage nach der Betrugsrelevanz der konkludenten Täuschung des Werbepartners mit gekauften Followern bei Vertragsschluss geklärt ist, stellt sich ferner die Frage, inwieweit der Influencer seine eigenen echten Follower durch die Verwendung von gekauften Followern betrugsrelevant täuscht. Bei der Anzahl und Echtheit der Follower handelt es sich wie obig bereits festgestellt, um Tatsachen.[80] Um ihre Relevanz, Größe, Beliebtheit und das Ansehen bei den Nutzern von sozialen Netzwerken zu erhöhen, kaufen einige Influencer

---

[78] *Krack* (Fn. 75) S. 70; Inwieweit dieses Argument der negativen Generalprävention Beifall verdient, ist aus kriminologischer Sicht mehr als fraglich. Dies ist jedoch nicht Teil dieser Arbeit. Kritik an der negativen Generalprävention findet sich u.a. bei Schönke/Schröder/*Kinzig,* vor §§ 38 ff. Rn. 3 m.w.N.

[79] *Hecker* (Fn. 67) S. 275, 281; *Hennings* (Fn. 69) S. 166 ff.; LK/*Tiedemann,* vor § 263 Rn. 36.

[80] Siehe oben: B I. 2. a); Vgl. Auch *Beck* (Fn. 7) S. 417.

Fake-Follower in Form von Social Bots.[81] Interessant erscheint jedoch die Frage, ob der Influencer auch gegenüber seinen echten Follower konkludent miterklärt, dass es sich bei seinen Follower ausschließlich um echte und nicht etwa um gekaufte Fake-Follower handele. Diese Frage wird relevant, wenn diese Follower Produkte erwerben, für die der Influencer in Beiträgen geworben hat. Im Folgenden wird die Relevanz dieser Beiträge für die Grundlage von vermögensrelevanten Entscheidungen der Follower diskutiert. Die Nutzer können zunächst Interesse an der Art oder Darstellung der Inhalte oder der Person des Influencers an sich haben. Sagen ihnen diese Inhalte oder auch die Person des Influencers zu, fangen sie regelmäßig an diesem zu folgen. Ein Faktor, welcher diese digitale Wirklichkeitsbildung beeinflussen kann, ist auch die Followeranzahl sowie andere Interaktionen wie Likes oder Kommentare. Diese haben nämlich auf andere Nutzer den Anschein, dass sich viele Nutzer mit dem Influencer auseinandersetzen und sich für diesen Interessieren.[82] Durch das allgemeine Interesse an einem Influencer können andere Nutzer dazu bewegt sein, ebenfalls diesen Influencer zu abonnieren. Aufgrund der vielen Interaktionen scheint dieser jedenfalls im Allgemeinen und möglicherweise auch für sie interessante Inhalte zu teilen. Die Werbebeiträge des Influencers sind jedoch für die Follower ein bloßes Nebenprodukt.[83] Aus diesem Punkt resultiert gerade der Vorteil des Influencermarketings, denn Influencer sind so authentischer und näher an der Zielgruppe als zum Beispiel klassische, für Marken werbende Prominente es sind.[84] Teile der Nutzer empfinden Influencer wie gute Freunde, die sie aus der Ferne beobachten können.[85] Auch Studien haben ergeben, dass zwei Drittel bis zu drei Viertel der deutschen Follower ein hohes Vertrauen in Influencer haben.[86] Diese besondere Nähe und Authentizität würde verloren gehen, wenn die Werbebeiträge mehr als nur ein Nebenprodukt des Inhaltes darstellen würden. Auf die Frage, wie die Follower diese Werbebeiträge einschätzen können, hat die Anzahl von Followern und Interaktionen auf diese Beiträge Einfluss.[87] Dies ist aber kein tragender Pfeiler der Wirklichkeitsbildung, sondern allenfalls ein kleiner Faktor, welcher für eine vermögensrelevante Entscheidung regelmäßig nicht ausschlaggebend ist.[88] Es ist somit anzunehmen, dass die Person des Influencers selbst ausschlaggebend ist. Hierfür spricht, dass der Einfluss der Influencer auf die Kaufentscheidung und Produktwahrnehmung zum einen von der Stärke der Beziehungen, zum anderen auch von der Glaubwürdigkeit der Community abhängt.[89] Sowohl die Beziehung zwischen dem Influencer und dem einzelnen Follower als auch dessen Glaubwürdigkeit entsteht durch die persönliche Adressierung der Inhalte sowie dessen Gesamteindruck. Durch die Followeranzahl als solches würde weder eine solch starke Beziehung aufgebaut, noch der Influencer für die Community glaubwürdiger

[81] Vgl. *Lichtnecker* (Fn. 13) S. 523 (525); *Beck* (Fn. 7) S. 417.

[82] *Beck* (Fn. 7) S. 417; Vgl. auch: *Lichtnecker* (Fn. 13) S. 523 (525); *Lichtnecker* (Fn. 9) S. 512 (516); *Leeb/Maisch* (Fn. 8) S. 29 (38); *Kilian* (Fn. 6) S. 365.

[83] *Beck* (Fn. 7) S. 418.

[84] *Dobbelstein/Walz* (Fn. 12) S. 45; *Laoutoumai/Heins* (Fn. 9) S. 84; *Kilian* (Fn. 6) S. 365.

[85] *Dobbelstein/Walz* (Fn. 12) S. 45; *Laoutoumai/Heins* (Fn. 9) S. 84; *Kilian* (Fn. 6) S. 365.

[86] *Kilian* (Fn. 6) S. 365.

[87] *Beck* (Fn. 7) S. 418; Vgl. *Lichtnecker* (Fn. 13) S. 523 (525); *Lichtnecker* (Fn. 9) S. 512 (516).

[88] *Beck* (Fn. 7) S. 418.

[89] *Nguyen* (Fn. 6) S. 150.

erscheinen. Vergleichen lässt sich dies mit einem Beispiel aus der klassischen TV-Werbung. Verbraucher kaufen zum Beispiel auch keine „Haribo Goldbären", weil sie wissen, dass Thomas Gottschalk als deren Werbegesicht eine bekannte Person des öffentlichen Lebens ist, sondern assoziieren allenfalls das positive Erscheinungsbild dieser Person in der Werbung mit dem Produkt.[90] Auch an diesem Beispiel zeigt sich, dass die Wirkung des Testimonials nicht allein aus der bloßen Bekanntheit des Prominenten herrührt. Die Verantwortlichkeit beim Betrug wird dem Täter dadurch zugeschrieben, dass dieser für die Tatsachen widerstreitende Entscheidungsgrundlage des Opfers zuständig ist.[91] Die Entscheidungsgrundlage des Nutzers ist jedoch von einem bloßen Werturteil des Influencers und dessen Vertrauen in diese Person geprägt. Somit liegt keine den Tatsachen widerstreitende Entscheidungsgrundlage vor. Auch im Hinblick auf das Ultima Ratio-Prinzip sollte mit dem Strafrecht in solchen Fällen restriktiv umgegangen werden. Eine betrugsrelevante Täuschung der Follower durch den Influencer kommt folglich nicht in Betracht.

III. Produktrezensionen durch Social Bots

Bei dem Phänomen des Astroturfings ist zunächst die Funktion von Produktrezensionen zu klären (III. 1.), des Weiteren ist es fraglich, ob es sich bei Produktrezensionen um Tatsachen handelt, mit welchen die Kunden getäuscht werden können (III. 2.).

III. 1. Funktionen von Produktbewertungen und das Phänomen des „Astroturfing"

Vertrauen in die Person oder in eine Sache gegenüber ist seit jeher ein essentieller Bestandteil von Nachfrage am Markt. Dieses Vertrauen hat sich evolutionär so entwickelt, dass sich ein enger Zusammenhang zwischen der Körperlichkeit und dem Vertrauen herausgebildet hat.[92] Dieses gilt nicht nur für Informationen, sondern auch für andere Menschen, denn das Vertrauen in Menschen, die man persönlich kennt, ist größer, weshalb man diesen leichter vertraut als gänzlich Unbekannten.[93] So vertraut man also einem guten Bekannten, der einem einen Restauranttipp gibt aufgrund der Tatsache, dass man diesen bereits über einen längeren Zeitraum kennt und ihn besser einschätzen kann, als einer absolut fremden Person.[94] Kunden haben sich so schon immer durch die „Mundpropaganda" über die Qualität und Zuverlässigkeit eines Anbieters ausgetauscht.[95] Durch die zunehmende Digitalisierung verlagern sich die Anbieter zunehmend in die digitale Welt. Hieraus ergibt sich die Konsequenz, dass die persönlichen Interaktionen zwischen den Kunden und Anbietern

[90] Vgl. *Kilian* (Fn. 6) S. 356 f.

[91] *Kindhäuser/Schumann,* in: Hilgendorf/Kudlich/Valerius, Handbuch des Strafrechts Band 5: Strafrecht Besonderer Teil II, 2020, § 33 Rn. 33; *Fischer,* § 263 Rn. 2.

[92] *Boehme-Neßler,* Vertrauen im Internet – Die Rolle des Rechts, MMR 2009, 439 (442).

[93] *Boehme-Neßler* (Fn. 93) S. 439 (442).

[94] Vgl. *Ruess/Bredies* (Fn. 10) S. 18.

[95] *Hugendubel/Zarm,* „Gekaufte" Kundenbewertungen Wettbewerbsrechtliche Analyse der Auswirkungen auf die Gesamtbewertung, IPRB 2020, 135; *Franz,* Die rechtliche Beurteilung von Bewertungsportalen, WRP 2016, 1195 (1196).

sowie zwischen den Kunden unter sich ausbleiben. Der Soziologe *Luhmann* ordnete das Vertrauen als soziales Phänomen ein, welches im entwickelten gesellschaftlichen System Komplexität reduziere und so Handlungsmöglichkeiten realisiere.[96] Anbieter und Kunden befinden sich in einer Situation asymmetrischer Information.[97] Kunden können jedoch dieser Situation entkommen, wenn sie einen Anbieter oder ein Produkt wählen, dem sie mehr Vertrauen schenken, wenn dieser bereits von mehreren anderen Kunden positiv bewertet wurde.[98] Der Kunde geht demnach davon aus, dass der Anbieter zuverlässig und berechenbar ist.[99] Authentische Produktrezensionen haben so einen großen Mehrwert für Kunden und Verbraucher.[100]

Die positiven Produktbewertungen von Kunden stellen einen, abgesehen von der positiven Kundenresonanz, hohen Wert für das Unternehmen dar, da diese Rezensionen anderen Kunden Vertrauen in der Kaufentscheidung geben und so den Absatz des Unternehmens beziehungsweise des Produktes fördern.[101] Um einen ökonomischen Vorteil durch den gesteigerten Absatz und der durch die Kundenmeinung beeinflussten Reputation einen Wettbewerbsvorteil vor Mitbewerbern zu erlangen, nutzen einige Unternehmen manipulierte Produktrezensionen.[102] Dieses Phänomen wird auch als „Astroturfing" bezeichnet.[103] Hierbei werden die positiven Produktrezensionen automatisiert durch Social Bots generiert.[104] Diese Unterform von Social Bots werden als sogenannte „sybil-accounts" oder „fraudulent accounts" bezeichnet.[105] Hierbei handelt es sich um falsche Nutzerkonten, die mit manipulativer Absicht unauthentische[106] Produktbewertungen auf den entsprechenden

---

[96] *Luhmann,* Vertrauen, 5. Aufl. 2014, S. 27 ff.; Vgl. Zur Funktion des Vertrauens beim Betrug: *Ellmer* (Fn. 49) S. 274 ff.

[97] *Diekmann/Wyder,* Vertrauen und Reputationseffekte bei Internet-Auktionen, ZZfSS (Kölner Zeitschrift für Soziologie und Sozialpsychologie) 54, S. 674 (690).

[98] *Diekmann/Wyder* (Fn. 98) S. 674 (690); *Namysłowska* in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 5 Rn. 157; *Lichtnecker,* Die Werbung in sozialen Netzwerken und mögliche hierbei auftretende Probleme, GRUR 2013, S. 135 (139).

[99] Vgl. *Brinkmann/Seifert,* „Face to Interface": Zum Problem der Vertrauenskonstitution im Internet am Beispiel von elektronischen Auktionen, ZfS (Zeitschrift für Soziologie) 30, S. 23 (24).

[100] So auch der BGH in BGH, Urteil. v. 20.02.2020 – I ZR 193/18 – Kundenbewertungssysteme auf Online-Handelsplattformen, GRUR 2020, 543 (548), Rn. 37 f.

[101] *Bundeskartellamt,* Sektoruntersuchung Nutzerbewertungen, Bericht gemäß § 32e GWB, Az. V-22/19, Oktober 2020, S. 68 f.; *Hugendubel/Zarm* (Fn. 96) S. 135; *Lichtnecker* (Fn. 99) S. 135 (139); Spindler/Schuster/*Micklitz/Namysłowska,* UWG, § 5 Rn. 157; *Dienstbühl,* Zur Haftung von Händlern für irreführende Produktbewertungen auf Online-Marktplätzen, WRP 2020, S. 821; *Franz* (Fn. 96) S. 1195 (1196).

[102] *Hugendubel/Zarm* (Fn. 96) S. 135; *Krieg/Roggenkamp,* Astroturfing – rechtliche Probleme bei gefälschten Kundenbewertungen im Internet, KR 2010, S. 698; *Bundeskartellamt,* Sektoruntersuchung, S. 55; *Sosnitza,* Bewertungen und Rankings im Internet, CR 2021, S. 329.

[103] *Dienstbühl* (Fn. 102) S. 821; *Sosnitza* (Fn. 103) S. 329; *Hugendubel/Zarm* (Fn. 96) S. 135.

[104] Unauthentische Produktrezensionen werden unter anderem auch durch bezahlte Produkttester, durch Mitarbeiter oder sonstigen Gefälligkeitsrezensenten getätigt. Vgl. *Bundeskartellamt,* Sektoruntersuchung, S. 55.ff. Diese Arbeit befasst sich jedoch lediglich mit unauthentischen Produktrezensionen durch Social Bots.

[105] *Thieltges/Hegelich* (Fn. 15) S. 363.

[106] Mit dem Begriff unauthentische Produktbewertung sind solche zu verstehen, die von einem Social Bot generiert wurde. Der Begriff „falsche Produktbewertungen" würde Rückschlüsse auf den Inhalt dieser Bewertungen geben. Der Inhalt ist jedoch im folgenden nicht von Bedeutung.

Seiten generieren.[107] Wie auch bei der im ersten Teil beschrieben Form des Followerkaufs werden bei dieser Form des Social Bots zumeist von kommerziellen Anbietern massenhaft Nutzerkonten geschaffen, welche algorithmisch gesteuert werden und als Agenten mit den vom Betreiber des Webshops gewünschten Aufgaben „beauftragt" werden, welche dann automatisch abgearbeitet werden.[108] Problematisch hieran ist, dass so keine Erfahrungen aus der Lebenswirklichkeit der Kunden diesen unauthentischen Produktrezensionen zugrunde liegen. Dadurch kann der Kunde nicht mehr davon ausgehen, dass der Anbieter zuverlässig und berechenbar ist.

III. 2. Tathandlung: Täuschen über Tatsachen

Es stellt sich somit folgende Frage: Handelt es sich bei dieser Einwirkung auf das Vorstellungsbild des Kunden um eine betrugsrelevante Täuschung (III. 2. 2.) über Tatsachen (III. 2. 1.)?

III. 2. 1. Stellen Produktrezensionen Tatsachen dar?

Fraglich ist, ob es sich bei Produktrezensionen überhaupt um Tatsachen handelt. Tatsachen sind, wie obig bereits erwähnt, dem Beweis zugängliche Zustände der Gegenwart und Vergangenheit.[109] Diese sind abzugrenzen von bloßen Werturteilen. Solche bilden den Gegensatz zu Tatsachenbehauptungen, da diese subjektive Wertungen zum Ausdruck bringen und somit nicht auf ihre Wahrheit überprüft sowie bewiesen werden können.[110] Werturteile drücken die positive oder negative Auszeichnung bestimmter Sachverhalte aus.[111] Sie erhalten ihren spezifischen, sie von den Tatsachenaussagen unterscheidenden Charakter aus der Verwendung von Wertbegriffen wie zum Beispiel „schön" oder „eklig".[112] Produktrezensionen beinhalten einen subjektiven Erfahrungsbericht des Kunden über die Qualität und der Beschaffenheit des Produkts und teilweise über das Einkaufserlebnis an sich. Positive Produktrezensionen enthalten mithin auch positive Wertbegriffe wie „schön", „gut" oder „super". Hierbei handelt es sich um subjektive Wahrnehmungen, welche weder auf ihre Wahrheit überprüft noch bewiesen werden können. Selbiges ist der Fall, wenn zum Beispiel ein Kunde aussagt, dass zum Beispiel ein bestimmtes Gericht „köstlich" sei und „das Beste, was er jemals gegessen habe", denn dadurch drückt er lediglich seine positive Auszeichnung aus. Probleme bei der Abgrenzung treten häufig im Bereich der Produktwerbung auf.[113] Werbung für Produkte hat einen kaufentscheidenden Einfluss sowie infor-

---

[107] *Thieltges/Hegelich* (Fn. 15) S. 363; *Jülicher/Röttgen* (Fn. 14) S. 15 (16).

[108] *Thieltges/Hegelich* (Fn. 15) S. 363.

[109] RGSt 55, 129 (131); BGHSt 15, 24 (26); *Fischer,* § 263 Rn. 6; MüKo/*Hefendehl,* § 263 Rn. 96; Graf/Jäger/Wittig/*Dannecker,* § 263 Rn. 14; HK-GS/*Duttge,* § 263 Rn. 6.

[110] LK/*Tiedemann,* § 263 Rn. 13; *Fischer,* § 263 Rn. 9.

[111] *Hilgendorf,* Tatsachenaussagen und Werturteile im Strafrecht, 1998, S. 179.

[112] *Hilgendorf* (Fn. 112) S. 180.

[113] *Hecker* (Fn. 67) S. 220; *Fischer,* § 263 Rn. 10.

matorische Wirkung auf den Kunden.[114] Produktbewertungen haben wie bereits erwähnt, erheblichen Einfluss auf das Kaufentscheidungsverhalten von Kunden und können so den Absatz des Unternehmens fördern.[115] Demnach könnte man zunächst annehmen, dass es sich bei Produktbewertungen um Werbung oder zumindest um werbeähnliche Aussagen handelt.[116] Diese sind, sofern es sich um übertriebene oder nicht ernsthaft gemeinte Aussagen handelt, nicht vom Tatsachenbegriff erfasst.[117] Die unauthentischen Produktbewertungen sollen jedoch gerade auf den Kunden einen authentischen Anschein machen, um so Vertrauen zu generieren. Daher ist ein solcher Ausschluss aufgrund der Natur der Sache nicht einschlägig. Werbung ist daher vom Anwendungsbereich des Betruges erfasst, wenn sie als unwahre und zur Irreführung geeignete Angabe beziehungsweise falsche Behauptungen über Tatsachen darstellen.[118] Die Produktbewertungen stellen jedoch wie Kundenmeinungen angenommen sie beinhalten lediglich wertende Aussagen und haben keinen falschen Tatsachengehalt, einen subjektiven Erfahrungsbericht und somit ein bloßes Werturteil dar. Im Ergebnis handelt es sich bei Produktbewertungen somit nicht um Tatsachen.

Es lässt sich jedoch für die Frage, ob es sich bei den unauthentischen Produktbewertungen um Tatsachen handelt, nicht nur am Inhalt der Aussage anknüpfen. Für den Kunden ist ferner relevant, ob die Produktbewertung von einem echten Kunden stammt und wie häufig positive Bewertungen vorkommen. Aus der soziologischen Perspektive ist die Echtheit des Bewertenden und die Eigenschaft als Kunde aus folgenden Gründen besonders relevant für den Kunden. Grundsätzlich besteht beim Austausch zwischen anonymen Akteuren für Tauschpartner ein hohes Risiko, denn der Käufer kennt die Qualität der verkauften Ware nicht und der Verkäufer hat keine Kenntnis über die Zahlungsfähigkeit des Käufers.[119] Dieses Risiko verschwindet jedoch, wenn sich die Interaktionen derselben Tauschpartner wiederholen, denn das Vertrauen wird über das vergangene Verhalten erlernt.[120] Im Internet erschwert sich jedoch das Problem der Anonymität, denn die Akteure sind optisch und physisch nicht wahrnehmbar, sondern können eine virtuelle Identität annehmen, in dem sie sich Fantasienamen oder Scheinadressen bedienen.[121] Anbieter und Käufer befinden sich mithin wieder in einer Situation asymmetrischer Information.[122] Hierbei wissen Käufer und Verkäufer nicht wie der andere handeln wird, was zu einer Notwendigkeit von Vertrauen führt.[123] Dieses Vertrauen lässt sich steigern, wenn der Käufer einen Anbieter mit einer

---

[114] *Hecker* (Fn. 67) S. 217.

[115] S.o.: III. 1. 1.; Vgl. *Bundeskartellamt,* Sektoruntersuchung, S. 68 f.; *Hugendubel/Zarm* (Fn. 96) S. 135; *Lichtnecker* (Fn. 99) S. 135 (139); Spindler/Schuster/*Micklitz/Namysłowska* UWG § 5 Rn. 157.

[116] Vgl. BGH WRP 2016, 974: Hier hatte ein Anbieter auf seiner Startseite mit „Kundenbewertung 4,8/5" geworben.

[117] Handbuch des Strafrechts/*Kindhäuser/Schumann,* § 33 Rn. 85; Zu den Kriterien der h.M.: *Hecker* (Fn. 67) S. 221 ff.

[118] *Hecker* (Fn. 67) S. 218.

[119] *Diekmann/Wyders* (Fn. 98) S. 647.

[120] *Diekmann/Wyders* (Fn. 98) S. 674.

[121] *Diekmann/Wyders* (Fn. 98) S. 674 (675).

[122] *Diekmann/Wyders* (Fn. 98) S. 674 (690).

[123] *König/Sumpf,* Hat der Nutzer immer Recht? Zum inflationären Rückgriff auf Vertrauen im Kontext von Online-Plattformen, in: Massen/Passoth (Hrsg.), Soziologie des Digitalen – Digitale Soziologie?, 2020, S. 250.

hohen Reputation wählt.[124] Bei dieser Auswahl vertraut der Kunde darauf, dass ein anderer Kunde sein in der Interaktion mit dem Anbieter erlerntes Vertrauen mit diesem teilt. Durch das Verwenden der Social Bots erhöht sich die Quantität der positiven Bewertungen um ein Vielfaches. Zwar lässt sich die Quantität der positiven Bewertungen auch durch die eigenen Mitarbeiter oder sonstige teilweise geldwerte Kundenanreizen steigern, jedoch nicht in der Mengenordnung, die die Social Bots generieren können.[125] Diese Quantität hat Auswirkungen auf das Kaufverhalten, denn haben mehrere Kunden gute Erfahrungen mit dem Anbieter gemacht, so erhöht sich die Reputation des Anbieters und die Wahrscheinlichkeit, dass der Kunde diesen auch auswählt. Anhand von repräsentativen Studien lässt sich belegen, dass Kunden von Onlineanbietern ihre Kaufentscheidung zunehmend auf der Grundlage von Produktrezensionen treffen.[126] Eine Studie des Branchenverband BITKOM hat ergeben, dass für 55% der gesamten und 66% der 16-29-jährigen Nutzer Produktrezensionen die wichtigste Informationsquelle beim Online-Shopping ist.[127]

Auch der Gesetzgeber hat dies erkannt und hat im Rahmen des Gesetzes zur Stärkung des Verbraucherschutzes im Wettbewerbs- und Gewerberecht die Herkunft von Produktbewertungen als wesentliche Information anerkannt und im neu eingeführten § 5b UWG normiert.[128] Macht der Unternehmer (Anbieter) die Bewertungen zugänglich, die Verbraucher im Hinblick auf Waren oder Dienstleistungen vorgenommen haben, so gilt es als wesentliche Informationen darüber, ob und wie der Unternehmer sicherstellt, dass die veröffentlichten Bewertungen von solchen Verbrauchern stammen, die die Waren oder Dienstleistungen tatsächlich genutzt oder erworben haben (Vgl. § 5b III UWG) . Zusammenfassend lässt sich also sagen, dass es sich bei der Quantität der Produktbewertungen und der vertrauensbegründenden Tatsache, dass diese von echten Kunden geschrieben werden, um zentrale Aspekte der Wirklichkeitsbildung handelt.[129] Dass es sich bei den Rezensenten um echte Menschen und vor allem um Kunden[130] des Anbieters handelt, ist genau wie die Quantität solcher Produktbewertungen, eine dem Beweis zugängliche Tatsache.

Bei den unauthentischen Produktbewertungen handelt es sich somit dem Inhalt nach nicht um Tatsachen, sondern um bloße Werturteile. Anders hingegen bei der Quantität der Produktbewertungen und der Identität der Bewertenden als menschlicher Kunden. Diese sind dem Beweis zugängliche Tatsachen.

---

[124] *Diekmann/Wyders* (Fn. 98) S. 674 (690).

[125] *Beck* (Fn. 7) S. 413; Zur Quantität bei politischen Nachrichten vgl. *Libertus* (Fn. 2) S. 20 f.; *Reinbacher* (Fn. 17) S. 458 f.

[126] *Dienstbühl* (Fn. 102) S. 821; Vgl. *Bundeskartellamt,* Sektoruntersuchung, S. 47 f.

[127] Pressemitteilung von BITKOM vom 27. 11. 2020 https://www.bitkom.org/Presse/Presseinformation/Online-Bewertungen-sind-wichtigste-Informationsquelle (Stand: 20.09.2022).

[128] § 5b eingef. mWv 28.5.2022 durch G v. 10.8.2021 (BGBl. I S. 3504), zur Umsetzung der Richtlinie (EU) 2019/2161. Inkrafttreten am 28.05.2022; Zur Begründung: Bt-Drs.19/27873 S. 19 ff.

[129] Vgl. *Beck* (Fn. 7) S. 413.

[130] Anders jedoch *Beck* (Fn. 7) S. 414 welche unzutreffender Weise nur auf die Eigenschaft des Rezensenten als Mensch abstellt.

III. 2. 2. Täuschung durch das Erstellen und Verwenden von unauthentischen Rezensionen

Der Anbieter müsste mit dem Erstellen der unauthentischen Produktrezensionen über die Quantität und die Echtheit der Kunden den Käufer täuschen.

Ob es sich beim Erstellen der unauthentischen Produktbewertungen um eine ausdrückliche oder konkludente Täuschung handelt, ist abhängig von der Art, wie die Produktbewertungen auf der Seitenoberfläche des Anbieters eingebettet werden.

Der Kunde wird häufig bereits bei der Suche nach einem Produkt mit den Rezensionen anderer Kunden konfrontiert, in dem sich an den Produktkacheln sich bereits ein Feld mit der durchschnittlichen Bewertung des Produktes findet. Der Kunde erhält hierbei keinen detaillierten Erfahrungsbericht, sondern lediglich eine Bewertung, etwa in Form von Sternen. Ferner besteht auch die Möglichkeit, die gesuchten Produkte nach diesen durchschnittlichen Kundenbewertungen zu sortieren. Ebenfalls verbreitet ist die Anordnung dieser Durchschnittsbewertungen zwischen dem Produktvorschaubild, dem Preis und dem Bestellbutton. Bewegt man die Maus auf diese Durchschnittsbewertung oder klickt diese an, so wird dem Nutzer häufig die genaue Verteilung der Bewertungen aufgeschlüsselt. Teilweise werden Produktbewertungen in Form von kurzen Erfahrungsberichten neben der eigentlichen Artikelseite eingeblendet. Am wohl verbreitetsten sind schließlich die ausführlichen Produktbewertungen, welche zum Teil einen ausführlichen Erfahrungsbericht sowie Fotos oder gar Videos von dem Produkt enthalten. Diese befinden sich in der Regel am unteren Ende der Seite, sodass der Kunde auf der Seite des Produktes nach unten scrollen muss, um diese zu lesen.

Die ausdrückliche Täuschung besteht in der ausdrücklichen Erklärung der Unwahrheit über Tatsachen.[131] Neben einer Erklärung in Wort und Schrift kann diese auch auf eine andere kommunikative Weise ausreichen, wenn diese aufgrund der Verkehrsanschauung keinen Zweifel hinsichtlich des Erklärungswerts bestehen.[132] Bettet der Anbieter die Rezension in Form von Sternen zwischen dem Vorschaubild, Preis und Bestellbutton ein, so könnte angenommen werden, dass er damit ausdrücklich über die Authentizität der Rezensionen täuscht, denn diese Stelle ist gerade dazu gewählt, dass der Kunde die Sternebewertung, als maßgebliche Entscheidungsgrundlage nutzt.[133] Diese Bewertung ist, wie bereits erörtert, für den Kunden nur relevant, wenn diese auch authentisch ist. Kritisch zu betrachten ist jedoch die Frage, ob diesen Bewertungen vor allem in der prominenten Platzierung überhaupt ein solcher Erklärungswert zukommt. Die Bewertungen sind so platziert, dass der Kunde sie nicht extra anklicken oder gar suchen muss, sondern zwangsweise wahrnehmen muss. Durch diese direkte Wahrnehmung könnte eine gewisse Nähe zu einer ausdrücklichen Erklärung liegen. Problematisch hieran wäre jedoch, dass dadurch die Grenze zwischen ausdrücklicher Täuschung und konkludenter Täuschung verschwimmen würde. Die Differenzierung ist jedoch äußert relevant, denn bei der konkludenten Täuschung wird im Vergleich zur ausdrücklichen Täuschung eine Erheblichkeitsprüfung und die Verteilung

---

[131] LK/*Tiedemann,* § 263 Rn. 24; *Fischer,* § 263 Rn. 18; MüKo/*Hefendehl,* § 263 Rn. 138.

[132] LK/*Tiedemann,* § 263 Rn. 24; *Fischer,* § 263 Rn. 18; MüKo/*Hefendehl,* § 263 Rn. 138.

[133] Vgl. *Bundeskartellamt,* Sektoruntersuchung, S. 37.

von Informations- und Irrtumsrisiken vorgenommen.[134] An die konkludente Täuschung sind somit größere Hürden gestellt. Abgrenzen lässt sich dies anhand der Frage, inwieweit man auf die Verkehrsanschauung zurückgreifen muss, um die Unwahrheit der Tatsachenbehauptung beurteilen zu können.[135] Muss man mehr auf die Verkehrsanschauung zurückgreifen, dann liegt eine konkludente Täuschung vor. In dieser Konstellation ist die Verkehrsanschauung, also die Frage, wie die Kunden dies Verstehen absolut notwendig, um den Produktbewertungen und der Einbettung dieser auf der Anbieterseite einen Erklärungswert beizumessen. Mithin handelt es sich bei dieser Konstellation nicht um eine ausdrückliche Täuschung. Anders hingegen verhält es sich in Fällen, in denen der Anbieter auf seiner Seite explizit darauf verweist. Hierfür blendet dieser beispielsweise ausgewählte unauthentischen Produktbewertungen ein und kommentiert diese zum Beispiel mit Aussagen wie: „Die Meinung unserer Kunden zum Produkt (…)" oder „Unsere Kunden sagen (…)". Hier erklärt der Anbieter ausdrücklich, dass es sich bei den Produktbewertungen um solche von echten Kunden handelt. Zusammenfassend lässt sich also sagen, dass abgesehen von Fällen, in denen der Anbieter die unauthentischen Bewertungen nicht explizit in Form einer Erklärung einbezieht, eine ausdrückliche Täuschung in den Konstellationen des Astroturfings nicht in Betracht kommt.

Es stellt sich also die Frage, ob in den Konstellationen, in denen es sich bei der Verwendung von unauthentischen Produktbewertungen nicht um ausdrückliche Täuschungen handelt, eine aktive Täuschung durch konkludentes Verhalten einschlägig ist. Diese ist einschlägig, wenn die Unwahrheit nicht ausdrücklich, aber nach der Verkehrsanschauung konkludent miterklärt wird.[136]

Anknüpfen lässt sich zunächst an das vom Anbieter beauftragte Platzieren der unauthentischen Produktbewertungen durch die verwendeten Social Bots an prominenten Stellen auf dessen Website. Durch das Platzieren der unauthentischen Produktbewertungen müsste schließlich der Anbieter miterklären, dass es sich bei den Bewertungen des Produktes um authentische Bewertungen handelt. Die bereits zuvor erwähnte verkaufsfördernde Wirkung von Kundenbewertungen kann erst eintreten, wenn die Kundenbewertung auch als Entscheidungsgrundlage einbezogen werden kann. Diese muss also dem potentiellen Kunden zunächst zugänglich gemacht werden. Das zugänglich machen erfolgt dadurch, dass die neue Bewertung zum Beispiel die Durchschnittsbewertung verbessert oder einen neuen Erfahrungsbericht enthält. Durch das bloße Erstellenlassen der Produktbewertungen sind diese zwar dem Kunden zugänglich gemacht, jedoch hat dieser sie so noch nicht zur Kenntnis genommen und zu seiner Entscheidungsgrundlage einbezogen. Das bloße Erstellenlassen der Produktbewertungen durch Social Bots ist somit eine Handlung, welche sich noch im Stadium des Versuchs befindet. Ein weiterer Anknüpfungspunkt besteht ferner im Verwenden der Produktbewertung. Die unauthentischen Produktbewertung müsste durch den Anbieter verwendet werden. Das Verwenden besteht im Nutzen der verkaufsfördernden Wirkung von Produktbewertungen. Diese müssen also dem potentiellen Kunden zunächst zugänglich gemacht werden. Das zugänglich machen erfolgt unter anderem durch die pro-

---

[134] LK/*Tiedemann,* § 263 Rn. 27.

[135] MüKoStGB/*Hefendehl,* § 263 Rn. 139; Matt/Renzikowski/*Saliger* § 263 Rn. 31; *Satzger* in: Satzger/Schluckebier/Widmaier, Kommentar zum Strafgesetzbuch, 5. Aufl. 2020, § 263 Rn. 39.

[136] BGHSt 51, 169; *Fischer,* § 263 Rn. 21; LK/*Tiedemann,* § 263 Rn. 28; Matt/Renzikowski/*Saliger,* § 263 Rn. 32.

minente Einbettung auf der Anbieterseite. Dies erfolgt, wie bereits zuvor erwähnt, unter anderem durch die Verbesserung der Durchschnittsbewertung oder der Darstellung einer neuen relevanten Rezension. Mithin liegt der Anknüpfungspunkt des Verwendens darin, dass der Kunde beim Aufrufen der Anbieterseite die Produktbewertung liest und diese Teil seiner Entscheidungsgrundlage wird. Anderweitig hätte die Bewertung wie beim ersten Anknüpfungspunkt keinerlei Einfluss auf das Entscheidungsverhalten beim Kauf. Ob der Anbieter beim Verwenden der Produktbewertung zugleich schlüssig miterklärt, dass es sich bei den Produktbewertungen nur um solche von echten Kunden handelt, erscheint zunächst fraglich. Für diese Frage ist es entscheidend, welcher Erklärungswert dem Gesamtverhalten des Täuschenden zukommt, dass heißt, ob der andere aufgrund der Kommunikationssituation vom Bestehen eines bestimmten Sachverhalts ausgehen darf.[137] Dass Produktbewertungen für die Kunden von Online-Shops eine essentielle und stark genutzte Informationsquelle sind, ist durch repräsentative Umfragen und daraus resultierenden Beiträgen in Fernsehsendungen und in der Fach- und Publikumsliteratur hinlänglich bekannt. Kunden nutzen diese, um ihr Geld für ein Produkt auszugeben, was ihren Vorstellungen und Erwartungen entspricht und um so die Gefahr zu vermeiden, ein „Versuchskaninchen" zu werden.[138] Die Aussagen von anderen Kunden in Produktbewertungen sind, wie bereits bei der Tatsachenfrage erörtert, ein essentieller Bestandteil der Wirklichkeitskonstruktion des Kunden. Da dem Kunden vor allem bei Produkten, welche selten vertrieben werden, häufig keine andere Möglichkeit bleibt, als auf die Angaben des Anbieters und die Produktbewertungen anderer Kunden zu verlassen, werden diese zu relevanten kontextualen Umständen.[139] Die unauthentischen Produktbewertungen sind aufgrund der Natur der Sache vom Anschein nach aufgrund der Platzierung und Darstellung identisch mit authentischen Bewertungen. Dies ist somit vergleichbar mit der Fallgruppe der Scheinrechnungen. In diesen Fällen täuscht der Täter konkludent durch das Versenden von suggestiv und manipulativ formulierten oder gestalteten Scheinrechnungen, welche jedoch ein Angebot enthalten.[140] Aufgrund der Gestaltung dieser Kommunikationssituation dürfen die Kunden davon ausgehen, dass der Anbieter miterklärt, dass es sich bei den Produktbewertungen um solche von echten menschlichen Kunden handelt.

Kritisch betrachtet könnte man jedoch zu dem Schluss kommen, dass der Anbieter durch die der Social Bots erstellten Produktbewertungen eine Gefahr für die potentiellen Kunden schafft und diese nicht beseitigt. Bei dieser Anknüpfung stellt die Handlung eine Täuschung durch Unterlassen dar. Jedoch ist an eine solche eine höhere Hürde gestellt, denn für den Anbieter müsste eine Garantenpflicht nach § 13 StGB zur Aufklärung bestehen.[141] Diese könnte jedoch durch die Anknüpfung an das Verwenden der Produktbewertungen umgangen werden. Ob dem Anbieter bei Schaffung der Gefahr oder dem späteren Vertragsschluss mit dem Kunden eine solche Garantenpflicht entsteht, kann jedoch dahinstehen. Die konkludente Täuschung beim Verwenden umgeht diese etwaige Garantenpflicht nicht,

[137] Schönke/Schröder/*Perron,* § 263 Rn. 14-15; Matt/Renzikowski/*Saliger,* § 263 Rn. 32.

[138] *Franz,* WRP 2016, 1195 (1196).

[139] *Beck* (Fn. 7) S. 413.

[140] *Fischer,* § 263 Rn. 28; MüKoStGB/*Hefendehl,* § 263 Rn. 121; Eine konkludente Täuschung wurde auch dann angenommen, wenn dies beim sorgfältigen Lesen erkennbar gewesen wäre (BGH 47, 1).

[141] *Fischer,* § 263 Rn. 38; Lackner/Kühl/*Kühl,* § 263 Rn. 12.

denn der Rechtsgrund für die zu erbringende Information ist zwischen den beiden Anknüpfungspunkten unterschiedlich.[142] Beim Unterlassen muss der Anbieter die Information erbringen, weil er aufgrund seiner Garantenstellung für die Irrtumsfreiheit des Kunden zu sorgen hat, hingegen er jedoch bei der konkludenten Täuschung dafür einzustehen hat, dass durch die Verwendung der unauthentischen Produktbewertungen ein Irrtum erwächst.[143]

III. 2. 3. Opfermitverantwortung

Im Rahmen der konkludenten Täuschung wird schließlich auch eine Verteilung von Irrtums- und Informationsrisiken vorgenommen.[144] Der Kunde vertraut darauf, dass die Produktbewertungen Erfahrungsberichte von echten, menschlichen Kunden darstellen, ohne diese jemals fernab der virtuellen Wirklichkeit wahrgenommen zu haben. So stellt sich die Frage, ob eine gewisse Leichtfertigkeit einen einschränkenden Einfluss auf die Täuschungshandlung haben kann. Neben den bereits erwähnten viktimodogmatischen Einschränkungen könnte eine solche Einschränkung der objektiven Täuschungseigenschaft aus dem höherrangigen Recht herrühren.

In Betracht kommt hierfür das Unionsrecht, genauer gesagt die UGP-Richtlinie (folgend: UGP-RL).[145] Das Unionsrecht hat Anwendungsvorrang, weshalb das nationale Recht verpflichtend unionsrechtskonform ausgelegt werden muss.[146] Diese Auslegung zielt darauf ab, dem Unionsrecht inhaltlich zur Geltung zu verhelfen und unionsrechtswidriges nationales Recht zu verdrängen.[147] Mithin besteht die in Art. 291 AEUV normierte Pflicht zur Unionstreue auch für Gerichte und betrifft daher auch das Strafrecht.[148] Nach der UGP-RL darf zur Gewährleistung der Warenverkehrsfreiheit der Schutz durch den Betrugstatbestand beispielsweise bei produktbezogenen Irreführungen erst dann beginnen, wenn ihnen auch ein durchschnittlich informierter, aufmerksamer und verständiger Verbraucher zum Opfer fallen kann.[149] Im Folgenden muss dabei zunächst die Seriosität und die Qualität der Anbieterseite berücksichtigt werden, denn dies ist dafür relevant, inwieweit der Kunde bei der Verwendung von Produktbewertungen auf diese als Grundlage der vermögensrelevanten Entscheidung vertrauen darf. Angenommen, die Website des Anbieters erscheint weniger vertrauenswürdig, da sie beispielsweise nicht über einen „trustedshop-Siegel" verfügt, kein Impressum enthält oder die Sprache der Textfelder in einem schlechten Stil sind. Ferner

---

[142] Handbuch des Strafrechts/*Kindhäuser/Schumann,* § 33 Rn. 17.

[143] Handbuch des Strafrechts/*Kindhäuser/Schumann,* § 33 Rn. 17; *Fischer,* § 263 Rn. 38; *Kasiske* (Fn. 48) S. 360 (370).

[144] LK/*Tiedemann,* § 263 Rn. 27; *Hennings* (Fn. 69) S. 99

[145] Europäische Richtlinie über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt, RL 2005/29/EG; Vgl. Handbuch des Strafrechts/*Kindhäuser/Schumann,* § 33 Rn. 37; *Hoyer,* Reichweite und Grenzen von Verbraucherschutz mithilfe des Betrugstatbestands, ZIS 2019, 412 ff. m.w.N.

[146] Grundlegend EuGH v. 10.04.1984 – Rs. 14/83 – von Colsen, Slg. 1984, 1891; LK/*Tiedemann,* vor § 263 Rn. 98; *Engelhart* in: Müller-Gugenberger, Wirtschaftsstrafrecht, 6. Aufl. 2015, § 6 Rn. 85; *Fischer,* vor 263 Rn. 6; *Hoyer* (Fn. 146) S. 412.

[147] Müller-Gugenberger/*Engelhart,* § 6 Rn. 87.

[148] LK/*Tiedemann,* vor § 263 Rn. 98; Vgl. BGHSt 37, S. 333, (336)

[149] Zum Verbraucherleitbild vor allem EuGH Slg. 1995, I-1923 ff. („Mars") Vgl. AK-StGB/*Gaede,* § 263 Rn. 23 m.w.N.; Handbuch des Strafrechts/*Kindhäuser/Schumann,* § 33 Rn. 37; *Hoyer* (Fn. 146) S. 412 ff. m.wN.

enthält eine solche Seite Produktbewertungen, welche ebenfalls sprachlich und inhaltlich unterdurchschnittlich gestaltet oder überfrachtet mit Superlativen über das Produkt und den Service des Anbieters sind. Bei einer solchen Ausgangslage lässt sich annehmen, dass ein durchschnittlich informierter, aufmerksamer und verständiger Verbraucher weitere Nachforschungen über den Anbieter und das Produkt mithilfe von Bewertungsportalen von Dritten macht oder im Bekanntenkreis nach Erfahrungen hierzu fragt. Mithin würden diese Verbraucher sich nicht durch unauthentische Produktbewertungen irreführen lassen.

Anders hingegen würde diese Annahme ausfallen, wenn man eine seriös wirkende Website eines bekannten Anbieters vor Augen hat. Hier könnte der Kunde zum einen durch Reputation von ihm bekannten Dritten oder durch die allgemeine Bekanntheit des Anbieters einen höheren Vertrauensmaßstab ansetzen als bei einem unbekannteren Anbieter.[150] Durch dieses höhere Vertrauen könnte man annehmen, dass auch weniger seriös wirkenden Produktbewertungen hingenommen werden. Den informierten und aufmerksamen Verbraucher würde dies somit irreführen. Erst recht würde sich dieser irreführen lassen, wenn die unauthentischen Produktbewertungen aufgrund ihres täuschend ähnlichen Anscheins von einer authentischen Bewertung nicht mehr zu unterscheiden wäre. Im Ergebnis würde sich ein durchschnittlicher, aufmerksamer und informierter Verbraucher in den praktisch relevanteren Konstruktionen irreführen lassen, weshalb eine Einschränkung der Täuschungseignung durch die UGP-RL nicht in Betracht kommt. Als einziger Anwendungsbereich käme diese Einschränkung bei Fällen von leichtgläubigen Kunden in Betracht.

Ob eine unionsrechtskonforme Einschränkung des Betrugstatbestands vorgenommen werden muss, ist jedoch umstritten.

Eine in der Literatur weitverbreitete Auffassung nimmt an, dass der sich am Leitbild eines verständigen und aufmerksamen Durchschnittsverbrauchers orientierende Täuschungsschutzstandard gleichzeitig den strafrechtlichen Täuschungsbegriff determiniere und die Betrugsstrafbarkeit nur dort erlaube, wo sich auch ein verständiger Durchschnittsverbraucher hätte täuschen lassen.[151] Hierfür spricht, dass das in Art. 5 Abs. 4 lit. a, 6 Abs. 1 UGP-RL normierte Verbot von irreführenden Geschäftspraktiken vollharmonisierende Wirkung entfacht, weshalb der Täuschungsschutzstandard weder über- noch unterschritten werden darf.[152] Vom nationalen Recht dürfen Geschäftspraktiken nicht untersagt werden, welche nach den Vorgaben der UGP-RL nicht als irreführend einzustufen sind.[153]

Die Rechtsprechung des BGH folgt dieser Auffassung jedoch nicht.[154] Nach Ansicht des 2. Strafsenats besteht die Pflicht zur richtlinienkonformen Auslegung im materiellen Strafrecht nicht vorbehaltlos, sondern nur dann, wenn der Regelungsinhalt der Richtlinie „nach

---

[150] Vgl. Zur Anbieterreputation und Vertrauen: *Diekmann/Wyders* (Fn. 98) S. 674 (675 ff.); *Ellmer* (Fn. 49) S. 274 ff.

[151] *Hecker/Müller,* Europäisches Verbraucherleitbild und Schutz vor irreführenden Geschäftspraktiken am Beispiel sog. „Internet-Kostenfallen" aus lauterkeits- und betrugsstrafrechtlicher Sicht, ZWH 2014, S. 329 (334); AK-StGB/*Gaede,* § 263 Rn. 23; *Dannecker,* Die Dynamik des materiellen Strafrechts unter dem Einfluss europäischer und internationaler Entwicklungen, ZStW 117 (2006), S. 697 (711 ff.); *Müller,* Urteilsanmerkung zu BGH, Urt. v. 5.3.2014 – 2 StR 616/12, – Routenplaner NZWiSt 2014, S. 387 (394 f.).

[152] *Hecker/Müller* (Fn. 152) S. 329 (334); *Hoyer* (Fn. 146) S. 412 (413).

[153] *Brand/Blatter,* Europarecht in der strafrechtlichen Fallbearbeitung, JuS 2016, 983, (986 f.); *Hecker/Müller* (Fn. 152) S. 329 (334)

[154] BGH, Urt. v. 5.3.2014, 2 StR 626/12 – Routenplaner, NJW 2014, 2595 (2586 ff.)

deren Sinn und Zweck auf die Strafnorm durchschlägt".[155] Das primäre Ziel der UGP-RL sei es, den Verbraucherschutz zu stärken, weshalb eine Einschränkung des strafrechtlichen Täuschungsschutzes dieses Ziel eher Konterkarrieren als erreichen würde.[156] Mithin verfolge die Richtlinie nicht den Zweck, Geschäftspraktiken, die auf eine Vermögensschädigung abzielen, straffrei zu stellen.[157] Hiermit schließt sich der BGH im Ergebnis an die früheren Urteile an, welche die viktimodogmatischen Ansätze ablehnten.[158]

Im Ergebnis kann dieser Streit in der Frage nach der Einschränkung der Täuschungshandlung bei unauthentischen Produktbewertungen jedoch dahinstehen, denn der Richtliniengeber hat in der Novellierung der UGP-RL diese Konstellation explizit berücksichtigt.[159] In der UGP-RL werden im Anhang I Geschäftspraktiken aufgelistet, welche immer unlauter sind, um so schutzwürdige Personengruppen zu schützen. Insoweit greift im Übrigen auch die pauschale Aussage des Senats nicht, nach dem eine richtlinienkonforme Auslegung des Betrugstatbestandes gerade solchen Verbrauchern den strafrechtlichen Schutz versage, die in besonderem Maße schutzwürdig sind.[160] In den Anhang I wurde durch die Richtlinie (EU) 2019/2161 nun die Nummer 23b eingefügt, nach welcher nun die Behauptungen des Betreibers, dass die Bewertungen eines Produkts von Verbrauchern stammen, die das Produkt tatsächlich verwendet oder erworben haben, ohne dass angemessene und verhältnismäßige Schritte unternommen wurden, um zu prüfen, ob die Bewertungen wirklich von solchen Verbrauchern stammen als unlautere Geschäftspraxis gilt. Mithin erfasst dieser neue Teil des Anhangs alle Konstellationen des Astroturfings, denn die Ausnahme durch eine Überprüfung ist bei den eigens durch Social Bots erstellten Produktbewertungen schlechterdings unmöglich.

Ob die Täuschungshandlung durch die UGP-RL objektiv eingeschränkt werden kann, bleibt weiterhin fraglich. Die wohl überzeugenderen Argumente liefern die Auffassungen, die eine Strahlung der UGP-RL auf den Betrugstatbestand annehmen.[161] In den Konstellationen des Astroturfings hat diese Richtlinie jedoch keine Einwirkung auf den Betrugstatbestand. Mithin hat auch eine gewisse Leichtfertigkeit des Kunden keinen einschränkenden Einfluss auf die Täuschungshandlung.

---

[155] BGH, NJW 2014, 2595 (2597).

[156] BGH, NJW 2014, 2595 (2597).

[157] BGH, NJW 2014, 2595 (2597); vgl. *Erb,* ZIS 2011, 368 (376).

[158] Siehe oben B II. c); Vgl. *Hecker/Müller* (Fn. 152) S. 329 (334); *Rengier,* Europäisches Verbraucherbild und Betrugsstrafrecht, in: Büscher/Glöckner/Nordemann/Osterrieth/Rengier (Hrsg.), Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz. Festschrift für Karl-Heinz Feezer zum 70. Geburtstag, 2016, S. 365.

[159] Richtlinie (EU) 2019/2161 des Europäischen Parlaments und des Rates vom 27.11.2019 zur Änderung der Richtlinie 93/13/EWG des Rates und der Richtlinien 98/6/EG, 2005/29/EG und 2011/83/EU des Europäischen Parlaments und des Rates zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union, ABl. Nr. L 328 vom 18.12.2019, S. 7; Hierzu auch *Sosnitza,* (Fn. 103) S. 329.

[160] *Hecker/Müller* (Fn. 152) S. 329 (334); So ist zum Beispiel die Falsche Behauptung, ein Produkt könne Krankheiten, Funktionsstörungen oder Missbildungen heilen immer unlauter. Hierzu vgl. BGHSt 34, 199.

[161] So u.a. *Hecker/Müller* (Fn. 152) S. 329; *Hoyer* (Fn. 146) S. 412; AK-StGB/*Gaede,* § 263 Rn. 23; *Dannecker* (Fn. 152) S. 697; *Müller* (Fn. 152) S. 387.

III. 2. 4. Ergebnis

Im Ergebnis lässt sich festhalten, dass ein Anbieter mit bei der Verwendung von unauthentischen Produktbewertungen betrugsrelevant täuschen kann. Bei Produktbewertungen handelt es grundsätzlich um subjektive Erfahrungsberichte und somit um bloße Werturteile. Bei Produktbewertungen, die von Social Bots erstellt wurden, kann jedoch auch an einer anderen Stelle angeknüpft werden. Die Tatsache, dass der Bewertende ein menschlicher Kunde ist, ist für die Wirklichkeitskonstruktion des potenziellen Kunden jedoch essentiell, weshalb an diese Eigenschaften als Tatsachen anzuknüpfen ist. Im Rahmen der Täuschung ist auch hier die ausdrückliche Täuschung wohl seltener relevant. Anbieter täuschen jedoch konkludent, wenn sie die unauthentischen Produktbewertungen verwenden. Dies liegt vor, wenn die Bewertung auf der Seite so eingebettet ist, dass der Kunde sie wahrnehmen kann und sie als Grundlage für eine vermögensrelevante Entscheidung verwendet. Diese strenge Täuschungshandlung wird auch nicht durch eine richtlinienkonforme Auslegung im Lichte der UGP-RL eingeschränkt, da diese aufgrund einer Novellierung Astroturfing explizit als unlautere Geschäftspraxis aufführt.

III. 3. Ergebnis

Das Phänomen des wirtschaftlich genutzten „Astroturfings" läuft der Funktion, der Überwindung der asymmetrischen Informationslage durch die Schaffung von Vertrauen zuwider. Diese Einwirkung auf den Kunden stellt eine betrugsrelevante Täuschung dar.

IV. Fazit und Ausblick

Im Ergebnis lässt sich festhalten, dass es sich beim Vortäuschen einer größeren Relevanz und Reichweite durch die Verwendung von gekauften Follower im Hinblick auf einen Werbepartner sowie bei der Praxis des Astroturfings um eine betrugsrelevante Täuschung handelt. Hier ist die Wirklichkeitsbildung des Opfers – nahezu alleinig – die Grundlage für eine vermögensrelevante Entscheidung. Anders hingegen bei der Täuschung über die Relevanz und Reichweite des Influencers gegenüber den übrigen realen Followern. Hier sind die Beiträge der Influencer wohl durchaus relevant für die Follower, jedoch sind diese aber keine tragenden Pfeiler der Wirklichkeitsbildung und somit für eine vermögensrelevante Entscheidung nicht alleinig entscheidend. Aufgrund des Ultima Ratio-Prinzip des Strafrechts ist diese restriktive Handhabung vorzugswürdig.

Vor dem Hintergrund des Ultima Ratio-Prinzip ist die Diskussion um die viktimodogmatischen Ansätze nochmals aufzugreifen. Rechtsvergleichend betrachtet geht das deutsche Opferschutzniveau im Vergleich zu anderen europäischen Rechtsordnungen wesentlich weiter.[162] Im französischen Strafrecht (Art. 405 c.p.) gilt grundsätzlich, dass eine einfa-

[162] *Basualto* in: Täuschung und Opferschutzniveau beim Betrug – zwischen Kriminalpolitik und Dogmatik in: Sieber/Dannecker/Kindhäuser/Vogel/Walter (Hrsg.), Strafrecht und Wirtschaftsstrafrecht. Festschrift für Klaus Tiedemann zum 70. Geburtstag, 2008, S. 606.

che Lüge keine Strafbarkeit begründet. Vielmehr bedarf es betrügerischen Kunstgriffen sogenannten *manoeuvres frauduleuses.*[163] Der französische Betrugstatbestand liegt dem Schweizer Betrugstatbestand zugrunde.[164] Dieser fordert jedoch das allgemeinere Merkmal der Arglist und somit ebenfalls eine qualifizierte Täuschungshandlung (Art. 146 chStGB).[165] Alldem zugrunde liegt, wie auch bei den viktimodogmatischen Ansätzen, das Prinzip der Selbstverantwortung.[166] Es wäre aus einer liberalen Perspektive durchaus wünschenswert, wenn auch in Deutschland das Strafrecht restriktiver angewendet werden würde, denn der Schutz für besonders gewichtige Rechtsgüter kann auch anderweitig und ist auch vorrangig durch das Zivil- und Wettbewerbsrecht zu schützen.[167] Dieser Gedanke lässt sich jedoch wie gezeigt, im Hinblick auf das Bestimmtheitsgebot und der Wortlautgrenze des Art. 103 II GG nicht im Rahmen der Gesetzesauslegung lösen, weshalb die Umsetzung nur durch den Gesetzgeber zu lösen ist. Im Hinblick auf das Täuschungsmerkmal bedarf es keiner Anpassung des Betrugstatbestands.[168] Schlussendlich ist der Straftatbestand des Betrugs im Hinblick auf das Täuschungsmerkmal in der Lage, mit diesen neuen, aus der Digitalisierung herrührenden Phänomenen umzugehen und kann somit die Wirklichkeitsbildung vor diesen Einflüssen schützen.

---

[163] LK/*Tiedemann,* vor § 263 Rn. 64 ff.; Selbiges gilt dem Grunde nach auch für Belgien (Art. 496 c.p.), Luxembourg (Art. 496 LuxStGB) und den Niederlanden (Art. 326 WvS).

[164] *Schwarz,* Die Mitverantwortung des Opfers beim Betrug, 2013, S. 32.

[165] Näheres zur Begründung hierfür findet u.a. bei *Schwarz* (Fn. 165) S. 32 ff.; *Hennings* (Fn. 69) S. 163; LK/*Tiedemann,* vor § 263 Rn. 52.

[166] *Basualto* (Fn. 163) S. 607; LK/*Tiedemann,* vor § 263 Rn. 35.

[167] Vgl. *Müller,* Urteilsanmerkung zu BGH, Urt. v. 5.3.2014 – 2 StR 616/12, – Routenplaner, NZWiSt 2014, 387 (395); *Hecker,* Produktwerbung, S. 277.

[168] So auch die Bundesregierung, im Hinblick auf die Frage zu Fake-Bewertungen, auf eine kleine Anfrage der FDP-Fraktion, BT-Drs. 19/16011.

Tamás, Dóra Mária
Ehemalige Studentin, Universität Szeged

DIE ANALYSE VON CYBER-MOBBING MIT DEN METHODEN DES RECHTSVERGLEICHS UND DER TERMINOLOGIELEHRE

I. Einführung[1]

In einer sich ständig verändernden, sich weiterentwickelnden Gesellschaft entstehen immer wieder neue, vom Rechtssystem zu regulierende gesellschaftliche Phänomene. Zu diesen gehört auch das Cyber-Mobbing. Ziel der im Artikel vorgestellten Analyse ist die Erforschung des Begriffs Cyber-Mobbing aus dem Blickwinkel des Rechtsvergleichs und der Terminologielehre und -arbeit. Dabei liegt der Fokus aus der Sicht der Rechtswissenschaften im Besonderen auf den geltenden anzuwendenden Rechtsvorschriften in Ungarn und der Auswertung einiger Rechtsstreitigkeiten und der Klassifizierung der Straftaten, wobei die Untersuchung auch die Aspekte der Terminologielehre und -arbeit umfasst, da es sich auch im Fall von Cyber-Mobbing um einen Rechtsterminus handelt, der mit den Methoden der begrifflichen Äquivalenz erforscht werden kann.

Innerhalb des Strafrechts gehört das Phänomen Cyber-Mobbing zum Bereich der Internetkriminalität. Von den typischen Merkmalen und Herausforderungen der Fälle dieses Gebietes sind Folgende zu erwähnen: *„Vor völlig neue Herausforderungen stellt die Internetkriminalität das Strafrecht, da Täter und Opfer sich häufig in völlig verschiedenen Rechtsräumen aufhalten oder der Geschädigte gar nicht weiß, dass er Opfer einer Straftat geworden ist"*.[2] Es scheint daher erwägenswert zu sein, diese Straftaten nicht nur in einer herkömmlichen Perspektive zu betrachten, und daher auch mit speziellen Mitteln zu interpretieren, zu behandeln, zu regeln und zu bekämpfen.

II. Die Darstellung der Methodik der Doppelanalyse und der Vergleich der zwei Methoden: zwei verschiedenen Seiten der gleichen Münze

Bevor wir uns mit der Analyse der Merkmale des Begriffs und der einzelnen Rechtsvorschriften befassen, lohnt es sich einen Blick auf die Eigenschaften der zwei verschiedenen Analysemethoden zu werfen. Der Rechtsvergleich ist ein Gebiet der Rechtswissenschaften,

[1] Hiermit möchte ich mich bei Ugróczky Mária, Viktor Vadász, Daniel Pöschl und den Dozenten und Lehrkräfte im Netzwerk Ost-West (Universitäten von Szeged und Tübingen), insbesondere Krisztina Karsai, András Lichtenstein und György Attila Németh, für die professionelle Unterstützung bei der Vorbereitung des Artikels bedanken.

[2] *Heike/Funk/Baker,* Einführung in das deutsche Recht und die deutsche Rechtssprache. 5., neubearbeitete Auflage, München, 2013, S. 138.

das sich mit der wissenschaftlichen Aufarbeitung der Rechtsprobleme mit dem Vergleich der verschiedenen nationalen Rechtssysteme, das heißt mit der Anwendung der Vergleichsmethode beschäftigt.[3] Das Gebiet der Terminologielehre verwendet auch Methoden des Vergleichs, und operiert im Fall der Terminologie mit dem Begriffsvergleich, währenddessen die einzelnen in Definitionen auffindbaren Begriffsmerkmale aufgezählt und miteinander verglichen werden, um den Grad der Äquivalenz zwischen den Begriffen feststellen zu können. Im Rechtsvergleich steht die Gegenüberstellung der Normen und Sachverhalte im Mittelpunkt, während in der Terminologielehre- und Praxis eine andere Abstraktionsebene, die Abgrenzung von allgemeinen und unterschiedlichen Merkmalen den Gegenstand der Untersuchungen darstellt. In ihrem Buch zählen[4] die drei klassischen Äquivalenzfälle als Ergebnis eines Begriffsvergleichs auf: vollständige Äquivalenz, Teiläquivalenz und fehlende Äquivalenz. Um einen übersichtlichen Vergleich zu schaffen, wurden die verschiedenen Merkmale in einer Tabelle aufgezeichnet (siehe Tabelle Nr. 1).

Rechtsvergleich	**Terminologielehre und terminologische Arbeitsmethoden im Recht**
Analyse aufgrund der verschiedenen Rechtssysteme mit Erforschung (Untersuchung) der Rechtsfamilien und -gebiete, Makroanalyse genannt[5]	Analyse aufgrund des Fachgebietes/der Domäne auf dem analysierenden Gebiet des Rechts
systematische Analyse von Rechtsinstitutionen, Mikroanalyse genannt[6]	systematische Analyse von Begriffen auf dem speziellen Gebiet des Rechts mit Aufzählung der spezifischen Merkmale und Einordnung der Ergebnisse der Begriffsanalyse in Äquivalenzfälle[7]
ein oder mehrere Rechtssysteme	eine oder mehrere Sprachen und deren Rechtssysteme
oft diachronisch (geschichtliche Prüfung)	im allgemeinen synchronisch (auf die Gegenwart konzentriert)
Wortlaut und Thelos, bzw. Kernbegriff und „Mondhof“ werden analysiert (Szilágyi 2002)	Einstufung des Begriffs in einem gut abgrenzbaren System (Begriffssystem)

Tabelle Nr. 1: Vergleich der verschiedenen Analysemethoden des Rechts und der Terminologielehre.

Der Rechtsvergleich und die Analyse der Äquivalenz tragen dazu bei, dass die verschiedenen Merkmale der Rechtsterminologie zum Vorschein kommen. Das Phänomen der unvollständigen Äquivalenz ist auf den verschiedenen Fachgebieten unterschiedlich vorhanden. *Drewer–Schmitz* stellt fest:[8] *„in den Fachsprachen ist das Phänomen der Teiläquivalenz unterschiedlich ausgeprägt; in der juristischen Fachsprache tritt es z. B.*

[3] *Fekete,* Jogösszehasonlítás, in: Jakab/Fekete (Hrsg.), Internetes Jogtudományi Enciklopédia, 2016, S. 1-8. (https://ijoten.hu/szocikk/jogosszehasonlitas#block-40).

[4] *Drewer/Schmitz,* Terminologiemanagement. Grundlagen, Methode, Werkzeuge, Berlin, 2017, S. 20-22.

[5] *Chiocchetti,* Legal Comparison in Terminology Work: Developing the South Tyrolian German Legal Language, in: Szoták (Hrsg.), Diszciplínák találkozása – nyelvi közvetítés a XXI. században/The Meeting of Disciplines: Language Mediation in the 21st Century, Budapest, 2019, S. 175-185. (https://150.offi.hu/kiadvanyok/diszciplinak-talalkozasa-nyelvi-kozvetites-21-szazadban).

[6] Ibid.

[7] *Tamás,* Bevezetés a jogi terminológiába a terminológus szemüvegén át. Második, átdolgozott kiadás, Budapest, 2019, S. 15-25.

[8] *Drewer/Schmitz* (Fn. 4) S. 34.

wegen der unterschiedlichen Rechtssysteme in verschiedenen Ländern deutlich häufiger auf als in anderen Fachsprachen (wie z. B. in der Informationstechnologie)".

Unter dem Aspekt der Terminologielehre weist die Rechtsterminologie weitere spezifische Eigenschaften auf, wie z. B.:[9]

- Zeitmäßigkeit wegen der sich ständig weiterentwickelnden Gesellschaft und neuen Phänomenen;
- starke Verbalität der Rechtsbegriffe wegen ihrer abstrakten Natur, oft ohne materielle Realität im Gegensatz zum Gebiet der Technik;
- Flexibilität in der Interpretation der Rechtsvorschriften neben dem Wortlaut um neue Erscheinungen deuten zu können;
- Systemgebundenheit (siehe Rechtsfamilie, -gebiet und -vorschrift).

Diese Eigenschaften beeinflussen auch die Ergebnisse einer Analyse, da Rechtsbegriffe abstrakter und schwieriger untereinander abgegrenzt werden können, als zum Beispiel im Fall der Technik. Die Aktualität spielt wegen der immer neuen Erscheinungen auch eine große Rolle.

Ein Vorteil im Fall eines Vergleichs von Rechtsvorschriften und Rechtsfällen zwischen dem ungarischen und dem deutschen Rechtssystem ist, dass beide zur gleichen, der sogenannten kontinentalen Rechtsfamilie gehören (siehe Makroanalyse), wobei das deutsche Rechtssystem traditionell ein Muster für das ungarische Rechtssystem darstellt. Ein Rechtsvergleich wird auch durch die Tatsache erschwert, dass im Fall einer neuen gesellschaftlichen Erscheinung oft Rechtslücken vorhanden sind, und der direkte Vergleich zwischen Rechtsinstitutionen deshalb nicht möglich ist (siehe Mikrovergleich), da ein größeres Umfeld zu erforschen ist. Zu einem Rechtsvergleich müssen auch Daten der deutschen Rechtsvorschriften und Rechtsfälle vorhanden sein, aber in diesem Artikel stehen die ungarischen Normen und Streitigkeiten im Vordergrund, während ein Rechtsvergleich in abgekürzter Form am Ende des Artikels auffindbar ist. Die Erscheinung des Cyber-Mobbings wird demgemäß in den folgenden Punkten analysiert.

III. Die Analyse von Cyber-Mobbing als Begriff

Im Internet sind verschiedene Definitionen des Cyber-Mobbings auffindbar. Unseren Ausgangspunkt stellen in deutscher und in ungarischer Sprache auffindbare Definitionen dar, wobei darauf zu achten ist, dass die Texte möglichst aus vertrauenswürdigen Quellen stammen und die Hauptmerkmale umfassend beschreiben. Für die deutsche Definition habe ich die Begriffsbestimmung auf der Website www.klicksafe.de gewählt, die innerhalb der Initiative „klicksafe" im CEF (Connecting Europe Facility) Telecom Programm der Europäischen Union für mehr Sicherheit im Internet erstellt wurde:

> „Unter Cyber-Mobbing (Synonym zu Cyber-Bullying) versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mithilfe von Internet- und Mobiltelefondiensten über einen längeren Zeitraum hinweg. Der Täter – auch „Bully" genannt – sucht sich ein Opfer, das sich nicht oder nur

[9] *Tamás,* Miért rögzítsünk jogi szakszavakat terminológiai adatbázisokban? Magyar Jogi Nyelv 2/2018, S. 30-32. (https://joginyelv.hu/beszamolo-a-jog-es-terminologia-cimu-konferenciarol/).

> schwer gegen die Übergriffe zur Wehr setzen kann. Zwischen Täter und Opfer besteht somit ein Machtungleichgewicht, welches der Täter ausnutzt, während das Opfer sozial isoliert wird.
> Cyber-Mobbing findet im Internet (bspw. in Sozialen Netzwerken, in Video-Portalen) und über Smartphones (bspw. durch Instant-Messaging-Anwendungen wie WhatsApp, lästige Anrufe etc.) statt. Oft handelt der Bully anonym, sodass das Opfer nicht weiß, von wem genau die Angriffe stammen. Gerade bei Cyber-Mobbing unter Kindern und Jugendlichen kennen Opfer und TäterInnen einander aber meist aus dem „realen" persönlichen Umfeld wie z. B. der Schule, dem Wohnviertel, dem Dorf oder der ethnischen Community. Die Opfer haben deshalb fast immer einen Verdacht, wer hinter den Attacken stecken könnte".[10]

Im Fall der ungarischen Definition habe ich mich auf die auf der Website der Unicef verfügbare Version gestützt:

> „Was ist Cybermobbing?
> Drei Faktoren unterscheiden das Mobbing von einmaligen Beschimpfungen oder anderen Konfliktsituationen. Erstens hat es eine starke, negative Auswirkung, wenn das Mobbing-Opfer sein alltägliches Leben wegen den Handlungen des Belästigers nicht leben kann – zum Beispiel, weil es ständig in Angst oder Unsicherheit lebt. Andererseits wiederholt sich das Mobbing, wenn auch nicht in regelmäßigen Abständen, der Täter kehrt regelmäßig zum Opfer zurück und wiederholt seine Handlungen, sei es körperlich, verbal oder sexuell. Das dritte Kriterium ist die Verschiebung der Machtverhältnisse: Der Täter verfügt immer über mehr Macht (er hat mehr Geld, ist stärker, hat mehr Freunde, ist lauter) und stellt diese Macht während des Mobbings zur Schau. Mobbing (bullying) kann zu Hause, in der Schule oder in anderen Gemeinschaften passieren, aber mit der Verbreitung des Internets ist auch das Cyber-Mobbing ein Teil des Alltags geworden. Auch beim Cyber-Mobbing kommen die drei Bedingungen zum Tragen: der Mobber vermittelt dem Gemobbten starke, negative Inhalte, wiederholt die Aktivität regelmäßig und erreicht dies durch Machtausübung. Im Internet geschieht dies oft durch das anonyme Posten von beleidigenden Kommentaren in sozialen Netzwerken oder durch das Teilen eines wenig schmeichelhaften Fotos oder eventuell einer Fotomontage der missbrauchten Person".[11]

Die gemeinsamen Begriffsmerkmale der obigen Definitionen sind folgende:

- Belästigung,
- Gefühl der Bedrohung und Furcht,
- längerer Zeitraum und Regelmäßigkeit,
- Machtungleichgewicht zwischen Täter und Opfer,
- Internet- und Mobiltelefondienste als Mittel,
- oft anonym,
- häufige Orte: Schule oder Wohnviertel,
- häufige Täter und Opfer: Kinder und Jugendliche.

[10] https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/cyber-mobbing-was-ist-das/

[11] https://unicef.hu/cyberbullying (Übersetzung aus dem Ungarischen).

Aufgrund der obigen Definitionen kann Cyber-Mobbing als eine Art andauernde Bedrohung und Furcht verursachende Belästigung angesehen werden, die während eines längeren Zeitraums regelmäßig unter Verwendung von Internet- und Mobiltelefondiensten als Mittel und oft anonym ausgeübt wird, wobei ein Machtungleichgewicht zwischen Täter und Opfer besteht, und am häufigsten in der Schule oder im Wohnviertel unter Kindern und Jugendlichen vorkommt.

Aufgrund der Begriffsanalyse der Terminologielehre ist zwischen dem deutschen Terminus Cyber-Mobbing und dem ungarischen Terminus *online zaklatás* eine vollständige Äquivalenz festzustellen, wobei der Begriff in beiden Definitionen die gleichen Hauptmerkmale aufweist. Die Terminologie verfügen in beiden Sprachen über Synonyme: in der deutschen Sprache wird neben „Cyber-Mobbing" noch „Cyber-Bullying" verwendet, während auf Ungarisch noch *internetes zaklatás, cyberbullying, kiberbulling, internetes megfélelmítés* oder *cyber-megfélelmítés* vorkommen.

Falls wir noch in anderen Quellen nachforschen, z. B. in der juristischen Fachliteratur, dann können wir weitere Merkmale und Einstufungen auffinden. Im Fachbuch mit dem Titel *„Közjogi fogalmakról közérthetően" (Öffentlich-rechtliche Begriffe im Klartext)*[12] wird Cyber-Mobbing unter Belästigung aufgezählt, das einen *„Verstoß gegen die Gleichbehandlungsklausel"* darstellt.[13] Die anderen aufgeführten Merkmale sind die Einschüchterung und Demütigung des Opfers, wobei der Vorsatz keine Erwartung in dieser Auflistung darstellt. Im Buch werden als Subtypen von Belästigung Cyber-Bullying, Belästigung in der Schule, sexuelle Belästigung und Belästigung am Arbeitsplatz erwähnt. Der Text macht im Fall von Cyber-Bullying auf die Vielfalt der Modi Operandi aufmerksam, z.B. zählen Textnachrichten mit anstößigem Inhalt und das Erstellen eines gefälschten Profilbildes auf einer sozialen Netzwerkseite auch dazu. Es besteht in Ungarn die Möglichkeit, sich in konkreten Fällen bei Verhalten, die die Menschenwürde verletzen, an einer Behörde zu wenden (früher an die Behörde für Gleichbehandlung, auf Ungarisch *„Egyenlő Bánásmód Hatóság"*), heute an das Büro des Kommissars für Grundrechte, Generaldirektion für Gleichbehandlung, auf Ungarisch „Alapvető Jogok Biztosának Hivatala, Egyenlő Bánásmódért Felelős Főigazgatóság"). Auch bei *Monori*[14] wird Cyber-Mobbing als eine Art der Belästigung diskutiert und als eine Devianz des Verhaltens im Internet erwähnt. Die Autoren zählen zahlreiche Untertypen auf, wie: das *Flaming* (z. B. Streit durch Beiträge in Online-Community-Foren), das *Harassment* (Online-Versendung verletzender, unwahrer Nachrichten), die *Denignation* (das Versenden, Posten oder Verbreiten von Gerüchten, Klatsch oder Gerüchten, die geeignet sind, den Ruf einer Person zu schädigen), die *Exclusion* (der Ausschluss von jemandem aus einer Online-Gruppe), die *Impersonation* (Identitätsdiebstahl, bei dem der Täter auf dem Online-Profil einer anderen existierenden Person erscheint und in deren Namen Nachrichten versendet, um deren Ruf zu schädigen), das *Outing* (Klatsch, Geheimnisse, unbefugte Weitergabe von persönlichen Informationen)

---

[12] *Márki/Szaniszló* (Hrsg.), Közjogi fogalmak közérthetően, Szeged, 2020, S. 410-411

[13] siehe Gesetz Nr. CXXV aus dem Jahr 2003 zur Gleichbehandlung und zur Förderung der Chancengleichheit (dieses Gesetz definiert den Begriff Belästigung unter § 10, aber es handelt sich hier nicht um eine strafrechtliche Rechtsform).

[14] *Monori,* Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái, In Medias Res 2/2016, S. 246-261.

und das *Sexting* (Veröffentlichung von sexuell aufreizenden und selbst provozierten Nacktbildern oder Nachrichten mit sexuellem Inhalt im Internet).

Pongó[15] hebt hervor, dass in der konservativen Rechtsschule *„die Absichtlichkeit (der Vorsatz), die Regelmäßigkeit und das Machtungleichgewicht"* die Grundmerkmale des Bullyings seien und nicht alle der Meinung sind, dass die neuen gesellschaftlichen Erscheinungen mit speziellen Mitteln behandelt werden müssen. Aufgrund seiner Forschungen in der wissenschaftlichen Fachliteratur akzeptiert *Pongó*[16] die folgende Definition: „Ein vorsätzliches und wiederholtes Verhalten, das durch ein elektronisches Gerät verwirklicht wird, um dem Opfer Schaden oder Verletzungen zuzufügen und darauf ausgerichtet ist, das Machtgleichgewicht zwischen Täter und Opfer zu stören".[17] Nach der Erforschung der Praxis, das heißt der Rechtsquellen und der Rechtsprechungspraxis, modifiziert und erweitert *Pongó*[18] seine Definition, die auch im zweiten Teil konkrete Vorschläge zu einer Regelung beinhaltet, was eigentlich untypisch für eine klassische Definition ist, aber folgenderweise:

> „Ein vorsätzliches, einmaliges oder wiederholtes Verhalten, das von oder zum Nachteil eines Schülers oder Schulangestellten durch ein elektronisches Gerät begangen wird, und das darauf abzielt, ein Machtungleichgewicht zu schaffen und irgendeinen der folgenden Tatbestände verwirklicht:
> (a) eine Verletzung der körperlichen oder seelischen Gesundheit oder Sachbeschädigung oder die Wahrscheinlichkeit des Eintretens eines dieser Ereignisse aufgrund der Umstände; oder
> (b) die Schaffung eines feindlichen erzieherischen Umfelds oder Entzug der Dienstleistungen, Vorteile und Möglichkeiten, die die Schule bietet.
> Die Schule hat die Befugnis, die Meinungsäußerung eines Schülers einzuschränken:
> (a) in der Schule, während der Schulzeit;
> b) bei Veranstaltungen oder Programmen, die von der Schule beaufsichtigt, finanziell unterstützt oder organisiert werden;
> c) im Fall der außerschulischen Meinungsäußerung mit elektronischen Mitteln, wenn eine ausreichende Verbindung zwischen der jeweiligen Meinungsäußerung und der Schuleinrichtung besteht und die Meinungsäußerung zu einer erheblichen Störung des Schulklimas führt."[19]

Diese zweite Version grenzt bei *Pongó*[20] das Phänomen in seiner Definition auf Kinder und Jugendliche ein. Im Gegensatz zu *Márki–Szaniszló*[21] ist auch hier, wie in der konserva-

---

[15] *Pongó*, A cyber-megfélemlítés és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére, Dissertation, Szegedi Tudományegyetem, Állam- és Jogtudományi Kar, 2017. (http://doktori.bibl.u-szeged.hu/id/eprint/4068/), S. 27.

[16] *Pongó* (Fn. 15) S. 34.

[17] Übersetzt aus dem Ungarischen, siehe: „Egy elektronikus eszköz által megvalósuló, szándékos és ismétlődő magatartás, amely kárt vagy sérülést okoz az áldozatnak, s célja az erőegyensúly felborítása az elkövető és az áldozat között"

[18] *Pongó* (Fn. 15) S. 23.

[19] Übersetzt aus dem Ungarischen.

[20] ibid.

[21] *Márki/Szaniszló* (Fn. 12) S. 410-411.

tiven Rechtsschule, der Vorsatz als einer der wichtigsten Merkmale aufzufinden. *Pongó*[22] weist auch darauf hin, dass die Vielfalt und Unterschiedlichkeit der Fälle, die fehlende einheitliche Rechtsauslegung oder mangelnde Rechtsprechungshinweise zu einer unvorhersehbaren, widersprüchlichen Anwendung der gültigen Gesetze führen.

III. 1. Die im Fall von Cyber-Mobbing anwendbaren ungarischen Rechtsvorschriften

Da die Rechtsvorschriften schon im Allgemeinen erwähnt worden sind, prüfen wir jetzt welche Rechtsvorschriften im ungarischen Rechtssystem in einem Fall von Cyber-Mobbing vor dem Gericht angewandt werden können. Vor allen werden wir uns auf das ungarische Strafgesetzbuch fokussieren, obwohl auch das ungarische Bürgerliche Gesetzbuch den Schutz des guten Rufes behandelt.[23]

Im ungarischen StGB ist kein sich ausdrücklich mit Cyber-Mobbing beschäftigender Tatbestand aufzufinden, aber die Rufschädigung ist seit 2013 Teil des Kodex.[24] Diese Tatbestände beschäftigen sich mit dem Anfertigen bzw. der Veröffentlichung von falschen Ton- oder Bildaufnahmen, die geeignet sind, die Ehre von Personen zu verletzen. Doch als der ähnlichste Begriff kann die Belästigung[25] im ungarischen StGB (nachstehend als uStGB) angesehen werden, der aber die elektronische Variante unerwähnt lässt:

> „§ 222 (1) Wer in der Absicht, einen anderen einzuschüchtern oder willkürlich in das Privatleben oder den Alltag eines anderen einzugreifen, diesen regelmäßig oder beharrlich belästigt, wird wegen einer Ordnungswidrigkeit mit Freiheitsstrafe bis zu einem Jahr bestraft, wenn nicht eine schwerere Tat vorliegt.
> (2) Jede Person, die zum Zweck der Erzeugung von Angst
> (a) eine andere Person oder einen Verwandten einer anderen Person mit der Begehung einer Straftat bedroht, die Gewalt oder öffentliche Gefahr gegen eine Person beinhaltet, oder
> (b) den Eindruck erweckt, dass ein Ereignis eintreten wird, das das Leben, die körperliche Unversehrtheit oder die Gesundheit einer anderen Person verletzt oder unmittelbar gefährdet,
> wird als Ordnungswidrigkeit mit einer Freiheitsstrafe im Höchstmaß von bis zu zwei Jahren bestraft.
> (3) Jede Person, die durch Belästigung.
> a) zur Verletzung seines Ehegatten, früheren Ehegatten, Lebenspartners oder früheren Lebenspartners,
> b) zum Nachteil einer Person, die unter seiner Erziehung, Aufsicht, Pflege oder Behandlung steht,

---

[22] *Pongó* (Fn. 15)

[23] siehe § 6:373 Ptk. *A jóhírnév megóvása*.

[24] siehe § 226/A Btk. *Becsület csorbítására alkalmas hamis hang- vagy képfelvétel készítése – Anfertigung von zur Herabwürdigung in der öffentlichen Meinung geeigneten Ton- oder Bildaufnahme* mit einer Freiheitsstrafe bis zu einem Jahr zu bestrafen, bzw. § 226/B Btk. *Becsület csorbítására alkalmas hamis hang- vagy képfelvétel nyilvánosságra hozatala – Veröffentlichung einer zur Herabwürdigung in der öffentlichen Meinung geeigneten Ton- oder Bildaufnahme* mit einer Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

[25] siehe § 222 uStGB *Zaklatás – Belästigung*.

(c) seine Macht- oder Einflussposition missbraucht; oder
(d) Verursachung einer Verletzung eines Amtsträgers an einem Ort oder zu einer Zeit, die mit der Ausübung seines Amtes nicht vereinbar ist wird in dem in Absatz 1 vorgesehenen Fall mit Freiheitsstrafe bis zu zwei Jahren und in dem in Absatz 2 vorgesehenen Fall mit Freiheitsstrafe bis zu drei Jahren bestraft."

Weitere Vorschriften im uStGB, die ähnliche Sachverhalte beinhalten, sind: die Beleidigung,[26] die Verleumdung,[27] die Verletzung des Briefgeheimnisses,[28] die Erpressung[29] und der verbotene Datenzugriff.[30]

Die aufgezählten und im Bereich von Cyber-Mobbing anwendbaren Rechtsvorschriften belegen die von *Pongó*[31] erwähnte Vielfalt der Fälle. Es kann auch vorkommen, dass die Rechtsanwendenden auch weitere Rechtsvorschriften miteinbeziehen müssen, z. B. Beihilfe zum Selbstmord.[32] Auch die Arten der verhängbaren Strafen variieren je nach Schweregrad und Alter des Täters. Die Sanktionen für Jugendlichen als Täter werden im uStGB in den §§ 109–126 geregelt. Im Allgemeinen werden Kinder unter 14 Jahren nicht bestraft, obwohl der § 14 *(Das Kindesalter)*[33] des uStGB auch Ausnahmen aufweist (siehe z.B. Mord, Körperverletzung, Terroranschlag, Raubüberfall), aber die mit Cyber-Mobbing verwandten Fälle werden hier nicht aufgezählt.

Unter den Maßnahmen kann auch ein Hinweis auf den Umgang mit elektronischen Daten aufgefunden werden. In § 63 Absatz 1 Buchstabe g) des uStGB steht: *„die endgültige Zugriffssperre elektronischer Daten",*[34] wobei dies in § 77 detailliert geregelt wird. Demgemäß können Minderjährige nicht bestraft werden, trotzdem werden die elektronischen Daten endgültig unzugänglich gemacht.

III. 2. Der Vergleich der Klassifikation von Rechtsfällen in Ungarn mit Cyber-Mobbing

Es lohnt sich einen Blick auf einige konkrete Rechtsstreitigkeiten zu werfen, da das Richterrecht oft die Funktion der Schließung von Lücken des kodifizierten Rechts erfüllt. In einer sich im schnellen Tempo weiterentwickelnden technologischen Welt und und infolge der dadurch neu erscheinenden gesellschaftlichen Phänomene ist der Gesetzgeber nicht immer in der Lage, jeden Sachverhalt vorauszusehen und ihn zu regeln. Wegen den mangelnden

---

[26] siehe § 227 uStGB *Becsületsértés* mit einer Freiheitsstrafe bis zu einem Jahr bestraft.

[27] siehe § 226 uStGB *Rágalmazás* mit einer Freiheitsstrafe von einem bis zu zwei Jahren zu bestrafen.

[28] siehe § 224 uStGB *Levéltitok megsértése* mit einer Freiheitsstrafe von einem bis zu zwei Jahren zu bestrafen.

[29] siehe § 367 uStGB *Zsarolás* mit einer Freiheitsstrafe von einem bis zu fünf oder mit einer Freiheitsstrafe von zwei bis zu acht Jahren zu bestrafen.

[30] siehe § 422 uStGB *Tiltott adatszerzés* wegen Verbrechen mit einer Freiheitsstrafe bis zu drei Jahren bzw. einer Freiheitsstrafe von ein bis zu fünf Jahren zu bestrafen.

[31] *Pongó* (Fn. 15)

[32] siehe § 162 uStGB. *Öngyilkosságban közreműködés* wegen Verbrechen mit einer Freiheitsstrafe von einem bis zu fünf Jahren zu bestrafen.

[33] *A gyermekkor*.

[34] az elektronikus adat végleges hozzáférhetetlenné tétele.

Rechtsvorschriften kommt es vor, dass Fälle mit gleichem Sachverhalt unterschiedliche Klassifikationen erhalten (unterschiedlich bewertet werden). Um dies zu untersuchen, können die abgeschlossenen Rechtstreitigkeiten analysiert werden.

Zum obigen Zweck wurden die im Online-Register des ungarischen Gerichts[35] auffindbaren anonymisierten Urteile untersucht und in einer Übersichtstabelle zusammengefasst (siehe Tabelle Nr. 2). Die kurz vorgestellten Fälle weisen verschiedene Grundsituationen (ehemaliges Ehepaar, Politiker, Drogensüchtiger) und Klassifikationen (Belästigung, Verleumdung und Nötigung) auf, die Straftaten wurden oft mit anderen Straftaten gemeinsam begangen, sind mit verschiedenen Telekommunikationsmitteln verbunden (Textnachrichten, E-Mails, Posts auf sozialen Netzwerken, Videos) und die Strafe geht von Verweis bis zur Freiheitsstrafe.

Gerichts-aktenzeichnen	*Gericht*	*Jahr der Verkündung des Urteils*	*Klassifizierung der Straftat*	*Kurze Beschreibung des Falles*
B.1026/2015/31	Győri Járásbíróság (Amtsgericht Győr)	2017	Beziehungsgewalt (kapcsolati erőszak bűntettében, Btk.212/A.§ (1) bekezdés, (2) bekezdés a) pont); Belästigung (zaklatás vétsége, Btk.222.§ (1) bekezdés, (3) bekezdés a) pont);	Strafe: 2 Jahre Probezeit; Mittel: Textnachricht, E-Mail, soziales Netzwerk (Facebook) zwischen früheren Ehegatten
Nr. 15.B.429/2017/10	Nyíregyházi Járásbíróság (Amtsgericht Nyíregyháza)	2017	Verleumdung (becsületsértés Btk. 227.§ (1). bek. a, b, pontja)	Strafe: Verweis (megrovás); Mittel: Video im Internet; eine Rede von einer politischen Pressekonferenz wird ins Internet gestellt, in der jemand beschuldigt wird, ein Lügner zu sein
6.B.620/2015/76	Nyíregyházi Törvényszék (Landgericht Nyíregyháza)	2018	Rauschgifthandelsdelikte (kábítószerkereskedelem bűntette, Btk. 176. § (1), társtettesként elkövetett kábítószer-birtoklás bűntette, Btk.178.§ (1) bekezdés I. fordulat, (2) bekezdés b) pont], zwei Anklagen wegen versuchter Nötigung in einem amtlichen Verfahren (2 rendbeli kényszerítés hatósági eljárásban bűntette kísérletében [Btk.278.§ (1) bekezdés, (2) bekezdés I. fordulata]	Strafe: 3 (drei) Jahre Freiheitsstrafe und 3 (drei) Jahre Ausschluss von öffentlichen Ämtern als Nebenstrafe; Mittel: Veröffentlichung eines Videos von Geschlechtsverkehr

Tabelle Nr. 2: Übersicht über einige Fälle, die mit einer Form von Cyber-Mobbing zu tun haben.

[35] siehe https://eakta.birosag.hu/anonimizalt-hatarozatok.

IV. Die Ergebnisse der Vergleichsanalyse aus dem Blickwinkel des Rechtsvergleichs und der Terminologielehre und -arbeit

Der Begriff von Cyber-Mobbing wurde unter dem Aspekt der Terminologielehre mit dem Vergleich von Definitionen der Grundbegriffe aus vertrauenswürdigen Quellen analysiert. In der Begriffsanalyse sind die Hauptmerkmale aufgezählt worden, wobei festgestellt werden konnte, dass der Begriff Cyber-Mobbing eine vollständige Äquivalenz mit dem ungarischen Begriff *online zaklatás* aufweist. In der Fachliteratur wird Cyber-Mobbing unter Belästigung behandelt *(Monori,*[36] *Márki–Szaniszló*[37]*),* bei *Pongó*[38] auf den Bereich der Schule eingegrenzt. Bei *Márki–Szaniszló*[39] wird der Vorsatz nicht als Hauptmerkmal und Bedingung erwähnt. Die Analyse der Rechtsinstitutionen in den ungarischen und deutschen Rechtssystemen war nicht der Hauptgegenstand des Artikels (obwohl die Zusammenfassung der Ergebnisse eines Rechtsvergleichs am Ende des Artikels auffindbar ist). Eine Analyse war auch von der Tatsache erschwert, dass dieses Phänomen nicht eindeutig und separat in Rechtsvorschriften behandelt wird und daher eine Forschung auf weiterer Ebene benötigt. Diese weiteren Untersuchungen wurden in den ungarischen Rechtsvorschriften und Rechtsfällen weitergeführt.

Die Aufzählung der im Zusammenhang mit Cyber-Mobbing verwendbaren Rechtsvorschriften und die folgende Auswertung von Rechtstreitfällen in Ungarn hat die Vielfalt in den Fällen und Klassifizierungen belegt. Es kommt auch vor, das Cyber-Mobbing nur eine Nebenerscheinung im Urteil ist.

Eine Einordnung der Begriffe ermöglicht im Bereich der Terminologielehre und -arbeit die Anwendung von ontologischen Mitteln, die eine Aufzeichnung der Relationen unter den Terminologien ermöglichen. Die ontologischen Elemente sind besonders nützlich, weil deren erfolgreiche Anwendung auf der Erkenntnis beruht, dass der Erwerb von Wissen nicht ausreicht:[40] *„Wir können unser Wissen nur dann in der Praxis anwenden, wenn wir die Beziehungen zwischen den verschiedenen Elementen kennen und in der Lage sind, sie zu beschreiben"*.[41] Die Möglichkeiten der Anwendung der Ontologie im Bereich der Terminologiearbeit wird in der Norm ISO 1087-1:2000[42] geregelt, in dem die folgenden als die beiden Hauptzweige der ontologischen Elemente identifiziert werden:

- hierarchisch (Unter- und Überordnung, Teil-Ganzes-Verhältnis) und
- assoziativ (z. B. zeitliche, kausale Beziehungen).

Im Fall einer Darstellung der Begriffsbeziehungen von Cyber-Mobbing (siehe Abbildung Nr. 1.) kann die Belästigung als Oberbegriff interpretiert werden, wobei die in den Rechtsvorschriften auffindbaren Begriffe assoziative Relationen aufweisen können, aber

---

[36] *Monori* (Fn. 14) S. 246-261.

[37] *Márki/Szaniszló* (Fn. 12) S. 410-411.

[38] *Pongó* (Fn. 15)

[39] *Márki/Szaniszló* (Fn. 12) S. 410-411.

[40] *Fóris,* Network Theory and Terminology, Knowledge Organization (International Journal) 6/2013, S. 422-429

[41] übersetzt aus den Englischen: „Concepts do not exist as isolated units of knowledge but always in relation to each other".

[42] Terminology work – Vocabulary – Part 1: Theory and application.

diese Einstufung kann nicht als vollständig angesehen werden, da diese Kategorien zu weiteren Folgen führen können (siehe Beihilfe zum Selbstmord).

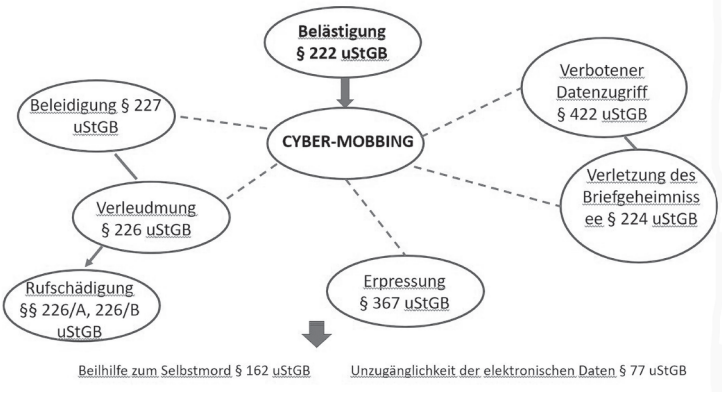

Abbildung Nr. 1.: Die ontologische Abbildung der Begriffsbeziehungen von Cyber-Mobbing.

Wie auch in der Vergangenheit, so werden auch in der Zukunft immer wieder neue gesellschaftliche Phänomene erscheinen, die eine genaue Beschreibung und Einordnung unter dem Aspekt der Terminologielehre und -arbeit und eine Interpretierung, Regelung und Behandlungsweise unter dem Aspekt des Rechts benötigen. Das Ziel dieser Studie konnte keine vollständige Analyse des Phänomens sein, sondern vielmehr nur ein Beispiel, um vorzustellen, welche Möglichkeiten die Untersuchung einer Neuerscheinung im Bereich der Terminologielehre und -arbeit und des Rechts bergen können.

V. Die kurze Zusammenfassung des Rechtsvergleichs von deutschen und ungarischen Rechtsvorschriften und Tatbeständen[43]

Es gibt im Fall von Cyber-Mobbing viele Ähnlichkeiten zwischen den beiden Rechtssystemen, vor allem wird dieses Phänomen in ungarischen und deutschen Rechtsvorschriften nicht eindeutig und separat behandelt. Hiermit werden nur die wichtigsten, aus der Analyse festgestellten Ergebnisse dargelegt.

Dem ungarischen Tatbestand Belästigung (§ 222 uStGB) steht die Nachstellung (§ 283 StGB) am nächsten, wobei als Gemeinsamkeiten die schwerwiegende Beeinträchtigung für Lebensgestaltung und die Bedrohung über Verletzung von Angehörigen erwähnt werden können. Unterschiede findet man im Hinweis auf die Verwendung von Telekommunikationsmitteln, da diese in der deutschen Norm auffindbar, während in der ungarischen Version nicht angegeben sind. Ein weiterer Unterschied ist, dass in der ungarischen Vorschrift das Adjektiv „regelmäßig“ und in der deutschen Variante „beharrlich“ angegeben wird. Diese letzte erwähnt auch die personenbezogenen Daten. Die Länge der Freiheitsstrafe ist auch verschieden, in Deutschland wird die tat mit 3 Jahren Freiheitstrafe bestraft, während in Ungarn in schwereren Fällen die Strafe 1 Jahr Freiheitsstrafe beträgt, ansonsten wird die Tat als Ordnungswidrigkeit eingestuft.

[43] Der Rechtsvergleich wurde mit Emma Erna Ebeling im Rahmen des Austauschsseminars des Netzwerks Ost-West zusammen ausgearbeitet.

Weitere deutsche Tatbestände wie § 185 Beleidigung StGB, § 186 Üble Nachrede StGB, § 187 Verleumdung StGB können mit den ungarischen § 227 Beleidung uStGB, 226 Verleumdung uStGB (Rufbeschädigung §§ 226a, 226b StGB) verglichen werden. Unter den gemeinsamen Merkmalen können die Aufzählung der Öffentlichkeit, von falschen Aussagen, die Rufschädigung des Ansehens der Person und die Freiheitsstrafe erwähnt werden. Abgesehen von der unterschiedlichen Zahl der Tatbestände ist in der ungarischen Rechtsvorschrift explizit die Begehung durch Audio, Video, Bild enthalten, während die deutsche Norm eine strengere Freiheitsstrafe vorschreibt.

Der deutsche Tatbestand § 240 Nötigung StGB (§ 253 Erpressung StGB) und der ungarische Tatbestand § 367 Erpressung uStGB weisen vor allem gemeinsame Inhalte auf wie Drohung, Motivationen, die den Täter zum Handeln, Dulden oder Unterlassen bringen und die Freiheitsstrafe.

Im Bereich vom verbotenen Datenzugriff können die folgenden Tatbestände miteinander verglichen werden: der § 202a Ausspähen von Daten im StGB mit dem § 423 Verletzung von Informationssystemen oder Daten im uStGB, der § 202b Abfangen von Daten im StGB mit dem § 422 Verbotenen Datenerwerb im uStGB, der § 202c Vorbereiten des Ausspähens und Abfangens von Daten im StGB mit dem § 424 Ausspielen der technischen Maßnahmen zum Schutz von Informationssystemen.

Der Tatbestand der Selbsttötung kann noch als eine fernere Folge in der Analyse miteinbezogen werden. In Deutschland ist der Suizid als mittelbare Täterschaft qualifiziert, während die Beihilfe zur Selbsttötung straflos ist. In Ungarn ist die Beihilfe zur Selbsttötung unter § 162 uStGB mit Freiheitsstrafe zu bestrafen.

Als Ergebnis des Rechtsvergleichs kann man auf wesentliche Rechtslücken hinweisen, wie die Unvollständigkeit bezüglich der vorhandenen digitalen Aspekte im Falls des ungarischen Tatbestandes Belästigung, § 222 uStGB und im Fall der deutschen Rechtsvorschriften bei Beleidigung: §§ 185 ff StGB. Einen Überblick über die ähnlichen Tatbestände verschafft die Abbildung Nr. 2. Die Neuerscheinung von Cyber-Mobbing ist mit der Belästigung § 222 uStGB und der Nachtstellung § 283 StGB am engsten verknüpft, während die anderen Tatbestände eher verschiedene Aspekte der Erscheinung abdecken.

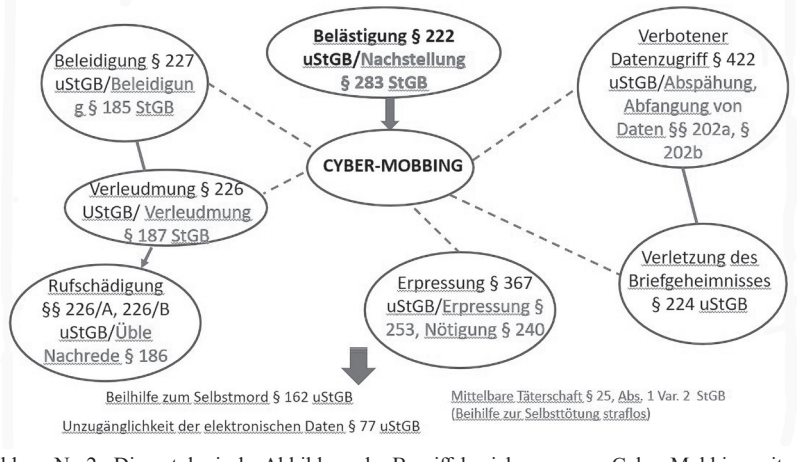

Abbildung Nr. 2.: Die ontologische Abbildung der Begriffsbeziehungen von Cyber-Mobbing mit einem Vergleich von ungarischen und deutschen Tatbeständen ergänzt.

Lectiones Iuridicae

Series Editor
Elemér Balogh
Professor

1. *Az Alkotmánybíróság és a rendes bíróságok – 20 év tapasztalatai*. Szeged, 2011.
2. *Kérdőív az alkotmányozásról*. Szeged, 2011.
3. *A szerződés interdiszciplináris megközelítésben*. Szeged, 2012.
4. *Az államok nemzetközi jogi felelőssége – tíz év után. In memoriam Nagy Károly (1932–2001)*. Szeged, 2013.
5. *A jó állam aspektusai, perspektívái. Az önkormányzatok változó gazdasági, jogi környezete*. Szeged, 2012.
6. *Das neue ungarische Grundgesetz*. Szeged, 2012.
7. *Opuscula Szegediensia 5. A Munkajogi és Szociális Jogi Doktoranduszok és Pályakezdő Oktatók ötödik konferenciája*. Szeged, 2013.
8. *Az alapjogvédelem nemzeti, nemzetközi és jogösszehasonlító aspektusai*. Szeged, 2013.
9. A *mi Alapvetésünk. A Szegedi Tudományegyetem Állam – és Jogtudományi Kara alkotmányjogi tudományos diákkörének tanulmányai az Alaptörvény Alapvetéséhez.* Szeged, 2014.
10. *Geistiges Eigentum und Urheberrecht aus der historischen Perspektive*. Szeged, 2013.
11. *Opuscula Szegediensia 6. A Munkajogi és Szociális Jogi Doktoranduszok és Pályakezdő Oktatók hatodik konferenciája*. Szeged, 2014.
12. *Jogvédelmi kaleidoszkóp. A jogvédelem elmúlt öt éve (2009–2014) Magyarországon*. Szeged, 2015.
13. *Fundamental Rights in Austria and Hungary. Research Seminar*. Szeged, 2015.
14. *A történeti alkotmánytól az Alaptörvényig*. Szeged, 2015.
15. *Jogalkotás és kodifikátorok. Vladár Gábor emlékülés*. Szeged, 2016.
16. *Alapjogok diákszemmel. A Szegedi Tudományegyetem Állam- és Jogtudományi Kara alkotmányjogi tudományos diákkörének tanulmányai egyes alapjogok magyar és nemzetközi vonatkozásairól*. Szeged, 2016.
17. *Húsz év mérlegen. Közbeszerzésünk múltja, jelene és jövője*. Szeged, 2017.
18. *A modern állam 21. századi közjogi kihívásai. Az állami funkciók változásai az európai integrációban.* Szeged, 2017.
19. *Recent Challenges of Public Administration. Papers Presented at the Conference of 'Contemporary Issues of Public Administration'*. Szeged, 2017.
20. *Recent Challenges of Public Administration 2. Papers Presented at the Conference of '2nd Contemporary Issues of Public Administration'*. Szeged, 2018
21. *Válási mediáció a gyerekek szempontjából*. Szeged, 2018.
22. *Gazdasági tendenciák és jogi kihívások a 21. században*. Szeged, 2018.
23. *Recent Challenges of Public Administration 3. Papers Presented at the Conference of '3rd Contemporary Issues of Public Administration'*. Szeged, 2019.
24. Kádár Noémi: *A közjegyző szerepe az Európai Unión belüli követelésbehajtásban*. Szeged, 2019.
25. *Gazdasági tendenciák és jogi kihívások a 21. században, 2*. Szeged, 2020.

26. Juhász Krisztina: *A szabálytalan migráció elleni uniós fellépés közép- és hosszú távú intézkedései az Európai Migrációs Stratégia alapján*. Szeged, 2020.
27. *Centenaria. Ende des langen 19. Jahrhunderts. The End of the Long 19th Century.* Szeged, 2020.
28. *Rendkívüli helyzetek és jog. Kalandozások a jog peremvidékén a COVID-19 apropóján*. Szeged, 2021.
29. *Recent Challenges of Public Administration. Papers presented at the conference of '4th Contemporary Issues of Public Administration' on 10th December 2021*. Szeged, 2022.
30. *Gazdasági tendenciák és jogi kihívások a 21. században, 3*. Szeged, 2022.
31. *Strafrechtsvergleichende Beiträge im Spiegel der digitalen Herausforderungen. Aufsätze ungarischer und deutscher Studenten. Konstanz – Szeged – Tübingen – Göcek.* Szeged, 2022.