Schriften zum Strafrecht

Band 373

Digitalisierung, Globalisierung und Risikoprävention

Festschrift für Ulrich Sieber zum 70. Geburtstag

Teilband II

Herausgegeben von

Marc Engelhart, Hans Kudlich
und Benjamin Vogel

Duncker & Humblot · Berlin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Satz: 3w+p GmbH, Rimpar
Druck: Das Druckteam Berlin
Printed in Germany

ISSN 0558-9126
ISBN 978-3-428-15971-0 (Print)
ISBN 978-3-428-55971-8 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Inhaltsverzeichnis

TEILBAND I

I. Grundlagen des (Straf-)Rechts und der Kriminalpolitik

II. Allgemeiner Teil des Strafrechts

III. Besonderer Teil des Strafrechts

IV. Wirtschaftsstrafrecht und Compliance

V. Strafprozessrecht

TEILBAND II

VI. Computer- und Informationsstrafrecht

VII. Strafrecht und Sicherheitsrecht

VIII. Internationales und ausländisches Strafrecht sowie Strafrechtsvergleichung

IX. Strafrechtliche Sanktionen, Strafvollzug und Kriminologie

Cybercrime und Strafrecht*

Von *Lorenzo Picotti*

I. Einführung: Der Einfluss der neuen Technologien auf das Strafrecht und das Werk Ulrich Siebers

1. Das Verhältnis zwischen Strafrecht und Informationstechnologien (sog. IT) steht seit etwa einem halben Jahrhundert im Blickpunkt von Lehre, Rechtsprechung und Gesetzgebung, sowie von den wichtigsten internationalen Organisationen,[1] die in wiederkehrenden „Wellen" und mitunter auch aufgrund dringender Notsituationen, tätig geworden sind, und mittlerweile ein immer umfangreicheres, wenn auch nicht immer systematisches neues Regelwerk, sowie wichtige theoretische Ausarbeitungen hervorgebracht haben.

Heute kann man nicht mehr nur noch von einem speziellen Gebiet des Straf- und Strafprozessrechts, dem „*Computerstrafrecht*", sprechen, wie man es bis vor einigen Jahren kannte und wie es dementsprechend in besonderen Kursen an den Universitäten gelehrt wird.

Heute braucht man vielmehr eine veränderte Sichtweise: man muss das *gesamte* Strafrecht, wie auch allgemein die Rechtsordnung, aus dem Blickwinkel der neuen Technologien und ihren Auswirkungen auf die Organisation und das gesamte Funktionieren des wirtschaftlichen, sozialen und politischen Systems betrachten. Die weit verbreitete Anwendung der Informationstechnologien beeinflusst nämlich die Formen der sozialen und zwischenmenschlichen Beziehungen im öffentlichen, privaten, wirtschaftlichen, kulturellen, nationalen und supranationalen Kontext, mit allen sich daraus ergebenden Folgen für die allgemeine Rechtstheorie und – soweit von Interesse – für den allgemeinen Verbrechensbegriff.

Der Strafrechtler muss sich mit anderen Worten mit der „Computer-" oder besser gesagt der „Cyberrevolution"[2] auseinandersetzen, denn der technologische Wandel hat gezeigt, dass diese von struktureller und strategischer Bedeutung nicht nur für die Entwicklung des Rechts, sondern vor allem für die Entwicklung der heutigen globa-

---

* Übersetzung von *Konstanze Jarvers*, Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Freiburg i. Br.

[1] In Europa von der OECD über den Europarat bis hin zur Europäischen Union und weltweit von den Vereinten Nationen, über die G 8 und die WHO bis zur WIPO.

[2] Siehe unten II.1.

lisierten Gesellschaft ist. Auf diese Weise wird der technologische Wandel zu der fortschrittlichsten Grenze, oder sogar zur „mobilen" Grenze, die sich unaufhörlich weiterbewegt und zukünftige Trends und gewaltige Möglichkeiten für weitere flächendeckende Entwicklungen aufzeigt, wie sie heute vor allem durch die Entwicklung und Anwendung der künstlichen Intelligenz und der Robotik antizipiert werden.

Man muss gerade deshalb von einer „Revolution" sprechen, weil dieses Phänomen alle Lebensbereiche und Interessen der Einzelnen und der Gemeinschaft betrifft. Außerdem geht es über die – an sich schon außerordentliche – Veränderung der Modalitäten und Inhalte von Informationen hinaus, die jedem in beliebiger Entfernung jederzeit und überall zugänglich sind.

Die Tatsache, dass man in Bezug auf die Auswirkungen dieser strukturellen Veränderungen auf die heutige Gesellschaft ein „Vorher" und ein „Nachher" bestimmen kann und muss, zeigt am besten, dass es sich um eine echte Revolution handelt.

Diese Auswirkungen wurden im Strafrecht von der wissenschaftlichen Arbeit Ulrich Siebers von Anfang an aufgegriffen. Sie war darüber hinaus konstruktiv und vorwärtstreibend, auch bei zahlreichen Gelegenheiten zur Zusammenarbeit mit internationalen Gremien oder nationalen Gesetzgebungsorganen. Wir wollen ihn mit dieser Schrift ehren, weil wir nicht nur seine national und international exzellenten Qualitäten als Gelehrter und Förderer der Strafrechtswissenschaften, sondern auch seine nicht minder anzuerkennende Großzügigkeit und Sensibilität durch die freundschaftliche Verbindung zu vielen Kollegen jeden Alters und jeglicher Herkunft, zu deren Kreis zu gehören auch ich die Ehre habe, zu schätzen gelernt haben.

2. Es war gerade die erste systematische Arbeit unseres Jubilars, die Ende der siebziger Jahre entstandene berühmte *blaue Monografie* „Computerkriminalität und Strafrecht"[3], die er unter der Leitung seines großen und heute betrauerten Lehrers Klaus Tiedemann aus seiner Doktorarbeit entwickelt hatte, die die Grundlagen für eine strukturierte dogmatische Ausarbeitung dieses neuen Bereichs des Strafrechts gelegt hat. Gleichzeitig hat sie dem Gesetzgeber grundlegende Orientierungspunkte für die Schaffung neuer Normen und Rechtsbegriffe gegeben, deren Notwendigkeit seitdem in immer mehr Strafrechtssystemen zu spüren ist.[4]

Die schnelle Entwicklung der Informations- und Kommunikationstechnologien und vor allem die verbreitete Anwendung neuer IT-Produkte und -dienste in immer breiteren gesellschaftlichen Bereichen führte Schritt für Schritt zu einer Ausweitung ihres Wirkungshorizonts, der Mitte der 1990er Jahre mit der Öffnung des Internetzugangs für die Öffentlichkeit explodierte. Es war ein historischer Wendepunkt, der schnell zu der neuen globalen Dimension führte, die wir heute als *Cyber-*

[3] *Ulrich Sieber*, Computerkriminalität und Strafrecht (1. Aufl. 1977), 2. Aufl., Köln 1980.

[4] Zu den wichtigen Beiträgen zu den Vorarbeiten für die Reform des Strafgesetzbuchs durch das 1986 beschlossene Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), das die ersten neuen Straftatbestände der Computerkriminalität enthielt, siehe insbesondere *Ulrich Sieber*, Informationstechnologie und Strafrechtsreform, Köln 1985.

space kennen. Eine Veränderung, die aus kriminologischer und strafrechtlicher Sicht den Übergang vom Begriff der *Computerkriminalität* zu dem viel weiteren und handfesteren Begriff der *Cyberkriminalität* markiert.[5]

Ulrich Sieber hatte die strukturell supranationale Dimension der von ihm aufgeworfenen wegbereitenden Fragen bereits bestens verstanden und betrieb auch systematisch rechtsvergleichende Forschung auf europäischer und weltweiter Ebene.[6] Nach einem unvergesslichen vorbereitenden Kolloquium, das er 1992 in der Würzburger Residenz organisiert und geleitet hatte,[7] leitete er auch die zweite Sektion des 1994 von der AIDP in Rio de Janeiro[8] organisierten XIV. Internationalen Strafrechtskongresses. Mit all dem hat er seine führende Position auf diesem Gebiet behauptet, wie seine zahlreichen wissenschaftlichen Beiträge in den folgenden Jahren zeigen,[9] die in unzählige Sprachen übersetzt wurden.[10] Hervorzuheben ist insbesondere der erhellende Bericht zum 69. Deutschen Juristentag, in dem die neuen Themen des materiellen Strafrechts systematisch mit den immer drängenderen des Strafprozessrechts und der internationalen Zusammenarbeit verwoben wurden.[11]

Darüber hinaus wurde sein Beitrag bezeichnenderweise in das wichtigste internationale Dokument zu diesem Thema, das Europaratsabkommen über Computerkriminalität aufgenommen, das am 23. November 2001 in Budapest zur Unterzeichnung aufgelegt wurde und zu dem unser Jubilar einen bedeutenden Beitrag geleistet hat. Das Abkommen stellt nach wie vor den wesentlichen Bezugspunkt für die Harmonisierung und Anpassung der nationalen Rechtsordnungen dar, und zwar nicht nur

[5] Siehe näher hierzu unten III.

[6] *Ulrich Sieber*, The International Handbook on Computer Crime, Chichester u. a. 1986; *Ulrich Sieber* (Hrsg.), Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-Study (prepared for the European Commission), Würzburg 1998. Vgl. dort auch den nationalen italienischen Bericht, herausgegeben von *Lorenzo Picotti* in Zusammenarbeit mit *Francesca Ruggieri* und *Marco Sforzi*.

[7] Siehe den entsprechenden Tagungsbericht mit allen eingereichten nationalen Berichten in *Ulrich Sieber* (Hrsg.), Information Technology Crime. National Legislation and International Initiatives, Köln u. a. 1994.

[8] Der entsprechende Tagungsbericht mit den vom Plenum angenommenen Empfehlungen ist abgedruckt in der Revue Internationale de Droit Pénal, 1994, und jetzt auf der Website www.penal.org. Für einen Kommentar hierzu siehe *Lorenzo Picotti*, Le „Raccomandazioni" del XIV Congresso Internazionale di Diritto penale in tema di criminalità informatica, in Riv. trim. dir. pen.ec. 1995, 1279 f.

[9] Vgl. im Hinblick auf die Europäisierung des Strafrechts nach Inkrafttreten des Vertrags von Lissabon insbesondere *Ulrich Sieber*, Computerkriminalität, in: Ulrich Sieber/Franz-Hermann Brüner/Helmut Satzger/Bernd von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, Baden-Baden 2011, § 24, S. 393 f.

[10] Hier soll nur die überaus wichtige (von *Marco Sforzi* auf Italienisch übersetzte) Studie über die strafrechtliche Verantwortlichkeit der Internet Service Provider erwähnt werden: *Ulrich Sieber*, Responsabilità penali per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di Internet, in: Riv. trim. dir. pen. ec., 1997, 743 f. und 1193 f.

[11] *Ulrich Sieber*, Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag, München 2012.

der europäischen Länder, sondern auch vieler wichtiger dem Abkommen beigetretener Länder anderer Kontinente, wie z. B. der Vereinigten Staaten, Japans, Südafrikas.

Die Herausforderungen, die die Informationstechnologie heute an das Strafrecht stellt, betreffen zum einen die weite Verbreitung ihrer Anwendungen (*Hardware* und *Software*); zum anderen betreffen sie weitere Entwicklungen: die zunehmende Automatisierung durch künstliche Intelligenz, deren Fähigkeit, enorme Datenmengen zu verwalten (die sogenannten *Big Data*), sowie die damit verbundene Ausbreitung der Robotik auf viele verschiedene Bereiche menschlicher Aktivitäten.

An dieser Stelle kann man nur einige problematische Überlegungen zu den heute drängenden Fragen anstellen, ausgehend von der radikalen Frage, „ob" das Strafrecht angesichts dieser neuen Realität[12] eingreifen kann und muss, und ob die Krise, die notwendigerweise seine traditionellen Begriffskategorien berührt, mit einer entsprechenden dogmatischen und normativen Entwicklung und Verfeinerung überwunden werden kann.[13]

II. Automatisierung und „Hyperkonnektivität" als Grundlage der Cyber-Revolution: das Konzept des Cyberspace

1. Für diesen Beitrag sollen zwei grundlegende Merkmale der „Cyberrevolution" hervorgehoben werden. Das erste ist die zunehmende *Automatisierung*, die sich von der „Datenverarbeitung", verstanden als rein „mechanische" Verarbeitung auf der Grundlage mathematischer Berechnungen,[14] bis zum Einsatz immer schnellerer und leistungsfähigerer elektronischer Prozessoren entwickelt hat. Diese führen digitale Programme aus, die nach immer ausgeklügelteren Algorithmen auf Bitsequenzen aufbauen, und können so *komplexe* und außerordentlich *präzise* Ergebnisse erzielen, und zwar unendlich viel *schneller* als es mit der intellektuellen Kraft eines Menschen aus Fleisch und Blut möglich ist. Diese Ergebnisse sind sogar immer autonomer und innovativer als die ursprüngliche Programmierung. Die neuen Programme lernen und korrigieren sich nämlich von selbst gemäß den Zwecken, für die sie konzipiert sind.

Das zweite, damit eng zusammenhängende Merkmal ist die *Netzwerk-Konnektivität*, die heute zu einer „Hyper-Konnektivität" geworden ist. Die wachsende Menge

[12] Siehe unten IV.

[13] Siehe unten V.

[14] Daher sprach man ursprünglich von einfachen „elektronischen Rechnern", wie der englische Begriff „computer" ausdrückt, der auf die sogenannte Turingmaschine zurückgeht (vgl. *Alan Turing*, On computable numbers, with an application to the Entscheidungsproblem, 1936). Turing schlug als erster ein mathematisches Modell vor, das den menschlichen Rechenvorgang simulieren konnte, indem er ihn in seine letzten Schritte zerlegte, die auch mechanisch hätten durchgeführt werden können.

der gespeicherten und verarbeiteten Daten, bis hin zum gewaltigen *Big Data*, wird ermöglicht und täglich gesteigert durch die Schnelligkeit der Sammlung und des Datenaustauschs, die durch die parallele Entwicklung von Netzwerken und Übertragungsstrukturen erreicht wird. Kürzlich haben wir den 50. Jahrestag des ersten Computernetzwerks, dem Embryo des Internets, gefeiert. Die Entwicklung von Kommunikationsprotokollen zwischen verschiedenen Systemen und zwischen Netzen von Netzen hat, ausgehend vom World Wide Web, zu einem permanenten Austausch und zur Nutzung von immer mehr Daten- und Informationen aller Art (einschließlich Audios, Videos und Bildern) geführt. Dadurch werden nicht nur die technologischen, sondern auch die sozialen Grundlagen des heutigen *Cyberspace* geschaffen, so dass man heute von einer „Infosphäre" spricht, in die wir alle dank der „Hyper-Konnektivität", ständig eintauchen.[15]

Mit dem Begriff *Cyberspace* verbindet man nämlich die Idee eines globalen „Raums" mit der der „Kybernetik". Fälschlicherweise wird der erste als „virtuell" bezeichnet, weil er eher ein unverzichtbarer Bestandteil der multidimensionalen und dynamischen Realität der heutigen Welt ist. Demgegenüber deutet die „Kybernetik" die Mechanismen und die Technik an, mit denen Lebewesen und Maschinen miteinander und mit der äußeren Umwelt kommunizieren und diese kontrollieren.[16]

Angesichts dieser Entwicklungen interessiert den Strafrechtler an der IT am meisten die *Automatisierung*, die immer wichtigere Teile der menschlichen Tätigkeit ersetzt und sogar weiterentwickelt.[17]

Durch die Robotik kommen zur Verarbeitung von Daten und Informationen noch körperliche Tätigkeiten, nämlich die Ausführung komplexer Handlungen hinzu. Diese reichen von massiven Beiträgen zur industriellen Produktion über die Erforschung von außerirdischen Gebieten wie dem Mars- oder Mondboden sowie die dortige Materialsuche und -gewinnung, bis hin zu ferngesteuerten heiklen chirurgischen Eingriffen. Im militärischen Bereich denke man an die Suche nach oder die Platzierung von Minen oder Sprengstoffen oder den Einsatz von Drohnen und intelligenten Waffen usw. Weitere Anwendungen betreffen unser tägliches Leben, von der Hausarbeit (putzen, Rasen mähen) bis hin zum automatisierten Fahren, wie es bereits zu-

[15] Zu den wichtigen theoretischen Entwicklungen siehe insbesondere *Luciano Floridi*, The Fourth Revolution. How the Infosphere is Reshaping Human Reality, Oxford 2014.

[16] Der Begriff stammt von dem Griechischen *kyber*, was Steuermann oder Lotse bedeutet, und wurde zu Beginn des letzten Jahrhunderts von Norbert Wiener für die neue Wissenschaft verwendet, die sich mit den Mechanismen beschäftigt, durch die Mensch, Tier und Maschine mit der äußeren Umwelt kommunizieren und diese steuern: *Norbert Wiener*, Cybernetics: Or Control and Communication in the Animal and the Machine (1. Aufl. 1948), 2. überarbeitete Auflage Paris 1961.

[17] Zu den konzeptuellen und rechtlichen Auswirkungen dieses technologischen Elements auf die Formulierung und Interpretation der Tatbestände der Computerkriminalität sei verwiesen auf *Lorenzo Picotti*, Diritto penale e tecnologie informatiche: una visione d'insieme, in: Alberto Cadoppi/Stefano Canestrari/Adelmo Manna/Michele Papa (Hrsg.), Cybercrime, Mailand 2019, Kap. II, S. 35 f., insbesondere S. 43 ff. auch für eine genauere Untersuchung der verschiedenen Straftaten.

nehmend bei PKWs, LKWs, Flugzeugen, Schiffen, Zügen, U-Bahnen usw. der Fall ist.

Um es auf den Punkt zu bringen: Der Mensch wird in immer weiteren Bereichen individuellen und kollektiven Handelns *ersetzt*, und zwar sowohl intellektuell bei Erforschung, Erwerb, Erfassen, Selektion und Speicherung neuer Informationen als auch bei der Kontrolle und Durchführung komplexer und voneinander abhängiger Aktivitäten, die sich in beeindruckender Weise entwickeln können.

2. Die grundlegende qualitative Bedeutung der *Automatisierung* wird schon länger in den strafrechtlichen Definitionen anerkannt, die in den wichtigsten supranationalen Quellen enthalten sind, und zwar in denen, die die Bekämpfung der Computer- und Cyberkriminalität stärken und harmonisieren sollen.

Hier soll nur Art. 1 der bereits erwähnten Cybercrimekonvention des Europarats und Art. 2 der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates über Angriffe auf Informationssysteme[18] genannt werden.

Neuartig ist dabei, dass die Informatik (aber noch mehr ihre Weiterentwicklung, durch die Kybernetik) bis zur Wurzel des menschlichen Handelns vordringt und zum einen seine *kognitiven Fähigkeiten* berührt, nämlich die „äußere" Welt zu kennen und aus ihr zu lernen, indem diese Systeme direkt Informationen und Daten suchen und beschaffen, wie es in den so genannten klugen Systemen geschieht; zum anderen berührt die Informatik die noch wichtigere, aber eng damit verbundene Fähigkeit zur *Selbstbestimmung*, indem sie unter den möglichen Alternativen die Daten und Informationen auswählt, die für „Entscheidungen" berücksichtigt werden sollen.[19]

[18] Dies sind die interessanten Definitionen dieser Richtlinie:

a) „Informationssystem" eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten;

b) „Computerdaten" jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann;

c) „juristische Person" jedes Rechtssubjekt, das den Status der juristischen Person nach dem anwendbaren Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung hoheitlicher Rechte und von öffentlich-rechtlichen internationalen Organisationen;

d) „unbefugt" ein in dieser Richtlinie genanntes Verhalten, einschließlich Zugang, Eingriff oder Abfangen, das vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde oder das nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist.

[19] Symptomatisch für diese Entwicklung ist die Zurückhaltung, mit der das europäische Rechtssystem die rechtliche Wirksamkeit vollständig automatisierter, die Rechte Einzelner betreffender Entscheidungen begrenzt, sie aber gleichzeitig immer häufiger anerkennt: Siehe bereits Art. 15 der RL 95/46/EG und jetzt Art. 22 Abs. 1 der VO 2016/679/EU vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, der wie folgt lautet: „Die betroffene

Heute kann man von einem *Äquivalent* des menschlichen „Willens" sprechen, der durch Computer oder besser durch sog. „intelligente Computersysteme"[20] ausgedrückt wird. Es findet bereits beispielhafte juristische und auch strafrechtliche Anerkennung, z. B. in Bezug auf Wirksamkeit von Rechtshandlungen oder Urkunden, die durch solche Systeme (wie z. B. beim Börsenhandel, oder bei Entscheidungen der Verwaltung oder mittlerweile auch der Justiz) automatisch erstellt werden. Natürliche oder juristische Personen hätten diese nicht in der gleichen Zeit, auf die gleiche Art und mit dem gleichen Inhalt erstellen können.

Aus diesem Blickwinkel scheint die Idee überwunden, dass die IT und die kybernetischen Systeme nur „Werkzeuge" in den Händen einzelner Personen seien. Sie sind vielmehr „intelligente Akteure", was bereits auch in der deutschen Literatur[21] festgestellt wurde. Dies ist aber immer im Verhältnis zur Menge und Qualität der Daten zu sehen, über die diese Akteure verfügen oder die sie erwerben können.

Zur Veranschaulichung: Es ist klar, dass ein *selbstfahrendes Auto* umso zuverlässiger sein wird, je mehr Informationen es autonom und schnell von der Außenwelt sammeln kann. Und zwar entweder mit optischen, akustischen oder thermischen Sensoren oder durch Verbindungen zu Terminals und Informationssystemen im Straßennetz (sog. *intelligente Straße*), die z. B. aktualisierte Daten über Wetter, Verkehr, Straßenbelag, eventuelle Hindernisse oder abnormales Fahrverhalten anderer liefern

Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Abs. 2 enthält aber eine Reihe von Ausnahmen und Bedingungen, die in der entsprechenden Bestimmung des Art. 11 der RL 2016/680/EU vom 27. 4. 2016 über die Verarbeitung personenbezogener Daten für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten weniger streng sind.

[20] Man spricht von „künstlicher Intelligenz" in verschiedenen Bedeutungen: Suchmaschinen können auf der Grundlage von Frequenzen, Präferenzen und Korrelationen, die durch die Suche, durch die von den Nutzern hinterlassenen Daten und durch die verwendeten Geräte (wie z. B. Cookies) gewonnen werden, Informationen (inklusive gezielter Werbung oder sozialen Gruppen mit ähnlichen Interessen, denen man beitreten könnte, usw.) anzeigen und personalisieren. Am anspruchsvollsten sind die Robotik, die Heimautomation und das Fahren von Fahrzeugen, auf das noch zurückzukommen sein wird. In der Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 7. 12. 2018 KOM(2018) 795, mit dem Titel „Koordinierter Plan für künstliche Intelligenz" ist folgende Definition enthalten: „Künstliche Intelligenz (KI) bezeichnet Systeme mit einem ‚intelligenten' Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen. Wir nutzen KI täglich, um beispielsweise unerwünschte E-Mails zu blockieren oder mit digitalen Assistenten zu sprechen. Mit der zunehmenden Rechnerleistung, der Verfügbarkeit von Daten und Fortschritten bei den Algorithmen hat sich KI zu einer der bedeutendsten Technologien des 21. Jahrhunderts entwickelt". Aus der endlosen Literatur zu den rechtlichen Gesichtspunkten vgl. *Woodrow Barfield/Ugo Pagallo* (Hrsg.), Research Handbook on the Law of Artificial Intelligence, Edgar 2018 sowie die folgenden Fußnoten.

[21] *Sabine Gless* et al., If Robots Cause Harm, Who Is to Blame: Self-Driving Cars and Criminal Liability, in: 19 New Criminal Law Review 2016, 412.

können. Auf dieser Grundlage kann das automatisierte Fahrzeug sofort in Echtzeit „Entscheidungen" treffen (Bremsen, Beschleunigen, Lenken usw.), und zwar unabhängig von jeglicher Kontrolle oder Einwirkung durch den Menschen.

Gleiches gilt für den ganzen riesigen Bereich des „Internet der Dinge" *(Internet of Things)*, von dem wir immer mehr umgeben sind. Das sind „Dinge", die sich, wenn auch nur um notwendige Wartungen oder Ersatzteilwechsel anzuzeigen oder zur Fernsteuerung (wie z. B. das banale Einschalten der Heizung im Ferienhaus), *automatisch* mit dem Netz verbinden. Dadurch kommunizieren und arbeiten sie ohne unser Wissen miteinander oder mit sachkundigen Unternehmen mit entsprechenden Algorithmen, um die notwendigen Schritte in Echtzeit durchzuführen.

In diesem Szenario muss unsere *Privatsphäre*, die auf einen immer entlegeneren Mythos schrumpft, eine andere Dimension und Qualität bekommen. Der Anspruch, „Dritte auszuschließen" oder zumindest die Verarbeitung personenbezogener Daten zu kontrollieren, muss geopfert oder, eleganter ausgedrückt, mit anderen betroffenen Interessen (Rechtsgütern), ausgeglichen werden.[22] Dabei überwiegt das Bedürfnis nach bestmöglicher Funktionalität der automatisierten Systeme in den verschiedensten Bereichen, von der eigenen und unser aller Sicherheit über das Gesundheitswesen, die Verwaltung, den Verkehr bis hin zu Produktion, Handel und sogar Werbung.

Für den Juristen und insbesondere für den Strafrechtler werden durch die Tatsache, dass die intelligenten Computersysteme keine bloßen Hilfsmittel mehr sind, sondern immer offenkundiger *autonom handeln* und sogar zu Robotern werden, neue Probleme bei der Zuschreibung von Verantwortlichkeit aufgeworfen. Dis gilt für die häufigen Fälle, in denen sie rechtswidrigen Schaden oder die Verletzungen individueller oder kollektiver Rechtsgüter oder sogar von Grundrechten verursachen, angefangen vom Leben und der persönlichen Unversehrtheit bis hin zur Freiheit der Selbstbestimmung, der Meinungsfreiheit oder der Vermögensverfügungsfreiheit usw. Ohne jedoch an dieser Stelle auf all die neuen Herausforderungen eingehen zu können, die die unaufhörliche technologische Entwicklung und ihre stetigen Auswirkungen auf die heutige globale Gesellschaft in naher Zukunft an das Strafrecht stellen werden,[23] möchte ich mich hier darauf beschränken, einige spezifisch strafrechtliche Aspekte, die sich aus der Untersuchung der gegenwärtigen Rechtslage ergeben, zu vertiefen, um auch für die künftige Forschung Anregungen zu bekommen.

[22] Siehe unter IV.2.

[23] Der nächste (XXI.) Internationale Kongress der Association International de Droit Pénal, der für 2024 geplant ist, wird ganz dem Thema „Artificial Intelligence and Criminal Justice" gewidmet sein. Dieses wird, wie üblich, in vier Bereiche gegliedert ein: der Allgemeine Teil befasst sich mit „Traditional Criminal Law Categories and AI: Crisis or Palingenesis?", der Besondere Teil mit „Old and New Criminal Offences: AI Systems as Instruments and Victims", das Strafprozessrecht mit „AI and Administration of Justice: Predictive Policing and Predictive Justice", und das internationale Recht mit „International Perspectives on AI: Challenges for Judicial Cooperation and International Humanitarian/Criminal Law". Siehe hierzu, sowie für wichtige bibliographische Angaben das von *Katalin Ligeti* herausgegebene Concept Paper, Artificial Intelligence and Criminal Justice, abrufbar unter www.penal.org.

III. Vom Computercrime zum Cybercrime: die Kriminalität im Cyberspace

1. Die Entwicklung der Informatik und Kybernetik hat mit dem erwähnten epochalen Schritt der Öffnung des Internets für die Öffentlichkeit die technische und strukturelle Grundlage des *Cyberspace* gefunden, in die wir heute eingetaucht sind.[24] Mit ihren radikalen Auswirkungen auf alle Bereiche der heutigen globalen Gesellschaft, einschließlich des Strafrechts, hat sie den Übergang von der Begriffskategorie des *Computer crime* (Computerdelikt) zu der – nicht nur kriminologischen, sondern auch strafrechtlichen – Kategorie des *Cybercrime* (Cyberdelikt) bewirkt.[25]

Auf die Computerdelikte hatte sich bezeichnenderweise noch 1989 der Europarat in seiner Empfehlung zur Computerkriminalität[26] bezogen, in der eine begrenzte Liste von Straftaten vorgesehen war, deren Einführung den nationalen Gesetzgebern vorgeschlagen wurde.

Von dieser Empfehlung ging auch die AIDP-Resolution zur Computerkriminalität aus, die 1994 in der Sektion II des oben erwähnten Kongresses von Rio de Janeiro unter dem Vorsitz von Ulrich Sieber verabschiedet wurde. Sie unterstrich im Übrigen bereits die Notwendigkeit, „Präventivmaßnahmen" einzuführen und spezifische Fragen zum Schutz der Privatsphäre, verfahrensrechtliche Gesichtspunkte und solche der internationalen Zusammenarbeit im Lichte der neu entstehenden technologischen Welt zu berücksichtigen.[27]

Angesichts der beschleunigten Entwicklung durch das Internet hat der Europarat nach intensiven Vorarbeiten, auch mit dem erwähnten Beitrag von Ulrich Sieber, nur wenige Jahre später die grundlegende Cybercrimekonvention von 2001 verabschiedet, in der ein wesentlich umfassenderes und vor allem (für die beitretenden Staaten)

[24] Siehe oben II.1.

[25] *Lorenzo Picotti*, Presentazione, in: ders. (Hrsg.), Il diritto penale dell'informatica nell'epoca di Internet, Padua 2004, S. VII.

[26] Vgl. Conseil de l'Europe, Recommandation n°R (89) 9 sur la criminalité en relation avec l'ordinateur, veröffentlicht mit dem Rapport final du Comité européen pour les problèmes criminels mit préface von *August Bequai*, La criminalité informatique, Strasbourg 1990. In einer ersten „Mindestliste" gab es acht Inkriminierungen, die neben dem Computerbetrug, der als die größte und gefürchtetste Bedrohung der neuen Kriminalitätsform angesehen wurde, der Reihe nach folgende Straftaten enthielt: Fälschung von Computerdaten, Beschädigung von Daten und Computerprogrammen, Computersabotage, unbefugter Zugang, unbefugtes Abfangen, unbefugte Vervielfältigung eines geschützten Computerprogramms und unbefugte Vervielfältigung einer Topographie für Halbleiterprodukte (die damals von grundlegender Bedeutung für die Entwicklung der Computerindustrie war). In einer zweiten „fakultativen Liste" wurde empfohlen, vier weitere Straftaten unter Strafe zu stellen: unbefugte Veränderung von Daten oder Computerprogrammen, Computerspionage, unbefugte Benutzung eines Computers und unbefugte Benutzung eines geschützten Computerprogramms.

[27] Siehe die vom XV. Kongress verabschiedeten allgemeinen Berichte und Empfehlungen unter www.penale.org. Hierzu auch *Lorenzo Picotti*, Le „Raccomandazioni" del XV Congresso Internazionale di diritto penale in tema di criminalità informatica, in: Riv.trim.dir.-pen.ec., 1995, 1279 f.

verbindliches systematisches Regelwerk vorgesehen ist. Dieses betrifft das materielle Strafrecht, das Verfahrensrecht und die internationale Zusammenarbeit, deren absolute Notwendigkeit sich inzwischen gezeigt hat.

Beschränkt man sich hier auf die wichtigsten materiellrechtlichen Inhalte, so ist darauf hinzuweisen, dass die Straftaten, die von den nationalen Rechtsordnungen eingeführt werden sollen, über die grundlegende Trias der zu schützenden Rechtsgüter, nämlich „Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen" (*Confidentiality, Integrity, Avalaibility*: sog. CIA) hinausgehen. Auf die CIA nehmen die Artikel 2 bis 6 Bezug, wobei an erster Stelle der rechtswidrige Zugang steht, an zweiter Stelle dann das rechtswidrige Ausspähen, gefolgt vom Eingriff in Daten und in ein System und der neuen *Vorbereitungshandlung* des Missbrauchs von Vorrichtungen.[28] Neben den beiden klassischen Computerstraftaten der Datenfälschung (Art. 7) und des Computerbetrugs (Art 8) sind am Ende nämlich noch Straftaten vorgesehen, die solche „Inhalte" betreffen, die nicht zwingend durch Daten oder Computersysteme übermittelt werden, wie die Kinderpornographie (Art. 9) oder Urheberrechtsverletzungen und damit zusammenhängende Straftaten (Art. 10).

2. Neben den Straftaten, die als *Computerdelikte im engeren Sinne* umschrieben werden können, weil sie unvermeidlich als wesentliche Tatbestandsmerkmale auch *ausdrückliche Beschreibungen* technischer Elemente (wie: „Computersystem", „Computerdaten", „Übertragung von Computerdaten", „Computerprogramm" usw.) enthalten, entsteht daher eine weitere Kategorie von Straftaten, die als „*Cyberdelikte in weiterem Sinne*" bezeichnet werden kann. Auch wenn diese nicht unbedingt die oben genannten technischen Elemente als Tatbestandsmerkmale enthalten, gebührt ihnen besondere Aufmerksamkeit, weil ihnen mit angemessenen Strafen begegnet werden muss, wenn sie online begangen werden. Um sie zu verfolgen und Beweise für ihre Begehung zu gewinnen, sind insbesondere technische Ermittlungsinstrumente und Methoden der Beweiserhebung und -sicherung sowie eine enge und effiziente internationale Zusammenarbeit unerlässlich. Diese sind dieselben, wie sie für Computerdelikte im engeren Sinne und für jede andere Straftat, die „elektronische Spuren" hinterlässt, vorgeschrieben sind (so auch Art. 14, Abs. 2, insbesondere Buchstabe c) der *Cybercrimekonvention*)

[28] Hiermit wird eine Handlung, die vor der Strafbarkeitsschwelle des Versuch liegt, als vollendete Straftat bestraft, nämlich die Herstellung, die Verbreitung und sogar der bloße Besitz von Vorrichtungen (Software und Hardware), die zur Begehung solcher Straftaten entwickelt oder sogar nur „in erster Linie dafür ausgelegt oder hergerichtet" sind: diese Voraussetzung macht das komplexe Problem von „*dual use*"-Vorrichtungen deutlich, die sowohl legal als auch illegal genutzt werden können. Man denke nur an Software, die von Systembetreibern verwendet wird, um auf die Systeme anderer zuzugreifen und dabei die damit verbundenen Sicherheitsmaßnahmen für Updates oder Sicherheitstests zu überwinden. Noch relevanter ist die Verwendung von Spionageprogrammen (sog. Trojaner oder Computerdetektoren) durch Polizeibeamte oder Geheimdienste zur Durchführung von Online-Durchsuchungen, mit dem Ziel, Straftaten zu ermitteln und nachzuweisen oder Telefongespräche oder Umgebungsdaten über die mobilen Geräte der Benutzer, auf die diese Spionageprogramme ohne deren Wissen installiert werden, abzuhören.

Mit der Entwicklung und Ausweitung des *Cyberspace* vergrößert sich die Kategorie der *Cyberdelikte* immer mehr und ist heute fast unbestimmbar. Sie kann nämlich jede Art von Straftat umfassen, sowohl *Computerdelikte* im engeren Sinne als auch allgemeine Delikte, die auch im *Cyberspace* begangen werden können. Hierzu gehören Straftaten, die durch „Kommunikation" und vor allem durch „Verbreitung"[29] von strafbaren Inhalten im Netz begangen werden. Sie sind, wie die Straftaten der Online-Verleumdung[30] oder der Kinderpornographie[31] zeigen, äußerst leicht zu begehen und haben unermesslich größere schädliche Auswirkungen, als wenn sie mit den traditionellen Kommunikationsmitteln (wie Post, Presse, Radio, Fernsehen, Fotos) begangen worden wären.[32]

Es entstehen aber auch viele andere Arten von Straftaten, die verschiedenste Rechtsgüter verletzen und sehr viel bedrohlicher werden, wenn sie im *Cyberspace* begangen werden, so dass nicht nur auf Ermittlungsseite, sondern auch auf normativer Ebene angemessene Reaktionen erfolgen müssen.

Man denke nur an die Straftatbestände, die nach und nach zur Bekämpfung des Terrorismus eingeführt wurden, der sich (auch) im Netz offenbart. Dieses wird sowohl als Ort der Propaganda und der Bekehrung, als auch als Mittel zur „Anwerbung", „Ausbildung" und Organisation anderer Vorbereitungstätigkeiten, wie z. B. Auslandsreisen in Gebiete, die für terroristische Aktivitäten ausgewählt wurden oder zur Finanzierung auch durch *Online*-Sammlungen, genutzt.[33]

Zu berücksichtigen sind ferner die neuen Tatbestände oder Erschwerungsgründe, die schrittweise in verschiedenen Rechtsordnungen eingeführt wurden, um solche Erscheinungsformen schwerer zu treffen, die auch *offline* auftreten können, wie *Cy-*

[29] Siehe hierzu *Lorenzo Picotti*, Profili penali delle comunicazioni illecite via Internet, in: Il diritto dell'informazione e dell'informatica, 1999, Nr. 2, 283 f.

[30] In diesem Sinne bereits *Lorenzo Picotti*, Profili penale, S. 303. In Bezug auf die neuere Lehre und Rechtsprechung siehe *Francesco Pio Lasalvia*, La diffamazione via web nell'epoca dei social network, in: Alberto Cadoppi/Stefano Canestrari/Adelmo Manna/Michele Papa (Hrsg.), Cybercrime, Kap. IX, S. 331 f.

[31] Siehe hierzu die vergleichende Studie von *Ulrich Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet – Eine strafrechtsvergleichende Untersuchung, Mönchengladbach 1999 und aktuell *Lorenzo Picotti*, Online Child-Pornography Offences: a Brief Overview, in F. Dünkel-FS, 2020 (S. 207 ff.).

[32] Weitere bedeutende Inkriminierungen der Cyberdelikte (im weiten Sinne) betrafen die Propaganda und die Aufstachelung zu Hass und Rassendiskriminierung, die insbesondere Gegenstand des vom Europarat am 28. Januar 2003 angenommenen Zusatzprotokolls zum Übereinkommen über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art sind.

[33] Vgl. *Ulrich Sieber*, Instruments of International Law: Against Terrorist Use of Internet, in: Marianne Wade/Almir Maljevic (Hrsg.), A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, New York u. a. 2010, S. 171 f.; zum italienischen Recht: *Lorenzo Picotti*, Terrorismo e sistema penale: realtà, prospettive, limiti, in: Riv. trim. Dir. Pen. Contemporaneo, 2017, 249 f.

berstalking, Cybermobbing, Rachepornos[34], bis hin zur Cybergewalt gegen Frauen, die der Europäische Gerichtshof für Menschenrechte kürzlich wieder in die Kategorie der „häuslichen Gewalt" aufgenommen hat.[35]

Angesichts der neuen Situation hat sich daher die Herangehensweise an die Computerkriminalität oder besser gesagt, an die Kriminalität „im" *Cyberspace*, Schritt für Schritt geändert, da sich diese nicht mehr auf eine geschlossene oder begrenzte Anzahl von Straftaten und damit von potenziellen Opfern beschränken lässt. Sie umfasst vielmehr eine wachsende Bandbreite von Rechtsverstößen und Grundrechtsverletzungen, von denen viele als *neu* eingestuft werden, weil sie das Ergebnis dieser technologischen Entwicklung sind.[36]

Ein Beispiel: Wenn und soweit sie im *Cyberspace* begangen wird, kann eine Erpressung ein Cyberdelikt (im weiteren Sinne) darstellen. Sie kann begangen werden, indem Daten eines fremden Computersystems durch eine widerrechtlich aus der Ferne installierte Schadsoftware verschlüsselt werden. Mit dem Eindringen in den Computer erzeugt der Täter eine Bedrohung oder *Gewalt*[37] und zwingt das Opfer, das seine Daten wiederbekommen möchte, dazu, ein ungerechtfertigtes Lösegeld (oft in Bitcoin, in anderer virtueller Währung oder im sog. Dark Web) zu zahlen, damit es den erforderlichen Entschlüsselungscode bekommt.

Ein weiteres Beispiel für ein allgemeines Delikt, das – auch was Gefährlichkeit, Verbreitung und Schwierigkeiten bei der Prävention und Repression betrifft – „neue"

[34] Illegale Verbreitung von sexuell eindeutigen Bildern oder Videos (Anm. d. Übers.).

[35] Vgl. EGMR, 5. Sektion, 11. Februar Beschwerde Nr. 56867/15, Buturuga ./. Rumänien.

[36] Bezeichnend ist, dass seit dem Inkrafttreten des Vertrags von Lissabon im Jahr 2009 die „Computerkriminalität" (im weiten Sinn) ausdrücklich Gegenstand der konkurrierenden EU-Zuständigkeit ist. Dies betrifft sowohl das materielle (Art. 83 Abs. 1 AEUV) als auch das Strafprozessrecht (Art. 82 AEUV). Siehe hierzu *Lorenzo Picotti*, La nozione di „criminalità informatica" e la sua rilevanza per le competenze penali europee, in: Riv.trim.dir.pen.ec., 2011, Nr. 4, 827 f. Hinzuzufügen ist, dass alle EU-Quellen, die den Grundsatz der „gegenseitigen Anerkennung" von strafrechtlichen „Urteilen und gerichtlichen Entscheidungen" der Mitgliedstaaten, gemäß Art. 82 AEUV (ehemals Art. 31 EUV), und den nationalen Umsetzungsvorschriften anwenden, die „Computerkriminalität" (seit 2002) in die „Liste der Straftaten", für die das Erfordernis beiderseitiger Strafbarkeit aufgehoben werden muss, aufgenommen haben: vgl. hierzu, mit den kritischen Aspekten der Umsetzung in die italienische Rechtsordnung, *Lorenzo Picotti*, Il campo di applicazione del mandato d'arresto europeo: i reati „in lista" e „fuori lista" e la disciplina della legge italiana di attuazione, in: Marta Bargis/Eugenio Selvaggi (Hrsg.), Mandato d'arresto europeo. Dall'estradizione alle procedure di consegna, Turin 2005, S. 127 f.

[37] Nach dem italienischen Strafgesetzbuch ist „Gewalt gegen Sachen" – eine Voraussetzung der Erpressung wie auch anderer Straftaten (z. B. die eigenmächtige Ausübung eigener Rechtsansprüche durch Gewalt gegen Sachen, Art. 392 c.p.) – auch dann gegeben, „wenn ein Datenverarbeitungsprogramm ganz oder teilweise verfälscht, verändert oder gelöscht wird oder wenn der Betrieb eines Datenverarbeitungs- oder Telekommunikationssystems behindert oder gestört wird" (Art. 392 Abs. 3 c.p., eingefügt durch L. 23 dicembre 1993, n. 547). Hierzu *Lorenzo Picotti*, Stichwort Reati informatici, in: Enc. Giur. Treccani, vol. aggiorn. VIII, Roma 2000, S. 16 f.

Charakteristika aufweist, wenn es im Netz begangen wird, ist die Geldwäsche. Sie kann durch elektronische Geldtransfers, Investitionen oder *andere Handlungen* im *Netz* (oder im *Dark Web*) erfolgen, zum Beispiel durch die Bewegung und den Austausch von virtuellen Währungen wie *Bitcoin* oder *Ethereum.* Diese basieren auf *Blockchainsystemen*, durch anonyme Handlungen, die geeignet sind, Geld oder sogar immaterielle Werte zu ersetzen und so die *Identifizierung* des kriminellen Ursprungs dieser Werte zu *erschweren* (sog. *Cyberlaundering*).[38]

Auch der ganze illegale Handel (mit Drogen, Waffen, bis hin zu Menschen oder Organen usw.) sowie die kompliziertesten Betrügereien, z. B. durch *Phishing*-Techniken, können im Cyberspace begangen werden. Hierbei kommt auch die künstliche Intelligenz zur Anwendung, die kriminelle Handlungen schneller, sicherer und geschützter macht, indem sie entweder den günstigsten Zeitpunkt oder die verletzlichsten Opfer auswählen.

IV. Das interaktive *web* und die doppelte Rolle der Nutzer als Täter und Opfer des Cybercrime: Neue zu schützende Rechtsgüter und Grundrechte

1. Das Netz hatte ursprünglich eine nur in eine Richtung verlaufende Struktur, in der der normale Nutzer *passiver* Empfänger von Information und Kommunikation war. Auf diese konnte er zugreifen, er konnte sie lesen oder erwerben, ihre Erzeugung und Verbreitung lag aber in den Händen eines relativ begrenzten Personenkreises (den sog. *Content Providern*, oder allgemeiner, den *Internet Service Providern* und *Webmastern*). Die Überwindung dieser Struktur war durch einen technischen Aspekt gekennzeichnet, der Anfang der 2000er Jahre mit der Entwicklung des sog. *web* 2.0 auftauchte. Dieses bot immer mehr Möglichkeiten der *aktiven Interaktion* zwischen den Nutzern, die nun ihre *eigenen* Inhalte in *Blogs*, *Foren* und *sozialen Netzwerken* erstellen und teilen konnten.

Hierauf folgte der sprunghafte Anstieg der Nutzung mobiler Geräte jeder Art (insbesondere *Tablets* und *Smartphones*), was durch die Weiterentwicklung der Speicher-, Verbindungs- und Grafikkapazitäten ermöglicht wurde. Hierdurch können die Nutzer selbst immer und überall verschiedenste und komplexe Multimedia-Inhalte (wie Audios, Videos und auch dreidimensionale Bilder) erzeugen und ins Netz stellen oder sich in Chats, Streamings oder Videokonferenzen in Echtzeit verbinden (sog. *web* 3.0). Heute spricht man sogar von einem *web* 4.0, das von der künstlichen Intelligenz beherrscht wird. In diesem erstellen und verbreiten die Nutzer nicht nur systematisch Informationen, Inhalte und Daten, sondern sie dienen – dank gezielter Konfigurierung von Orten, Diensten und Apps im *Cyberspace* – auch als unerschöpf-

[38] Dieses Phänomen ist auch Gegenstand der RL 2018/1673/EU vom 23. 10. 2018 über die strafrechtliche Bekämpfung der Geldwäsche. Hierzu *Lorenzo Picotti*, Profili penale del cyberlaundering: le nuove tecniche di riciclaggio, in: Riv.trim.dir.pen.ec., 2018, Nr. 3–4, 590 f.

liche Quelle für solche Daten, die (mit oder ohne ihr Wissen bzw. ihre Einwilligung) systematisch aus all ihren Aktivitäten, ihrem Browsen und ihren Nutzungen ermittelt werden. Auf diese Weise ist das Cyberspace zu einer riesigen Datenbank geworden, anhand derer systematisch Profile aller dort agierenden Personen erstellt und ihre Vorlieben, kulturellen, ideologischen und politischen Orientierungen sowie ihr Konsum und ihre Ausgaben ermittelt werden können. Hiermit ist auch die beeindruckende Entwicklung von Werbung, Handel, sowie unternehmerischen, produktiven und wirtschaftlichen Aktivitäten aller Art verbunden.[39]

Der Nutzer wird dadurch zu einem potentiellen *Opfer* sowie zu einem potentiellen *Täter* von Verletzungen schutzwürdiger Rechte,[40] parallel zu dem, was im realen Leben geschieht, aber auf eine völlig neue Art mit qualitativ viel einschneidenderen Wirkungen.[41]

Hier soll das Beispiel von *Minderjährigen* genügen, die das *Netz* als festen und manchmal krankhaft konditionierenden Bestandteil ihres täglichen Lebens als „Digital Natives" nutzen: Daher entwickeln sie nicht nur bessere Fähigkeiten bei der Verarbeitung von Informationen sowie der Entwicklung sozialer Beziehungen, sondern es entstehen auch sehr alarmierende Phänomene wie *Sexting*, *Cybermobbing*, *Rachepornos* oder Misshandlungen, die mit unterschiedlichsten auch tödlichen Gefahren verbunden sind (*Blue Wahle*[42] ist ein tragisches Beispiel) und die die persön-

[39] So wird das Cyberspace immer strukturierter und entwickelt sich zu einer riesigen Datenbank (deshalb sprechen wir von *Big Data*), die von Suchmaschinen und Systemen der künstlichen Intelligenz erfasst und verarbeitet wird. Diese Systeme schaffen eine immer verfeinerte „*Web*-Semantik", mit der immer höherwertigere Informationen gefunden und verarbeitet werden. Mit dem erreichten Grad an technologischer Automatisierung und Leistungsfähigkeit bei der Sammlung, Speicherung und Verarbeitung von Daten werden digitale *Alter Egos* geschaffen, die die Menschen immer mehr „ersetzen", wenn es darum geht, zu erkennen und zu entscheiden, welche Maßnahmen ergriffen und welche Positionen eingenommen werden sollen. Parallel hierzu gibt es in verschiedenen Bereichen beunruhigende Konzentrationen oder sogar Monopoltendenzen bei den Giganten des Webs. Dies hat sich bereits in den Kartellermittlungen und -verfahren der Europäischen Kommission gegen Facebook, Google, Amazon usw. gezeigt.

[40] Vgl. *Lorenzo Picotti*, I diritti fondamentali nell'uso ed abuso dei Social Network. Aspetti penali, in: Giur. merito, 2012, Nr. 12, 2522 f.

[41] In Anwendung der Definition der RL 2012/29/EU vom 25. 10. 2012 über den Schutz der Opfer von Straftaten können die Opfer von Cyberdelikten als transnationale Delikte (wie auch die speziell geschützten Personen wie Kinder oder diskriminierte Personen) oft als „gefährdet" angesehen werden, da sie keine „Staatsangehörigen" der Mitgliedstaaten sind, in denen die Tat begangen wird.

[42] „Blue Whale Challenge" ist ein Spiel für Teenager, dessen Ursprünge noch unbekannt sind und das sich im Internet verbreitet hat. In Italien wurde ein 23-jähriges Mädchen wegen Stalking und schwerer Nötigung angeklagt, weil sie zusammen mit einem heute 16 Jahre alten Mittäter eine Mitschülerin dazu gezwungen hatte, sich als erste von 50 Mutproben Schnitte am Körper zuzufügen und ihnen davon Fotos zu schicken.

liche Entwicklung und die erfolgreiche Eingliederung in das reale Leben irreparabel beeinträchtigen können.[43]

Die allgegenwärtige Ausbreitung des *Cyberspace* und der dadurch ermöglichten rechtswidrigen Verhaltensweisen schafft ein dringendes Bedürfnis nach einem angemessenen strafrechtlichen Schutz, da *Rechtsgüter* verletzt werden, die eines entsprechenden Schutzes würdig und bedürftig sind. Sie sind identisch (wie z. B. Ehre, Ansehen oder Vermögen) sehr ähnlich (wie z. B. Integrität von Daten und Systemen) oder jedenfalls nicht geringwertiger (wie z. B. IT-Vertraulichkeit und Datenschutz) als die Rechtsgüter, die bereits strafrechtlich geschützt sind, wenn die entsprechenden Straftaten *offline* begangen werden. Die neuen Besonderheiten der Rechtsgüter, die im *Cyberspace* verletzt werden können, verleihen diesen oft eine größere und manchmal sogar eine grundlegendere Bedeutung, wie im Falle des IT-Vertraulichkeit und der IT-Sicherheit.[44]

2. Bezeichnend ist die Entwicklung des Rechtsgutes der Vertraulichkeit, das die neue Dimension der *IT-Vertraulichkeit* erreicht hat. Dies ist ein Grundrecht, das verstanden wird als das Recht auf einen *exklusiven* IT-*Raum*, der als solcher *frei von Eingriff bzw. Zugang* und Manipulation durch Dritte bleiben muss, da er ein wesentliches Mittel für das heutige individuelle und gesellschaftliche Leben ist. Sogar der Staat darf dieses Recht nur in den abschließend vom Gesetz vorgesehen und gerichtlich überprüfbaren Fällen einschränken.[45] Es wird von der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte auf Art. 8 der Konvention und vom Gerichtshof der Europäischen Union auf Art. 7 der EU-Grundrechtecharta gestützt.[46]

[43] Vgl. die Daten der wichtigsten internationalen und nationalen Stellen, die sich mit dem Schutz von Kindern im Internet befassen: Hinweise hierzu bei *Ivan Salvadori*, Sexting, minori e diritto penale, in: Alberto Cadoppi/Stefano Canestrari/Adelmo Manna/Michele Papa (Hrsg.), Cybercrime, Kap. XIII, S. 567 f.

[44] Hierzu gleich unten IV.2.

[45] Zur „IT-Vertraulichkeit" als neues Rechtsgut, das sich von der Vertraulichkeit der Kommunikation und der Privatsphäre unterscheidet, siehe *Lorenzo Picotti*, Reati informatici, S. 20; Für ein aktualisiertes Bild siehe *Ivan Salvadori*, I reati contro la riservatezza informatica, in: Alberto Cadoppi/Stefano Canestrari/Adelmo Manna/Michele Papa (Hrsg.), Cybercrime, Kap. XVII, S 656 f. Was die Rechtsprechung betrifft, so erkennt das Bundesverfassungsgericht dieses „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" unabhängig vom Datenschutz an, das von dem umfassenden allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) mitumfasst ist, indem es Grenzen und Bedingungen für die sog. Online-Durchsuchung skizziert, BVerfG v. 27. 2. 2008 – 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274; dazu *Ulrich Sieber*, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen (2007); italienische Kommentierung von *Roberto Flor*, Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online-Durchsuchung, in: Riv. trim. dir. pen. ec., 2009, S. 695 f.

[46] Es umfasst die computergestützte und telematische Kommunikation *als solche*, und zwar unabhängig von ihrem „persönlichen" oder besser zwischenmenschlichen Charakter, wie er hingegen bei den traditionellen Korrespondenzformen (Telefon, Telegramm, Brief) vorausgesetzt wird: So rechtfertigt sich die Unabhängigkeit der genannten Inkriminierungen gemäß Art. 3 der *Cybercrimekonvention* und Art. 4 der RL 2013/40/EU, die ergänzt werden durch

Das eigenständige Recht auf den Schutz der *eigenen* „persönlichen Daten" weist – egal wo diese aufbewahrt oder verarbeitet werden und auch unabhängig von der Informationstechnologie – eine autonome Tragweite auf. Diese geht jetzt weit über den ursprünglichen angelsächsischen Begriff der *Privacy* hinaus, der als bloße Schutzbarriere für das Privatleben (das Recht, „allein gelassen zu werden") vor ungerechtfertigtem Eindringen durch die *Massenmedien*, damals vor allem die Presse, angesehen wurde.[47]

Heute, in der allgegenwärtigen Dimension des *Cyberspace*, wird dieses neue Grundrecht nicht nur seit dem am 28. Januar 1981 in Straßburg zur Unterzeichnung aufgelegten Übereinkommen Nr. 108 des Europarats „zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten" besonders gewürdigt, sondern findet auch in Art. 8 der EU-Grundrechtecharta eine eigene Gestalt. Darin werden die Rechte der Person an ihren eigenen Daten mit dem damit einhergehenden und immer stärker werdenden Bedürfnis nach ihrer „Verbreitung", also der Verfügbarkeit für Dritte abgewogen. Diese Verfügbarkeit ist eine wesentliche Voraussetzung für verschiedenste Dienstleistungen, die auch, aber nicht nur zugunsten des Betroffenen erbracht werden (z. B. Gesundheits- und Sozialdienste, die Erfüllung aller Arten von vertraglichen Verpflichtungen oder die Personalisierung von Werbung oder anderen Dienstleistungen, die auf dem sog. „Profiling" des Nutzers basieren).[48]

Also muss man heute neue und differenzierte Regelungen schaffen, um die Bedingungen und Grenzen festzulegen, wann die Verarbeitung dieser Daten zulässig ist, und zwar in jeder Phase, von der Sammlung, Speicherung, Übermittlung und Verbreitung bis zur Bereitstellung an Dritte. Hierbei sind die Grundprinzipien der Notwendigkeit und Verhältnismäßigkeit mit den entsprechenden Sicherheitsgarantien anzuwenden, sowie die Verantwortlichkeit der Verarbeitenden und anderer beteiligter Personen für die Risiken zu bestimmen, denen die Rechte anderer ausgesetzt sind.[49] Hierzu gehören das Recht auf Information über die Zwecke und Methoden

---

den rechtswidriger Zugang zu Informationssystemen gemäß Art. 2 und 3 sowie die in Art. 6 und 7 geregelten „vorbereitenden" Straftaten, für deren Verwirklichung „persönliche" Inhalte nicht erforderlich sind.

[47] Man beachte den historischen Beitrag von *Samuel D. Warren/Louis D. Brandeis*, The Right to Privacy, in: Harvard Law Review, 1890, Nr. 5, 193 f.

[48] Zur Entstehung dieses „neuen" Rechts, als das Recht, die eigenen Daten und deren Verbreitung zu kontrollieren, siehe in der italienischen Lehre die grundlegenden Beiträge von *Stefano Rodotà*, beginnend mit seiner wegweisenden Monographie Elaboratori elettronici e controllo sociale, Bologna 1973 bis hin zu seiner letzten: Il mondo nella rete – Quali diritti quali vincoli, Roma-Bari, 2014.

[49] Nach dem in Art. 8 der Grundrechtecharta enthaltenen europäischen Modell, muss eine mit durchgreifenden Kontroll-, Genehmigungs-, Untersuchungs- und Sanktionsbefugnissen ausgestattete Aufsichtsbehörde die Wirksamkeit der Regelung gewährleisten. Sie soll das Ungleichgewicht zwischen dem Betroffenen und den für die Verarbeitung Verantwortlichen ausgleichen. Letztere können nämlich mit Einwilligung des Betroffenen enorme Datenmen-

sowie die Inhaberschaft an der Datenverarbeitung, damit man diese verschiedenen Phasen der Verarbeitung „zulassen" oder zumindest ihre verschieden Phasen „kontrollieren" kann, bis hin zur Inanspruchnahme des sog. Rechts auf „Vergessenwerden".[50]

Eng verbunden mit diesen neuen Rechtsgütern ist auch das ebenso neue Rechtsgut der *IT-Sicherheit*, heute besser bekannt als *Cybersicherheit* (sog. *Cybersecurity*). Diese ist nicht mehr nur als eine *Obliegenheit* des Betroffenen zu verstehen, die dazu dient (auch strafrechtlichen) Schutz der *eigenen* Interessen zu erhalten, und deshalb „disponibel" ist, wie es sich noch aus der in Art. 3 der RL 2013/40/EU, sowie in Art. 615-*ter* c.p. vorgesehenen Voraussetzung für die Strafbarkeit des rechtswidrigen Zugangs zu Informationssystemen ergibt. Die IT-Sicherheit ist schon lange zu einer *Pflicht* geworden, deren Verletzung in vielen Bereichen auch bestraft wird, wie das z. B. Art. 169 des italienischen Datenschutzgesetzes in der Fassung von 2003 gegenüber Inhabern von personenbezogenen Daten bestimmte, die nicht den durch spezielle Ministerialerlasse festgelegten und aktualisierten „Mindestsicherheitsanforderungen" entsprachen.[51] Heute werden angesichts der neuen VO 2016/679/EU, der so genannten Datenschutzgrundverordnung, andere und weitergehende Verpflichtungen zur Risikobewertung und -vermeidung sowie zur angemessenen Reaktion auf unerwünschte Ereignisse festgelegt. Diese wenden sich nicht nur an die für die Datenverarbeitung Verantwortlichen, sondern auch an die Auftragsverarbeiter, an Programmierer, In-Stallers usw., und zwar bereits bei der Planung und Konfiguration der Systeme *(by design)*.

Wegen der engen globalen Verflechtung aller Dienste und Aktivitäten im *Cyberspace* zeigen die neuesten Bestimmungen, dass die Sicherheit der Netze und Informationssysteme eher eine allgemeine „präventive" *Garantiedimension* besitzt. Dies gilt für alle Dienste, Funktionen und Beziehungen, und damit auch für die Rechte, die dort ausgeübt werden. Auf diese Weise wird die IT-Sicherheit zu einem indisponiblen öffentlichen Rechtsgut, weil sie einen *kollektiven* Wert besitzt, dessen konkrete Gestaltung von den hierzu besonders befugten Behörden festgelegt und kontrolliert wird.

Bei dieser Entwicklung werden *Internet Service Provider* immer wichtiger. Für ihre verschiedenen Dienstleistungen und Aktivitäten werden ihnen zwangsläufig immer strengere zivil-, verwaltungs- und strafrechtliche Pflichten und eine entsprechende Verantwortung auferlegt. Die rechtliche Grundlage und deren präzise und

---

gen erfassen und kontrollieren. Der Betroffene kann die Einwilligung häufig nicht verweigern, weil er sonst auf die an sie gebundenen Dienste und Leistungen verzichten muss.

[50] Dieses Recht wurde vom Gerichtshof der Europäischen Union in seinem historischen Urteil (Große Kammer) vom 13. Mai 2014, Rechtssache C-131/12, Google Spain gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, feierlich anerkannt und ist nun in Art. 17 der VO 2016/679/EU (Datenschutzgrundverordnung) enthalten.

[51] Siehe hierzu *Lorenzo Picotti*, Sicurezza, informatica e diritto penale, in: Massimo Donini/Massimo Pavarini (Hrsg.), Sicurezza e diritto penale, Bologna 2011, S. 217 f.

notwendigerweise differenzierte Abgrenzung wirft jedoch erhebliche rechtliche (wie auch rechtspolitische) Probleme auf. Die Rechtsprechung der Europäischen Gerichte in Straßburg und Luxemburg in den letzten Jahren zeigt deutlich die Unzulänglichkeit der Regelung der RL 2000/31/EG über den elektronischen Geschäftsverkehr. Diese orientiert sich noch immer am Modell der Haftungsbefreiungen und „Privilegien" für Internetdienstanbieter, wie es der US-*Millennium Copyright Act* von 1997 umschreibt. Insbesondere durch die Kategorie der so genannten aktiven Host-Provider, die dank der neuen Technologien und vor allem der künstlichen Intelligenz die von ihnen gehosteten und im Netz zur Verfügung gestellten Inhalte auswählen, katalogisieren, präsentieren und in vielerlei Hinsicht grundlegend kontrollieren können, hat sich eine weite Auslegung ihrer Verpflichtungen zur Zusammenarbeit mit den Behörden sowie zur Entfernung illegaler oder schädlicher Inhalte aus dem Netz entwickelt.

V. Schlussbemerkungen: Die Notwendigkeit einer Anpassung der Strafrechtskategorien und Stärkung der Garantien im *Cyberspace*

1. Die andauernde Entwicklung und Ausbreitung des *Cyberspace* hat zur Folge, dass die Wirkung des geltenden (Straf-)Rechts verpufft.

Einerseits fördert bzw. erzwingt sie sogar dessen ständige Anpassung. Eine solche ist die wesentliche Voraussetzung dafür, dass das Recht seine Regulierungsfunktion aufrechterhalten kann, und das dank aller ihm zur Verfügung stehenden Mittel: von der „evolutionären" Auslegung bis zur analogen Anwendung, von der Änderung oder Schaffung von Gesetzen bis hin zur Entwicklung innovativer begrifflicher und dogmatischer Kategorien, für die die Lehre Ulrich Siebers seit langem den Weg bereitet hat.

Andererseits scheint die Cyberrevolution, wie jede *strukturelle Realität*, die den Überbau bedingt, gerade die Beziehung der IT-Technologien zum Recht neu zu bestimmen, indem sie ihre Aufgaben und Einsatzmöglichkeiten berührt, und schließlich ihren wesentlichen Kern infrage stellt: Die Technologie scheint in Konkurrenz zur *Regelungsfunktion* der Rechtsordnung, ihrer primären Funktion, zu stehen, da der von Natur aus „technische Kodex" für sich in Anspruch nimmt, auch das neue Gesetzbuch zu sein: „Code is Law", um das berühmte Buch von Lawrence Lessig zu zitieren.[52] Der technologische Selbstschutz und die Selbstregulierung, die sich die großen Herren des Netzes vor allem selbst auferlegen, tendieren dazu, „Recht" zu werden oder dieses zu ersetzen, weil die von ihr geschaffenen „Regeln" in Echtzeit wirksame Sanktionen liefern können. Die drastischste Folge ist der Ausschluss von Diensten, Netzen und Internetverbindungen, weil damit das Verhalten von Nutzern,

[52] *Lawrence Lessig*, Code and Other Laws of Cyberspace (1st ed. 1999), 2nd ed., New York 2006.

Konkurrenten und Dritten unmittelbar beeinflusst werden kann, bis hin zu dem Punkt, an dem die Ausübung ihrer (Grund-)Rechte eingeschränkt werden kann.

Schon seit einiger Zeit ist klar, dass die utopische oder romantische Vorstellung unhaltbar ist, dass das „Netz" ein rechtsfreier Raum sei,[53] ein Freihafen der Anarchie oder der totalen Freiheit, der nicht begrenzbar sei durch die Staatsgewalt, die nur innerhalb ihrer geografischen Grenzen ihre Souveränität ausüben kann. Auch aus der obigen kurzen Untersuchung ergibt sich die Notwendigkeit eines effektiven (straf-)rechtlichen Schutzes von oftmals vorrangigen Rechtsgütern, die im *Cyberspace* auf immer neue Art und Weise verletzt werden. Diese Verletzungen erfolgen manchmal geräuschvoll, manchmal verdeckt und still und zwar nicht nur durch Cyberkriminelle bzw. entsprechende kriminelle Organisationen, sondern auch durch missbräuchliches Verhalten, das durch die neue außergewöhnliche Machtkonzentration gefördert wird. So sehr, dass der Entwurf einer *Internet Bill of Rights*, einer „Verfassung für das Internet",[54] maßgeblich gefördert, ausgearbeitet und mitgetragen wurde. Hiermit sollten die Grundrechte im Cyberspace – ausgehend von denen, die in den internationalen Konventionen enthalten sind und von den Gerichten nach und nach ausgearbeitet wurden – gegenüber jedermann anerkannt und garantiert werden.[55]

Das Hauptkriterium muss sein, dass das, was *offline* illegal ist, *online* nicht legal sein kann, auch wenn es in neuen und unerwarteten Formen auftritt.

Dieses Prinzip muss aber angemessene Mittel finden, um wirksam zu werden. Hierzu gehört eine klare rechtliche Definition der illegalen *Inhalte* und *Handlungen*, die im Cyberspace zu bestrafen sind. Dabei sind die Neuartigkeit und Komplexität der sich dort abspielenden Beziehungen und der Techniken, mit denen sie sich entwickeln, zu berücksichtigen: Daher kann nicht jede Frage oder jeder Schutzbedarf mit der einfachen begrifflichen Ausweitung der geltenden Normen und traditionellen dogmatischen Kategorien auf die neuen Phänomene gelöst werden.

Es ist deshalb offensichtlich, dass ein allgemeiner rechtlicher Rahmen entwickelt werden muss, in den auch neue Kriterien für die Zurechnung der strafrechtlichen Ver-

[53] Siehe in der italienischen Literatur *Govanni Ziccardi*, Hacker – Il richiamo della libertà, Milano 2011, mit zahlreichen bibliografischen und Rechtsprechungshinweisen, auch in Bezug auf die amerikanische Praxis.

[54] Ausgehend von der „Internet Magna Carta" von *Tim Berners Lee* und der Studie des „Berkman Center" der Harvard University haben sich auf internationaler Ebene eine Reihe von Initiativen entwickelt, darunter die Arbeit des „Internet Governance Forum" und der „Dynamic Coalition on Internet Rights and Principles". Hierauf nimmt auch die in Italien von der 2014 vom Präsidium der Abgeordnetenkammer eingesetzten Kommission unter dem Vorsitz von *Stefano Rodotà* durchgeführte Studie Bezug, die am 28. 7. 2015 eine kurze, aber effektive „Erklärung zu den Rechten im Internet" vorgestellt hat. Sie besteht aus einer Präambel und 14 Artikeln, in denen ebenso viele Rechte anerkannt werden: vgl. https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf.

[55] Vgl. *Rodotà*, Il mondo nella rete, S. 61 f., 69 f.

antwortung eingefügt werden, die die besonderen Merkmale der im *Cyberspace* begangenen strafrechtlich relevanten „Handlungen" berücksichtigen.

Das *Novum* der technologischen Entwicklung und insbesondere der Cyberrevolution, die angesichts der nächsten anwendungsbezogenen Entwicklungen (künstliche Intelligenz und Robotik), voraussichtlich zu weiteren tiefgreifenden Veränderungen führen wird, muss auf der juristisch-strafrechtlichen Ebene bewusst gestärkt und darf gewiss nicht unterschätzt werden. Nur so kann man angesichts der unbestreitbaren Notwendigkeit einschneidender Reformen die Festigung der gleichfalls primär erforderlichen rechtsstaatlichen Prinzipien einer demokratischen Gesellschaft garantieren. Diese kann sich ihrer Regulierungs- und wenn nötig Sanktionierungsaufgabe, angesichts des „technischen Codex" und der „de facto"-Regulierung durch die Machtverhältnisse im Cyberspace, nicht entziehen, erst recht nicht in Zukunft in einer Welt, die von Robotern beherrscht werden wird.

2. Die Grundbegriffe Handlung und Erfolg, Kausalzusammenhang und objektive wie subjektive Zurechnung usw. sind angesichts der *Automatisierung*, der *Entmaterialisierung*, der andauernden *Interaktion* und *Interdependenz*, die das *Cyberspace* charakterisieren, zu überdenken. Dabei muss man aber immer berücksichtigen, dass es im Grunde um die sich im Cyberspace abspielenden zwischenmenschlichen Beziehungen und Interessenkonflikte geht.

Wesentlicher Teil der Handlung ist hier gerade nicht die körperliche Bewegung, sondern sie wird nun von der Computertechnologie und damit von der *Automatisierung* dominiert, die dann die Kausalität beeinflusst, als ein Zurechnungszusammenhang zu einem Erfolg, der eher als deren wenn auch begrifflich abtrennbare rein naturalistische „Folge" angesehen werden kann. Der Erfolg kann nämlich außerhalb des *Cyberspace* eintreten, wenn z. B. Tod, Verletzung, Personen- oder Vermögenschäden durch *Roboter*, *selbstfahrende Autos*, Cyberterrorismus oder *Cyberextorsion* verursacht werden; der Schaden kann auch ein immaterieller bzw. psychischer sein, wie z. B. bei Cybermobbing oder *Cyberstalking*. Oft kann die Vollendung aber auch komplett „innerhalb" des *Cyberspace* liegen, wie bei der Beeinträchtigung der Funktionsfähigkeit eines Systems aufgrund eines DoS-Angriffs, infolge einer Vielzahl von Computer-„Aktionen", die von einer eigens für diesen Zweck programmierten und aktivierten Software gestartet und ausgeführt werden. Der Grundbegriff der Tatbestandserfüllung muss daher nicht nur bei Computerdelikten im engeren Sinne, sondern auch bei Cyberdelikten im weiteren Sinne einen immer relevanteren „Anteil" von Handlungen berücksichtigen, die im Netz oder sogar durch Computersysteme erfolgen. Sie geschehen bei der Ausführung von Programmen, die auf mehr oder weniger ausgefeilten und komplexen Algorithmen basieren, die von Menschen (Herstellern, Servicetechnikern, Inhabern, Nutznießern usw.) konzipiert, aktiviert oder kontrolliert werden. Dabei ist es aber schwer, ihnen rechtlich die Begehung oder gar den entsprechenden bewussten Willen zuzurechnen, der erforderlich ist, damit der für die Tatschuld erforderliche Vorsatz oder jedenfalls die subjektive Vorwerfbarkeit erfüllt ist.

Aufgrund der genannten technischen Merkmale der *Automatisierung* und der „*Hyper-Konnektivität*",[56] die sich auf den Verkehr, die Bereitstellung und die Beständigkeit von Daten und Inhalten im Netz erstrecken, muss auch der Begriff der Vollendung der im *Cyberspace* begangenen Straftat überdacht werden.

Es breiten sich nämlich nicht nur die „Wirkungen" in Zeit und Raum aus, wie sich beispielhaft im Google-Fall gezeigt hat, wo es um das Recht auf „Vergessenwerden"[57] ging, sondern auch der strafrechtlich relevante Zeitraum der Tatbestandserfüllung wird durch die automatisierten Funktionen der Speicherung, des Teilens und des Verkehrs, die nur teilweise von Betreibern und Nutzern der Computersysteme *ex ante* oder *ex post* „beherrschbar" sind, verlängert und in gewisser Hinsicht dauerhaft.

Diese besondere Dauerhaftigkeit der Cyberdelikte kann auch nicht auf ein bloßes, strafloses *post factum* reduziert werden, denn die *Verlängerung* der *tatbestandmäßigen* Handlung und/oder des *tatbestandsmäßigen* Erfolgs kann nicht von den technischen Elementen getrennt werden, aus denen sie bestehen. Dabei werden, wie gesagt, für die Tatbestanderfüllung die besonderen durch die IT bestimmten Merkmale vorausgesetzt, durch die der Täter den Tatbestand erfüllt.

Einen methodologischen Hinweis liefern kann die traditionelle dogmatische Unterscheidung zwischen dem Zeitpunkt der formalen Vollendung der Straftat, der eintritt, wenn die wesentlichen Tatbestandsmerkmale in ihrem Mindestinhalt verwirklicht worden sind, und dem Zeitpunkt der materiellen Beendigung, der eintritt, wenn die Straftat in ihrem spezifischen verletzenden Inhalt *endgültig* „erschöpft" ist, weil der maximalen Grad der Schädigung des geschützten Rechtsgutes erreicht ist.[58]

Man kann nun nicht sagen, dass sich das Cyberdelikt in der ziemlich langen *Zwischenzeit* „erschöpft", die zwischen Vollendung und Beendigung liegt und in der die Verletzung bestehen bleibt oder sich sogar verschlimmert.

Das Phänomen ist wohl nicht unter die echten Dauerdelikte (wie z. B. die Entführung) zu fassen, die voraussetzen, dass die Fortdauer der Rechtsgutsverletzung (hier im Beispiel die persönliche Freiheit des Opfers) von einer direkten und gleichzeitigen willentlichen Handlung des Täters abhängt, der sie jederzeit abbrechen könnte (daher sprechen Einige von einer gemischten Straftat, einem Begehungsdelikt bei der

---

[56] Siehe oben II.

[57] Siehe oben Fn. 50.

[58] Diese Unterscheidung, die bereits in der allgemeinen Verbrechenslehre von *Francesco Carrara*, Momento consumativo del furto, in: Lineamenti di pratica legislativa penale, Torino 1874, S. 229 f., anerkannt wurde, wird nicht nur in den italienischen Lehrbüchern übernommen: vgl. *Ferrando Mantovani*, Diritto penale – Parte generale, 10. Aufl., Padua 2017, S. 425 f.; *Hans-Heinrich Jescheck/Thomas Weigend*, Lehrbuch des Strafrechts – Allgemeiner Teil, 5. Aufl., Berlin 1996, § 49 III, S. 517. In Bezug auf die Absichtsdelikte siehe auch *Lorenzo Picotti*, „Dolo specifico" und Absichtsdelikte – der sog. Handlungszweck zwischen gesetzlicher Formulierungstechnik und dogmatischen Begriffen, in Wolfang Frisch-FS, Berlin 2013, S. 363 ff.; *ders.*, Zwischen ‚spezifischem' Vorsatz und subjektiven Unrechtselementen – Ein Beitrag zur typisierten Zielsetzung im gesetzlichen Tatbestand, Berlin 2014, S. 35 ff. (Übersetzung von Thomas Vormbaum).

anfänglichen Herbeiführung und einem Unterlassungsdelikt bei der späteren Aufrechterhaltung des rechtswidrigen Zustands).[59]

Die besondere *Automatisierung* und „*Hyper-Konnektivität*" der IT, die die Ausbreitung und Dauerhaftigkeit der Straftat im *Cyberspace* bestimmen, entziehen sich zwangsläufig der direkten und kontinuierlichen nachträglichen Kontrolle des Täters, der sich ihrer bedient hat.

Es handelt sich daher also um eine neue dogmatische Kategorie, die die Besonderheiten dessen, was im Cyberspace passiert, für die Vielzahl der möglichen Straftaten erfassen muss.

Man denke nur an die einfache online begangene üble Nachrede, die nach ihrer formellen Vollendung, die mit der ersten „Kommunikation" des den Ruf anderer schädigenden Inhalts an mehrere Personen (auch durch Veröffentlichung auf einer Website oder in einem sozialen Netzwerk) erfolgt, zu einer Verlängerung, Verschlimmerung und Ausbreitung der Verletzung in Zeit und Raum führt. Diese wird vom Täter nicht mehr beherrscht, ist aber sicher vorhersehbar und zum Zeitpunkt der Handlung akzeptiert. Dasselbe gilt für die Verbreitung von Kinderpornografie, die Straftat des „Rachepornos", die Verbreitung von Hassreden im *Cyberspace* usw.

Die *tatbestandsmäßige Handlung* weist daher eine *verlängerte bzw. hinausgezögerte Vollendung* auf, die über den Zeitpunkt der formalen Vollendung hinausgeht und bis zur materiellen Beendigung andauert, die schwer, aber nicht unmöglich festzustellen ist. In diesem verlängerten Zeitraum ist es, wie auch bei der entsprechenden Ausbreitung im globalen Cyberspace, wohl dogmatisch nicht richtig, von einer menschlichen *tatbestandsmäßigen Handlung* zu sprechen, weil sie nicht mehr auf die Beherrschung durch den bewussten Willen oder jedenfalls auf die aktuelle Beherrschbarkeit durch den Menschen zurückgeführt werden kann, auch wenn die daraus resultierende tatbestandsmäßige Verletzung, sicherlich immer noch als *direkte Folge* eines solchen Verhaltens im Cyberspace entsteht.

Es scheint nun ein eigener *Erfolgsbegriff* zu entstehen, der sich vom traditionellen naturalistischen unterscheidet, wenn er auch in Bezug auf die Verletzung des Opfers und der geschützten Interessen und Rechte *gleichwertige* Merkmale aufweist. Die Voraussetzungen und Grenzen der objektiven Zurechnung und der subjektiven Vorwerfbarkeit (aufgrund von Vorsatz oder Fahrlässigkeit) müssen aber im Lichte der IT und des ihr zugrunde liegenden, im *Cyberspace* etablierten Konfliktverhältnisses bestimmt werden. Die Entscheidung, sich auf die Automatisierung und die „Hyperkonnektivität" mit all den oben erwähnten technischen Besonderheiten zu verlassen, hat zur Folge, dass sie der Täter kennt oder zumindest kennen kann, sie in Kauf nimmt, und damit die Verantwortung für die Folgen übernimmt.

[59] Zu den Kennzeichen des Dauerdelikts in der italienischen Lehre vgl. u. a. *Mario Romano*, Commentario sistematico del codice penale, 3. Aufl., Mailand 2004, Pre-Art. 39, §§ 118 f., S. 344 f.; zum *postfactum* siehe die Monografie von *Salvatore Prosdocimi*, Profili penali del postfatto, Mailand 1982.

Wenn der Vollendungszeitpunkt, nach dem das zeitlich und räumlich anwendbaren Strafrecht zu bestimmen ist, diese weitere Verlängerung und Ausbreitung der tatbestandsmäßigen Handlung im *Cyberspace* umfassen muss, so muss der Beginn der Verjährung z. B. auf den Zeitpunkt der materiellen Beendigung verschoben werden, weil der Strafanspruch, wie bei Dauerdelikten und solchen mit verlängerter Vollendung, bis dahin fortbesteht.[60]

Daraus folgt, dass nach den allgemeinen Grundsätzen eine strafrechtlich relevante Beteiligung Anderer (z. B. anderer Nutzer sozialer Netzwerke, die die Nachricht oder den verletzende Inhalte billigen und verbreiten, oder *Internet Service Provider*, die z. B. der Verpflichtung zur Sperrung oder Löschung nicht nachkommen), nach Art. 110 c.p. bzw. §§ 27 ff. StGB sowohl durch aktives Tun als auch durch Unterlassen möglich ist.[61]

Die wichtigsten Garantenstellungen, die die Provider durch ihre die rechtlichen Interessen von Nutzern und Dritten gefährdenden Tätigkeiten innehaben, müssen in breiterem Umfang anerkannt, aber auch gesetzlich präzisiert werden. Dies gilt aber nur für die Risiken und innerhalb der Grenzen, wie die Gefahrenquellen, aus denen sie stammen, beherrschbar sind. Der Grund hierfür liegt in der Tatsache, dass sie, wegen der klugen Systeme und der künstlichen Intelligenz, im neuen technologischen Kontext immer weniger passive, rein technische und automatische Funktionen erfüllen. Um den Umfang der Pflichten zu bestimmen, deren Einhaltung technisch und persönlich durchsetzbar ist, und deren Verletzung daher zu einer strafrechtlichen Verantwortung führen kann, können natürlich nicht die zivilrechtlichen Modelle der verschuldensunabhängigen Produkthaftung angewendet werden. Ebenso wenig anwendbar ist das Modell der Verantwortlichkeit eines Unternehmens für Straftaten, die Personen in übergeordneter oder eventuell auch untergeordneter Position vorgeworfen werden können, weil es deren strafrechtliche Verantwortung voraussetzt.

Dies sind jedoch weite, noch nicht eingehend erforschte, die Grundbegriffe der Verbrechenslehre[62] betreffende Bereiche, die offen sind für eine erneute Reflexion

[60] Der Begriff der Straftat mit „verlängerter Vollendung" wurde vor Kurzem in der italienischen Rechtsprechung entwickelt und betrifft Straftaten wie Korruption oder Wucher, die *alternative* Vollendungszeitpunkte aufweisen können, weil ihre Verwirklichung auch durch mehr als eine Handlung erfolgen *kann*: wenn z. B. aufgrund rechtswidriger Vereinbarungen oder Versprechen, mit denen die Straftat bereits vollendet ist, mehrere Zahlungen erfolgen, ist die materielle Rechtsverletzung erst mit der letzten Zahlung beendet und somit beginnt erst mit dieser die Verjährung zu laufen (siehe Art. 158, Abs. 1 c.p. und ausdrücklich zum Wucher Art. 644-*ter* c.p.).

[61] Siehe in diesem Sinne die Entscheidung des Kassationsgerichtshofs vom 27. 12. 2016, n. 54946, Tavecchio, mit der die Verurteilung eines *Bloggers* bestätigt wurde, der einen Text mit beleidigenden Ausdrücken auf seiner Website „gelassen" hatte, obwohl er auf deren Inhalt aufmerksam gemacht worden war.

[62] Neben den Begriffen Handlung und Erfolg beziehe ich mich auf die schon länger genannten Begriffe Kausalität, Unterlassung, Beteiligung, Versuch, Vorsatz und Fahrlässigkeit,

und dogmatische Ausarbeitung durch den Strafrechtler. Dieser muss, gerade um seine Aufgabe als Jurist nicht zu verfehlen, seine intellektuellen Werkzeuge und Begriffskategorien an die neue technologische Praxis anpassen können, gerade um die wesentliche Bedeutung eines auch strafrechtlichen Schutzes in diesem Bereich zu bekräftigen und gleichzeitig die grundlegenden Prinzipien und Garantien einer demokratischen Rechtordnung zu bewahren.

Abschließend sei gestattet, noch einmal an die Arbeit und das Beispiel von Ulrich Sieber zu erinnern, der einen wichtigen Teil seines Engagements unserer Association Internationale de Droit Pénal (AIDP) gewidmet hat, die für die Themen der modernen globalen Gesellschaft besonders empfänglich ist. Ein solches war – 20 Jahre nach dem genannten Kongress in Rio 1994 – auch 2014 Gegenstand des XVIII. internationalen Kongresses (zufällig wieder in Rio de Janeiro) mit dem übergeordneten alle vier Sektionen betreffenden Thema „Informationsgesellschaft und Strafrecht".[63]

Angesichts der rasanten Weiterentwicklungen, die durch die Etablierung und die Ausbreitung immer anspruchsvollerer Anwendungen der künstlichen Intelligenz und der Robotik anstehen, wird der nächste XXI. Internationale Kongress, der für 2024 geplant ist, dem Thema „Künstliche Intelligenz und Strafjustiz" gewidmet sein.[64]

Hierzu wird unser Jubilar wieder seinen unersetzlichen Beitrag an Wissen und Erfahrung einbringen können, auf einem Gebiet, das er seit vielen Jahren als ein kluger und vorausschauender Wegbereiter erforscht hat. Und dies ist der aufrichtige Wunsch, den wir ihm und auch uns allen gegenüber zum Ausdruck bringen.

vgl. *Lorenzo Picotti*, Internet e responsabilità penali, in: Giovanni Pascuzzi (Hrsg.), Diritto ed informatica, Mailand 2002, S. 117 f.

[63] Die vier Resolutionen zum allgemeinen Teil, besonderen Teil, Strafprozessrecht und internationalen Strafrecht und die allgemeinen Berichte finden sich auf der Website www.penale.org.

[64] Siehe hierzu Fn. 23.

Menschenrechte in der digitalen Krise

Von *Johanna Rinceanu*

I. Einführung

Für den Schutz und die Durchsetzung von Menschenrechten birgt das 21. Jahrhundert als Zeitalter der Digitalisierung zweifellos zahlreiche neue Chancen. Es schenkt Dissidenten, Protestierenden, Menschenrechtsorganisationen und -aktivisten erstmals weltweit eine Stimme. Sie machen den digitalen Raum zu ihrer (Welt)Bühne: „lokal ist global".[1]

Betrachtet man jedoch die jüngsten Entwicklungen im deutschen IT-Straf- und Ordnungswidrigkeitenrecht, scheint das Informationszeitalter die Menschenrechte eher in eine neue „digitale Krise" zu stürzen und zwar direkt vor unserer Haustür. Insbesondere der Katalog des § 1 Abs. 3 Netzwerkdurchsetzungsgesetz (NetzDG) hat einer Vielzahl der – seit langem hoch umstrittenen – Tatbestände rund um Meinungsäußerungsfreiheit und Informationsfreiheit[2], Kunstfreiheit, Recht auf Privatsphäre, aber auch Religionsfreiheit neue Aktualität verliehen. Private IT-Diensteanbieter werden in diesem Prozess zu Hütern praktischer Konkordanz wider Willen und zu Gatekeepern an der Schwelle der Menschenrechte.

Abermals realisieren sich Risiken, die *Ulrich Sieber* bereits vor über 20 Jahren im CompuServe-Verfahren[3] identifiziert hat. Die Schnittstelle von Menschenrechten, Strafrecht und Digitalisierung eignet sich daher wie kaum eine andere für einen Festschriftbeitrag.

Im Folgenden wird das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken vorgestellt und kritisch beleuchtet (II.), auf die Kompetenzabsicherung näher eingegangen (III.) sowie die Vereinbarkeit des NetzDG mit den Grund- und Menschenrechten diverser Akteure im digitalen Raum analysiert (IV.). Im Anschluss wird die „virale" Verbreitung des NetzDG vorgestellt (V.). Schließlich wird ein kritischer Blick auf den Entwurf eines Gesetzes zur Bekämp-

[1] *Internet & Gesellschaft Co:llaboratory*, „Menschenrechte und Internet" – Zugang, Freiheit & Kontrolle, Abschlussbericht 2012, S. 19.

[2] Zur Informationsfreiheit der Nutzer siehe *Sieber/Nolde*, Sperrverfügungen im Internet – Nationale Rechtsdurchsetzung im globalen Cyberspace?, 2008, S. 77 ff.

[3] Vgl. *Sieber*, JZ 1996, 429 ff. und 494 ff.; *id.*, Verantwortlichkeit im Internet: Technische Kontrollmöglichkeiten und multimedialrechtliche Regelungen, 1999.